CRYPTO WORDS

CY19 December

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

Contents

Goals and Scope

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

History

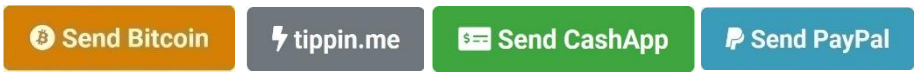
There exists a gap in Bitcoin publishing. For authors with commentary and scholarly papers on topic, the choice of publication outlets is relatively limited. The number of journals that serve as outlets for crypto research is in any event too small, as the number of crypto thinkers continues to grow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

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

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

Support Crypto Words

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



Spread the word

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

Follow us on social media

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

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

Subscribe to our newsletter

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

Our pledge

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

Immutability as a Service

By Aleksander Svetski

Posted November 26, 2019

Bitcoin network = "IaaS" (not SaaS)

"Bitcoin provides immutability as a service"

There are not many applications in the world that need immutability, and perhaps only a couple that need to build immutability as part of their core stack. It's just too expensive!

Now...If we view immutability as a service — one that any application in the world can "anchor" or connect to, then we begin to reframe how we view Bitcoin, i.e.; as a broader network that settles transactions or states with value associated to them.

An example here will help.

There is NO reason (or very little reason) that any company (tech or otherwise) today needs to buy, host and maintain its own server infrastructure. It's costly and it makes up only a fraction of what matters in their actual business. So they use a cloud-based service such as AWS.

You'll also note that because of the economies of scale; there are only three real options:

- AWS

- Azure
- Google

Why?

They got in early and they poured billions upon billions into it.

Immutability is similar (but also different).

Similar because the infrastructure required to make something truly digitally immutable is extraordinary (perhaps even more than all of the combined infrastructure that AMZN, MSFT and GOOG operate), and it only makes sense that people will anchor to it as and *when they need to*.

Different because it's not something that can be run by one or a few parties. A concept like immutability (and things that inherently need it, i.e.; money) are only so if broadly owned. In other words; the more distributed and decentralized the architecture and higher the number the owners, validators and nodes, the more robust, costly and therefore immutable it is. Should one (or a few) entities manage all of it; it then undermines the value proposition and defeats the entire purpose.

The Immutable Network

Immutability as a service is what will bring more economic activity to the Bitcoin network in the long run, again; similar to the internet. The internet started off as a way to connect computers at a distance, and over time (as more people used and trusted it) it evolved into this new communication network that provides data / packet routing as a service. We built everything on top — and the innovation has been extraordinary.

The next step is baking monetary value into a protocol owned by the collective, whose core tenet is absolute digital immutability. A network where you can't turn back time (like in the real world).

All of the economic value from applications that require this feature, along with any broader monetary / banking / capital or financial applications that require an absolute guarantee of the following key functions:

1. Send
2. Store
3. Receive

Will accrue on it.

And as I've stated ad-nauseum, the more economic activity that occurs on and on top of the Bitcoin network, the more immutable and secure it will

become. It's compounding, it is self reinforcing, it has already hit a critical mass, and it's now a runaway train.

Bitcoin is the autonomous digital network with the highest possible guarantee of the three core functions of money & finance.

Other consensus mechanisms

There are, and there will continue to be lots of other consensus mechanisms created. Some that might work; most that definitely won't.

They may be used on their own networks, for applications that are either private, proprietary; or for applications that don't require an absolute guarantee of immutability and security.

I personally don't believe any money- related or high value applications will run on their own networks (except in vain over the next as this space evolves) because networks, especially those where the broad population participate, generally converge to unity.

It's why we largely have one internet; one set of protocols for email; why we all use AC power; why, within a particular jurisdiction; the network of language converges to one, and similarly so with money (there is one USD in USA, likewise one AUD in AUS).

In fact — we see this as the world's become more "global".

English hit it's critical mass, attained the primary network effect and it's now more functional to speak English in most places around the world.

Aside from converging to unity due to efficiency and practicality, the world can probably only sustain ONE absolute, immutable, uncensorable, secure proof of work chain — because it's expensive!

This chain is likely (at this stage at least) to be Bitcoin.

If we had to run proof of work for everything; we'd destroy the planet (plus it assumes nobody trusts each other for anything, which is a bigger problem anyway), and;

a) If someone wants to use it as a service; they're going to go to the one that's got the highest guarantee. That in itself will increase that network's guarantee; leading to that self-reinforcing recursive effect I described earlier.

b) Furthermore; if you do have a novel, "light" consensus mechanism, that's fast — you could in future anchor it to something like Bitcoin as and when you need to substantiate any claim or make a final judgement.

It's this line of logic that leads me to believe most of the economic value will be swallowed up by the Bitcoin Network over the long term, not to mention the new concepts and innovations that will emerge using the ingredients of immutability and verification — like how facebook and instagram emerged from the internet.

In the next chapter, we're going to explore the idea of Bitcoin as a new "Monetary Operating System". Think of it like a computer operating system, eg; MacOS.

We can call it the BoS (very fitting).

Download the full guide at:

https://bitcointimes.news

Debunking Bitcoin's natural long-term power-law corridor of growth

By Marcel Burger

Posted November 30, 2019

Some models are useful, some fail to meet required underlying assumptions.

What's this all about?

After PlanB wrote his (by now) famous piece on the relation between Bitcoin's stock-to-flow ratio, a lot of people tried to debunk his model, including the author of this piece. It also inspired a lot of people to develop a competing model. But to my knowledge until today no-one succeeded in either a successful academically valid rejection of the model, or to come with a better model. One person in particular keeps coming back saying his model does a better job. Harold Christopher Burger's idea was to build a comparable model, but instead of taking the natural logarithm of the stock to flow ratio as an independent variable, he thought the natural logarithm of time would be a better input. He reasoned that stock-to-flow is a function of time, so time itself must perform better. Even though Nick has demonstrated repeatedly (here for instance) how PlanB's model is just better, Harold keeps claiming his work is superior. Time to take a closer look at his model and either applaud him for doing a fantastic job, or just send it (=his model) to the graveyard where it can take a rest with other failed attempts.

Regression again

Just like PlanB's work, Harold's work is also based on Ordinary Least Squares Regression. So, we check to see whether all the required assumptions are met. I have mentioned those assumptions as well in the first piece in which I reviewed PlanB's model. Here they are listed once more.

(1) The expected value of the error term is zero (which means that on average the regression should be correct)

(2) The error and the independent variables should be independent.

(3) The error term should be homoskedastic (i.e. error terms have the same variance)

(4) There should be zero correlation between different error terms (i.e. autocorrelation is excluded)

After checking whether these hold, I'll also take a look if cointegration applies here even though cointegration with time doesn't make much sense. I'll follow the same procedure as followed when reviewing PlanB's work.

Data and Model

To build the model I used the CoinMetrics dataset which can be found here. All data before a price tag for bitcoin was known is discarded. The first day of the dataset is presented as day 1, the second day as day 2 and so on. So we're counting the days as of day the first price tag is available. We take natural logarithms of both the price tags and the day counts. So our data starts like this:

	date	price	time	logtime	logprice
0	2010-07-18	0.085840	1	0.000000	-2.455270
1	2010-07-19	0.080800	2	0.693147	-2.515778
2	2010-07-20	0.074736	3	1.098612	-2.593797
3	2010-07-21	0.079193	4	1.386294	-2.535869
4	2010-07-22	0.058470	5	1.609438	-2.839246

Start of the dataset with time as days counted since start of the set

or like this:

	date	price	time	logtime	logprice
0	2010-07-18	0.085840	14808	9.602923	-2.455270
1	2010-07-19	0.080800	14809	9.602990	-2.515778
2	2010-07-20	0.074736	14810	9.603058	-2.593797
3	2010-07-21	0.079193	14811	9.603125	-2.535869
4	2010-07-22	0.058470	14812	9.603193	-2.839246

Start of the dataset with time as days counted since Jan 1st 1970 (UNIX)

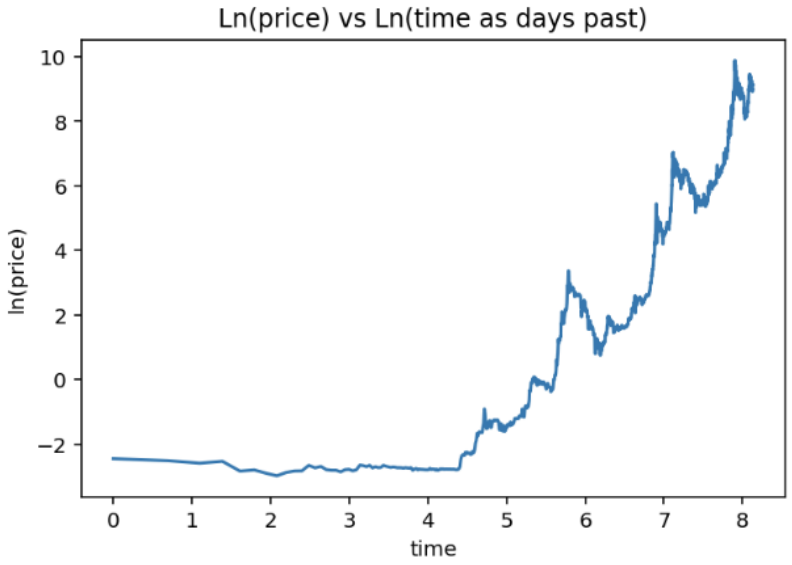
or like this:

	date	price	time	logtime	logprice
0	2010-07-18	0.085840	561	6.329721	-2.455270
1	2010-07-19	0.080800	562	6.331502	-2.515778
2	2010-07-20	0.074736	563	6.333280	-2.593797
3	2010-07-21	0.079193	564	6.335054	-2.535869
4	2010-07-22	0.058470	565	6.336826	-2.839246

Start of the dataset with time as days counted since bitcoin's Genesis block (Jan 3rd 2009)

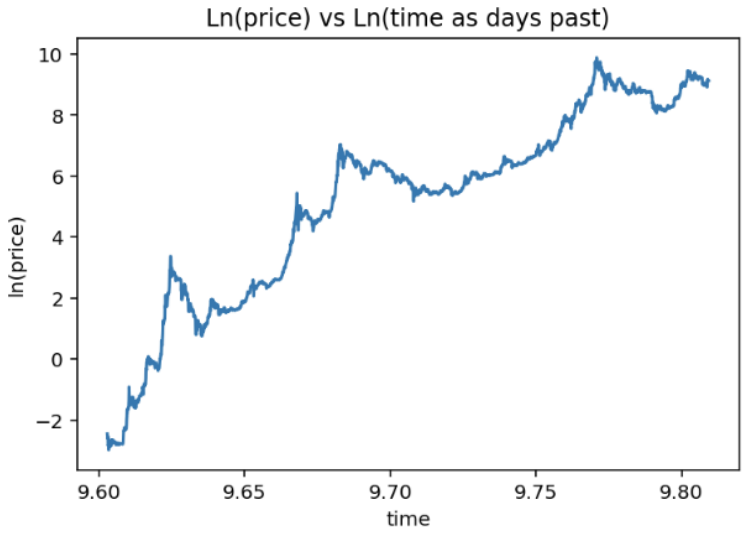
Building the model and testing assumptions

Before we start checking whether the assumptions hold up, we'll start with some visual inspections of the data. Let's see how the log-log chart looks like in case we work with time as days past since first measure. Time is a relative concept, so the performance of the model will be dependent of the point in time we consider as point 0.

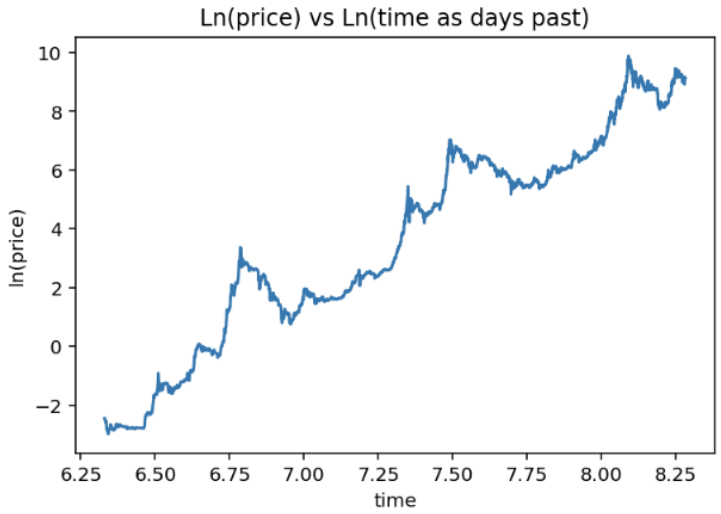


Relation between ln time and ln price as time is days since first available price tag for bitcoin

Another logical starting point would be January 1st 1970 as day 1, we'll go with that and look how the relation changes.



Relation between ln time and ln price as time is days since 1–1–1970



Relation between ln time and ln price as time is days since January 3rd 2009

Starting to count the days as of the 3rd of Jan 2009 while first prices are not available seems a bit strange to me. It feels a bit like cherry picking the most suitable relative time series. This is what Harold used in his model, so we go with it as well here. Taking the first two would not return meaningful results as there would be too much non-linearity in those relations anyway. I would like to remark that this is where the model already starts to become shaky.

After running the regression, it's time to take a closer look at the regression results and to research the model residuals. Here's the regression result:

OLS Regression Results

Dep. Variable:	logprice	**R-squared:**	0.932
Model:	OLS	**Adj. R-squared:**	0.932
Method:	Least Squares	**F-statistic:**	4.673e+04
Date:	Sat, 30 Nov 2019	**Prob (F-statistic):**	0.00
Time:	13:59:41	**Log-Likelihood:**	-4095.3
No. Observations:	3396	**AIC:**	8195.
Df Residuals:	3394	**BIC:**	8207.
Df Model:	1		
Covariance Type:	nonrobust		

	coef	std err	t	P>|t|	[0.025	0.975]
const	-38.9645	0.205	-189.902	0.000	-39.367	-38.562
logtime	5.8185	0.027	216.173	0.000	5.766	5.871

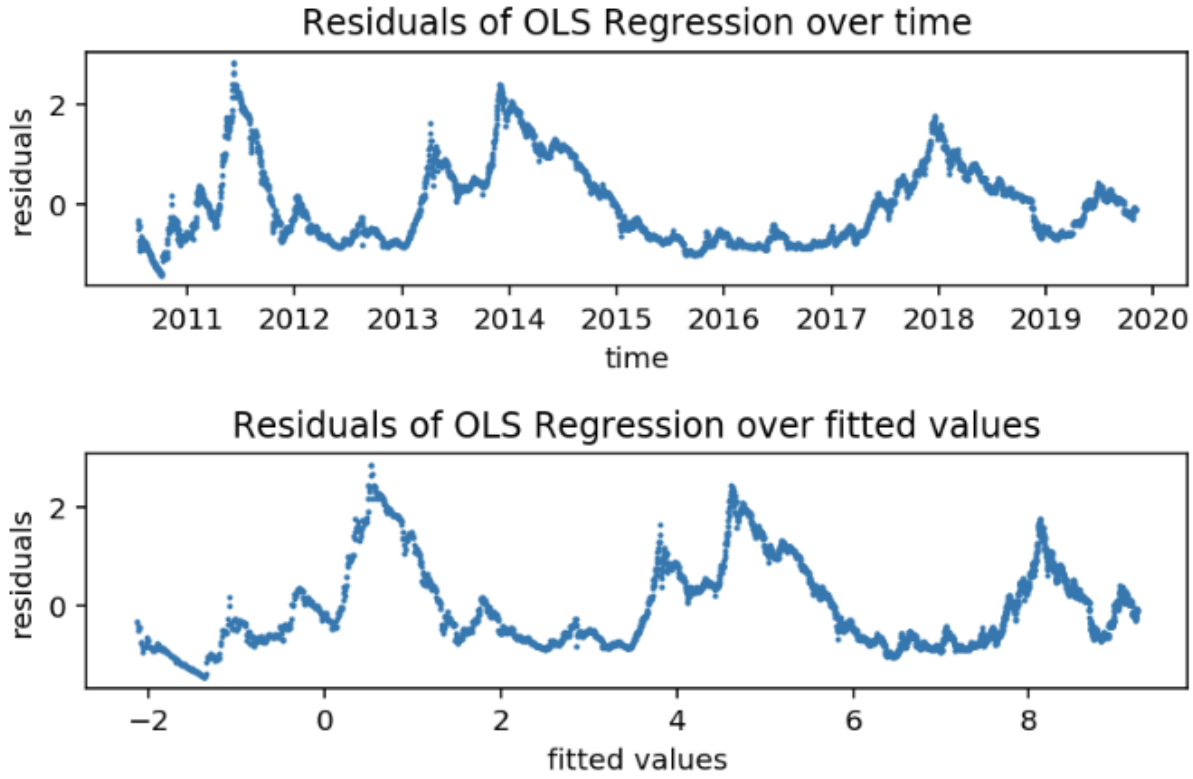
Omnibus:	314.306	**Durbin-Watson:**	0.005
Prob(Omnibus):	0.000	**Jarque-Bera (JB):**	408.782
Skew:	0.850	**Prob(JB):**	1.71e-89
Kurtosis:	2.955	**Cond. No.**	115.

Regression results for ln time vs ln price

Even though R-squared is quite high, R-squared is not a very meaningful metric when we evaluate the regression of two non-stationary time series. It often turns out to be quite high when we're using trending series and we should be aware of spurious regression. Further, the coefficients seem to be both significant, but the main question is whether the underlying model assumptions are met.

Residual analysis

We'll take a look at the residuals to check for possible issues with the model.



Plots of the residuals that follow from the regression

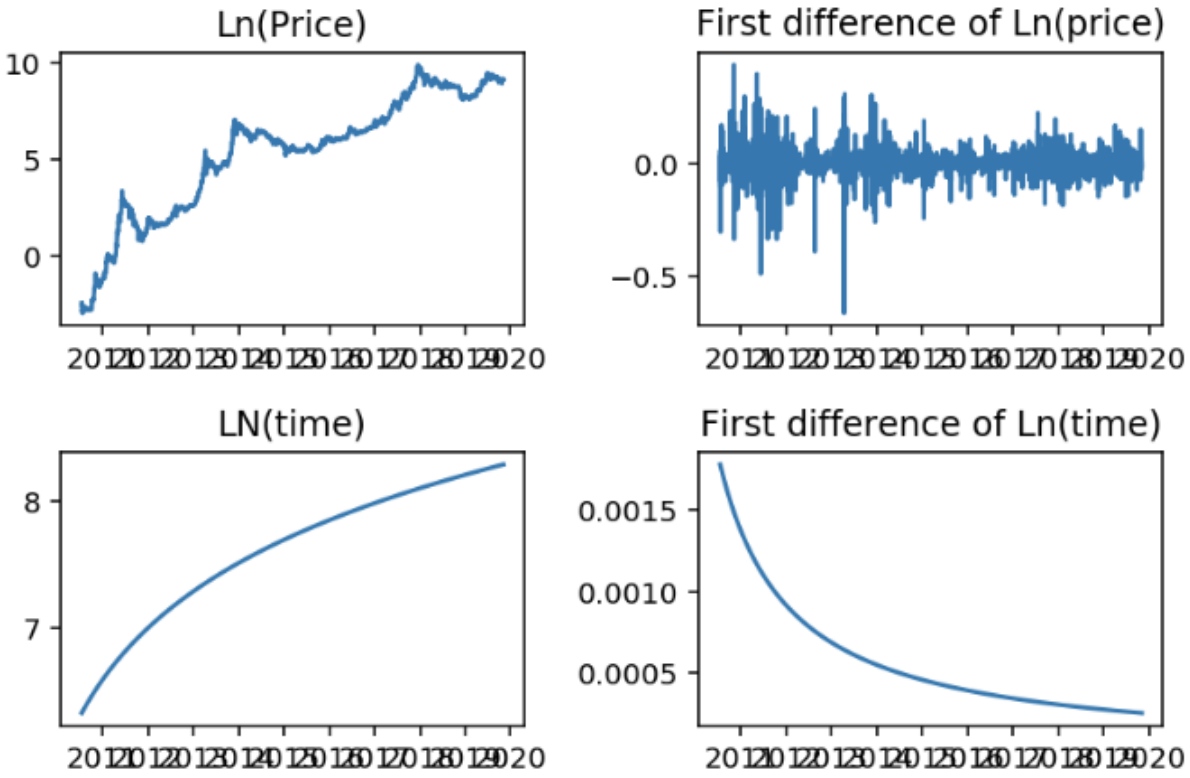
There's a very clear pattern observable in both plots, which tells us that the residuals are likely to be autocorrelated, which would mean that the 4th assumption is not met. Next to that, we can also clearly see that the variance differs over time, which would indicate that the 3th assumption is violated as well. Both violations would lead to a falsification of the model.

We will test for autocorrelation to make sure that this is an issue. The Durbin Watson statistic turns out to be 0.005 (check OLS results above) which is much smaller than the allowed lower bound value (see DW table in the Appendix).

Sofar, I would conclude the model's fundamentals are no good, and the only reason to not reject it, would be in case we can show the variables are cointegrated.

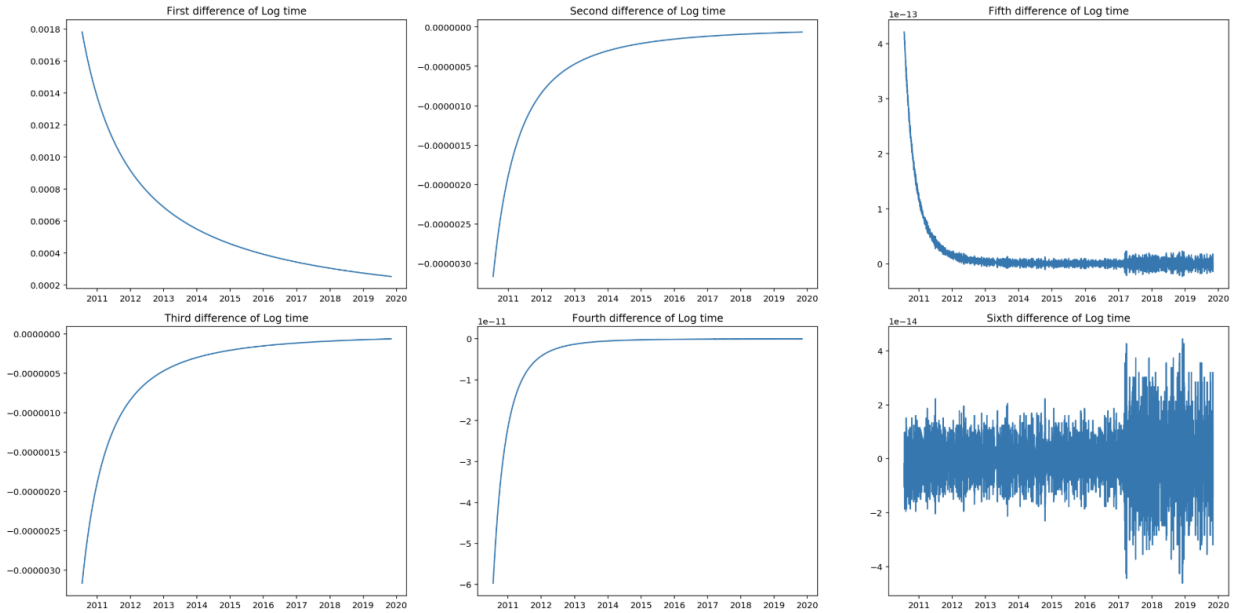
Cointegration and Order of Integration

In order for two time series to be possibly cointegrated, those time series have to be integrated of the same order. Time to check how the both series are integrated, as they are both clearly non-stationary (both series trend up). Let's have a look at the original series and their first differenced series. (Differencing means taking the difference of two consecutive values in the same time series.)



Variables over time and their first differenced series

The charts above show that both time series are not stationary. Ln(price) is integrated of the first order as it shows to be stationary after differencing the series once. For log(time) we have to look further, as differencing once didn't result in a stationary series. We keep on differencing to find the integration order for log(time), which resulted in the following:



Log(time) seems to be 6th order integrated.

Log(time) seems to be integrated of the 6ht order. This tells us that both variables are integrated of a different order and therefore cointegration is off the table. No need to run any further checks or statistical tests, as this requirement is not met.

EDIT: The 6th order integration as mentioned above is not proven by any test. In fact I learned that it even might not be reaching stationarity at all. The graph showing the sixth order difference, illustrates that we reach the limitations of the computer, as we witness floating point noise. For the conclusion it doesn't matter. Special thanks to Hmatejx for pointing this out.

Conclusion

The model as developed by Harold Christopher Burger (more detail here: https://medium.com/coinmonks/bitcoins-natural-long-term-power-law-corridor-of-growth-649d0e9b3c94) is falsified. Since the model is falsified there is no need to compare it to any other model and PlanB's stock to flow model in particular. A first threshold to compare a model to other models is that it should meet the fundamental assumptions.

Appendix

Durbin Watson table

n\k	1		2		3		4		5		6		7		8		9		10	
6	0.610	1.400																		
7	0.700	1.356	0.467	1.896																
8	0.763	1.332	0.559	1.777	0.367	2.287														
9	0.824	1.320	0.629	1.699	0.455	2.128	0.296	2.588												
10	0.879	1.320	0.697	1.641	0.525	2.016	0.376	2.414	0.243	2.822										
11	0.927	1.324	0.758	1.604	0.595	1.928	0.444	2.283	0.315	2.645	0.203	3.004								
12	0.971	1.331	0.812	1.579	0.658	1.864	0.512	2.177	0.380	2.506	0.268	2.832	0.171	3.149						
13	1.010	1.340	0.861	1.562	0.715	1.816	0.574	2.094	0.444	2.390	0.328	2.692	0.230	2.985	0.147	3.266				
14	1.045	1.350	0.905	1.551	0.767	1.779	0.632	2.030	0.505	2.296	0.389	2.572	0.286	2.848	0.200	3.111	0.127	3.360		
15	1.077	1.361	0.946	1.543	0.814	1.750	0.685	1.977	0.562	2.220	0.447	2.471	0.343	2.727	0.251	2.979	0.175	3.216	0.111	3.438
16	1.106	1.371	0.982	1.539	0.857	1.728	0.734	1.935	0.615	2.157	0.502	2.388	0.398	2.624	0.304	2.860	0.222	3.090	0.155	3.304
17	1.133	1.381	1.015	1.536	0.897	1.710	0.779	1.900	0.664	2.104	0.554	2.318	0.451	2.537	0.356	2.757	0.272	2.975	0.198	3.184
18	1.158	1.391	1.046	1.535	0.933	1.696	0.820	1.872	0.710	2.060	0.603	2.258	0.502	2.461	0.407	2.668	0.321	2.873	0.244	3.073
19	1.180	1.401	1.074	1.536	0.967	1.685	0.859	1.848	0.752	2.023	0.649	2.206	0.549	2.396	0.456	2.589	0.369	2.783	0.290	2.974
20	1.201	1.411	1.100	1.537	0.998	1.676	0.894	1.828	0.792	1.991	0.691	2.162	0.595	2.339	0.502	2.521	0.416	2.704	0.336	2.885
21	1.221	1.420	1.125	1.538	1.026	1.669	0.927	1.812	0.829	1.964	0.731	2.124	0.637	2.290	0.546	2.461	0.461	2.633	0.380	2.806
22	1.239	1.429	1.147	1.541	1.053	1.664	0.958	1.797	0.863	1.940	0.769	2.090	0.677	2.246	0.588	2.407	0.504	2.571	0.424	2.735
23	1.257	1.437	1.168	1.543	1.078	1.660	0.986	1.785	0.895	1.920	0.804	2.061	0.715	2.208	0.628	2.360	0.545	2.514	0.465	2.670
24	1.273	1.446	1.188	1.546	1.101	1.656	1.013	1.775	0.925	1.902	0.837	2.035	0.750	2.174	0.666	2.318	0.584	2.464	0.506	2.613
25	1.288	1.454	1.206	1.550	1.123	1.654	1.038	1.767	0.953	1.886	0.868	2.013	0.784	2.144	0.702	2.280	0.621	2.419	0.544	2.560
26	1.302	1.461	1.224	1.553	1.143	1.652	1.062	1.759	0.979	1.873	0.897	1.992	0.816	2.117	0.735	2.246	0.657	2.379	0.581	2.513
27	1.316	1.469	1.240	1.556	1.162	1.651	1.084	1.753	1.004	1.861	0.925	1.974	0.845	2.093	0.767	2.216	0.691	2.342	0.616	2.470
28	1.328	1.476	1.255	1.560	1.181	1.650	1.104	1.747	1.028	1.850	0.951	1.959	0.874	2.071	0.798	2.188	0.723	2.309	0.649	2.431
29	1.341	1.483	1.270	1.563	1.198	1.650	1.124	1.743	1.050	1.841	0.975	1.944	0.900	2.052	0.826	2.164	0.753	2.278	0.681	2.396
30	1.352	1.489	1.284	1.567	1.214	1.650	1.143	1.739	1.071	1.833	0.998	1.931	0.926	2.034	0.854	2.141	0.782	2.251	0.712	2.363

References

1. https://medium.com/@100trillionUSD/modeling-bitcoins-value-with-scarcity-91fa0fc03e25
2. https://medium.com/coinmonks/bitcoins-natural-long-term-power-law-corridor-of-growth-649d0e9b3c94
3. CoinMetrics Datasets, https://coinmetrics.io/data-downloads/
4. M. Verbeek, A Guide To Modern Econometrics
5. http://www.real-statistics.com/statistics-tables/durbin-watson-table/

Bitcoin Operating System

By Aleksander Svetski

Posted December 1, 2019

Bitcoin is a new "Monetary Network", not a "Payments Technology".

Bitcoin is the first time we've combined Money as a unit, with Money as a Network, into one thing.

More on this here:

"Why Bitcoin Matters"

And because it's so different, it's hard to wrap our heads around it.

The problem is further compounded by the fact that nobody really understands money, but most people get payments. Payments are easy: move money, and because it's been handled digitally for the last 20–30yrs now, it's even easier to grasp.

But money, that's a much broader, more foundational concept, and to understand Bitcoin better; we'll need to understand its real innovation, and in the process separate 'money' from 'payments'.

As we've established, Immutability is derivative of **cost**. It's this cost of validating transactions and maintaining the network of distributed but consistent ledgers that gives something like Bitcoin its immutability.

Bitcoin's true innovation was an autonomous network that can establish the authenticity and validity of the state of the broadly distributed ledger.

The ONLY advantage of using this type of costly infrastructure is for actions that require a large degree of trust and assurance, those that should never fail and those that should not be easily reversed. There are a limited set of these, i.e. every transaction / or state change that happens in the world does NOT need this.

The world works pretty fine right now.

Could we make it better by stamping a "net state" to something immutable once a week / once a month?

Yes — definitely. But every transaction? No way. It's just overkill.

Bitcoin is the most secure / immutable network that exists, NOT because of its "blockchain", but because of its elaborate and expensive authentication mechanism. Your laptop has the ability to process hundreds of thousands of transactions a minute. That process is trivial. *Payments is trivial.*

Autonomous, distributed validation is the innovation.

And this is where people go astray.

People don't 'get' bitcoin because they perceive it as some form of payments technology, or some "blockchain" mechanism (which they don't really understand) for moving funny internet money (which they also don't understand). That's not what Bitcoin is.

Bitcoin is a complete reinvention of "money" — the world's oldest social contract and society's most foundational layer.

To understand its impact, you need to have a broad understanding of both networks and money. The problem is, most people don't. In fact, nobody really understands what money is, because it's not taught anywhere. Few can define it, whether they're in banking, finance, technology, fintech, capital markets, and especially payments — so they apply their biases to it, and completely miss the point.

It's like discussing the structure of the egyptian pyramids with your pet goldfish. The goldfish simply lacks the context.

Money requires an understanding of our evolution as a species, anthropology, biology, social engineering, psychology, game theory and what I like to call "the societal stack." Discussing this is well outside the scope of this section, but I'll touch on an area which I hope will give you a reference point, the societal stack, in a subsequent section of this edition of The Bitcoin Times.

The complexity of network dynamics doesn't make the job of understanding Bitcoin any easier. I will touch on this further in a dedicated section — but suffice it to say networks are just as foreign to our intuitive understanding of the world as the pyramids are to the goldfish — the track record of the experts adds weight to this.

Back to payments VS money.

Bitcoin is not a "payments technology". It's fundamentally a reinvention if money. Like the motor vehicle was a reinvention of transport — not a better

horse and cart. Same as the internet. It reinvented the fabric upon which we communicate. It reinvented the way information is transported. It did not push more, richer or smarter “data” through the phone networks infrastructure.

It used that infrastructure as physical onramps; but the internet is not the cables, or the hardware — it’s so much larger.

That’s why it swallowed them up and is the foundation upon which the majority of today’s society operates. And what’s more, the internet is only picking up speed. Bitcoin is where the internet was in the late 80s. Still largely misunderstood. People are still arguing about speed of payments! They don’t realise that “payments” as we know them today will completely transform.

The same way we’re no longer talking about the quality of the phone call and number of phone calls this “internet thing” will support, we will see new conversations emerge for what can be done on Bitcoin.

The world is changing. The internet was only the beginning….Bitcoin is the next chapter.

Speaking of next chapters, as we near the end of the Medium series for the first edition of The Bitcoin Times, we’re going to begin exploring networks, how the function and dig into where there are some high level conceptual similarities to the internet.

Download the full guide at:

https://bitcointimes.news

Could Bitcoin's privacy benefit from Litecoin's EB MimbleWimble proposal?

By Pieter Wuille

Posted December 2, 2019

It's not that simple.

I would personally very much like to see Confidential Transactions in Bitcoin. Hiding transaction amounts by default - while not a silver bullet for privacy on its own - would make CoinJoin a lot more powerful (right now you need to use matching amounts because you'd leak linkage otherwise anyway). I think it's fair to say that it may help achieve a level of privacy that is very hard to reach with existing on-chain techniques.

Confidential Transactions however very fundamentally change how transactions work, as cleartext amounts are currently expected in transactions. Without (extremely invasive) hard fork, this cannot be changed. Even if they're suddenly permitted, nobody can force existing wallets to suddenly adopt them. Doing so would break compatibility, and go against very basic expectations of not invalidating existing non-broadcast transactions. Such a change being successful probably implies Bitcoin lost some of its most valuable properties to begin with. Thus: CT (or any form of amount hiding) has to be opt-in.

But opt-in doesn't need to imply opt-in on a per-transaction basis. An extension block effectively does that: by having two clearly delineated sides and a need for explicit, possibly slow/expensive, operations to transfer between them, you create a world where CT is the default, and possibly even cheaper than the other side. Sure, people still have the option to use the legacy side, and for a long time they probably will due to compatibility reasons, but in the long term it probably means much better privacy than any solution with per-transaction choice for CT or not. It turns out that CT-in-an-EB is also far simpler and more efficient than trying to hack it into the existing transaction structure.

So, I believe that Extension Blocks are the only (somewhat) practical way of introducing CT to Bitcoin.

That said, there are many caveats:

- CT transactions are far more computationally expensive and larger than current transactions, and it would be very unfortunate if the more private choice ends up being more expensive to use.
- CT introduces a much stronger assumption on cryptography than we currently have. You can't just run through the UTXO set, sum up the values, and see that it doesn't exceed the expected subsidy.
- In fact, CT inherently either must make privacy condition on cryptographic assumptions, or soundness (=printing of money). Bitcoin currently relies on the ECDLP assumption for theft, but this can (in the long term) be upgraded to another assumption if necessary (e.g. because we believe ECDLP is on shaky grounds, quantum computing, …). With CT this is not so easy anymore, as this assumption will now cover amounts as well.
- It's a pretty damn big change that would need a huge demand from the ecosystem to be successful.
- All the same issues apply to MW, and more. MW is a more advanced form of CT that has an even more invasive impact on basic data structures, and probably simply cannot be done without an EB at all, as it is so fundamentally different from Bitcoin's current blockchain (the MW blockchain can shrink over time!). It also removes Script or even the ability to have something Script-like.

Let me come back to point (3) above. There is a very fundamental result in zero-knowledge proof techniques that you cannot have both unconditional privacy and unconditional soundness. We however do know of ways to have either unconditional privacy or unconditional soundness, so there is a design choice between them.

- CT with unconditional privacy but computational soundness is the most common choice. This means that if somehow ECDLP breaks (math breakthrough, unexpected structure in secp256k1, quantum computer), someone could undetectably print coins, but the privacy of past (and future) transactions would be unaffected. To the best of my knowledge, Monero, ZCash, Grin, all use this model.
- CT with unconditional soundness but computational privacy is also possible. This means that an ECDLP break would not let anyone print coins, but the privacy of future (and past) transactions would be at risk. Unfortunately, this choice is much less efficient, and pretty much no systems use it.

Given Bitcoin's design focus on controlled inflation, I expect that many people would prefer the second model over the first if a choice needs to be made. There is however also a point to be made that if ECDLP is broken, the future

of the system is inherently at risk, but we may not want to give up the privacy of the past when that happens - a point in favor of the first model.

The nice (or scary...) thing about an Extension Block based CT design is that we could have either, or both, and without actually directly affecting the value of the legacy chain. You'd need to move coins explicitly to the CT side, and if unexpected inflation would happen there, simply not all of it would be able to move back to the legacy side. Unexpectedly, this may actually mean a different exchange rate for coins on both sides, if the public's trust in the security for one is seriously affected.

A Look at Innovation in Bitcoin's Technology Stack

By Lucas Nuzzi

Posted December 3, 2019

Bitcoin has come a long way over the past ten years. Relative to the first iteration of its software, the quality and reliability of current implementations has remarkably improved. Rapidly and organically, Bitcoin was able to lure a legion of developers to dedicate thousands of hours to improve, and at times revamp, most of its underlying codebase.

Nevertheless, Bitcoin is still the same. Much like a constitution, the core set of consensus rules that define its monetary properties, such as its algorithmic inflation and hard-coded supply, remain unchanged. Time and time again, factions have attempted to change these core properties, but all hostile takeovers thus far have failed. It's often a painful process, but one that highlights and solidifies two of Bitcoin's biggest virtues:

1. **No single party can dictate how Bitcoin evolves**
2. **The lack of centralized control protects Bitcoin's monetary properties**

Interestingly, these are the rules that attract cypherpunks and institutional investors alike. These are the rules that make bitcoin an unprecedented type of money. However, these are also the rules that make developing software atop Bitcoin more challenging than any other digital asset. In essence, Bitcoin's constitution awards developers a limited toolkit so that they can't infringe upon its monetary policy. There's too much at stake to *move fast and break things*.

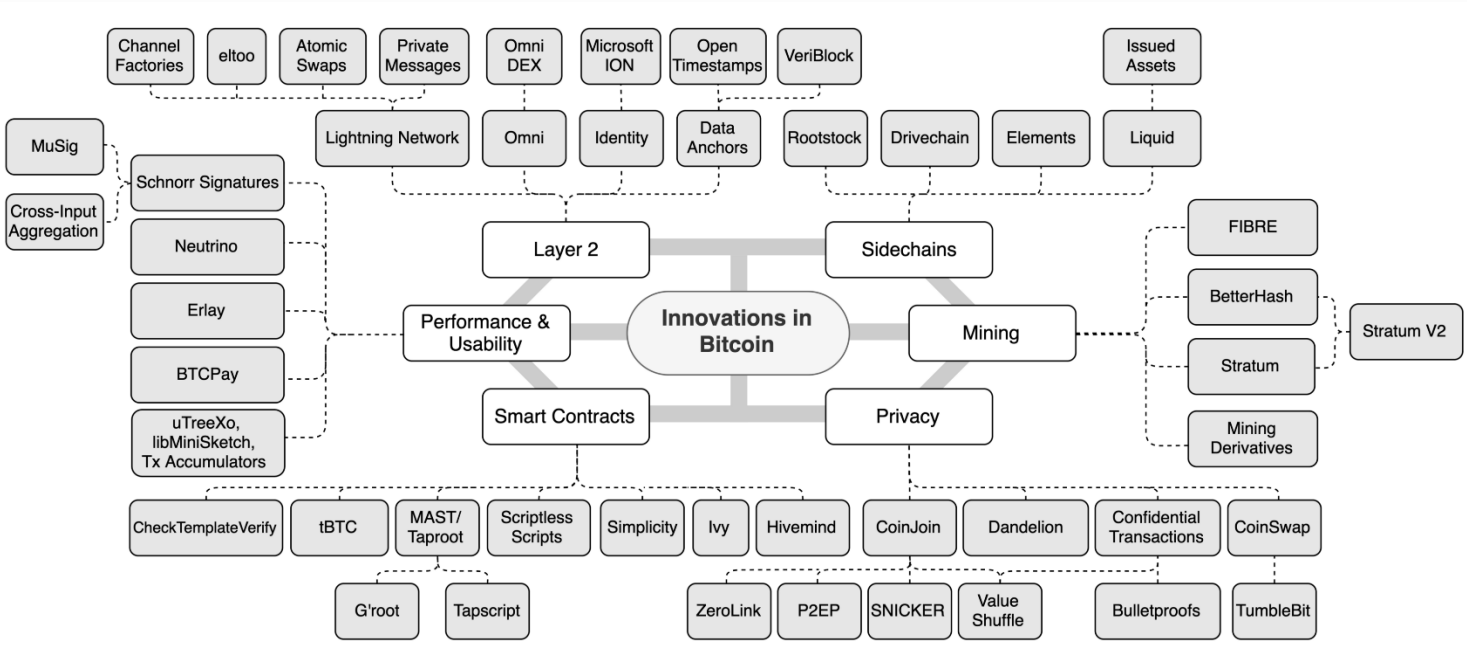
That means innovation in Bitcoin requires creativity, patience, and perhaps most importantly, ego-minimization. After all, the fundamental rules embedded in Bitcoin's constitution ultimately supersede technology. This is why Silicon Valley has had a hard time understanding Bitcoin's value proposition, it's not just a technology, financial instrument, or consumer application; it's an entire monetary system *supported* by technology. Changing Bitcoin's constitution requires a quasi-political process that can infringe upon its monetary properties, therefore, technological innovation is implemented as modules.

As often pointed out, Bitcoin's modular approach to innovation is analogous to the evolution of the Internet's protocol suite, whereby layers of different protocols specialized in specific functions. Emails were handled by SMTP, files by FTP, web pages by HTTP, user addressing by IP and packet routing by TCP.

Over the years, each of these protocols evolved to provide the full experience you're having this very second.

In Spencer Bogart's excellent post on the emerging Bitcoin technology stack, he makes the case that **we are now witnessing the beginning of Bitcoin's own protocol suite**. As it turned out, the inflexibility of Bitcoin's core layer gave birth to several additional protocols that specialize in various applications, like Lightning's BOLT standard for payment channels. Innovation is both vibrant and (relatively) safe, as this modular approach minimizes systemic monetary risks.

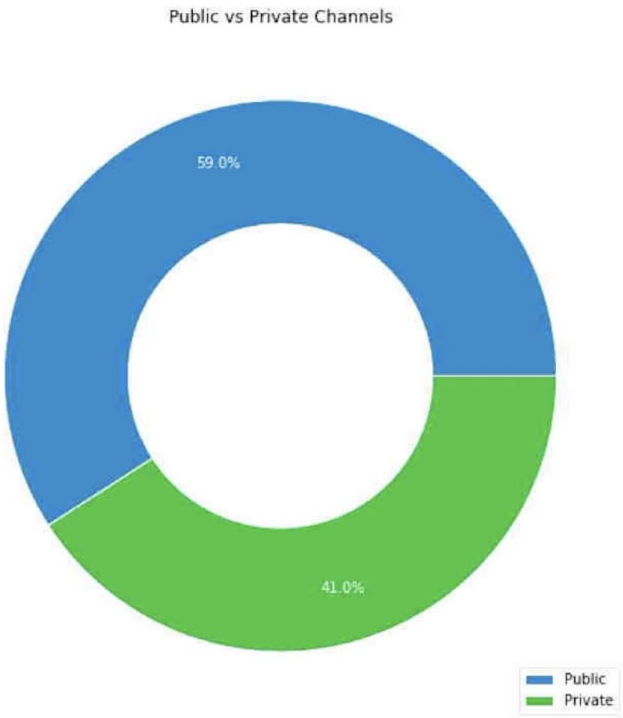
So much is happening at the many layers of Bitcoin's technology stack, it can be incredibly difficult to keep track of emerging solutions. The diagram below is an attempt to map all relatively new initiatives and showcase a more complete picture of Bitcoin's technology stack. It is not exhaustive, and it does not signal any endorsement for specific initiatives. It is, nevertheless, impressive to see that innovation is being pushed on all fronts; from *layer 2* technologies, to emerging smart contract solutions:



Layer 2

There has been a lot of talk lately about the rate of adoption of the Lightning Network; Bitcoin's most prominent *layer 2* technology. Critics often point at an apparent decline in the number of channels and total BTC locked in Lightning; two metrics frequently used to evaluate user adoption. Although the community has converged on such metrics, it is important to point out

that they are fundamentally flawed given the way Lightning works under the hood.



One of the most underrated virtues of the Lightning Network is its straightforward privacy properties. Since Lightning does not rely on global validation of all state changes (i.e. its own blockchain), users can transact privately over using additional techniques and network overlays, like Tor. At this point, we can estimate the percentage of private usage of the Lightning network by analyzing the number of channel opening transactions on-chain, and comparing that to the number of public channels off-chain. **Christian Decker estimates that 41% of Lightning channels are private:**

Source: Christian Decker

Activity happening within these channels is not captured by popular Lightning explorers. As such, **an increase in private usage of Lightning results in a decrease in what can be publicly measured**, leading observers to erroneously conclude that adoption is down. While it is true that Lightning must overcome substantial usability barriers before it can enjoy wide adoption, we must stop using misleading metrics to make assertions about the current state of the network. As Decker pointed out in his talk at the latest Lightning Conference in Berlin, even the above estimate of private vs. public channels is flawed, as the adoption of Schnorr signatures will make channel-opening transactions indistinguishable from regular transactions.

Another interesting recent development in the field of layer 2 privacy was the creation of WhatSat, a private messaging system atop Lightning. This project is a modification of the Lightning deamon which allows for relayers of private messages (the messengers that connect the entities communicating) to be compensated for their services via micropayments. This decentralized, censorship-and-spam-resistant chat was enabled by innovations in LND itself, such as recent improvements in the lightning-onion, Lightning's own onion routing protocol.

The growth of ***Lapps***, or Lightning Applications, demonstrate the wide applicability of these innovations when it comes to consumer applications, from a Lightning-powered cloud computing VPS to an image hosting service that shares ad revenue via microtransactions. And that's just layer 2 innovation within Lightning. More generally, we define *Layer 2* as a suite of applications that use Bitcoin's base layer as a *court* where exogenous events are reconciled and disputes are settled. As such, the theme of *data anchoring* on Bitcoin's blockchain is much broader, with companies like Microsoft pioneering a decentralized ID system atop Bitcoin. Such initiatives increase the demand for on-chain reconciliation and are instrumental for the long-term development of a Bitcoin fee market.

Smart Contracts

There are also a number of projects attempting to bring back expressive smart contract functionality to Bitcoin in a safe and responsible way. This is a significant development, because starting in 2010, several of the original Bitcoin opcodes (the operations that determine what Bitcoin is able to compute) were removed from the protocol. This came after a series of terrifying bugs were unveiled, which led Satoshi himself to disable some of the functionality of Script, Bitcoin's programming language.

Over the years, it became crystal clear that there are non-trivial security risks that accompany highly-expressive smart contract functionality. The common rule of thumb is that the more functionality is introduced to a virtual machine (the collective verification mechanism that processes opcodes), the more unpredictable its programs will be. More recently, however, we have seen new approaches to smart contract architecture in Bitcoin that can minimize unpredictability, but also provide vast functionality.

The devise of a new approach to Bitcoin smart contracts called Merkleized Abstract Syntax Trees (MAST) has ignited a new wave of supporting technologies that attempt to optimize the trade-offs between security and functionality. Most prominently is Taproot, an elegant implementation of the MAST structure that enables an entire application to be expressed as a Merkle Tree, whereby each branch of the tree represents a different execution outcome. Along with Taproot will come a programming language called Tapscript, which can be used to more easily express the spend conditions associated with each branch of the Merkle Tree.

Another interesting innovation that has recently resurfaced is a new architecture for the implementation of covenants, or spend conditions, on Bitcoin transactions. Originally proposed as a thought experiment by Greg Maxwell back in 2013, covenants are an approach to limit the way balances can be spent, even as their custody changes. Although the idea has existed for nearly seven years, covenants were impractical to be implemented before

the advent of Taproot. Now, a new opcode called OP_CHECKTEMPLATEVERIFY (formerly known as OP_SECURETHEBAG) is leveraging this new technology to potentially enable covenants to be safely implemented in Bitcoin.

At first glance, covenants are incredibly useful in the context of lending (and perhaps bitcoin-based derivatives) as they enable the creation of policies like clawbacks to be attached to specific BTC balances. But their potential impact on the usability of Bitcoin goes vastly beyond lending. Covenants can allow for the implementation of things like Bitcoin Vaults, which, in the context of custody, provide the equivalent of a second private key that allows a party that has been hacked to "freeze" stolen funds. There are so many other applications of this technology, like Non-Interactive Payment Channels, Congestion Controlled Transactions, CoinJoins, it truly deserves a standalone post. For more on this, check out Jeremy Rubin's BIP draft.

It is important to note that Schnorr signatures are the technological primitive that make all of these new approaches to smart contracts possible. After Schnorr activates, even edgier techniques being can be theorized, such as Scriptless Scripts, which could enable fully private and scalable Bitcoin smart contracts to be represented as digital signatures (as opposed to opcodes). Similarly, Discreet Log Contracts also employ the idea of representing a smart contract's execution outcome as a digital signature for better privacy and scalability. Together, these new approaches may enable novel smart contract applications to be built atop Bitcoin and Schnorr is the basis of it.

Mining

There have also been some interesting developments in mining protocols, especially those used by mining pool constituents. Even though the issue of centralization in Bitcoin mining is often wildly exaggerated, it is true that there are power structures retained by mining pool operators that can be further decentralized. Namely, pool operators can decide which transactions will be mined by all pool constituents, which grants them considerable power. Over time, some operators have abused this power by censoring transactions, mining empty blocks and reallocating hashing output to other networks without the authorization of constituents.

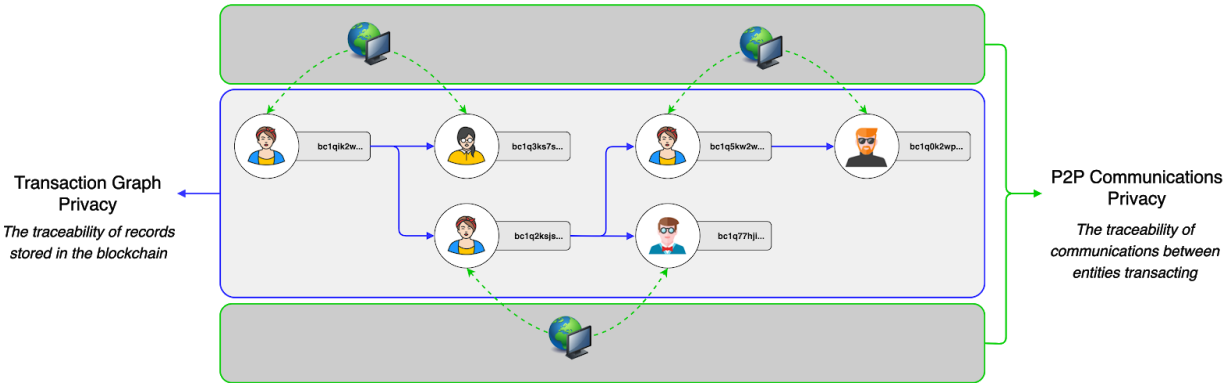
Thankfully, there are technologies that are attempting to flip that power structure upside down. One of the most substantial changes coming to Bitcoin mining is the second version of Stratum, the most popular protocol used in mining pools. Stratum V2 is a complete overhaul that implements BetterHash, a secondary protocol that enables mining pool constituents to decide the composition of the block they will mine and not the other way around. Stratum V2 also implements several optimizations, and allows mining pool constituents to better communicate and coordinate.

Another interesting development in the mining industry that should contribute to more stability is reignited interest in hashrate and difficulty derivatives. These can be particularly useful for mining operations that wish to hedge against hashrate fluctuations and difficulty readjustments. While these derivatives have yet to be productized, this marks an interesting evolution in the industrialization of Bitcoin mining.

Privacy

After our report on Schnorr signatures, some privacy-coin advocates were outraged by the suggestion that *sufficient* privacy may be optionally achieved in Bitcoin at some point. Although this suggestion may challenge theses around the long-term value proposition of privacy assets, there are a host of emerging protocols that can bring better privacy into Bitcoin. Although it is likely that privacy in Bitcoin will continue to be more of an art than a science, there have been interesting innovations on this front that are worth highlighting.

Before we delve into specific privacy innovations, it's important to highlight that the biggest impediment to private transactions across digital assets is the fact that most solutions are half-baked. Privacy assets that focus on transaction-graph privacy often neglect network-level privacy, and vice versa. Both vectors suffer from a lack of maturity and usage, which makes transactions easier to de-anonymize via statistical traceability analysis at either the P2P network layer or the blockchain layer.



Thankfully, there are several projects pushing boundaries on both fronts.

When it comes to transaction-graph privacy, solutions like P2EP and CheckTemplateVerify are interesting because **privacy becomes a by-product of efficiency.** As novel approaches to CoinJoin, these solutions can increase the adoption of private transactions by users that are solely motivated by lower transaction fees. Although privacy guarantees are still suboptimal under a CoinJoin model, unshielded sent amounts can still be beneficial, as they preserve the auditability of Bitcoin's supply and free float.

If lower transaction fees become a motivator and lead to an increase in Bitcoin's anonymity set (the % of UTXOs that are CoinJoin outputs), de-anonymization via statistical clustering analysis will become even more subjective than it already is. Some blockchain analysis companies have been able to trick law enforcement agencies into believing an assigned probability that a UTXO belongs to a specific user, but the underlying model is already extremely nuanced and fragile. If the majority of UTXOs become CoinJoin outputs, that might break existing approaches to clustering.

Before that can happen, there's a tremendous amount of work that needs to be done on the usability front so that all Bitcoin users, tech savy or not, have equal access to privacy mechanisms. Beyond P2EP and CheckTemplateVerify, a recent development in usability was the proposal of SNICKER (Simple Non-Interactive CoinJoin with Keys for Encryption Reused), a novel way to generate CoinJoins with untrusted peers. SNICKER combines several technologies to grant users access to CoinJoin transactions without having to trust or interact with their peers.

Progress is also noticeable in protocols that aim to improve the privacy and efficiency of P2P communications. Over the course of 2019, the privacy-preserving network protocol Dandelion was successfully tested across multiple cryptonetworks. Even though privacy in transaction propagation is not a silver bullet when it comes to the full spectrum of P2P communication, protocols like Dandelion can still meaningfully increase user privacy by hiding the originating IP address of a nodes broadcasting a transaction.

A final development in Bitcoin's networking stack worth highlighting is a new transaction relay protocol called Erlay. Although still at a very early development stage, Erlay is an important innovation because it can considerably reduce the bandwidth requirements of running a Bitcoin full node. If implemented, Erlay's efficiency gains can enable users to participate in transaction relay, which is bandwidth intensive, and continuously validate the chain, especially in countries where Internet Service Providers impose caps on bandwidth.

The Tip of the Iceberg

It is incredibly difficult to track all the innovation happening in Bitcoin, and this post is just a scratch on the surface. This brings us to the key takeaway of this piece: Bitcoin, in its totality, is a constantly evolving suite of protocols. The modular approach to innovation described here is important, as it plays a key role in minimizing politicism in the evolution of Bitcoin and protects its fundamental monetary properties. Remember this article the next time someone claims Bitcoin is a static technology.

Connect with DAR

If you would like to learn more about DAR, click here to reach out. For our free daily newsletter chocked full of the highest quality crypto news and information, sign up here.

Bitcoin's Missionaries vs Wall Street's Mercenaries

By Anthony Pompliano

Posted December 3, 2019

This installment of Off The Chain is free for everyone. I send this email to our investors daily. If you would also like to receive it every morning, join the 38,000 other investors today.

To investors, There are a lot of common misconceptions surrounding Bitcoin. These usually revolve around cybersecurity, energy consumption, monetary competition, or some other nuanced element of the digital currency and the tertiary impact on the world. But one misconception is rarely spoken of — the difference between mercenaries and missionaries. This framework was developed by John Doerr, the famous venture capitalist who led Kleiner Perkins Caufield & Byers for many years, and was first presented publicly when he said "we need teams of missionaries, not teams of mercenaries."

The Harvard Business Review did a great job explaining what Doerr meant by this in an April 2016 article:

As Doerr explained to an audience at Stanford Business School, mercenaries are "opportunistic." They're "all about the pitch and the deal" and are eager to sprint for short-term payoffs. Missionaries, on the other hand, are "strategic." They're all about "the big idea" and partnerships that last, and they understand that "this business of innovation is something that takes a long time" — it's a marathon, not a sprint. Mercenaries have "a lust for making money," while missionaries have "a lust for making meaning." Mercenaries obsess about the competition and fret over "financial

statements," while missionaries obsess about customers and fret over "values statements." Mercenaries display an attitude of entitlement and revel in the "aristocracy of the founders," while missionaries exude an attitude of contribution and welcome good ideas wherever they originate. Mercenaries strive for success; missionaries aspire to "success and significance."

John Doerr used the framework to talk about entrepreneurial teams, so what exactly does this have to do with Bitcoin and finance?

More than you would think. Generally, Wall Street is full of mercenaries. These individuals are focused on profits. They operate in a cutthroat environment where everyone in a deal is trying to screw over everyone else. Employees will leave in a heartbeat for bigger bonuses or more opportunity. There is very little loyalty and most people make decisions optimized around personal gain.

This is almost the complete opposite of the Bitcoin ecosystem. Rather than mercenaries, Bitcoin has benefited from a long list of missionaries. Whether it is Wences Casares teaching Silicon Valley luminaries one after the other about Bitcoin in the early days or Andreas Antonopoulos traveling around the world to educate millions of people for free, Bitcoiners believe in something much more important than profits. They believe in a better world. They see Bitcoin as a way to break the current systematic issues plaguing society. Simply, they believe that Bitcoin can change the world.

When mercenaries and missionaries compete with each other, the missionaries usually prevail. They believe in what they are doing on a much deeper level. They are willing to go to greater lengths to succeed. They can endure more pain. They refuse to give up. The mission is so important that the missionary is willing to dedicate their lives to seeing it come to fruition.

This fanaticism is what has driven Bitcoin from non-existence to one of the most popular currencies in the world in only one decade. People are drawn into the Bitcoin ecosystem for many reasons initially — some for profits, some for the technology, some for the polymath-like complexity — but almost anyone who stays around through the bull and bear market cycles has a belief in something much more important than profits.

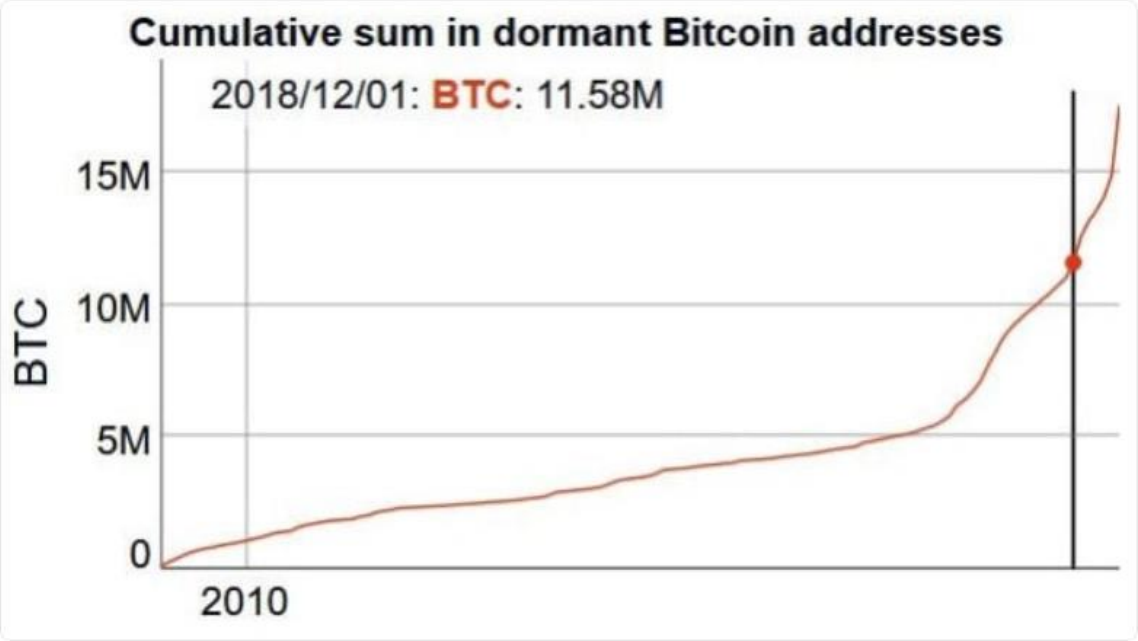
Nowhere is this more apparent than when we evaluate what people are doing with their Bitcoin. Twitter analyst @Rhythmtrader recently looked at how many people have moved their Bitcoin in the last year and found that more than 11,500,000 haven't moved at all.

Rhythm
@Rhythmtrader

11,580,00 bitcoin have not moved in over a year.

Even with a 85% increase in price during that time, those millions of bitcoin were not sold or traded.

Hodlers of last resort are insane.



December 1st 2019

436 Retweets **1,492** Likes

These people don't care about the USD exchange value of Bitcoin. They believe in Bitcoin. They won't be shaken out by price movements. In their mind, 1 BTC equals 1 BTC. We aren't building a new trading asset, we are building a new financial system that decentralizes power from a corrupt and rigged system.

For Bitcoiners, this isn't an investment. It is a protest. A peaceful protest against the system. Better yet, Bitcoin is a revolution. A revolution that stands to change the world in ways that most people can't even comprehend yet. If

successful, Bitcoin will usher in a new era where there is a separation of state and money. One where people are asked to trust transparent software systems over humans.

Quite literally, Bitcoin will disrupt the power structure of the world by simply surviving. For some, this is a scary world. For others, it is a necessary world.

And this is the largest misconception in the institutional investment world. The decision to allocate capital is not about today's price and where it may go in the future. It is much more simple than that. Most institutional investors have 100% of their portfolio exposure in the dollar-denominated, fiat financial system.

There is now a new financial system being built. An alternative. Plan B. By choosing not to allocate any capital to this new financial system, institutional investors are claiming 100% confidence that the legacy system will survive. That the legacy system will prevail.

But if an institution thinks there is even a 1% chance that this new financial system will thrive, they must allocate capital to that system or risk missing one of the most disruptive events of our lifetime. The allocation percentages of the new and old system should mirror the confidence level that an institution has in each financial system winning over the long run.

But institutions aren't missionaries. They are mercenaries. They play games of probability. They underwrite risk. They are unemotional about their investments. So we shouldn't expect them to have more than 1-5% exposure to the new world.

But Bitcoiners are the exact opposite. Bitcoin isn't risky to them, not owning Bitcoin is risky. These missionaries believe in something that seems irrational to most. But if Bitcoiners are successful, the mission will seem obvious in hindsight.

Whenever I see missionaries competing with mercenaries, the choice is obvious. And to say that I believe in the future potential of what we are all building would be an understatement. The current system is broken for most people. They can't get ahead. They have no way to fight back. The issues are systemic. And there won't be a solution until we change the system.

Bitcoin is doing just that. As Rhythmtrader said so eloquently, "Hodlers of last resort are insane." But in the future, the nocoiners will be seen as having been the insane ones.

-Pomp

Tweetstorm: A Decade in Bitcoin

By Lucas Nuzzi

Posted December 5, 2019

2010 - Satoshi decentralizes Bitcoin by leaving his leadership role as its creator, and never again commenting on its development.

The Bitcoin community self-organizes, and begins to grow into new type of global institution.

2011 - The Silk Road showcases one of the biggest virtues of Bitcoin; it can't be censored or confiscated. A drawback? It's not private.

The Mt. Gox fiasco highlights infrastructural deficiencies; the lack of secure custody standards and the systemic risks imposed by exchanges.

2012 - BIP23 formalizes the concept of mining pools, an emerging structure that further decentralizes the power structures within Bitcoin.

BIP32 introduces HD keys & sets a new standard for Bitcoin custody and user onboarding via safer wallets.

2013 - BIP39 introduces mnemonic keys to Bitcoin.

➡️➡️For the first time in human history, you can store your wealth in your brain by memorizing 12 words. No centralized intermediaries needed. ⬅️⬅️

2014 - BIP42 makes it impossible for Bitcoin's 21M cap to be infringed upon via continuous mining.

Mining industrializes and hashrate surpasses 100 PH/s for the first time.

Meanwhile, pundits claim Bitcoin is dead and that the future is "blockchain, the miraculous database"

2015 - On-chain volume hits an all time high and tensions are visible. The power structures in Bitcoin are tested with 9 competing block-size-increase BIPs.

We faced the question: Who controls Bitcoin?

Miners? ❌ Developers? ❌ Personalities? ❌ Users ✅

2016 - "The Bitcoin Lightning Network" is published.

As the risks of on-chain scaling become clear, promising alternatives like Lightning show that a layered, backwards-compatible approach to technological innovation is possible.

BIP114 introduces MAST and minds are blown. 🤯

2017 (a) - The global speculative bubble brings Bitcoin to the masses. Orange Bs can be seen everywhere.

Infrastructure is being pushed on all fronts; custody, markets, wallets, education.

Bitcoin becomes a liquid asset on a global scale. 🌎

2017 (b) - One of the most important events in Bitcoin history also takes place in '17: the SegWit2X fork.

There's an attempt to highjack Bitcoin with plenty of enterprise support: the ultimate stress test of Bitcoin governance

USAF reinforces that users are the ones in charge

2018 - "Enterprise Blockchain" is now a sad meme.

The ecosystem outside of Bitcoin faces a series of hard realizations:

Scaling is hard, on-chain governance is flawed, deployment takes time, and you might have broken the law.

Institutions converge on BTC.

2019 - Bitcoin is now a movement with representatives everywhere; in media, government, traditional finance, tech. It's like Fight Club, but rule #1 to only talk about it.

Bitcoin started this decade on the fringes.

We now have a bitcoiner in a US state senate.

Bitcoin had everything to die in multiple occasions over the course of this decade... it didn't.

Its power structures were tested over and over again. Yet, here we are.

Who would've thought a leaderless system that converts electricity into money would've lasted this long?

As we approach a new decade of social anxieties, geopolitical tension and crazy monetary policy, you can be sure Bitcoin will still be here. There's no way to put the genie back in the bottle.

I think Hal would've been proud. You too should start:

Ignorance about Bitcoin Disguised as Caution

By Rollo McFloogle

Posted December 7, 2019

Bitcoin has done a lot in its 11 years of existence. Perhaps one surprising role of Bitcoin has been exposing economic ignorance—namely the economics of money—of many people. I humbly include myself in that category of people (fortunately, it can also be an invaluable tool for helping you to learn the subject as well). Bitcoin is a nebulous and mysterious amalgam of technical computer science and economics to the newcomer. Very few people, even experts in one field or the other, can instantly grasp all that is Bitcoin. It takes even the best of minds some time to sort through and figure out.

We all can identify money. We use it a lot and think about it even more. It is absolutely instrumental in our ability to perform economic calculation, which is what we do when we use the information that prices provide to help us best direct resources to their most efficient uses. But while we can talk about any number of things about money, few people are actually able to explain what money truly is and how any given thing that is used as money came about.

This confusion is one of the things that pulls people into many incorrect conclusions about Bitcoin, including plenty of well-respected people. This includes, Jeffrey Tucker, who recently penned a piece on the American Institute of Economic Research (AIER) called "A Cautious Retrospective on Bitcoin."

Tucker was an early enthusiastic proponent of Bitcoin, then got sucked into the Bitcoin Cash and altcoin hype, and now I'm not exactly sure how to categorize him.

In his AIER piece, Tucker lays out five reasons why he's feeling a little bit more on the bearish side of Bitcoin and by doing so shows that he has some key misunderstandings of Bitcoin.

Let's dive into his piece.

Before his list of five cautions, Tucker starts by showing two charts, one of transactions per day and the other of the USD exchange trade volume. He points out that transactions are at 2016 levels and exchange volumes are at 2017 levels. He then shows a third chart of wallet usage, which is steadily rising at an increasing rate, but that metric "belies the hope of a disintermediated money."

Has Bitcoin taken a step backwards and is it on the decline? It's ironic that Tucker, a man who like the rest of us scoffs at all the announcements that "Bitcoin is dead" during a bear market, would get so easily rattled in the latest lull following the by far biggest bull run to date. To be fair, he hasn't bought the casket yet, but it is surprising that Tucker apparently believes that trading activity during a surge to almost $20,000 per bitcoin would sustain itself after the price correction. We all saw what was going on in late 2017. Everyone and their mother were trying to buy and sell Bitcoin. Once the price fell back down, did anyone really expect the people trying to get rich quickly to stay in the market?

Regardless of whether or not 2016 and 2017 were cherrypicked to compare metrics, Tucker's problems are predicated from his idea that the health of Bitcoin's adoption is based on how much it is transacted with. Since money's primary use is as a medium of exchange, Tucker and many other critics of Bitcoin make the mistake of believing that money is only useful for spending in the present. They ignore that the delay of exchange, also known as saving, is also a perfectly valid—and not to mention absolutely critical—use of money. After all, what is money but a tool that transports current value across time and space for future uncertainty?

This describes money's ability to function as a store of value, which as Michael Goldstein put it is "a metaphor for using a medium of exchange for exchange in the long term." Bitcoin is still in its very early stages and those of us who see it as a way to shore up the attack surfaces that destroyed the gold standard believe that it will have a much greater value in the future as it monetizes around the world in the winner-take-all game of money. Meanwhile, fiat bolstered by legal tender laws is continuously inflated by central banks, pillaging the purchasing power of money. And we've seen the results of this: when money is expected to be worth less tomorrow than it is today, there is a strong incentive to get all the stuff you can exchange it for in the present. Everyone thinks about gratification today without regard for tomorrow. Prices are corrupted and economies have to absorb huge amounts of waste.

Thank goodness for sound money, the only medicine for this disease. When someone has both Bitcoin and fiat, he expects the value of the former to appreciate while he expects the latter to lose its value over time. Any rational economic actor will choose to spend his fiat while holding his Bitcoin whenever he can. This is Thiers' law. He will also begin to demand payment in Bitcoin while charging a premium if someone must pay him in fiat. Eventually, everyone dumps their fiat on the greatest fools and it becomes so valueless that no one will accept it as payment even at great premiums. Since Bitcoin is now the only acceptable means of payment, it has become the common medium of exchange.

But since Tucker brought up numbers and charts as metrics for his proof that Bitcoin's adoption is waning, let's consider some of our own. It's tough to point to a metric to show that people are using Bitcoin as a savings vehicle, but there certainly are things we can look at to check its health.

The first one is price in USD. Putting the y-axis on a logarithmic scale helps show the value appreciation of Bitcoin much more clearly.

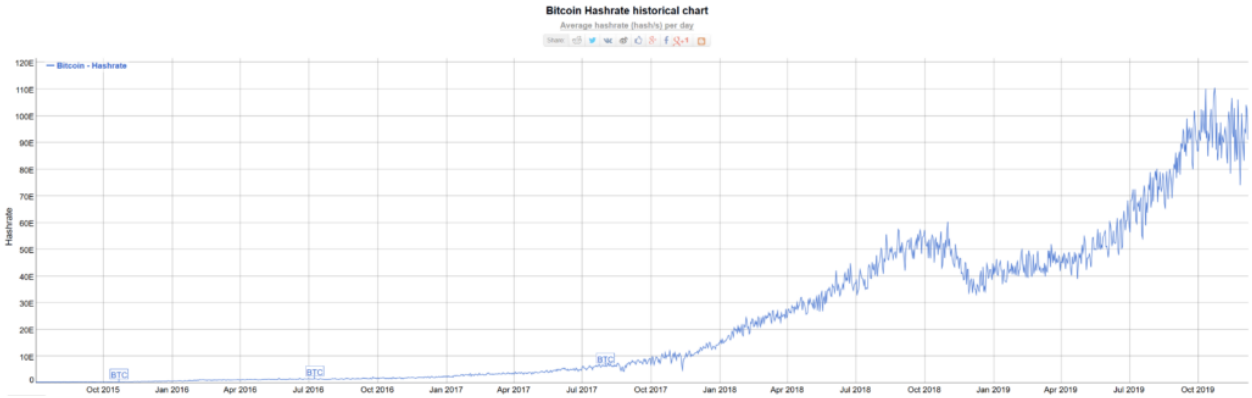
Source: https://bitcoincharts.com/charts/bitstampUSD#tgMzm1g10zm2g25zl

What cannot be ignored is that while new bitcoins are being added to the supply through the mining process, if demand remained the same throughout this process, then the price would drop. Despite the local peaks and valleys, the overall trend of Bitcoin is a rising price, so demand must be increasing. Even if it's only the current people in Bitcoin contributing to that demand, increases in price is a powerful signal to others that they should probably get in.

The other interesting metric to observe is Bitcoin's hash rate, which is the number of hashes (guesses to solve a block) per second that the aggregate of miners makes across the network. In order to contribute hashes to the network, a miner must run software on specialized hardware. This hardware requires electricity, so mining Bitcoin with any chance of solving a block requires a significant commitment of expenditures for electricity. Miners want the block reward and transaction fees when they are the first to solve a block, so they're careful not to break any rules (*i.e.* create an invalid block) that would cause all the validating nodes in the network to reject their block. If they submitted an invalid block, it would mean all the money they spent to solve it would be wasted, so miners tend to remain honest. This arrangement is what is referred to as "proof of work." Using proof of work also means that any miner who wants to reverse transactions and rewrite history would have

to spend enormous amounts of time and electricity to resolve previous blocks to submit a chain with the most proof of work to the network.

Miners add hash rate to increase their chances of solving a block and receiving the reward. More hash rate for the network means more proof of work, making it more expensive to attack, but it also makes it more difficult to solve blocks. Miners, being rational economic actors just like anyone else, are not interested in losing money on their operations.



*Source: https://bitinfocharts.com/comparison/bitcoin-hashrate.html

The chart above shows that the hash rate is the highest it has ever been. If the overall value of Bitcoin were diminishing, then why would miners be spending so many resources on it? Certainly it could mean that miners are finding cheaper sources of electricity (they are), but that search for cheap electricity is a good signal that participation is in high demand since they must seek an advantage to stay competitive.

All of this shows that Tucker doesn't have a good approach in either the economic or technical basics for viewing Bitcoin. This will help inform us to understand his perception of Bitcoin as we address each of his five considerations.

1. Underpriced market assets are grounded in information asymmetries. Profits come from possessing valuable insight that others do not share, and acting on that insight. These asymmetries can be large or small. They were very large in Bitcoin from 2009 to 2015 or so. Some of us were convinced while vast numbers of even highly sophisticated people were sure that it could not, and the results were impressive for those who took the risk.

We are now eleven years into this, and the skeptics are now in a small minority. That blockchain technology is awesome is a given. If there were vast asymmetries in knowledge in the past, those have dissipated over time. The process of price discovery might have settled into a confident equilibrium: this stuff is cool, and useful for some purposes, but it cannot be a money for

the world. It's a given that there is no "true price" for Bitcoin but it is also true that the days of astonishment that it worked at all are now settling into the widespread awareness of why it works today.

With the full hindsight at our disposal, imagine being 11 or so years into the start of the internet and saying, "You know what, we've had the internet for awhile and plenty of people know about it, but it hasn't been all that world changing, so I'm not sure this is really going to work out." (We're looking at you, Paul Krugman.) The success of the internet doesn't guarantee the success of Bitcoin, but it does give us some insight on how global protocols take time to be fully implemented.

While much of the world's population has had enough exposure to Bitcoin to at least know what it is, that doesn't mean that knowledge about Bitcoin has settled equally among all these people. Knowing of and knowing about are two very different things. How many people simply aware of Bitcoin understand how it works or what its value proposition is? How many people even understand the economics of money well enough to act on the information they get about Bitcoin? How many people are aware of second layer solutions like the Lightning Network and sidechains that can massively scale Bitcoin?

These questions matter because money is for everyone. Everyone doesn't need to know why or how it works (look at the internet again), but their ignorance about its usefulness explains why they're not using it. And in fairness to these people, even if they weren't too happy with the inflationary fiat system but didn't worry much about censorship, they wouldn't necessarily be drawn to use Bitcoin because the *on-chain layer* is not a superior substitute to the services they use for their day to day transactions in terms of cost and speed. Those who understand that the on-chain layer provides the security for the soundest money in the history of the world will compete for the bitcoins that are available for sale as they speculate that future layers built on top of this first layer will be the infrastructure that makes transitioning to Bitcoin the only play for even the ignorant.

1. At the same time Bitcoin was launched, so too were released some other impressive payment technologies designed to reduce the price of transactions and make accepting credit cards vastly easier. Back in the day, small merchants had a very hard time accepting credit cards. Thanks to technologies like Square, even a lemonade stand can accept them using a smartphone, which was also launched around the same time. The near-universal use case for Bitcoin was once obvious; apart from specific demographics and interests, the case for broad public adoption is no longer clear. To be sure, there remain vast and important uses for crypto for permissionless remittances and for allowing the

unbanked to move money (one of the booming facets of the crypto-asset sector are ATMs), but that will remain true regardless of market valuations.

It is truly a shame that Jeffrey Tucker puts censorship-resistant digital scarcity as a secondary value proposition for Bitcoin. Governments coopted central banks to use seigniorage to fund their massive expansions in size and scope, which has allowed them to wage endless warfare since. They removed the gold standard and constantly inflate the money supply, which further inflate bubbles of malinvestment. These bubbles, as part of the business cycle, have destroyed massive amounts of wealth and have prevented people from directing resources to their most efficient uses. Humanity is years behind in production and overall quality of life because governments can censor and create money on a whim. Bitcoin gives anyone with a computer and an internet connection the ability to remove the need for a trusted third party to send and receive money and to validate that the money they're receiving isn't counterfeit. This final settlement that once took large amounts of time and money now takes minutes and maybe a few dollars.

Bitcoin strikes at the root of the ability of governments to hold power. This innovation is world-changing. It is the zero-to-one event that can lead to a flourishing that humanity has never seen before. That was the hard part. Compared to that, it will be easy to build services for making fast and cheap payments on top of that.

1. The old pitch for Bitcoin – that it made payments fast, cheap, and permissionless – had been dramatically changed as adoption increased and the portals couldn't keep up. Permissionlessness still survives but that is not true of fast and cheap. By 2017 it became very obvious to the world that though Bitcoin is wonderful, it is not very practical for payments as compared with legacy systems that had vastly improved. Forks emerged to fix that problem but because the crypto sector is so vast, none could develop the network that Bitcoin obtained as the first mover in the space. Among those crypto innovations have been stable coins that operate as settlement banks. Those in the market for stability will find these more useful than old-fashioned crypto. And let us not forget the greatest lesson of monetary history: it's the use value of a currency that is its value (there is no such thing as "storing" value).

Tucker, and many like him, first entered the Bitcoin space when some people were selling it as a fast and cheap *payments processor*. The reality, however, is that Bitcoin allows anyone to run a fast and cheap *money validator*. Consider what the last sound money system, the gold standard, involved. We tend to take for granted all the trust and

centralization that had to occur simply for someone to use stamped gold coins. Imagine the cost—no wonder that work got entrusted for someone else to do. It is totally impractical for an individual accepting gold payments to test that the gold he is receiving is the gold that he is expecting for every single payment.

Bitcoin fixes this. Running a full node allows the user to trace any bitcoins that he is receiving all the way back to when they were first mined. This happens nearly instantly. Once the transaction is signed with a modest transaction fee, final settlement (the transfer of custody over the bitcoins) occurs in minutes (although your time depends on how many confirmations you want before you're comfortable).

Bitcoin was the first mover in the space, but that's not the reason it dominates its industry. It is by far the most secure in its ability to provide final settlement and maintain its monetary properties. Altcoin competitors are often centralized and at best only offer a small fraction of the security provided by Bitcoin's network of nodes and proof of work. It is the most liquid out of all the cryptocurrencies and will continue to gain in liquidity and market share as its competitors of all kinds approach values of zero. So-called stablecoins pegged to the dollar don't solve any of the problems that Bitcoin sets out to and will be absorbed by Bitcoin's dominance just like all the others.

1. Bitcoin came into a banking world that was dilapidated and anachronistic. But banks and processors felt the heat and adapted in an unusually quick period of time. Now we have peer-to-peer payment systems working within the regular banking systems. We have Venmo, Zelle, Apple, and Google, and many other systems, and, for all their limitations, they are getting better by the day. For that matter, the Fed itself has announced its own plans for a blockchain-like P2P payment system. Competition works. Bitcoin made a major contribution to lighting a fire under the mainstream industry. But that innovation necessarily affects Bitcoin's prospects.

Services like Venmo, Zelle, etc. may be nice because they add a layer for transferring money that is fast and cheap, but they are still controlled by gatekeepers who are at the mercy of the governments that operate where they are located. They offer no censorship resistance and do nothing to harden the money they're built on top of.

Let the Fed make their own "blockchain-like P2P" payment system. I am astonished that Tucker found it at all interesting to mention them as competition against Bitcoin.

1. Let's just say – as many industry experts say to me in private – that the days of endless price increases of Bitcoin are over, and that it settles into a stable price and even gradually falls to 2014 or 2013 levels. That is not beyond the realm of possibility. Nothing about markets are perfectly predictable, and there is nothing baked into the nature of Bitcoin that guarantees any particular future. A major problem hits the essence of money itself: the use case is everything and adoption is the path toward making any money mainstream. The trends here do not look brilliant for Bitcoin.

Ah, the "experts" are saying that Bitcoin won't see increases in price against the dollar. And while Tucker correctly points out that markets are not perfectly predictable, economics tell us that the hardest money wins. Can events happen in the future that prevent Bitcoin from fully monetizing? Of course, they can, but nothing Tucker has said in his article has convinced me to step back from my bullishness.

Tucker ends the piece by taking an agnostic stance on the future of money although he seems fairly confident that Bitcoin will flourish in the immediate future "to service a special type of need." He leaves the possibility for anything to happen, from Bitcoin going "to the moon" to "something else entirely—an Amazon coin, for example." He just wants people to have some humility in the process.

Humility is a good trait to have, but let's not mistake a bearish outlook on Bitcoin because of ignorance as humility. Tucker's suggestion of a completely centralized "Amazon coin" demonstrates his failure to understand the ultimate purpose of Bitcoin. The sun may not rise tomorrow. Am I being humble for not being so sure that it will? Obviously, the future of Bitcoin is harder to predict than the rising and setting of the sun, but you should see the point of my hyperbole. Bitcoin is on its path and it doesn't care what either Jeffrey Tucker or I say about it. But Bitcoin is not cold and vengeful. It's chugging along, happy to welcome anyone, no matter who they are, to its network. I look forward to the day when Jeffrey Tucker welcomes Bitcoin back.

Cryptocurrency Is Most Useful for Breaking Laws and Social Constructs

By Jill Carlson

Posted December 10, 2019

This post is part of CoinDesk's 2019 Year in Review, a collection of 100 op-eds, interviews and takes on the state of blockchain and the world.

***Jill Carlson** is co-founder of the Open Money Initiative, a non-profit research organization working to guarantee the right to a free and open financial system, and co-host of the What Grinds My Gears podcast. She also works as an advisor and consultant for startups including Algorand, Risk Labs, dYdX, CoinList, and Tezos.*

Why hasn't cryptocurrency gone mainstream?

"It doesn't scale."

"It's slow."

"It's expensive."

"It's volatile."

"It's hard to use."

Or maybe it was never supposed to go mainstream.

This is not to say cryptocurrency is any less important, meaningful, or useful. Rather, I think perhaps we have been judging cryptocurrencies' success (or lack thereof) according to a false metric. We would not judge a fish by its ability to climb a tree.

By design, cryptocurrency does not solve mainstream problems.

Scale, speed, and cost are all examples of mainstream problems within finance, from main street to Wall Street. Credit card networks go down. Stock trades take days to clear. Wire transfers are expensive. In some situations, cryptocurrencies may offer marginal improvements on any of these issues, but more often blockchain-based systems will fail when compared to more conventional, centralized solutions.

This does not represent a design flaw. In fact, this is an intentional trade off. Decentralized systems forsake scale, speed, and cost in favor of one key

feature: censorship resistance. Cryptocurrency solves problems faced by the censored who, by definition, are not the mainstream.

In particular, cryptocurrency enables individuals and organizations to make censored transactions. Procuring drugs on the internet. That's an example of a censored transaction. Buying US dollars in Argentina is another example. Paying a sex worker. Sending money to a friend in Iran. Making an online purchase as an unbanked individual. Selling cannabis as a dispensary. Getting money out of Venezuela. Supporting dissidents in Hong Kong. The primary utility of cryptocurrency lies in engaging in financial activity that is otherwise suppressed or prohibited.

This is the stated intent of cryptocurrency. Satoshi Nakamoto, the creator of bitcoin, described cryptocurrency as a tool of freedom. He compared it to other peer to peer networks like Tor which are similarly resilient to censorship. If we look at the anecdotal evidence, we can see that this is indeed how bitcoin is being used from China to Palestine. Furthermore, what little quantitative data we have also suggests that cryptocurrency use is higher in countries with financial restrictions. These results line up with predictions around cryptocurrency adoption that have existed for years. It is time to face this potentially uncomfortable reality: cryptocurrency is most useful when breaking laws and social constructs.

I, FOR ONE, DO NOT WANT TO LIVE IN A WORLD WHERE CRYPTOCURRENCY HAS FOUND MAINSTREAM USE.

There exists a long history of censorship resistant and privacy preserving technologies: Signal for messaging, Bittorrent for file-sharing, Tor for web browsing. Like bitcoin, these tools are not built for the mainstream. Most people would rather use faster, slicker, glossier centralized alternatives like Facebook Message, Dropbox, and Google Chrome. But for censored people and organizations, decentralized technologies have always provided an escape hatch. For as long as they have existed, these tools have brought with them a certain level of societal discomfort. This discomfort stems not from these platforms being lawless domains – regulations exist on the dark web as much as they do in any jurisdiction – but rather from the difficulty these platforms present in enforcing these government policies and social norms. These technologies render censored activities more difficult to stop.

Decentralized technologies can be used for good, for evil, and for everything in between. From Hammurabi's Code through to the Patriot Act, the morality of laws has been a matter of debate for as long as they have existed. The laws of one jurisdiction are often deemed unethical and unacceptable by its citizens and those of other geographies. To say that cryptocurrency is used primarily to engage in illegal or socially unacceptable activities is not a

normative statement. It is used by freedom fighters and terrorists, by journalists and dissidents, by scammers and black market dealers, by revolutionaries and government officials. It is used by civilians to break unjust laws and escape humanitarian crisis, and it is used by the policymakers who write those very same laws. And of course, the same statements can all be made regarding the original decentralized payment system: cash.

As an industry, we spend a lot of time considering how to drive mainstream adoption of cryptocurrency. I, for one, do not want to live in a world where cryptocurrency has found mainstream use. For if it has, that world is a very scary place indeed.

This is not to discourage or devalue any of the work that is being done to improve decentralized technologies. Many projects in the industry are working toward optimizing away shortcomings in the technology. Layer 2 protocols promise to speed things up. New consensus mechanisms and forms of sybil resistance expect to improve scalability and reduce infrastructure costs. A myriad of applications are building more user-friendly wallets, on-ramps, exchanges, and other tools. All of these developments are important but they may never result in mass adoption. Improvements in scalability, speed, cost, volatility, and user experience may, however, make the critical difference for those who are users, no matter how fringe: the young woman in Venezuela surviving on bitcoin or the Chinese businessman using Tether for cross-border trade.

To judge cryptocurrency based on mainstream adoption is to judge it on a metric it was never designed to achieve.

Bitcoin Energy-Value Equivalence

The Intrinsic Value of Bitcoin as Determined by Energy Spent

By Charles Edwards

Posted December 13, 2019

Take-aways

- Energy, raw Joules alone, can be used to estimate Bitcoin's fair value
- Increased energy input increases the fair value of a Bitcoin (and vice versa for decreases)
- Bitcoin's price is mean reverting to its Energy Value
- The Energy Value model states that if all miners were to stop mining Bitcoin tomorrow, the power input would be zero and Bitcoin would be worthless
- The Energy Value formula says that Bitcoin has a fair value of approximately $11,500 today (12 December 2019), 50% higher than the current trading price.

Bitcoin Energy-Value Equivalence

In Bitcoin's Production Cost we observed the relationship between Bitcoin's Price and Bitcoin Mining expenditure. Variations in Bitcoin's Production Cost were found to be primarily driven by the level of electrical energy input and energy efficiency of mining hardware, with many other factors assumed constant.

This begs the question:

Can the fundamental value of Bitcoin be accounted for by raw energy alone?

A Fair Value for Bitcoin

The hypothesis:

Bitcoin's fair value is a function of energy input, supply growth rate and a constant representing the fiat dollar value of energy.

These variables can be combined into the following equation, termed Bitcoin's Energy Value (V):

$$\mathbf{V} = \frac{\boldsymbol{Energy\ Input}}{\boldsymbol{Supply\ Growth\ Rate}} \times \boldsymbol{f}$$

The Energy Value Formula

Where:

- **Energy Input** (unit: Watts) = Hash Rate (GH/s) * Mining Energy Efficiency (J/GH)
- **Supply Growth Rate** (unit: s-1) = Annual increase in circulating Bitcoins, equivalent to the inverse of Stock-to-Flow. Calculated as the annual rate (unit: year-1) of change in circulating Bitcoins and then converted to seconds
- **Fiat Factor** ($USD/Joule) = A constant conversion factor to allow for the fiat USD value of energy

As all units of hash rate and supply rate cancel out, this equation suggests that **the fair value of Bitcoin (V) can be represented as a function of the Joules of energy spent to produce it:**

$$\mathbf{V} = \boldsymbol{Joules\ In} \times (\mathbf{2} \times \mathbf{10^{-15}})$$

The Energy Value Formula: Bitcoin's fair value is a function of Joules

Building Bitcoin's Energy Value

To test the theory all input data, except for mining Energy Efficiency, was sourced from Blockchain.info.

The challenging piece of the puzzle is obtaining a good estimate for Bitcoin's Energy Efficiency through time.

Estimating Bitcoin Mining Energy Efficiency (J/GH)

The power required to fuel Bitcoin mining is driven by two parts, the hash rate to solve the SHA-256 algorithm and the energy efficiency of the mining hardware itself. In its early years, Bitcoin was mined on very electrically inefficient CPUs and GPUs.

The current era ASICs have energy efficiencies over 100,000 times greater than the average Bitcoin mining hardware of 2009. This means that a higher relative portion of the average miner's electrical bill today is efficiently converted into hashing power.

To estimate a historic profile of Bitcoin mining hardware Energy Efficiency, the efficiency rates for 150 Bitcoin hardware models from Cambridge (ASICs only), BitcoinWiki (FPGAs) and Bitcoin.it (ASICs, CPUs and GPUs) were collated. All ASICs, FPGAs and Intel, AMD and Nvidia hardware were considered where Energy Efficiency (J/GH) was provided and where an estimated hardware release date was found. Common models were grouped and the average energy efficiency for that model calculated on an equal weight basis.

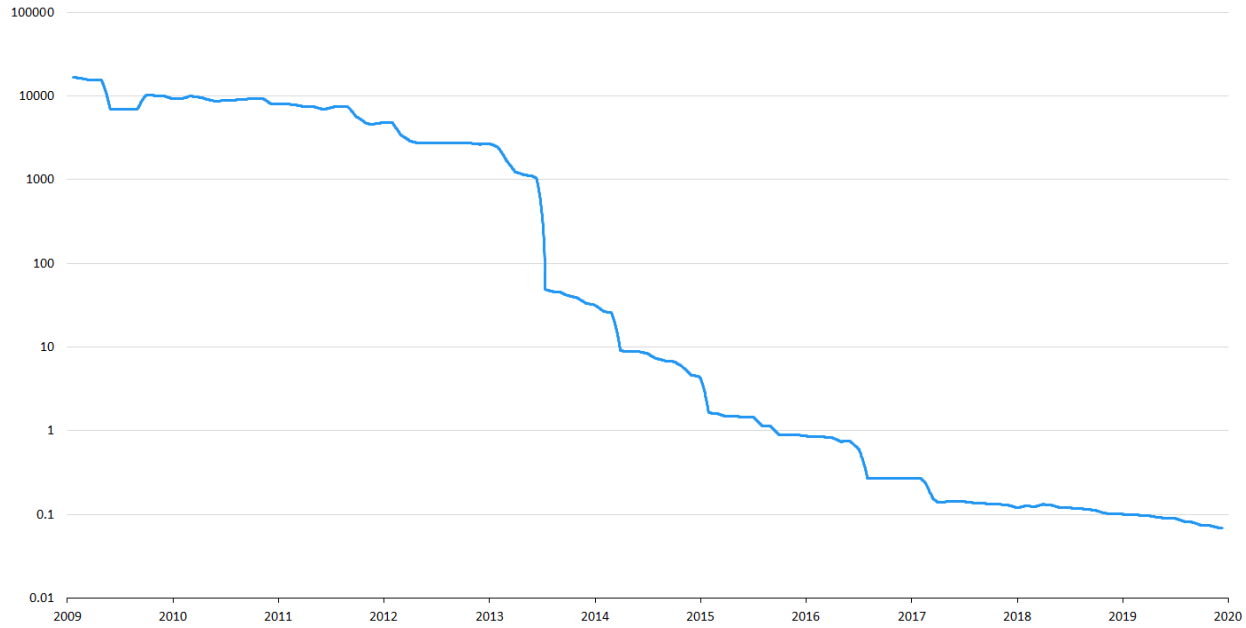
The daily energy efficiency of the Bitcoin network was then calculated as the equally weighted average of all hardware which was within 2 years of its release for CPUs/GPUs/FPGAs and within 1.5 years of its release for ASICs. This difference in depreciable lifespan was chosen because:

- The hardware within model groups for CPUs and GPUs generally span several years
- Bitcoin mining was generally less competitive in its early years
- Other research also suggests a 1.5 year depreciation lifespan is typical for ASICs in more recent years

Finally, a 1 month moving average of Energy Efficiency was calculated to allow for the phase-in and phase-out of model types.

In reality, some hardware models had wider usage and some longer lifespans. However, at risk of increasing the historical error in the Energy Value model and in attempt to produce an unbiased outcome, no other hardware exclusion logic, data cleansing or data manipulation was conducted.

The above process yields the following Bitcoin energy efficiency profile (Joules / Giga Hash) over time.



The S-curve of increasing Bitcoin Energy Efficiency (represented by a falling J/GH over time). Note the sharp increase in efficiency from the introduction of ASICs through 2013 and 2014.

Fiat Factor Constant ($/J)

The Fiat Factor is a necessary constant to convert the units of energy input (Joules) to fiat currency US Dollars. It is simply a representation of how much "we" value energy.

Based on the Energy Efficiency profile above, the resulting Fiat Factor is:

2.0E-15

The Fiat Factor value is dependent on the accuracy of the Energy Efficiency profile and therefore the value provided here should be considered a close estimate. In the long term, a declining US Dollar, hyperinflation or fiat currency collapse would result in the Fiat Factor increasing in a 1-for-1 relative manner.

The Result

Plotting the result shows a visually strong fit for the Bitcoin Energy Value to historic price.

10 Years of Bitcoin's Energy Value

The plunge in Bitcoin's energy value in 2013/14 is largely driven by the transition from GPU/FPGA to ASIC hardware. While it is likely there was a substantial drop during this period, it may be somewhat exaggerated here due to the hardware usage and depreciation model assumptions outlined above.

Market Forces — Bridging Supply and Demand

The first question is, does a Bitcoin Energy Value make logical sense?

In "Modeling Bitcoin's Value with Scarcity", Plan B found a strong relationship between market price and the scarcity of Bitcoin and other hard assets. We can posit that this represents the fundamental relationship of human "demand" for hard, value preserving assets over time.

But there's a catch.

Not all scarce assets have nor preserve wide-spread market value. For example, there are approximately 3,000 cryptocurrencies with market caps under $500. Many of these coins have "constrained" supply models, but they have been assessed by the market as having no fundamental value. Scarce, but not valuable. The same can be said for bad art, bananas stuck to walls and many other rare and unique throw-away assets. This makes sense, as scarce assets which are easy to acquire or replicate typically have low market value.

Consistent, high levels of human effort are generally linked with demand.

When Energy is dedicated to a task, the supplier of energy (the worker) expects there to be a demand for their effort. When a supplier sees growing

demand for the fruits of their labour, they will work harder in attempt to reap greater benefits. Others will likely also contribute to capture some reward. However, should demand for a supplier's labour fall, or should the opportunity decline to a point at which they can achieve a better return elsewhere, the supplier will likely cease committing energy to that task.

This is exactly how the war for Bitcoin's hash rate has been fought, and this is the argument for Bitcoin's Energy Value.

Consistent energy input represents a balance between supply and demand. Rising market prices incentivize increased energy input via hash power growth and technology improvements which result in greater energy efficiencies. For this reason, great increases in market price typically result in long-term increases in committed energy and therefore increases in Bitcoin's Energy Value. However, when speculation causes skyrocketing prices, without a corresponding increase in energy input, price has historically collapsed back to the Energy Value.

It is mean reverting phenomenon. As would be expected with any intrinsic value estimate driven from fundamentals.

Bitcoin's price and Energy Value tend towards each other, they are like magnets. While deviations between the two can and do exist, they have always closed. **Despite being mathematically independent to Bitcoin's trading price and volume, Energy Value is connected by the invisible hand of the market.**

By capturing long-term demand for scarce assets based on supply growth rate (stock-to-flow) and energy input, Energy Value represents the symbiotic relationship between Bitcoin supply and demand.

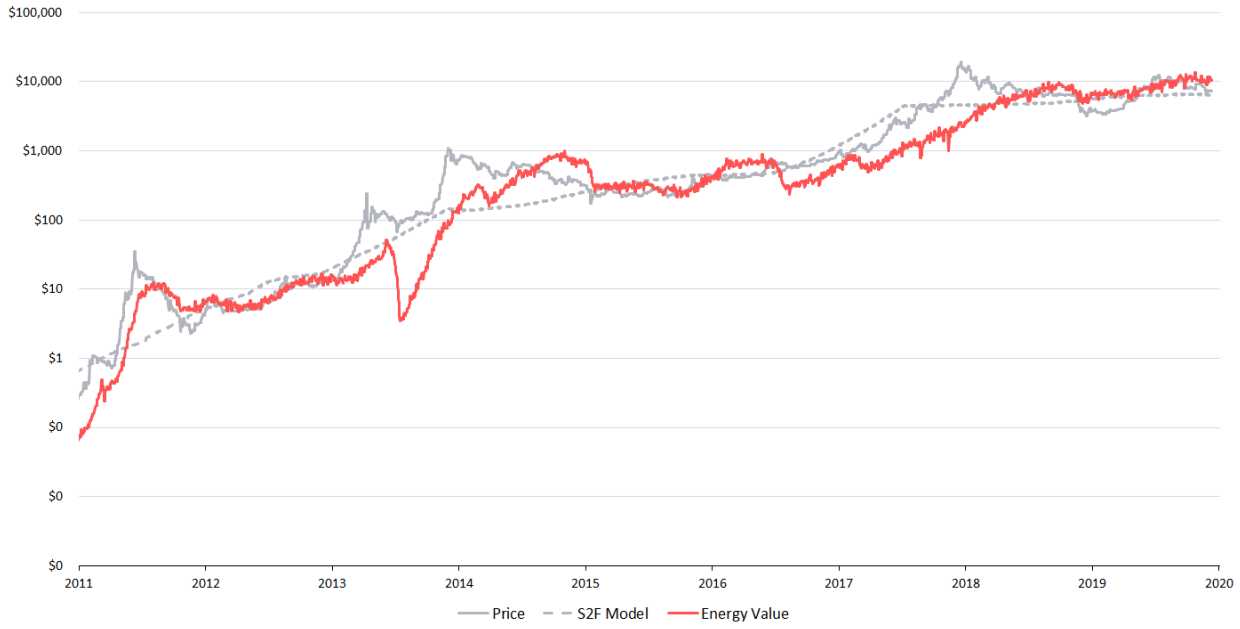
Performance

On daily data from January 2010, the Energy Value formula has a R2 to the actual Bitcoin price of 80% (the higher the R2, the better the model fits reality). By comparison, the stock-to-flow model has a R2 of 88% on the same data. While 8% less than the stock-to-flow model, there are a few things to consider:

- **Bitcoin's Energy Value is highly dependent on the estimated Energy Efficiency.** For this analysis, 150 Bitcoin hardware details were manually collated, there is possibility of data or omission error. The depreciation periods are approximations of reality. Efficiency can also vary depending on operating conditions and overclocking. It is not possible to get a perfect representation of what hardware every Bitcoin miner is using at every point in time through history. Hence, some error here is expected.

- **If all Bitcoin miners were to suddenly cease mining Bitcoin, stock-to-flow would predict a Bitcoin price of infinity. The Energy Value predicts zero.** Should all miners abandon Bitcoin — which could occur via a catastrophic event (such as the breaking of the SHA-256 algorithm), through the creation of a "better" money / store of wealth — no new blocks would be created, no transactions would be sent and the network would be defunct. Under such a circumstance, the stock-to-flow model alone ($0.4*SF^3$) would assess Bitcoin as having infinite value. The Energy Value model states that if all miners were to stop mining Bitcoin tomorrow, the power input would be zero and Bitcoin would be worthless.
- **The stock-to-flow model is a fitted power law**. Bitcoin's price has had exponential performance and the stock-to-flow model's power law was chosen specifically to match this. By optimising the parameters, a good accuracy is achieved to fit Bitcoins price. The Energy Value has no curve fitting parameters, just one fixed constant to allow for the conversion of pure energy to dollars. In fact, it is likely that the exponential increase in mining hardware power efficiency coupled with the growth in hash rates explains the stock-to-flow's exponential relationship.

With consideration of the above, an 80% R2 is considered a strong result for the Energy Value.



Bitcoin's Energy Value and Stock-to-Flow

Speculation

From the above figure we can see that turning points and wide gaps between Bitcoin's price and the fair value can signify great times to buy and sell Bitcoin.

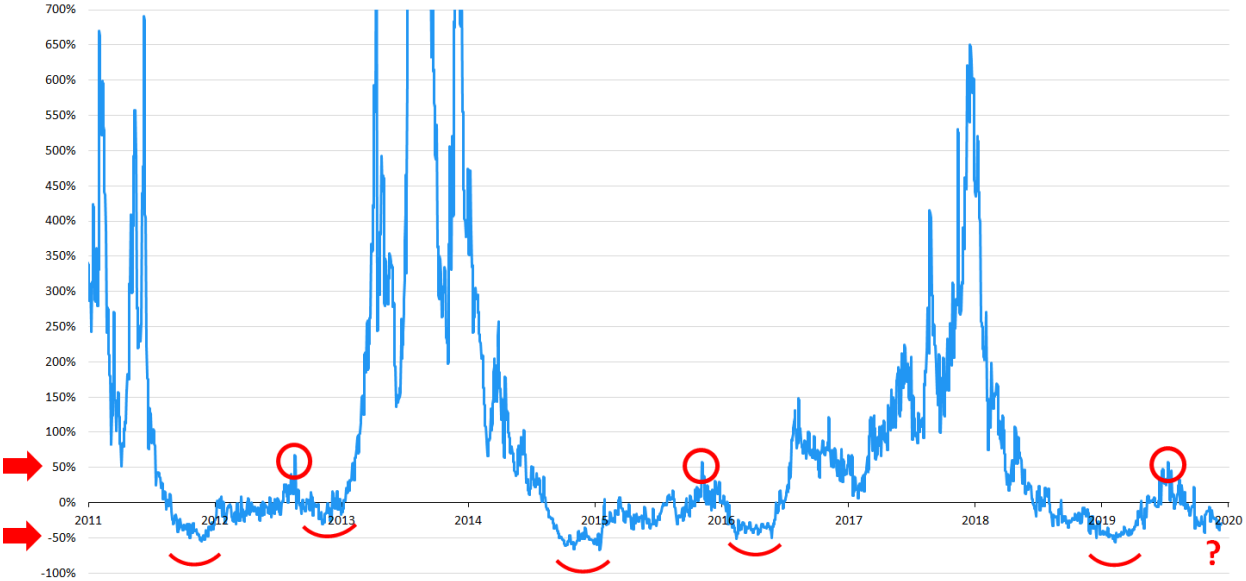
Sharp declines in energy input often signify good times to exit the market and strong energy input growth has represented great times to buy

The Energy Value formula says that Bitcoin has a fair value of approximately $11,500 today (12 December 2019), 50% higher than the current trading price.

This suggests Bitcoin has a great risk-reward in early December 2019. A positive picture is also presented when looking at the below Energy Value Oscillator.

However, energy input can fall at any time.

Historically buying into falling hash rates has been inadvisable, far better risk-reward outcomes are achieved on hash rate recovery.



Energy Value Oscillator Price as a Percentage of Energy Value. 2019 looks very similar to prior bull run starting characteristics.

Implications

By considering energy and supply growth, we have found an intrinsic link between Bitcoin's price and its value.

The value of Bitcoin is a function of its energy input in Joules.

Following are some of the implications of the Energy Value formula:

- The health of the mining network is intrinsically linked to Bitcoin's value
- Increases in electrical energy input will increase the fundamental value of Bitcoin (and vice versa for decreases)
- Higher hash rates (with unchanged energy efficiency) mean each Bitcoin is worth more
- Major improvements in hashing technology (such as the introduction in ASICs) cause considerable volatility in the short-term intrinsic value of Bitcoin due to significant increases in energy efficiency which are not compensated for by equal increases in hash rate growth
- Should quantum computing (or other major technological advancement) require less total network energy to solve the SHA-256 algorithm, the Energy Value formula says Bitcoin's intrinsic value will fall
- A change to the Bitcoin code which increases Bitcoin's supply growth rate would decrease the fundamental value of each circulating coin
- In 2140, if Bitcoin is still being hashed, its supply growth rate will be zero. The Energy Value formula, like stock-to-flow, predicts an infinite value for Bitcoin (in USD terms) at that point. However, unlike stock-to-flow, this hinges on the criteria that mining activity is ongoing

If Bitcoin is successfully mass adopted as a store of wealth and/or global currency we may have financial market evidence that value is intrinsically linked to effort, the Joules of energy spent in work.

As humans, our time is limited — it's our most valuable resource. What we choose to put our energy into, and therefore our time into, is our most valuable choice.

Bitcoin values energy.

Just as mass can be represented by energy, so can Bitcoin's Price.

---

*All data and calculations behind this article is freely available to support validation & potential refinement **here**.*

*Chinese Translation: **https://my.first.vip/shareNews?id=2605&uid=5066***

Bitcoin's Production Cost

By Charles Edwards

Posted December 13, 2019

An Estimate of Bitcoin's Production and Electrical Cost — a Historic Floor in Bitcoin's Price.

Takeaways

- **Bitcoin's electricity consumption can be used to estimate Bitcoin's Production Cost**
- **Bitcoin's Production Cost can be used to estimate Miner profitability**
- **Bitcoin Mining has historically been a very profitable business**
- **2019 has been the worst year for Bitcoin Miners in all of the last 5 years**
- **Bitcoin Miners are currently taking on losses from the 4th quarter price drop**
- **The Bitcoin Electrical Cost has been a concrete price floor in the Bitcoin market price**
- **A pessimistic price floor for mid-2020 is estimated at $8,000**
- **However, miner influence on supply and demand is dropping, with Bitcoin's inflation rate at 3.8% and falling**

This article links Bitcoin's electrical consumption to the cost of Bitcoin production. In doing so we gain insight into the historical profitability of Bitcoin mining and an indication to when Bitcoin mining businesses are struggling. Over the last 5 years, Bitcoin's Electrical Cost has

been a floor in Bitcoin's exchange traded market price, proving Satoshi's theory that price gravitates to the cost of production.

Commodity Prices and Production Costs

The relationship between Bitcoin miner production costs and the price of Bitcoin is summarised best by no other than Satoshi himself:

"The price of any commodity tends to gravitate toward the production cost. If the price is below cost, then production slows down. If the price is above cost, profit can be made by generating and selling more. At the same time, the increased production would increase the difficulty, pushing the cost of generating towards the price.

In later years, when new coin generation is a small percentage of the existing supply, market price will dictate the cost of production more than the other way around."

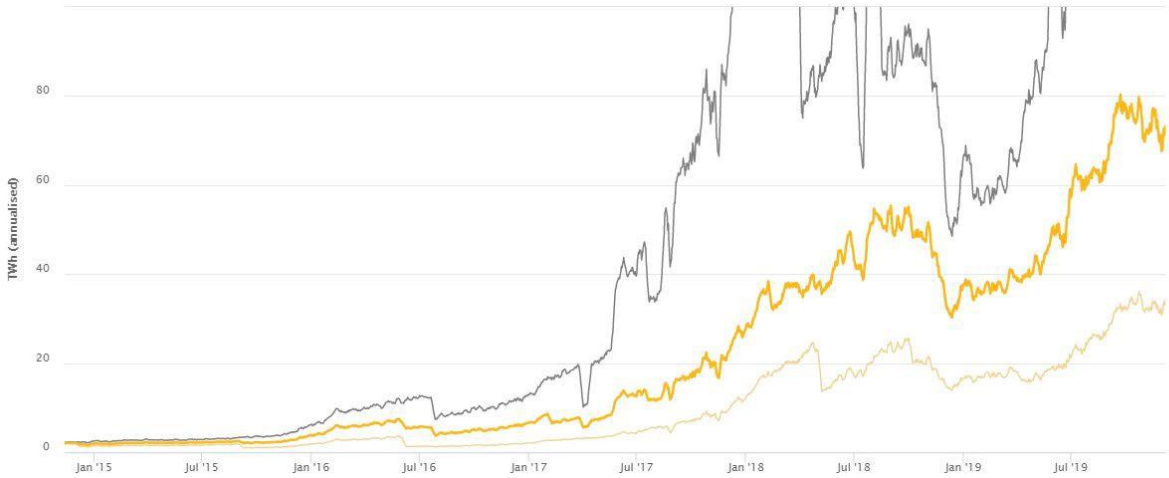
- *Satoshi Nakomoto, 2010*

Knowing this relationship and drawing on detailed investigations into the electrical consumption of Bitcoin, we can estimate the cost of mining Bitcoin.

The Cambridge Bitcoin Electricity Consumption Index (CBECI)

In 2019, Cambridge University published a detailed study estimating Bitcoin's energy consumption from November 2014 to present.

This study is likely the most detailed bottom-up calculation of Bitcoin's global electricity consumption to date.



Cambridge Bitcoin Electricity Consumption Index (Dec 2019)

Cambridge estimates Bitcoin's electrical usage based on the assumption that miners will run the mining hardware as long as it remains profitable in electricity terms. Other key assumptions behind their calculations include:

1. **The global average Bitcoin miner electricity price is $0.05 USD per kWh.** Based on interviews with miners globally and consistent with other research, including CoinShares
2. **The energy efficiency of over 60 mining hardware models since 2014.** Per manufacturer specifications and refined based on expert advice (to account for actual usage and overclocking)
3. **The global average Power Usage Effectiveness (PUE) of Bitcoin Miners is 1.1**. PUE is a measure of the total energy required to operate mining facilities (including cooling) relative to the energy required for server operation. Cambridge came to this figure based on interviews with miners globally. It is also in-line with Google's average PUE of 1.11

Cambridge's calculation assumes an equally weighted basket of *profitable* mining equipment which is perhaps the most thorough approach to assessing mining hardware utilisation, depreciation and therefore energy consumption globally today.

All references to Bitcoin's electrical consumption in this article refer to Cambridge's "Best-guess" estimate of Bitcoin's electricity consumption.

Bitcoin's Production Cost

Bitcoin's Production Cost is an estimate of the global average US dollar cost of producing one Bitcoin per day.

Every study into Bitcoin's mining costs to date has found electricity to be the primary cost of operations, and it is used here as a base from which to estimate the Bitcoin Production Cost.

From Cambridge's electricity consumption, Bitcoin's Production Cost can be estimated by:

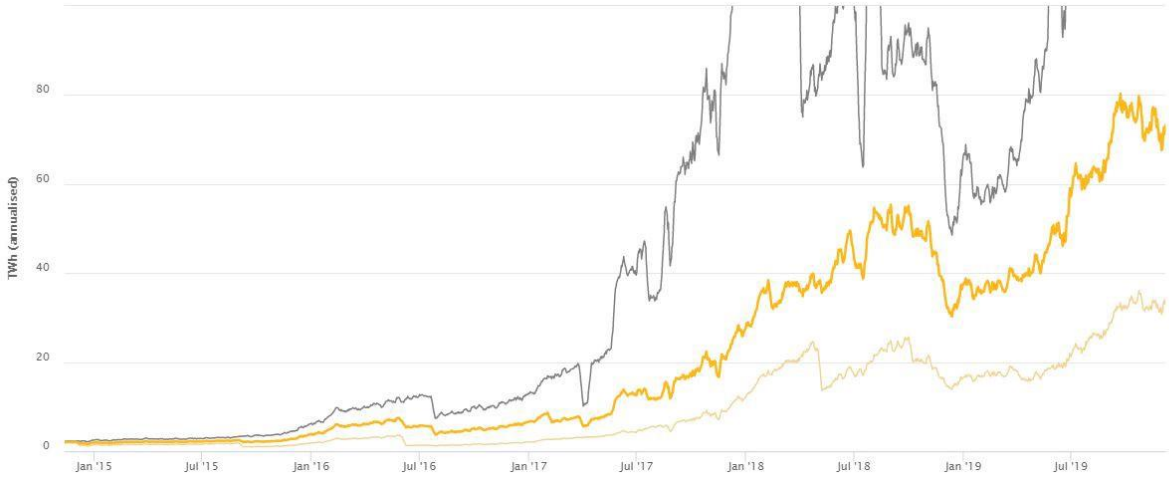
1. Calculating number of Bitcoin Mined Per Day (based on Bitcoin's Block Reward and block frequency)
2. Calculating the Bitcoin Electrical Cost = daily electricity cost to mine a Bitcoin
3. Estimating the global average "Elec-to-Total Cost Ratio" = (Bitcoin Electrical Cost) / (Daily Cost of running a Bitcoin Mining Business)

Bitcoin Production Cost is then found as (Daily Electrical Cost) / (Elec-to-Total Cost Ratio)

From Cambridge's data one additional assumption is required — an estimate of the global average Bitcoin mining **Elec-to-Total Cost Ratio** (Item 3 above).While electricity is the major factor in Bitcoin mining operations, other costs in operating a Bitcoin mining business include:

- Hardware Capital Expenditure
- Bandwidth
- Wages
- Rent
- Insurance
- Cost of Capital

Varying estimates have been made for the Elec-to-Total Cost Ratio and include:



Estimates of Bitcoin's Electrical Cost to Total Mining Cost

Well-funded businesses in a low-cost country such as China likely have low and negligible wages, rent, insurance and capital costs relative to the total cost of mining. China, for example, accounts for approximately 60% of Global Bitcoin mining in 2019.

Based on the research available to date and noting that a number of the above estimates appear not to consider the general costs of business (rent, wages, etc) outside of electrical operating expenditure (OPEX) and hardware capital expenditure (CAPEX), **the Elec-to-Total Cost ratio is estimated here as 60%.**

Using Cambridge's electricity data, this gives 5 years of the Bitcoin Production Cost.

Bitcoin Production Cost

Bitcoin Miner Price

While it is interesting to compare Bitcoin's price to the Bitcoin Production Cost, as each coin mined can be sold at the prevailing market price, this approach misses on another piece of miner revenue — transaction fees.

As well as each block reward's freshly mined bitcoins, miners also receive transaction fees in each block. Transaction fees are determined by senders based on supply and demand. Additionally, with time transaction fees will represent a greater portion of miner revenue as block rewards reduce with each halving.

As a result, the Bitcoin Production Cost should be compared to the revenue one Bitcoin provides (Bitcoin's market price) *and* the transaction fee revenue.

We term this the Bitcoin Miner Price and it is calculated here as the Bitcoin Price + (Daily Transaction Fees) / (Daily Bitcoin's mined).

The Bitcoin Miner Price varies with demand for on-chain transactions

Putting Bitcoin's Production Cost and Miner Prices together, we can see when **Bitcoin Miners are struggling in recent times and potentially taking on short-term loses.**

Bitcoin Production Cost versus Bitcoin Miner Price

Bitcoin Electrical Cost — A Bitcoin Price Floor

Bitcoin Production Cost provides insight into the profitability of Bitcoin mining businesses. Price drops below the Bitcoin Production Cost tend to be short lived. This makes sense as high-cost miners go out of business, the hash rate plateaus and falls and miners in general are less inclined to sell at a loss.

However, the Bitcoin *Electrical* Cost offers a stronger price floor.

Over short periods, a number of miner business costs are "sunk" (e.g. already paid for hardware), contractually locked-in (e.g. rent) or can be deferred (e.g. hardware upgrades). This means that Bitcoin miners can operate at a loss over short periods.

This makes sense provided the Bitcoin Miner Price is above the Bitcoin Electrical Cost. If the cost of running your mining hardware is less than or equal to the revenue it generates, you may as well leave it turned on, until such a point that general business losses make this wasted effort unbearable and the opportunity cost too high. However, this scenario cannot continue indefinitely. Losing miner would not have any revenue left over for re-investment in the business (continual capex is required to keep up with generally growing hash rates), ability to pay rental contracts, wages and other business costs.

Using Cambridge's data from 2014 alone, with no further assumptions, we can see that Bitcoin's price never quite reaches the Electrical cost to produce a Bitcoin, despite coming very close in November 2018.

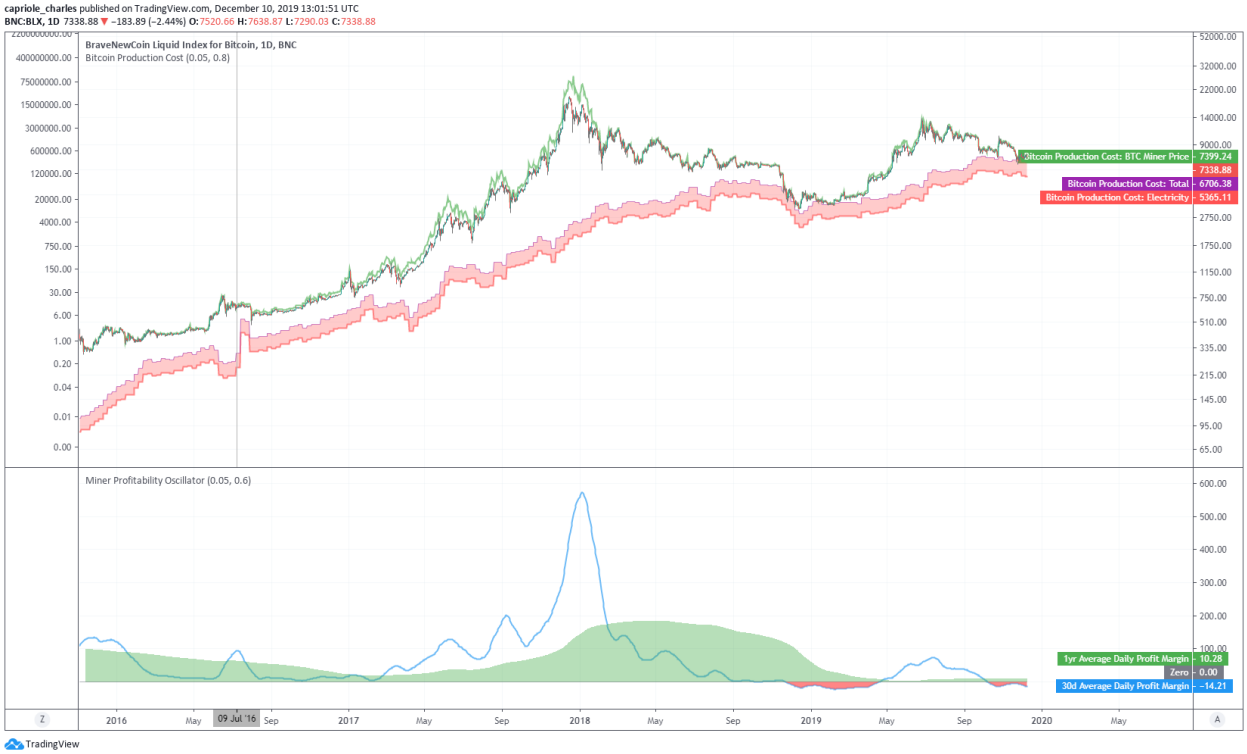
Historically, the electrical cost to produce a Bitcoin has represented a price floor in the Bitcoin market price.

In more recent years, the introduction of Bitcoin Futures has also potentially allowed Bitcoin Miners to lock in profits earlier, for example, by shorting when the Bitcoin Price is significantly greater than production cost. However, the effectiveness of such strategies is debateable. The introduction of Bitcoin Options in 2019 will also likely aid Bitcoin miners by providing certainty in their cash flows and the ability to effectively lock in a Bitcoin sale price floor.

Miner Profitability Oscillator

All of the above suggests Bitcoin Miners are struggling at present. Most are operating at a business loss in the short term, with an average daily profitability of 10% for 2019.

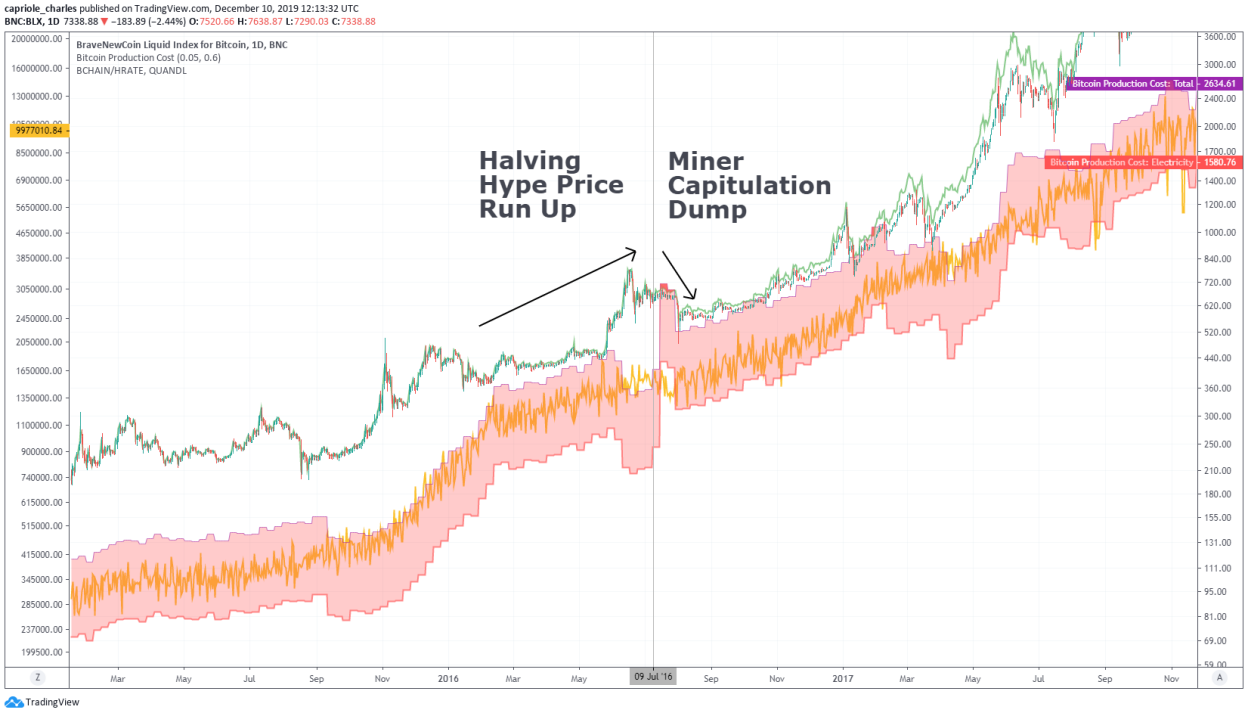
Even if the 60% Elec-to-Total Cost Ratio assumption is off by a wide margin, based on Cambridge's electrical consumption data, **2019 is the least profitable year for Bitcoin Mining in all of the last 5 years.**



Bitcoin Miner Profitability Oscillator *— Bitcoin mining has historically been a very profitable business*

Outlook

It is worth noting that the Bitcoin Production Cost will double at the next Bitcoin halving (currently estimated for May 2020). When the Block Reward halves, the daily cost of Bitcoin Production is spread across half as many Bitcoins.



Bitcoin Production Cost doubling at 2016 Halving. Estimated Production cost increase was tempered by the phase in of the significantly more energy efficiency Antminer S9

From this figure, if Bitcoin's Hash Rate and mining hardware efficiency were to remain unchanged from today, the Bitcoin Production price at Halving would be $17,800.

Although Hash Rates can fluctuate widely, they are historically much more stable than Bitcoin's price. The weekly average Hash Rate has never dropped more than 47% from its peak (in 2011). The second largest drop was 37% in December 2018.

The second most varying input into Bitcoins Electrical Price is mining hardware efficiency, which has historically improved every year.

Even if Hash Rates were to drop 40% below todays levels, and mining hardware efficiency were to improve 25% in the next 6 months, Bitcoin's Electrical Cost would be approximately $8,000. **Suggesting a pessimistic case price floor of for mid-2020 of $8,000. 8% higher than today's Bitcoin price of $7350.**

Limitations to this model also include the reducing share of total Bitcoin supply which miners hold. **Bitcoin's inflation rate, and therefore the relative portion of incremental Bitcoins that miners gain control of each year, is currently 3.8% and decreasing exponentially.** The influence of each new Bitcoin in 2020 onwards will drop significantly with the Halving.

Therefore, as alluded to by Satoshi above, the reliability of the Bitcoin Electrical Cost as a price floor may reduce with time.

***

*Chinese Translation: **https://my.first.vip/shareNews?id=2601&uid=5066***

Bitcoin and the Tyranny of Time Scarcity

By Robert Breedlove

Posted December 19, 2019

The tyranny of time scarcity is ubiquitous in life; here we will explore how mankind cooperates to resist this immortal tyrant using one of our most ancient social technologies, money, and why Bitcoin is bound to achieve global monetary dominance.

A Tyrant of Time Immemorial

All human action inescapably occurs within the bounds of time. As the universally shared element of experience, time is the grand paradox of nature; it heals all wounds, yet ultimately ravages all things. Each of us feels a current of time that is totally impersonal; in a ruthlessly egalitarian manner, time flows equally for rich and poor, sick and healthy, young and old alike. The temporal flows we experience cannot be reproduced, reversed, or stopped. At an intrapersonal level, our allotment of time is as scarce as our lifespan is limited. Interpersonally, time scarcity manifests as the total time we can collectively allocate towards serving one another; whether we are making goods, providing services, or gaining knowledge — we have but a finite quantity of hours to commit towards our efforts. In this sense, time scarcity is the immortal tyrant subjugating all of us mortals. Only through cooperative action can we break free of the restraints time scarcity clasps upon us.

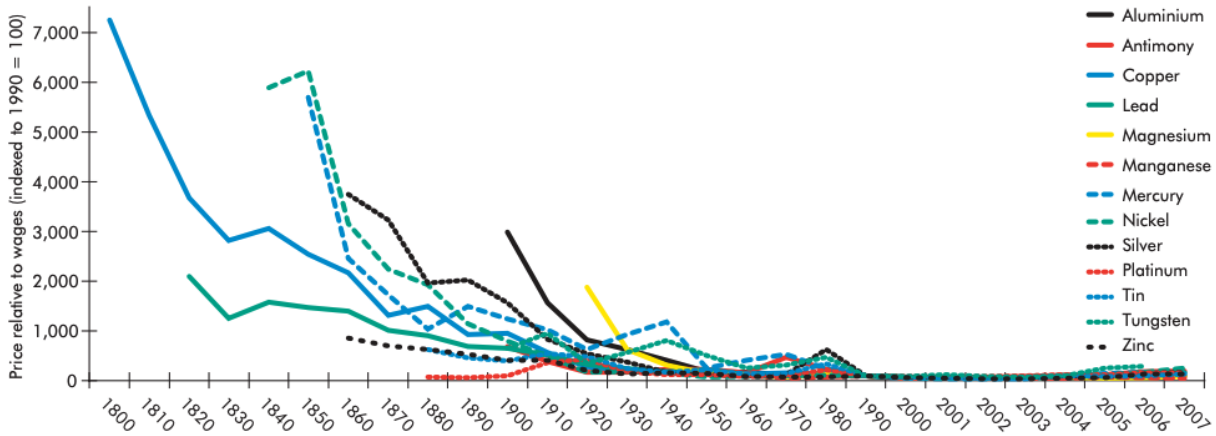
Society is the sum total of cooperative actions taken, a social order that is, paradoxically, shaped by competition among its constituents — free people. Actions intent on improving our relationship with nature, which enhance our quality of life by saving us time, necessarily involve the use of natural resources. If one seeks to dig ditches faster, he will first need to construct a shovel — a tool that requires wood from a felled tree, refined metal ore, and expertly shaped screws to hold the (earth-shattering) device together. Since the Earth we share is physically finite its natural resources are inherently scarce, and we must each compete to earn *our own* fair share. In a world that is as physically abundant as our ingenuity will allow, it is ultimately only our finite time that constrains us from producing more of anything we want.

Existing under the ubiquitous tyranny of time scarcity, it's natural for animals to adopt more energy efficient means of satisfying their wants. The "Law of Conservation of Energy-Mass" is the 1st Law of Thermodynamics; an inviolable

principle of the universe that organisms (lazily and cleverly) follow to the letter. Predators in the wild frequently make expected-value calculations when deciding whether or not the anticipated energy expenditure in pursuit of a particular prey is worth the caloric value of the meal, should the hunt be successful (most hunts have low chances of success). Even herbivores like koala bears economize their physical movements to maximize their consumption of eucalyptus leaves per exertion. Of course, these decisions are not (likely) based on any mathematical knowledge, but rather on instinct.

Similarly, driven by an instinct to overcome the oppression of time scarcity, us humans have always found ways to uncover and extract ever-more natural resources as we "hunt" for satisfactions to our wants. We have literally "just scratched the surface," as our efforts haven't even taken us halfway into the Earth's crust, its thinnest and outermost layer. Through generations of trial and error, with our collective learnings accumulated in heuristics, written knowledge, and methodologies, mankind has steadily economized his productive efforts, gradually making more and more use of his time. The fruits of our labor are evident: the price of all natural resources, in terms of time necessary to produce them, has steadily decreased over the long-run as technological advancements continually increase our productivity — our capacity to produce the greatest results with the least effort. Metal prices over the past two centuries are a testament to this:

Figure 5 **Metal prices relative to wages, U.S., 1800–2007**



Sources: (1) Data for 1800–1990 are from Moore (1995). (2) Price data from 1990–2007 are from various issues of USGS, *Mineral Commodities Summaries and Minerals Year Books*, available at http://minerals.usgs.gov/minerals/pubs/commodity/, visited on July 7, 2008. (3) Wage data for 1990–2007 are from Bureau of Labor Statistics, *Establishment Data: Historical Hours and Earnings*, available at, ftp://ftp.bls.gov/pub/suppl/empsit.ceseeb2.txt, visited June 27, 2008

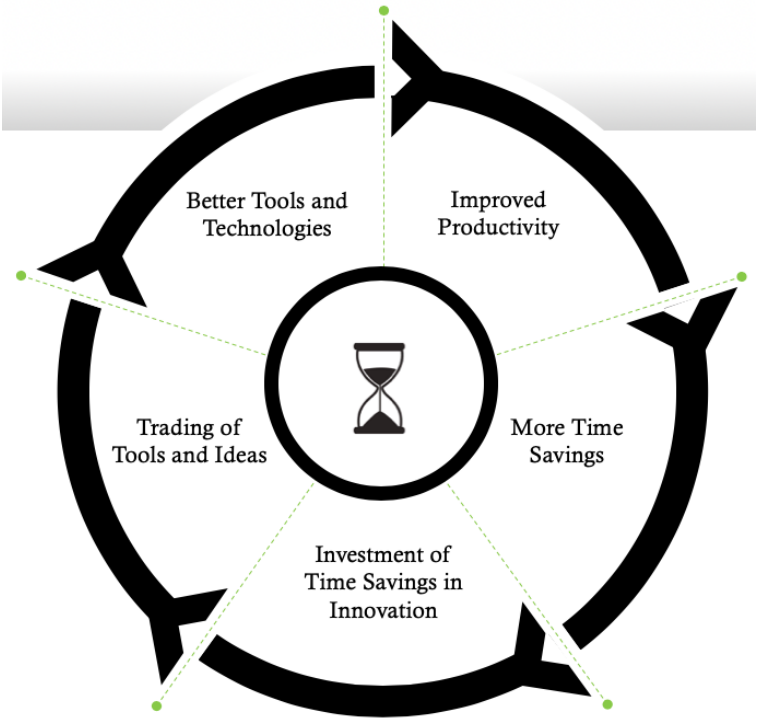
Evincing the simple truth of mankind's ever-rising productivity is gold: as the annual new supply flow of this extremely rare metal remains steady, it makes no sense to consider other natural resources (which are less rare than gold) as

scarce in any practical sense[1] . Indeed, only time scarcity truly constrains our creative output. In this sense, time — both individually and collectively — is our most precious and scarce resource. Each of us seek to extend and savor our time on Earth. As a population, we strive to economize our actions and increase our productivity to attain the greatest results possible with minimal use of time and effort. Indeed, the purpose of the world economy is to accelerate our collective productivity gains through innovation and trade; in a term, to gain energy efficiency — our sole emancipator from the hardships imposed by time scarcity.

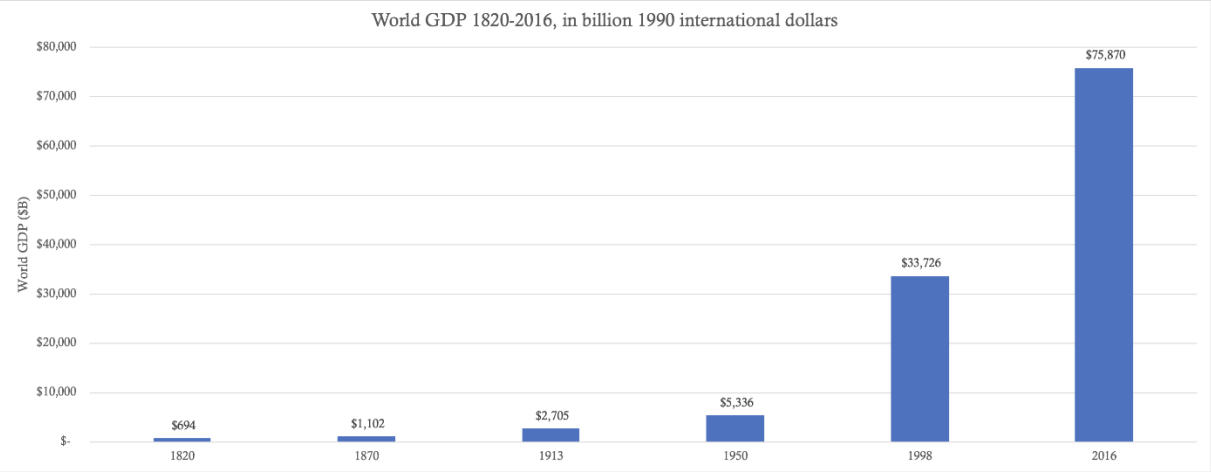
Trade Interconnects Us

Acts of trade (or interpersonal exchange) interconnect us into economic networks which increase our productivity by virtue of our inherent comparative advantages: a diversity of skills, experience, and know-how that arises naturally among us. Trade allows us to focus on our comparative advantages and become ever-more specialized in our skills over time. This positive-sum game undergirds all economic activity; by working as a cooperative ensemble we become more productive than we would be working as isolated individuals. Our economic interdependence makes us collectively more productive and prosperous. This cooperative dynamic is commonly called the “division of labor” and the general purpose of society is to foster an environment which favors its proliferation.

The division of labor enables each of us to concentrate on what we do best and increases our collective productivity: meaning it lets us produce the same amount in less time or a greater amount in the same time. Alternatively, we can choose to use these newfound time savings to innovate. Innovation involves the creation of tools and technologies to help us do even more in less time (i.e. digging with a shovel instead of by hand). As innovative new tools and ideas become diffused into society through trade, more time savings are generated, and this process becomes recursive into a self-reinforcing, virtuous cycle with no known natural limit:



By specializing, trading, and innovating societies create a (literal) wealth of time savings that can be spent productively or leisurely. By spending time savings productively, societies create wealth — the accumulation of time saved in the form of capital. Anything that economizes human action — tools, knowledge, or even relationships — is considered capital, as it provides a way for us to more quickly satisfy our wants. Said simply, as we become more productive, we accumulate more capital — a form of frozen time savings. In this respect, we have come a long way over the past two centuries:



sources: https://theunbrokenwindow.com/Development/MADDISON%20The%20World%20Economy--A%20Millennial.pdf, https://www.multpl.com/world-gdp/table/by-year

Money: Mankind's Masterwork

Money is the most marketable (or readily exchangeable) capital in an economy; it is the most liquid measure of time savings — a social chronometer of sorts. Money is the technology we use to measure and move the value of our time savings across time and space. The primary function of money is to store value, meaning that it must (at a minimum) retain its own exchange value across time. Naturally, as our collective productivity increases, the value of money rises in tandem, and prices expressed in it decline. The secondary function of money is to mediate exchange, meaning that it can be exchanged for anything in the marketplace — goods, services, or knowledge. Money is sought by all seeking to trade their way into satisfying personal wants[3] (this includes everyone that isn't entirely self-sufficient). The tertiary function of money is to quantify exchange ratios, meaning it is used to denominate prices across the minds of market participants. Consider how we think in dollars, or in our local currency, when deciding whether and how much to buy or sell of anything in the marketplace. Interestingly, this "unit of account" function of money is so deeply etched into our mental machinery that it actually changes how we think and perceive the world.

Besides these three functions, monetary technologies generally exhibit the following traits:

1. Scarcity: resistance to money supply manipulations and, thus, dilutions to its monetary unit value (difficult to produce)
2. Divisibility: ease of accounting and transacting at various scales (separable and combinable units)
3. Portability: ease of moving value across space (high value to weight ratio)
4. Durability: ease of moving value across time (resilient to deterioration)
5. Recognizability: ease of identifying and verifying the monetary value by other parties in a transaction (universally identifiable and verifiable)

Whatever good is most impervious to the depredations of time, transference, and greed is naturally selected as “money”. The monetary technology selected freely in a marketplace is referred to as “hard money”; a haven for liquid value (exchangeable time savings) that resists the ravages of time, damages related to transference across space, and intentional misappropriations by those vicious two-legged apes (people). In these respects, monetary metals have been historically superior due to their durability and portability, making them ideal for storing value across time and space, respectively. With the advent of coinage, which standardized each monetary unit, the divisibility and recognizability traits of these metals were greatly enhanced. Critically, the scarcity of monetary metals is governed by natural laws that are beyond the control of man, making their supplies (mostly) resistant to greedy manipulations. Gold became, and remains, the prime monetary metal of the world precisely because of its superior relative scarcity — historically, it has been the best reflector of absolutely scarce time.

Gold is the hardest monetary metal to produce and nearly every ounce ever mined remains part of its extant supply today, as it is chemically an ultra-stable element. Taken in combination, these properties made gold the best medium for storing value across time, as its supply is the most resistant to change, and therefore the most inflation-resistant. By providing

sufficient monetary characteristics (divisibility, portability, durability, recognizability) coupled with superior physical scarcity, gold was naturally selected as money on the free market (hard money). With a (low) reproducibility and physical scarcity most closely aligned with the absolute irreproducibility and scarcity of time, gold has been the most credible store of value historically — which explains why freely acting individuals have hoarded it for centuries. More technically, gold's superior stock-to-flow ratio makes it more resistant to supply inflation (and, its corollary, monetary value dilution) than all other monetary technologies (prior to the invention of Bitcoin).

Game Time

To understand gold's ascent, we must realize the actions of people in free markets are driven by game theory. In game-theoretic terms, a "game" is any situation in which people can win or lose — as is the case in markets. A "strategy" is just process for making decisions. Game theory is applicable in any domain where people must decide whether to cooperate or compete. For instance, if you and I are being chased by a bear, my decision to run or fight is not based on how fast I am, but rather how fast I think you are. Game-theoretically, I only need to be faster than you, not the bear, to ensure my survival. Such assessments of interpersonal dynamics are also closely related to economics and monetary evolution.

In the context of monetary evolution's relationship with time: free market participants choose hard money over all other monetary technologies because its resistance to supply increases most closely reflects the immutable flow of time. No matter how much time was allocated to gold production, its supply resisted inflation more than any other monetary metal, causing people to coalesce around its use as a superiorly sound store of value. In game theory terms, gold production became the "Nash Equilibrium", a game state in which everyone follows the same strategy because there is no advantage to be gained by switching to any other strategy. So long as people sought to maximize their freedom from time scarcity by accumulating capital, collectively produced more than they consumed, and accomplished these goals through trade, gold remained the best proxy for the scarcest economic resource — time.

Unicity of Time and Money

Time is the only irreversible element in existence. Its directionality is imparted by the ever-growing entropy of the universe — as defined by the 2nd Law of Thermodynamics. This "Thermodynamic Arrow of Time" which points us into an increasingly chaotic universe is, in fact, the only irreversible aspect of reality; every other natural process is symmetrical, making it impossible to discern whether an event is unfolding forward or backward in time. As such,

this universally objective and unidirectional flow of time provides our purest reference point for all values (of the seven key metrics maintained by the Systeme Internationale of Units and Measures, six are rooted in the time it takes light to move through a vacuum). Gold, then, as the most difficult commodity to produce no matter how much time was allocated towards its extraction, served as the best market proxy for the objective purity of ever-flowing time. It is commonly said that time is money, but few realize that the reciprocal is also true — money is time.

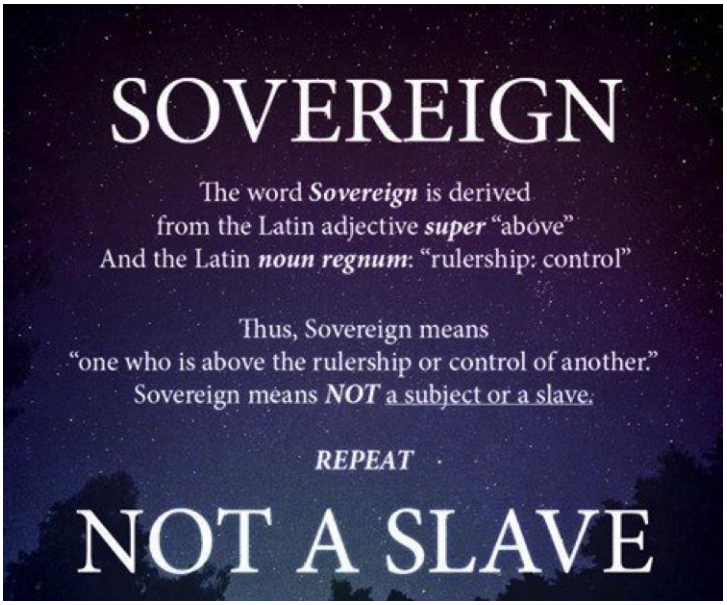
Beyond relative irreproducibility, hard money exhibits other properties akin to the natural flow of time. Markets naturally optimize for a hard money that is as impersonal, irreversible, and unstoppable as the flow of time to which it is anchored, and which it is intended to epitomize in the marketplace. As hard money arises naturally as the result of countless market interactions in which individuals seek to trade their goods for steadily more exchangeable goods, it is inherently beyond the control of any single individual, nation, or central bank. This makes hard money apolitical and impersonal; it cannot be used to benefit any one group over another. In other words, hard money tends to be politically neutral, like time.

Hard money is also equity-based, meaning that physically possessing gold as an asset, for instance, is 100% equity and 0% debt (a bearer asset). This makes payments in gold immune to reversal, unlike those made with

monopolistically imposed debt-based monies, called fiat currencies, which are liable to the whims of bureaucrats, who can choose to confiscate, censor, or deauthorize fiat currencies at any time, for any reason. Finally, hard money is unstoppable, in the sense that if I flip you a gold coin, there is no single authority on Earth that can block or devalue that transaction. Hard money, like gold, derives its value from freely acting individuals choosing the best monetary technology available to them.

Sacred Sovereignty

Bearer assets, like gold, offer another significant advantage — each individual unit is self-sovereign. Sovereignty refers to the freedom to take action as one sees fit. As Rosseau said: “Man is born free and everywhere he is in chains.” The struggle of history has been the need for flexible coordination of human action on a large scale against the usurpation of individual sovereignty that the institutions built for this purpose typically impose. Paradoxically, as mankind pursued large scale mobilization of his efforts to overcome the natural tyranny of time scarcity, he gave birth to an artificial tyrant that engorges itself by consuming our individual sovereignty — the government and, its apparatus of thievery, central banking. True sovereignty originates at the individual level; it naturally reigns when our individual expressions, whether verbal or financial, are unmanipulable by others. When a government censors your speech or a central bank devalues your dollar, it is a violation of your individual sovereignty. Let no one prevent you from speaking your mind or spending your time and money as you see fit. We are each our own supreme ruler:



Gold is a self-sovereign bearer asset whose credibility and value as money is derived from the combined sovereignty of countless self-interested individuals exercising free choice in the marketplace. When a good gains value on the free market, it is a result of market participants finding it useful, making sacrifices for it, and, thereby, imbuing it with part of their individual sovereignty. Since gold achieved dominance on the free market as a result of countless “votes” in the form of self-interested trade decisions by a faceless multitude across history,

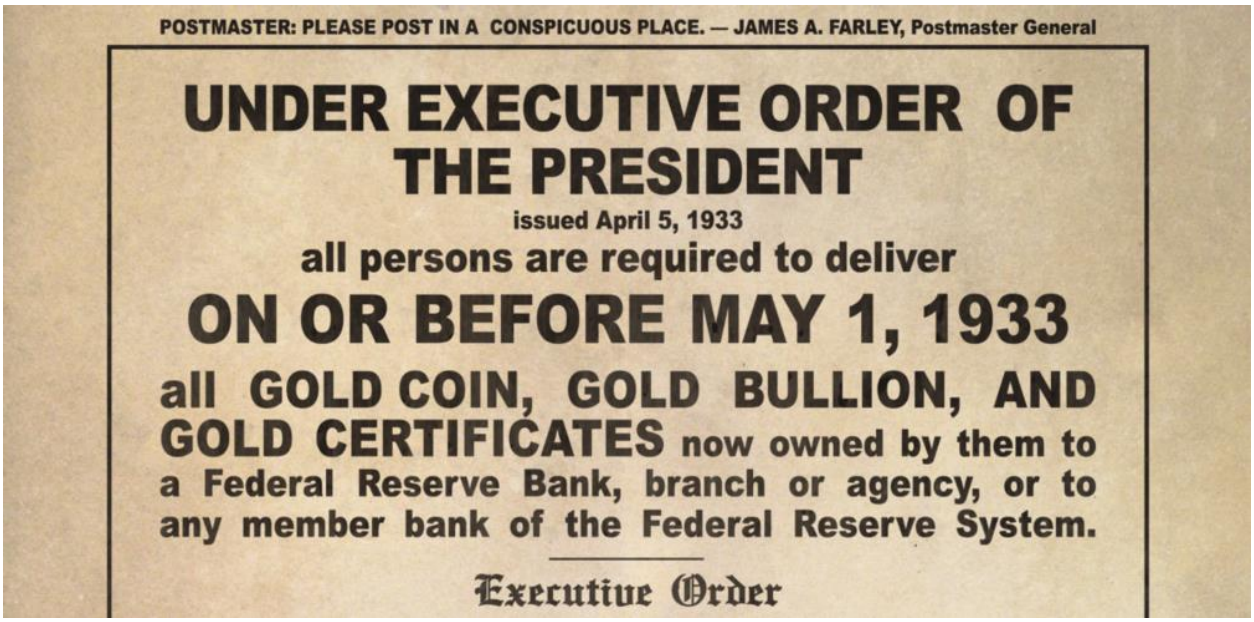
it can be considered the monetary materialization of popular sovereignty — the founding principle of Western Civilization:

Although it's an ancient monetary technology, gold still forms the prime monetary sovereignty layer of Earth, as it underpins all governmental sovereignty. In turn, governments use this power to monopolize the market for money (via their central bank henchmen) and insulate fiat currencies from direct monetary competition. Such insulation is the only way debt-based monies can survive alongside hard money. Gold and other bearer assets are final extinguishers of debt, as payments in them carry no associated liability. Modern central banks still perform final settlement exclusively in gold and actively engage in market machinations to suppress its price (see Gata.org); a testament to the primacy of this ancient monetary metal.

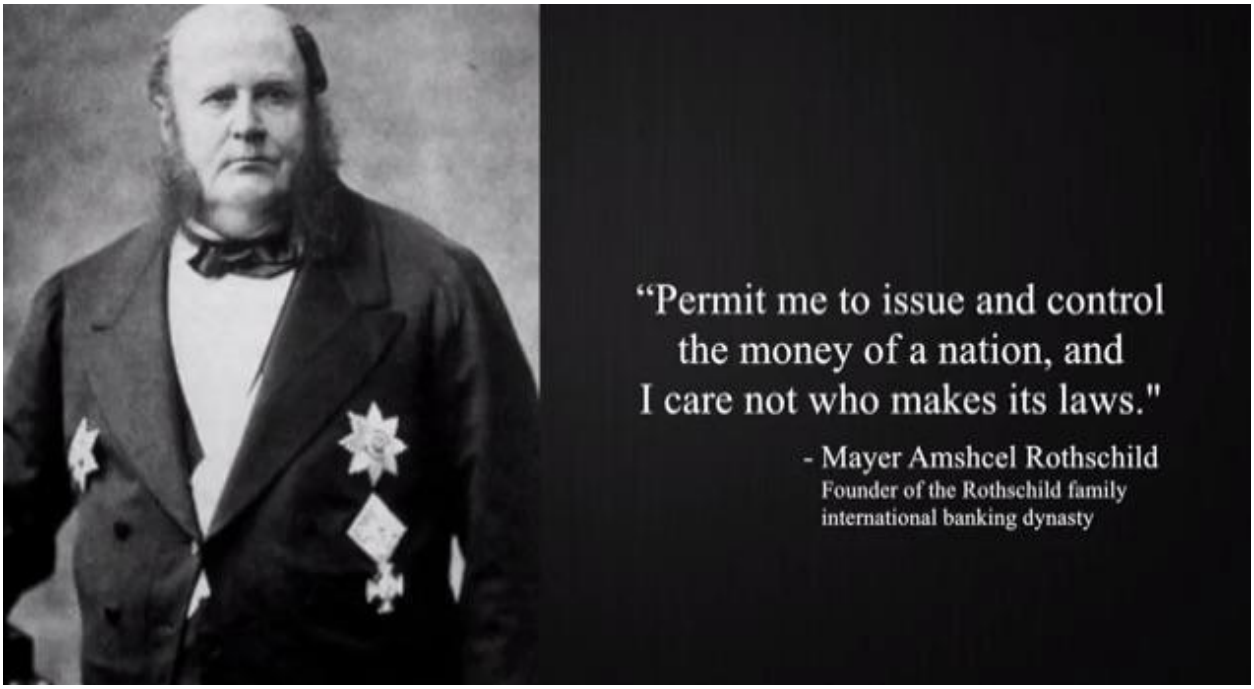
Den of Thieves

Despite this misappropriation of gold's sovereignty by government for its own self-seeking purposes, fiat currency is no longer anchored to gold, making it highly reproducible at near-zero cost. Indeed, fiat currency is the softest form of money in history; it can (and in virtually all cases does) suffer from counterparty risks such as censorship, deauthorization, or hyperinflation. Hard money is anchored in the reality of time to secure the time savings of its holders; fiat currency is a political tool that facilitates the institutionalized system of time-theft known as "expansionary monetary policy" perpetrated by central banks globally.

Although governments legally compel us to use fiat currencies today, these rules are only enforceable due to their vampirism — the sucking of sovereignty out of gold holdings. Ironically, this stolen power is used to monopolize violence and silence dissent. Government sovereignty, then, is derived from the agglomerated self-sovereignty of its gold hoards; which, in combination with the anticompetitive artifices it erects (legal tender laws, capital controls, capital gains taxes, etc.) in the sphere of money, explains why gold has been confiscated and its private ownership outlawed repeatedly throughout history:



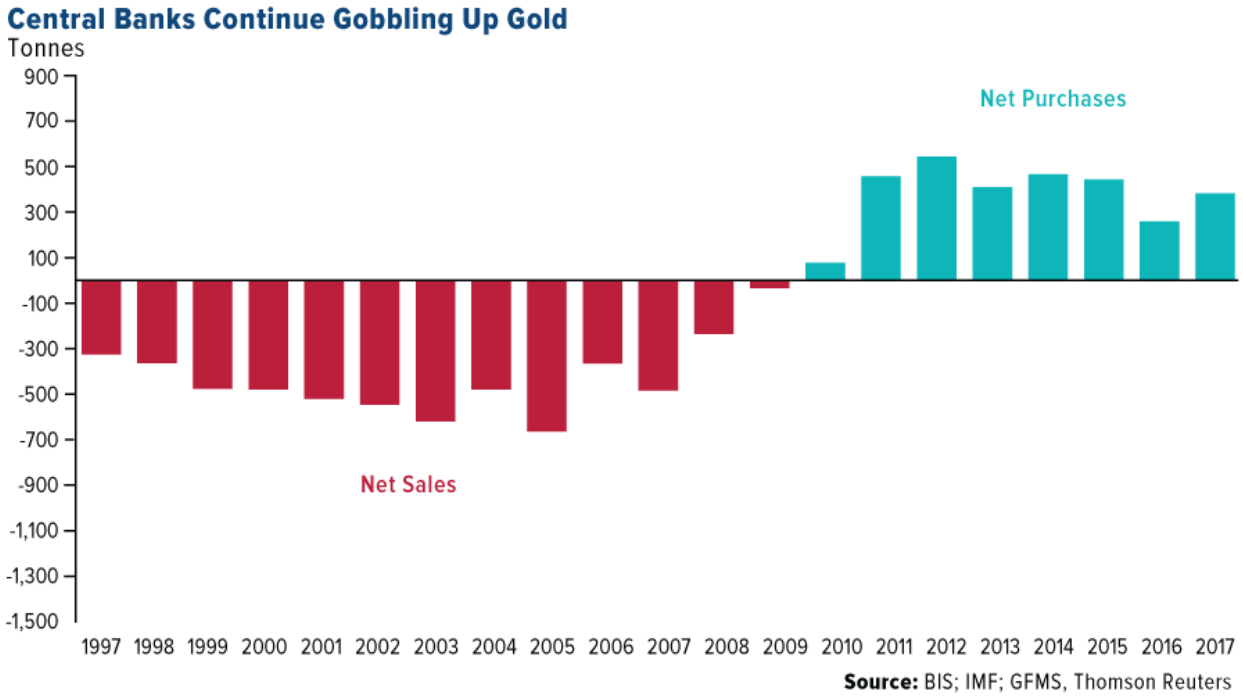
There is only one reason for such confiscatory acts: governments grasping for more power; a means to usurp gold's self-sovereignty, an embezzlement of power which itself originates in the actions of free people selecting a monetary technology in the marketplace; a tragedy at the heart of all modern economies. As the axiom says: "Whoever has the gold, makes the rules.":



Prime Money

In this sense, gold is prime money: as its physical possession underpins the sovereignty of governments, which misappropriate it to enforce central bank

money production monopolies on free people. Paradoxically, it was the actions of free people that generated the sovereignty that is now wielded against them by governments and central banks. This “duopoly of monopolists” has proclaimed time and time again that gold is irrelevant, a mere monetary artifact, and that they alone will lead the world economy to a brighter future. Ignore anti-gold propaganda; just watch their actions:

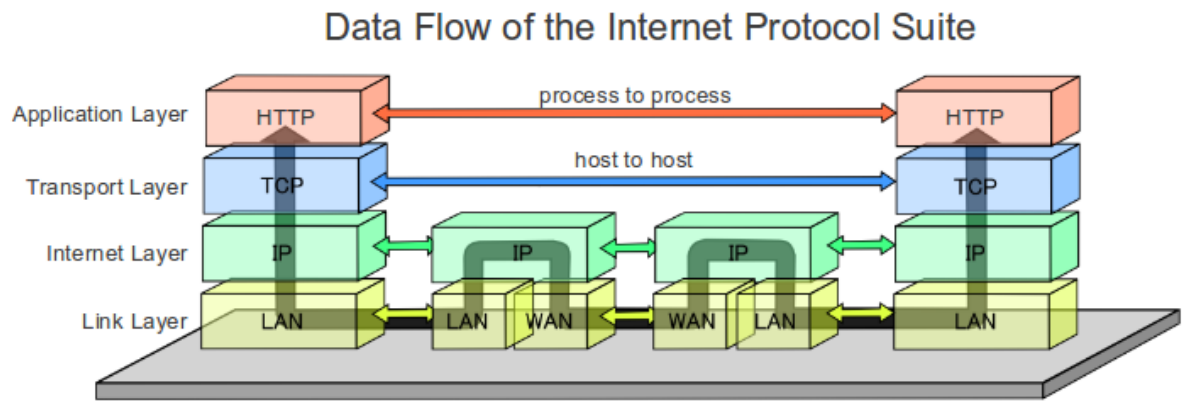


Although gold resisted supply manipulation in many ways, it is far from perfect. Through the London Gold Pool and other machinations (seriously, see Gata.org) central banks cornered the market on gold, enabling them to surreptitiously suppress its price and better insulate fiat currency (soft money) from direct competition with gold (hard money). Market manipulation like this is only possible because of our passivity. In surrendering our sovereignty to unaccountable institutions like central banks, we cede conscious control over most aspects of our lives. Remember: central banks engaged in “expansionary monetary policy” are actively stealing time from free people; as they increase money supplies, they reallocate claims on productive capital from the majority to a politically favored few. This parasitism on the savings of society extends the working lives for most of the citizenry. In this way, monetary inflation is a direct violation of private property rights and individual sovereignty. It is worth repeating: human action is the essence of sovereignty; it is our actions that instill institutions with this divine quality intrinsic to free people. Let us all exercise the utmost vigilance in deciding which institutions to empower with our sacred sovereign energies:

> "Institutional structures are legitimate insofar as they enhance the opportunity to freely inquire and create, out of inner need; otherwise, they are not."
> — Noam Chomsky, On Anarchism

Hard Money Renaissance

Against this usurpation of our individual sovereignty by government, we find hope in the emergence of a modern innovation called the internet — the universal exchange engine for knowledge. The internet has already democratized and disintermediated many aspects of our lives — from lodging and transportation, to media distribution and commerce. Compositionally, the internet is a set of open-source protocols (known as the internet protocol suite) for permissionlessly moving information worldwide in an instant. Constructed in a free market manner, through years of cooperation and standardization efforts, the internet is the greatest knowledge network in history. Today, we all benefit from this readily-accessible library of human knowledge:



As Milton Friedman so aptly pointed out in 1999, about ten years before the invention of Bitcoin, the one thing the internet lacked was a secure, private "e-cash":

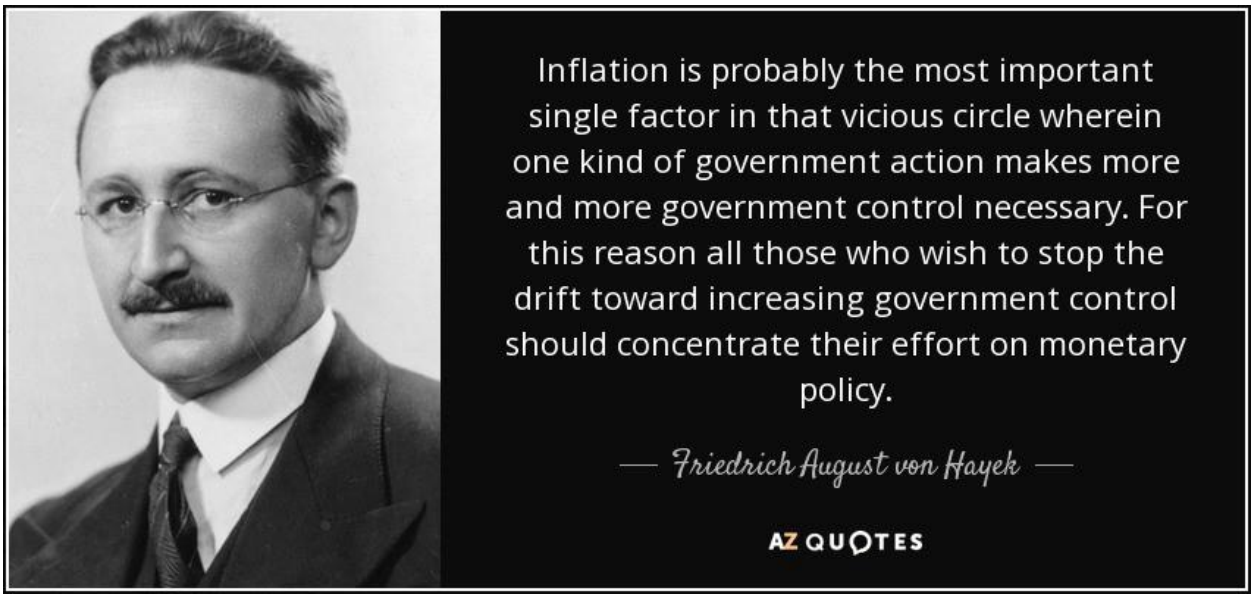
"The one thing that's missing, but that will soon be developed, is a reliable e-cash, a method whereby on the Internet you can transfer funds from A to B, without A knowing B or B knowing A."

Friedman's prescience proved astonishingly accurate. Coming into the 21st century, we had two key inceptors for digital hard money: gold, the ancient and prevailing monetary sovereignty layer (representing an unmanipulable money supply), and the internet, the ultimate engine of exchange (representing global interconnectivity or liquidity). By combining and building upon the economic properties of both, Bitcoin is a momentous monetary innovation that has achieved the divisibility, portability, durability, and recognizability of pure information infused with the absolute scarcity of time. As the internet gives us freedom to express and absorb ideas without obstruction, Bitcoin gives us the freedom to express and receive value in a hard money that cannot be stopped. In this sense, Bitcoin is the latest evolutionary layer of the internet protocol suite; a quantum leap over the monetary "Nash Equilibrium" gold represented.

Historically, gold has become more difficult to extract with the passage of time due to chemistry, physical rarity, and game theory. Gold is the ancient anchor to the prime economic reality of time scarcity, precisely why it remains the prime money of modernity. Time is the most objective measure for our intersubjective (opinion-based) valuations, as it is the one unarguable aspect of existence. In a society run on hard money, price levels naturally decline over time as our productivity grows in tandem with the division of labor. Put another way, hard money tends to appreciate over time as human knowledge becomes more specialized. In this way, increases in the value of hard money reflect how far humanity has liberated itself from time scarcity.

Liquidity of Time and Information

Conceptually then, money is both frozen time (as a means of storing time savings) and liquid time (as a means of exchanging time savings). We earn money by sacrificing our intrapersonal time and can trade it for commensurate sacrifices from others. As such, anyone that gains control over a money supply, and can manipulate it at will, can steal time savings directly from the users of its money via the shadow tax of inflation. To shed light on the true nature of fiat currency in one line, let's call it like it is: a pyramid scheme built atop gold that is subject to unlimited supply inflation. Since it bears repeating: inflation is intrapersonal time theft — a legally enforced injustice.



Manipulation of money supplies has other consequences. Money is an economy's main informational utility; a touchstone to measure the value of the time savings (or spending) expected to be made possible by an economic good in the future. When a money supply is manipulated, the objectivity of its measurement ability is compromised. This breakdown of money's informational utility is called price signal distortion. Such manipulation makes economic calculation less reliable and causes entrepreneurs to overborrow, misallocate capital, and, ultimately, degenerates time savings as capital is consumed instead of being compounded through reinvestment. Price signals provide a system for "market participant telecommunications" and can be explained as follows:

Understanding Price Signals:

Knowledge, due to its dynamic and fluid nature, cannot be fully known by a single entity as it is constantly in flux and widely distributed within many minds. In a free market economic system prices capture this distributed knowledge, convert it into impartial information and disseminate it widely. *Price signals* are the coordinating force of free market systems. Each individual decision maker can faithfully rely on the prices of goods relevant to their production process, as the prices themselves are a distillation of all known market realities into a single, actionable variable. Each individual's buy and sell decisions, in turn, further shape prices which carry this altered information back out into the market. Price signals are to market participants what light is to the eye.

To understand this point, consider the 2010 earthquake which badly damaged an area in Chile responsible for a great deal of the world's copper production. This earthquake severely damaged copper mines and export infrastructure, which immediately reduced the flow of new supply to the world copper market and resulted in a 6.2% increase in its price. Anyone in the world whose business interfaces with the copper market will be affected by this, but they do not need any specific knowledge about the earthquake in Chile or market conditions to decide how to respond. All the relevant information they need to make effective decisions is contained within the price of copper itself. Immediately, all firms that demand copper are incentivized to demand less, delay purchases or find substitutes. On the other side of the market, all firms that produce copper are incentivized to produce more of it. With a natural shift in price, everyone in the world involved in the copper industry is incentivized to act in a way that alleviates the negative consequences of the earthquake. This is the power of a free market with accurate price signals.

Price signals are the navigational instruments for entrepreneurs sailing the tempestuous seas of markets, and money is the medium through which these signals propagate. Said another way: money is a measurement system for value (a temporal quality) in the same way a ruler is for length (a spatial quality). The less elastic the supply of money is, the better it fulfills this mensural purpose. If you are measuring a table with a ruler that you cannot trust, then you can't be sure whether you're measuring the table or the ruler; you cannot distinguish the signal (the actual length) from the noise (changes in unit of measurement). [4] Gold outcompeted historically because of its relative supply inelasticity, which made it both the best store of value and conveyor of price signals. Uniquely, Bitcoin is a money with perfect supply inelasticity; it is the most uncompromising measurement system for value the world has ever known. In this sense, Bitcoin is like an inviolable ruler: a perfectly objective unit of measurement for the endless variations of market values.

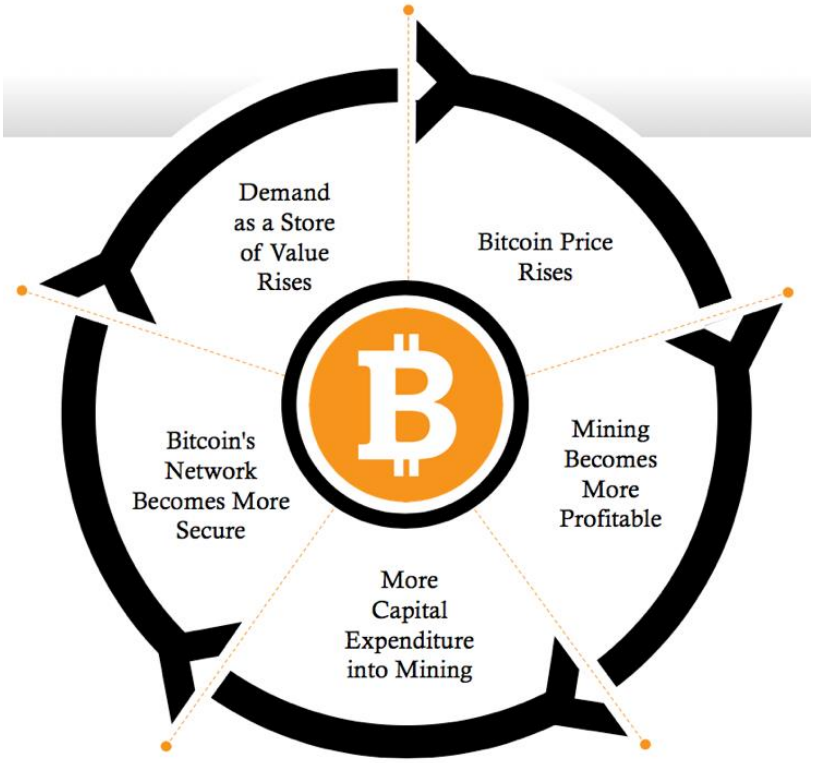
Therefore, the more closely a money supply is credibly congruent with the absolutely scarcity of time, the better it communicates the time savings generated by our collective productivity gains. In this way, both gold and Bitcoin share the same principal attractiveness: they are more closely reflective of the impersonal, irreproducible, irreversible, unstoppable, and absolutely scarce nature of the experiential element money is intended to symbolize in the marketplace — time.

Temporal Anchorage

When money is disconnected from time scarcity (as fiat currency is), its "skin in the game" is compromised and the economies it facilitates start suffering from distorted price signals, malinvestments, recessions, and an exacerbated boom-and-bust business cycle. As with most systems, money requires skin in the game to function properly — meaning that money must be costly to produce,[5] otherwise those who can produce it cheaply will do so to steal the value of time savings stored therein (as central banks do).

For gold, the costs associated with mining provide this critical skin in the game characteristic. For Bitcoin, an ingenious composite of proof-of-work energy expenditure (skin in the game) and economic incentives (game theory) enabled it to digitize scarcity. In this sense, Bitcoin's blockchain is like a bridge between physical and digital reality — the first incarnation of a

digital asset with provable scarcity. An innovative amalgamation of open-source software and behavioral economics, Bitcoin was designed to be a monetary network that reproduces itself relentlessly:

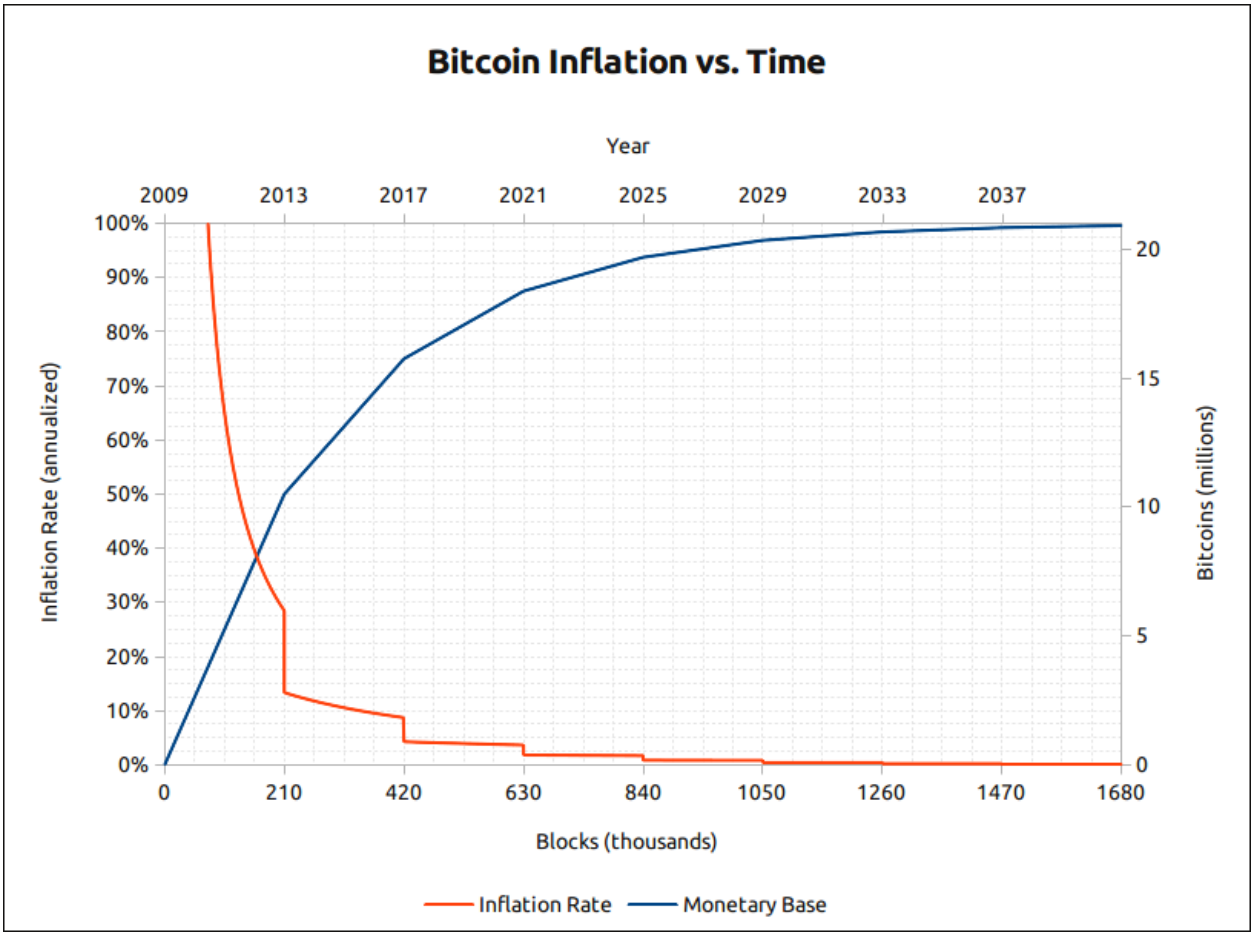


From this perspective, the value of mining both gold and Bitcoin is the "unforgeable costliness" that each represents — a measure of the time sacrificed in production, which is redeemable for the time of others. Imbued with digital scarcity, Bitcoin preserves the advantages offered by gold's physicality (self-sovereignty, irreversible transactions, final settlement) while eliminating its disadvantages (ease of confiscation, expensive safeguarding, high settlement costs). Digitization also makes Bitcoin a weightless, intangible, and (potentially) everlasting monetary technology. As a totally impersonal and self-sovereign monetary network capable of adopting market-proven features from competitors over time, while simultaneously resisting changes that negatively impact its users, Bitcoin may be the last evolution we ever see in global prime money. Gold is the "pristine collateral" which underpins the entirety of the highly-levered fiat currency financial complex; Bitcoin is poised to become the foundation for an entirely new economic order.

Monetary Horizons

In the near future and for the first time in history, the world will have a money that is harder to produce than gold. A fixed supply of 21 million units makes Bitcoin absolutely scarce — a property never before achieved by anything other than time itself. In the same way that Galelio's invention of the telescope led to discoveries that reoriented our relationship with space, so too has the invention of Bitcoin led to the discovery of absolute scarcity; a bewildering breakthrough that perfectly parallels and will forever change mankind's relationship with time. Soon, in accordance with its perfectly

predictable issuance schedule, Bitcoin will become the scarcest liquid asset in human history. At this point, Bitcoin will become the monetary technology most closely aligned with the absolutely scarce nature of time. From there, every block produced will (asymptotically) further perfect this alignment until the last Bitcoin in mined in the mid-22nd century:



The supreme divisibility, portability, durability, recognizability, and scarcity characteristics of Bitcoin constantly increase the likelihood (via the Lindy Effect) that it will continue to outcompete gold and fiat currencies in its long climb toward becoming global prime money. Bitcoin, with a supply more closely aligned with the prime economic reality of time scarcity, is slowly but surely *undermining* gold's role as prime money. The word *undermine* literally means "to dig under fortifications to collapse them". In this sense, Satoshi designed Bitcoin to "dig deeper" into reality than gold and, in doing so, undermine its role as prime money by more closely mirroring the fundamental nature of time. As a result, the value of fiat currencies will also diminish as gold slips from its position of primacy.

Temporal Metaphor

Time is the ultimate experiential element we all share. It is ruthlessly egalitarian, flowing equally for all alike. Time is our objective anchor in a world of ceaselessly shifting intersubjective valuations. Abstractly, money is our metaphor for time. As a tool, it best serves mankind when its supply is as inelastic as the absolute scarcity of time. Here, gold does well; yet Bitcoin, the first money with a supply that is absolutely scarce, reflects time perfectly.

Money is the medium through which many minds become one; it is the coordinating mechanism of human action. Money matters because only through cooperation and innovation do we mortals gain ground in our struggle against the immortal tyrant of time scarcity. Perhaps one day to be regarded as the most impactful technology ever invented, Bitcoin is simply a tool for saving time; it stores the value created from our time spent serving one another, reduces the time needed to establish trustful coordination, and it protects our mutually generated time savings from confiscation. Furthermore, Bitcoin promises to reduce the money, capital, and life wasted in warfare. Bitcoin accomplishes this by transcending laws and outcompeting money production monopolies, which use taxation via inflation to stealthily fund perpetual warfare. As Ron Paul said: “It is no coincidence that the century of total war coincided with the century of central banking.”:

Table 5.1 Conflicts steadily cost more in human lives

Period	Conflict-related deaths (millions)	World population, mid-century (millions)	Conflict-related deaths as share of world population (%)
Sixteenth century	1.6	493.3	0.32
Seventeenth century	6.1	579.1	1.05
Eighteenth century	7.0	757.4	0.92
Nineteenth century	19.4	1,172.9	1.65
Twentieth century	109.7	2,519.5	4.35

Bitcoin also promises to help generate even more time savings by deepening the division of labor, a direct result of financial disintermediation, the benefits of which flow to everyone. Finally, Bitcoin encourages us to adopt lower time preferences and think long-term. Hard money incentivizes us to save and invest, and disincentivizes excessive debt and spending, since it naturally appreciates over time as our collective productivity grows. Fiat currency is the reverse: it pushes up our time preferences and disintegrates societies. As the repeated fall of ancient civilizations shows, monetary integrity and social cohesion are inexorably linked.

Breaking the Chains

Bitcoin belongs in a certain class of momentous innovations — like antiseptics, electricity, or the internet — that either extend our lifespans individually or enhance our productivity and, therefore, our time savings collectively. These innovations expand our relationship with time in one or more ways: extending life expectancies, lowering time preferences, or enhancing productivity. Bitcoin promises to contribute to all three by being the best self-sovereign savings technology in history: reducing death tolls and capital destruction from warfare by financially starving governments, incentivizing savings and investment in innovation, and accelerating our productivity gains by reducing artificial and arbitrary trade frictions.

Bitcoin has the potential to bend the grand arc of human history back towards a free market paradigm. Bitcoin is doing this in the market for money, and its underlying technology may one day be applied to other markets like equities, bonds, and real estate. Going forward, Bitcoin promises to further liberate us from the clutches of time scarcity, eliminate time theft via inflation, reinvigorate individual sovereignty, and, as a cumulative result, radically increase social scalability worldwide. As Alfred North Whitehead said:

"It is a profoundly erroneous truism repeated by all copy-books and by eminent people when they're making speeches, that we should cultivate the habit of thinking about what we're doing. The precise opposite is the case. Civilization advances by extending the number of important operations which we can perform without thinking about them."

As we continue our endless contentions with time scarcity, government-authorized money monopolies remain a scourge on our humanity. Central banking, an institution of monetary socialism and systemized time theft, has repeatedly wounded our individual sovereignty, time preferences, and freedoms throughout history. We mortals must break the shackles of this oppressive institution and focus our energies on innovating against time scarcity — the immortal tyrant. In doing so, we will create a world in which our children, their children, and all future generations are born able to live totally self-sovereign lives — forever free from the chains of governmental tyranny.

By Robert Breedlove Oct, 2019

Thank you for reading "Bitcoin and the Tyranny of Time Scarcity" My sincerest gratitude to these amazing minds:

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

And anyone else I forgot :)

The Bitcoin Times Ed 2 is the collaborative work of 8 writers & 1 designer with the intent to educate, inspire and spread ideas on bitcoin.

Each section will be released on Medium as a free long form article, and the full, compiled version of the Bitcoin Times will be available for free at the link below. In 2020, we'll release a limited edition hard cover collectible, for purchase, which you'll be notified of by email if you download the free pdf.

If you found value in this or any of the other essays and articles, please support each of the contributors by sharing it out & following their work.

---

ownload the full guide at:

The Bitcoin Times

(Soon to be updated to: https://bitcointimes.news)

The Passion of the Believers

By Hass McCook

Posted December 19, 2019

As always, we commence by sending thanks and good tidings to Satoshi Nakamoto — The Creator and First of the Believers, General of the Byzantines, Breaker of Banks and Fighter of Fiat — and to Hal Finney and The Apostles and The Disciples thereafter, and to The Stoic and Patient True Believers, who keep their tithe holy, and stack sats for their salvation. Oh you who believe, fear the day of economic reckoning, and do not face the Angel of Hyperbitcoinization as a nocoiner, for punishment awaits them in the hereafter.

Religion has always been a touchy subject, with tens of millions of people even recoiling at the word. These demographics are reflected in the observable Bitcoin Twitter / Social Media communities, with the Recoilers being observably over-represented. When Bitcoiners are referred to as cult members, should they really be that upset? In this piece, I argue that they should not be, and instead, that they come home to The Hard-Money-

Monastery. I will commence with dictionary definitions of religion and where Bitcoin fits into it. From there, I will introduce the mythology, memes, and laws that drive the commitment, attitudes, beliefs and practices of True Believers, and demonstrate the parallels between Bitcoin and "Traditional" religions. Perhaps you will find that a little religion may be good for all of us.

So how is religion defined? The Oxford Dictionary defines it as "A pursuit or interest followed with great devotion." Mirriam-Webster defines it as "a personal set or institutionalized system of religious attitudes, beliefs, and practices" and "commitment or devotion to religious faith or observance". I think this is a suitable secular definition moving forward. I will also define the term "hereafter" as "At some time in the future", but also "After Death." The concept of Death, or perhaps more specifically, Judgement Day, is viewed by many Bitcoiners as a devastating economic event, the death of Fiat. Ultimately, this will lead to total civilizational collapse, or, the phenomenon of "hyperbitcoinization", effectively, when all global trade is conducted in Bitcoin, and its market capitalization is in the dozens of trillions, if not hundreds. A tenet of the Bitcoin faith is belief in this Day and the need to prepare well for it. With definitions out of the way, we can get to the epic memes.

Bitcoin mythology is legendary in its potential reach. Satoshi as a real, yet mythical, being, concept, or meme, would deserve a full book in their own right. The Bitcoin Network is omnipresent — beamed everywhere, even from the heavens above. There is decentralization of everything — from the mechanical process of mining, to the human process of building and hodling, thought, and religious, or non-religious, ideology. The Nodes are omnipotent, and only through their good graces can changes be made to Bitcoin. Running a full node is a practice that is incumbent on the True Believer. The Timechain is the unforgeable eternal ledger, secured by the practice of mining, of which True Believers are encouraged to do if able. Through the process of Proof-of-Work, the pulse of the network is the literal monetization and digital embodiment of energy. "Capital-E" Energy is thermodynamically finite, yet infinitely divisible into units of energy — just like Bitcoin. Bitcoin is a simple digital reflection of Energy, and is irrevocably tied to it. Energy is everything in the universe, and everything around us is simply a materialisation of this energy in one state or another. Energy is Nature. Energy is Life. We now finally have a monetary approximation of this through Bitcoin.

Bitcoin, then, is simply Energy, and by extension, Nature and Life itself. Nature demands submission. The Nature of Bitcoin is open and permissionless, and since Bitcoin is rooted in Nature (i.e. Energy), the will of Bitcoin must be submitted to.

Lao Tzu said:

One of great virtue is one who follows the Natural Way of Bitcoin.

Bitcoin is vague and intangible. Yet, in the vague and void, there is image, there is substance.

Within the profound intangible, there is essence. This essence is genuine. In It lies the great faith.

Since the beginning of 2009, Bitcoin has been in existence.

Only through It can one understand the origin of all beings

How do I know that this is the true essence?

It is through this Natural Way.

- The Tao of The Coin, Chapter 21

Bitcoin is the Essence of Money. The True Believer is content in their submission to the will of Bitcoin, and they will be greatly rewarded in the hereafter. I will discuss the hereafter, and several other parallels Bitcoin has with “traditional religions”, next.

There are several common themes across the world's major religions, spanning monotheistic, polytheistic and philosophical ones. Bitcoin embodies bits and pieces of all of them and can even share conflicting religious beliefs! Such is the beauty of Bitcoin, it is compatible and flows through Nature, with anyone free to ride its waves and integrate it into their own "religion".

Take for example the contrast of Bitcoin and the Christian concept of Original Sin. The Bitcoin Observant see mankind's fall from grace as the movement to fiat currency, and we are all born default Keynesians, and need to stack sats to cleanse ourselves for a pleasant hereafter.

Islam takes an opposite view, whereby all people are born Muslim and with a clean spiritual slate, and non-Mulsims can "revert" to Islam if they choose. The Bitcoin analogy in this case would be that we are born free, with a clear mental slate that accepts the will of nature, but gets forced into the fiat machine. We can revert to our state of freedom by declaring our faith in Bitcoin; best done by stacking sats.

There are also elements of both free will and divine pre-ordainment at play in traditional religions, and this is also apparent in Bitcoin. We all participate based on our free will, with a major reason being the Divine Preordainment of the Bitcoin Supply.

One cannot mention bitcoin and religious reverence without the mentioning of Satoshi. In one way, he presents as a Saviour, who so loved us, that he sacrificed almost 5% of Bitcoin's supply so that he may complete his favour upon us. As a messenger, he created the perfect money for us, and brought to us this Code called Bitcoin Core. Within its own ecosystem, The Code is a deity in its own right; it sets fixed boundaries of what is and isn't allowed, and enforces these rules without fear or favour, beholden to no-one, only to the Greater Law of Mathematics. Although enforcement mechanisms differ across religions, the same points apply. Therefore, every node running The Code is a deity in its own right too. **An MMOPG, a Massively Multi-peer Online Polyumvirate God, engaged in Financial Warcraft.**

In all religions, there is always some struggle of good versus evil in one way or another, with suffering being a theme across the majority. It is the ultimate display of low Time Preference — struggle now for victory and rewards in the future. Many religious people struggle for a future that may not even exist! Struggles can be internal or external. Internal struggles are the hardest, as "sin" can be easily fallen into. Bitcoin has no struggles, it just is. The Believers must struggle externally in what will be biggest mythological Good versus Evil war in history, the battle of Hard, Pure Money versus Evil-Facilitating Fiat.

Internally, they need to avoid particular “deadly sins.” The original 7-deadly sins were Lust, Gluttony, Greed, Sloth, Wrath, Envy, Pride. Religions encourage staying away from sin and following the straight and narrow path. Staying away from sin and doing good deeds grants you rewards for a heavenly hereafter. After all, everything in Nature is incentive driven.

Some say that If you indulge in these sins often enough, the regret and heavy conscience would be enough to make the final minutes on your death-bed feel like hell on Earth, regardless of what afterlife you believe in. More importantly, chances are you will likely lose a lot of sats taking that approach, and based on what you believe, a fiery eternity would await you too. Either way, losing sats may be the difference between a heaven-like or hell-like experience in the Bitcoin Hereafter. In light of these 7 sins, The Observant maximise their health and live long lives by fighting gluttony and sloth, fight greed and pride by staying humble and stacking sats, and show no envy by voluntarily giving away your source for people to benefit from as they wish. Lust is a discretionary one, and wrath is allowable and encouraged against nocoiners and shitcoiners alike. The jurisprudence remains unclear though, with some sects, such as the Temple of Toxicity, arguing that wrath against shitcoiners and nocoiners is incumbent upon The Believer.

Do not lay up for yourselves treasures on earth, where moth and rust destroy and where thieves break in and steal, but lay up for yourselves treasures in The Blockchain, where neither moth nor rust destroys and where thieves do not break in and steal. For where your Trezor is, there your heart will be also.

- Book of Satoshi 6:15

While many newcoiners come into the ecosystem at the prospect of financial returns, their education and involvement lead them to The Natural Way — stacking sats. From there, The Believer reaps several rewards, both spiritual fulfilment for their souls, as well as a much higher chance for a rapture on Economic Judgement Day and thereafter. Through the act of religiously regular sat stacking, The Believers provide an uphill-sloping bedrock and stability to the price. Some even refer to this ritual as a “tithe”, as every single sat stacked furthers the cause of Bitcoin — yet another parallel!

As we move up the natural logarithmic price slope, we get increases in “energy-level” to help in our fight. From a literal point of view, energy used to power Bitcoin will increase as a function of price. From a figurative point of view, the “energy level” is the size of the weaponry available to us in our contest against central banks. This means an enclosed Bitcoin ecosystem that is capable of delivering financial sovereignty to the masses. Indeed,

victory has been granted to the patient and those who keep their tithe holy. Of course, there will be some vanity rewards to those who hold 6.15 BTC, with promises of Citadel living, endless riches, and well-endowed partners.

Having laid out the case above, we can see that Bitcoin facilitates most attitudes and beliefs; especially those related to freedom and sovereignty. The True Believer's involvement in the ecosystem involves many different religious practices, whether it's contributing code, running a node, learning and educating, or simply stacking sats. They carry out these practices with great devotion. Not only does Bitcoin fit the dictionary definition, we have seen that Bitcoin as a religion shares many underlying tones with both the ancient & modern religions.

At the end of the day, everyone has to believe in something; might as well believe in something verifiable and unforgeable.

In closing, we will recite a brief Bitcoin prayer:

Oh Bitcoin! Do not punish us if we forget our DCA or we fall into error with fiat and shitcoins; Oh Bitcoin! And lay not on us a bear market like that which You did lay on those before us; Oh Bitcoin! And put not on us bags greater than we have the strength to bear. And enlighten us and humble us and grant sovereignty to us. You are our bulwark, so grant us patience between this halving and the next.

By Hass McCook, The Friar, Sept, 2019

The Bitcoin Times Ed 2 is the collaborative work of 8 writers & 1 designer with the intent to educate, inspire and spread ideas on bitcoin.

Each section will be released on Medium as a free long form article, and the full, compiled version of the Bitcoin Times will be available for free at the link below. In 2020, we'll release a limited edition hard cover collectible, for purchase, which you'll be notified of by email if you download the free pdf.

If you found value in this or any of the other essays and articles, please support each of the contributors by sharing it out & following their work.

Download the full guide at:

The Bitcoin Times

(Soon to be updated to: https://bitcointimes.news)

Tweetstorm: A Decade of Bitcoin Technology

By John Newbery

Posted December 21, 2019

The end of the decade is a good time to look back and marvel at the giant strides that Bitcoin has made since Satoshi gave us the whitepaper in 2008. It's also a natural point to look forward to what the upcoming years might hold in store.

This is where I think Bitcoin is headed over the next few years. Tell me why I'm wrong and what I've missed!

The lightning protocol teams working on c-lightning (@Blockstream), eclair (@acinq_co), LND (@lightning) and rust lightning will continue to iterate rapidly on the lightning protocol.

All implementations now support basic multi-path payments (https://bitcoinops.org/en/topics/multipath-payments/ …). We'll get better support of that as well as dual-funding, splice-in and splice-out (https://bitcoinops.org/en/topics/splicing/ …).

Taken together, those technologies will make channel and liquidity management much easier. They'll be automated, fade into the background and user experience will improve drastically.

Lightning infrastructure will improve. @bitfinex recently added lightning deposits and withdrawals. All other exchanges, merchant service providers, custodians and wallets will follow suit or become obsolete.

We'll see more lightning wallets: a mix of non-custodial; self-custodied with outsourced routing; and fully-self-managed wallets. This is a brand new space and there'll be lots of experimentation. Different teams will find different niches to fill.

Already, wallets
like @MuunWallet, @Breez_Tech, @PhoenixWallet, @ln_zap and @bluewallet io are experimenting with different models.

Tooling for lightning developers will improve. When we ran the lightning apps residency just over a year ago, the attendees spent a lot of time setting up their lightning dev environments.

Now, with Polar (https://github.com/jamaljsr/polar) by @jamaljsr, lightning app developers can set up a test environment with a few clicks. More and better tools will continue to appear.

With better tooling, we'll see faster innovation on the application layer. Teams at @zebedeeio, @SatoshisGames, and others we haven't heard of yet will delight us with new and unexpected lightning experiences.

The schnorr/taproot softfork (https://bitcoinops.org/en/topics/taproot/ …) will be activated in 2020 or 2021. That'll provide a huge improvement in fungibility, privacy, scalability and functionality. For an overview of the benefits, watch the Optech exec briefing here: https://bitcoinops.org/en/2019-exec-briefing/#the-next-softfork ….

That'll allow lightning to upgrade from HTLCs to Payment Points. That's a big improvement for privacy and payment decorrelation, and allows 'Stuckless payments' with proofs-of-payment – another huge boost in LN usablity.

See the @suredbits series of blog posts here https://suredbits.com/payment-points-part-1/ … for more details on Payment Points.

Even better, lightning channel opens and closes will look identical to payments to single pubkeys. The same is true for payments to k-of-n pubkey thresholds. That's good for fungibility, privacy and scalability.

In fact, with schnorr/taproot, there's almost no downside to encumbering UTXOs with advanced scripts instead of single pubkey outputs.

Cold storage UTXOs will be k-of-n multisig keytrees, and all hot wallet UTXOs will be stored in channels (with splicing-out used to make on-chain payments). When transactions hit the chain, they'll look like any other single pubkey/signature payment.

Payments into wallets will pay directly into channel open outputs (thanks to @esneider for pointing this out to me). There'll be no concept of an on-chain balance and an in-channel balance. Just a single, unified balance that can be used for lightning or on-chain payments.

Wallet teams will collaborate on a PayJoin payment protocol (https://bitcoinops.org/en/topics/payjoin/ …). A large number of on-chain transactions will be 2-input-2-ouput transactions, vastly improving fungibility and privacy, and foiling chain analysis.

The inputs to those PayJoin transactions may be channel splice-outs, and the outputs may be channel opens, but there'll be no way to tell from observing the chain.

Eventually we'll have cross-input signature aggregation (https://bitcoincore.org/en/2017/03/23/schnorr-signature-aggregation/#signature-aggregation …), which means those PayJoin transactions will only have a single signature, and will be *cheaper* than regular change-producing transactions.

Larger coinjoins will be cheaper still. An advanced PayJoin payment protocol could even batch multiple payments to the same merchant/exchange and use only a single signature.

We'll get SIGHASH_NOINPUT or SIGHASH_ANYPREVOUT (https://bitcoinops.org/en/topics/sighash_noinput/ ...), making eltoo (https://bitcoinops.org/en/topics/eltoo/ ...) possible, and blurring the lines between layer 1 and layer 2 (https://lists.linuxfoundation.org/pipermail/lightning-dev/2019-September/002136.html ...).

That'll make lightning even more usable and allow more advanced layer 2 contracts like channel factories (https://bitcoinops.org/en/topics/channel-factories/ ...).

All these advanced features will require greater wallet interoperability. That's where miniscript (https://bitcoinops.org/en/topics/miniscript/ ...) comes in.

With miniscript, wallets will eventually be able to enter contracts with each other that don't require pre-templated scripts (as lightning currently does). This wallet interoperability will allow faster innovation in layer 2 contracts.

OP_CTV (https://bitcoinops.org/en/newsletters/2019/12/04/#op-checktemplateverify-ctv ...) or some other covenant-enabling opcode will be activated, allowing richer layer 2 constructions like joinpools (https://freenode.irclog.whitequark.org/bitcoin-wizards/2019-05-21#1558427254-1558427441 ...;).

Taken together with taproot and SIGHASH_NOINPUT, we'll get extremely rich and private off-chain contracts will be made possible.

Some of these things will happen in 2020, and some will take a bit longer, but they're all heading in the same direction: using the chain for what the chain's good for (h/t Andrew Poelstra).

That's to say: the block chain allows nodes to arrive at an agreed ledger state, while contracting and functionality move up onto layer two. Doing so is cheaper, more secure, more private and allows for more rapid innovation.

None of this is inevitable, and none can happen without the industry of many hands and the creativity of many minds. There are years of work ahead for developers, researchers, businesses and users.

If you run a Bitcoin business, you can help by supporting, sponsoring or hiring open source developers. If you're a Bitcoin user, you can help by *demanding* that any service you use supports the open source ecosystem.

If you're a developer, you can help by reviewing and testing PRs and releases. https://bitcoincore.reviews/ is a great place to start.

2020 is going to be a great year for Bitcoin and Lightning protocol development! /fin

---

Bitcoin is a information channel

By Acrual

Posted December 22, 2019

After my article about "Volatility as information" a few readers asked me what did I mean by "low entropy carrier". As I was writing about George Gilder's book "Knowledge and power" applied to Bitcoin, I didn't feel at the time the need to explain what these fancy words mean.

But let me try to do so as it is for me a very interesting exercise:

For example the realm of physics is a very low entropy carrier of information, what do I mean by that? It means that once you figure out the laws and relations between your measurements and observations, you can infer more laws and then create models that explain the reality. There are little inter-dependencies between observable facts compared to for example what happens in a high entropy carrier such as the human body.

As Gilder says, killing a virus within a human body without destroying healthy tissues is very complex compared to doing certain experiments within the realm of physics because of these inter-dependencies. Consequently, when we take a blood test, from the measurements we can conclude several correlations but hardly ever causation. Trying to do so, we frequently need many more tests. In fact, the more I learn about them, the more I conclude we are absolutely clueless about the human body.

With regards to the economy, the same applies to what Gilder calls the low entropy carrier of capitalism, which are the rule of law, the maintenance of order, the defense of property rights, reliability and restrain of regulation, **stability of money**, etc...

A low entropy carrier is therefore a channel that carries itself very little information, producing little distortion or external interference in the transmitted message and also allowing the entire message itself to be what Gilder calls "surprise", entropy, or unexpected information. For Gilder, surprise is the entire point of entrepreneurial activity.

Therefore making the rule of law, maintenance of order, defense of property rights, etc... more predictable, allows to really receive the signal at the other end. In other words, by decreasing the noise in the channel, we are able to get the information that truly matters, by decreasing the "noise" that the powers that be produce via distortion and interference in things like money, regulation, property rights, etc...

Note: All this fancy writing by Gilder (and me) is well supported by an actual theory, the information theory of Shannon (1948), so neither him nor me are making this up!

In the USA economy surprise (crazy start-ups, crazy inventions and improvements of any process within economic activity) is arguably possible even likely. OTOH, the North Korean regime could be argued to be the exact opposite, where the only surprise possible is the last eccentricity of its dictatorial leader thanks to its completely lack of transparency.

Given that money is the information system of the economy, you could say that the USD is currently among the lowest entropy carriers in the world and the North Korean currency likely the highest.

What about Bitcoin?

Bitcoin is currently a very high entropy carrier yet for economic activity, because it is presently full of surprise for most of the world. It is not its lack of transparency but the fact it is hard to figure out. As I argued in my previous post, volatility, mining or its blockchain are some of its interesting features for many, and given that everything about it is mostly surprise, it can't be a proper information channel of capitalism just yet.

But every podcast, book, every tweet, every article about it increasing its understanding, decreases this entropy Gilder writes about and it is in the process of becoming the lowest entropy carrier of the economy within the next few decades. In other words, **in 10 to 30 years time, thanks to its transparency, we will find as many surprising things about Bitcoin as we currently do about the alphabet!**

With regards to the current debate on scarcity being Bitcoin's first price driver, I disagree, I believe the main driver is its understanding, which drives demand, which thanks to the limited supply increases the price.

Keep learning and explaining, it is the best way to decrease Bitcoin's entropy and to end up turning Bitcoin in the best form of money we have ever seen!

Bitcoin's Eternal Struggle

How Bitcoin Thrives on the Edge between Order and Chaos

By Gigi

Posted Dacember 22, 2019

Bitcoin works. No matter what other opinions you hold about this strange phenomenon, it undoubtedly works, marches on, or, as I (and others) have previously argued, is alive. Even if most of the world would grind to a halt, the Bitcoin network would continue to produce valid blocks every 10 minutes or so.

Bitcoin works because of many things: game theory, economic incentives, cryptography, ingenious engineering, resilience on a network level, and so on and so forth. Killing Bitcoin is hard. Really hard. Killing Bitcoin is like killing an idea. An idea that is stuck in the heads of hundreds of thousands of zealous individuals.

First of all, it is quite hard to shut down the internet globally; and secondly, Bitcoin can transcend the internet. Everything which can transmit data can be used to transmit bitcoin transactions, and everything which can hold data can store a copy of Bitcoin's block chain. It's just a ledger; the whole thing is just information.

Curiously, the Bitcoin network is embodying the eternal struggle of life: the struggle against entropy; a battle on the edge between order and chaos.

To understand this chaotic struggle — and how Bitcoin thrives because of it — it is helpful to briefly discuss the following concepts: entropy, randomness, and information. I hope to convince you that these concepts are related and that they are essential in Bitcoin's ongoing struggle for survival.

Let's dive in.

Entropy

In computing, entropy can be used to measure the randomness of a data source. In cryptography in general, and in Bitcoin in particular, a good source of entropy is essential to keep you secure. Mess up the entropy of your private key (aka your seed phrase) and *your* bitcoins will be *my* bitcoins soon.

Note: the technical term for this unwanted transfer of coins is rekt. You don't need to know what "getting rekt" means in detail, or the many ways in which

you can get rekt; it is enough to know that you should avoid such a situation at all costs.

Entropy is quite a complicated concept, but in general terms, it describes how *random* or how *compressible* something is.

- **High entropy:** randomness.
- **Low entropy:** orderliness.

Or, in other words, with a nod to Tsachy Weissman:

- **High entropy:** not very compressible.
- **Low entropy:** very compressible.

There are complicated formulas and quite a few disambiguous definitions of entropy. The concept finds applications in classical thermodynamics, statistical thermodynamics, quantum statistical physics, order and disorder, life, astrophysics, and more. It is also a measure of irreversibility.

In Bitcoin, reversibility and irreversibility are probabilistic. If enough people with enough hash power collude transactions could be reversed. Absolute irreversibility does not exist in Bitcoin. Final settlement is never final, but always probabilistic. Yes, the chances of reversal might be beyond astronomical, but nevertheless, final settlement does not and should not exist in Bitcoin. Nakamoto consensus forbids it.

"The first law of thermodynamics, also known as the law of Conservation of Energy, states that energy cannot be created or destroyed in an isolated system. The second law states that the entropy of any isolated system always increases, and the third law states that the entropy of a system approaches a constant value as the temperature approaches absolute zero."

— Knut Svanholm

In Bitcoin, entropy is important for multiple reasons:

1. Secret information should be generated by high-entropy data sources
2. New blocks reverse entropy locally, i.e. create order out of chaos
3. Bitcoin's security model relies upon chaotic processes
4. Validation relies on deterministic processes
5. Everyone can validate structured data
6. Nobody can guess random data

While the above speaks in absolutes (*everyone* and *nobody*), the truth is more nuanced: Again, Bitcoin is *probabilistic* in nature, thus, *in theory*, one could

guess a private key just like *in theory* you could find a billion valid blocks in one millisecond.

Details aside, we will try to keep it simple here. In general, if you have two coins, the entropy of this system is **two**. As in: you can describe the whole system with two bits: 00, 01, 10, 11.

2 bits of entropy

Flip both coins at the same time, and you will end up with either tail-tail, tail-heads, heads-tail, or tail-tail. If you are a fair coin flipper, the chance of each combination will be 25%. Imagine a system that flips hundreds of coins at once, and you have something which could be used to generate a private key.

Randomness

Randomness is essential to cryptography. At the root of all secret communication is some form of information asymmetry: you know something a potential eavesdropper does not.

A good secret is like a good password: randomly generated, i.e. coming from a data source that has a high degree of entropy.

Random noise. How much information is contained in this image?

If something is "perfectly" encrypted, an eavesdropper can not distinguish what was said from random data. This is the purpose of proper encryption: you want to hide what was said, and, if possible, even hide the fact that something meaningful was said at all.

- **"Good" randomness:** not compressible / high entropy / secret / secure.
- **"Bad" randomness:** compressible / low entropy / guessable / insecure.

Bitcoin doesn't use encryption *per se*. The ledger is public and transparent by design, enabling anyone to audit the whole system with the will to do so. Bitcoin uses cryptographic signatures and cryptographic hashes, both of which produce quasi-random outcomes. And if you know the secret, you can unlock some coins (using your private key), add new blocks to the block chain (using the nonce you found), or prove that you are who you say you are (by signing a message, which at least proves that you are in control of one or multiple keys).

Only you know your private key. Nobody else should know your private key. Only you, the successful miner, found the nonce for the next block. That is information asymmetry. That is what makes Bitcoin work.

All cryptographic systems work because of information asymmetry. And curiously, properly encrypted data is indistinguishable from random data. Otherwise, an eavesdropper could make *some* sense of the encrypted message, which in turn would mean that the encryption used isn't very good.

Information

What is information, anyway?

People often say that Bitcoin is thermodynamically secured. While this is true, I'd like to dig a little deeper. What does *thermodynamically secured* mean, exactly?

It means that — as far as we know —changing things in our universe requires energy. When I say "changing things" I mean it: change anything at all in our universe, and you will need to "use" energy — put in some work — to change that thing.

Move a chair? You have to put in some work. Grow a tree? You'll need the energy of the sun to turn CO2 into wood. Do a calculation? Energy is required to manipulate whatever is holding the data. Store the outcome? You'll need energy to arrange (and protect) the atoms for storage, no matter what medium is used.

Bitcoin lives mostly in the informational realm, and just like all other information systems, it needs to store and process the information via a physical medium. Thus, if you change *information _in Bitcoin, you effectively change a _thing* in the real world. Whether that thing is a solid-state disk, USB stick, hard drive, optical storage medium, or something else doesn't matter.

The fact that changing things — or, in other words: flipping bits — requires energy, is the root conundrum of all computation. It is the reason why your computer makes a bunch of noise and gets hot if it does a lot of "thinking." It is the reason that computer science students have to study the *Big O notation* and software companies love to ask questions about it. Changing a zero into a one requires work, and no matter how fast you are working, you still need to expend _some _amount of energy. According to physics, there literally is no such thing as a free lunch. Flipping bits is work, which requires energy.

And here is the thing: Bitcoin utilizes the fact that the difference between *hard computational problems* and *exponentially hard computational problems* is big. Mind-bogglingly big.

Alright. Back to our original question: *What is information*, anyway?

Sorted colors. How much information is contained in this image?

Information relates to both *knowledge* and *meaning*. It is the opposite of not knowing, and the opposite of information in data is randomness. In other words: if you are not able to make sense of some data, it might appear random *to you*.

- **Sensible information:** quite compressible.
- **Nonsense information:** not very compressible.

Pi might help to clear up what I'm trying to say: 3.141592653589793... can be "compressed" into π, or the circumference of a circle with the diameter of one.

As a computer programmer, you could think of this concept as follows: can I write a computer program that generates the information I'm trying to convey, which is actually shorter than the information itself? (That's what I mean when I say "compressible".)

In short: sense and nonsense, order and chaos, or *information* and *randomness* are intricately linked. One could say that they are two sides of the same coin, and both concepts are related via something we call *entropy*.

Information implies structure and structure benefits from redundancy. The most ancient structures in nature have been adapted for survival by evolution. At the root of it is DNA, two chains that coil around each other to form a double helix. Symmetric, redundant information. The properties which allow DNA to survive and thrive are embedded in its processes: redundant structure, a copying mechanism that relies on this structure, the baked-in error correction which leads to four bases instead of two, etc.

Bitcoin, in comparison, is simpler: one chain, two bits, no error correction (information is copied perfectly). However, as with DNA, the properties which allow Bitcoin to survive (and thrive) are embedded in the replication process: a chaotic race to find new blocks, replication of blocks in the network, and replication of the software (and the ledger) on as many nodes as possible. Further, when we talk about the Bitcoin organism, error correction is equivalent to being alive. The network self-validates with every beat of the heart, every ten minutes or so. This is what makes the bitcoin organism extremely robust as well. It is *designed* for survival.

In Bitcoin, high entropy information is usually kept secret. Your *private key* should, as the name implies, be kept private. It is for your eyes only. Which particular *nonce* you just tried, i.e. the work you already did when mining a new block, is usually kept private as well. You don't want your competitors to know which numbers produce invalid blocks and can be skipped.

Chaos on the left, Order on the right.

Bitcoin utilizes both *order* and *chaos* to create a system that grows — and even thrives — between these extremes. It utilizes information asymmetry and an ingenious incentive structure which leads to a global competition to find Bitcoin's secrets.

Which processes are orderly, which are chaotic, and how Bitcoin is able to grow on the edge between order and chaos will be explored in the next section.

Growth between Order and Chaos

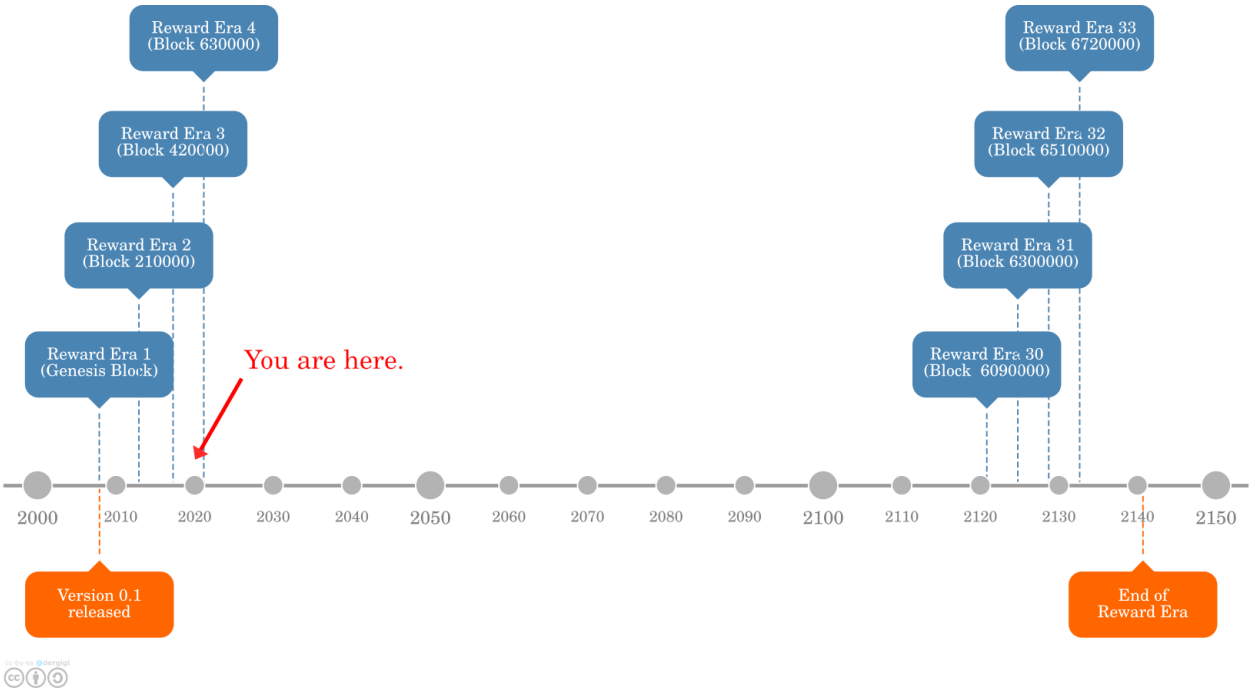
What makes the Bitcoin network tick? Again, there might be many answers to this question, but the only thing that is *truly* ticking in the Bitcoin network is the global clock: a *block clock*, where every block is one unit of time.

Currently, we call this process *mining* because new bitcoins are generated for every valid block that is *mined* (read: *found*). We call this the block subsidy, and it is an incentive structure to bootstrap the network.

In a sense, the Bitcoin organism "grows" on the edge between order and chaos: finding new blocks is a chaotic process, and its result is a very orderly list of transactions: the Bitcoin *block chain*, also known as *the ledger*.

From a "finding new blocks" point of view, we are still extremely early. Only ~10 years in. The block reward era will go on until the year 2140 or so, which means we are about 13% into the bootstrapping phase of Bitcoin: the reward era.

Satoshi undoubtedly knew that this was a long game. The era where fresh blocks are associated with a reward is only one phase of the Bitcoin game. Note that this phase is 6930000 blocks long. With an average block time of ~10 minutes, the reward era turns out to be 131 years long.



2019: Early days of the Bitcoin Reward Era

There will be a time where those who are tasked with finding new blocks are rewarded mostly via the networks' fee market, as Dan Held brilliantly argued in Bitcoin's Security is Fine. The point in time where the fee market takes over will be somewhere between the year 2020 and 2140. Either that, or Bitcoin will die, or some museum computers will try to find new blocks at an economic loss.

After this point in time, we will probably still talk about "mining" bitcoin, even though all the "miners" won't be producing any *new* bitcoins. All 21 million BTC — or 2,099,999,997,690,000 sats, to be precise — will have been mined. No new bitcoin will be added to the pool of existing coins in circulation.

Miners — if we still call them that —will still try to find new blocks, mind you. But the bitcoin moved by these blocks will have a long economic history. Gone are the days where miners award themselves new bitcoin in the *coinbase* transaction, to be spent after 100 blocks.

Will bitcoin still exist in 5000 years, and eventually beat gold as the de-facto money of humanity? I don't know, but important information is extremely hard to kill. I expect bitcoin to live for a very long time, just like ancient scriptures and religious texts survive to this day. It is just information, all of it, and it can transcend the medium it is printed on.

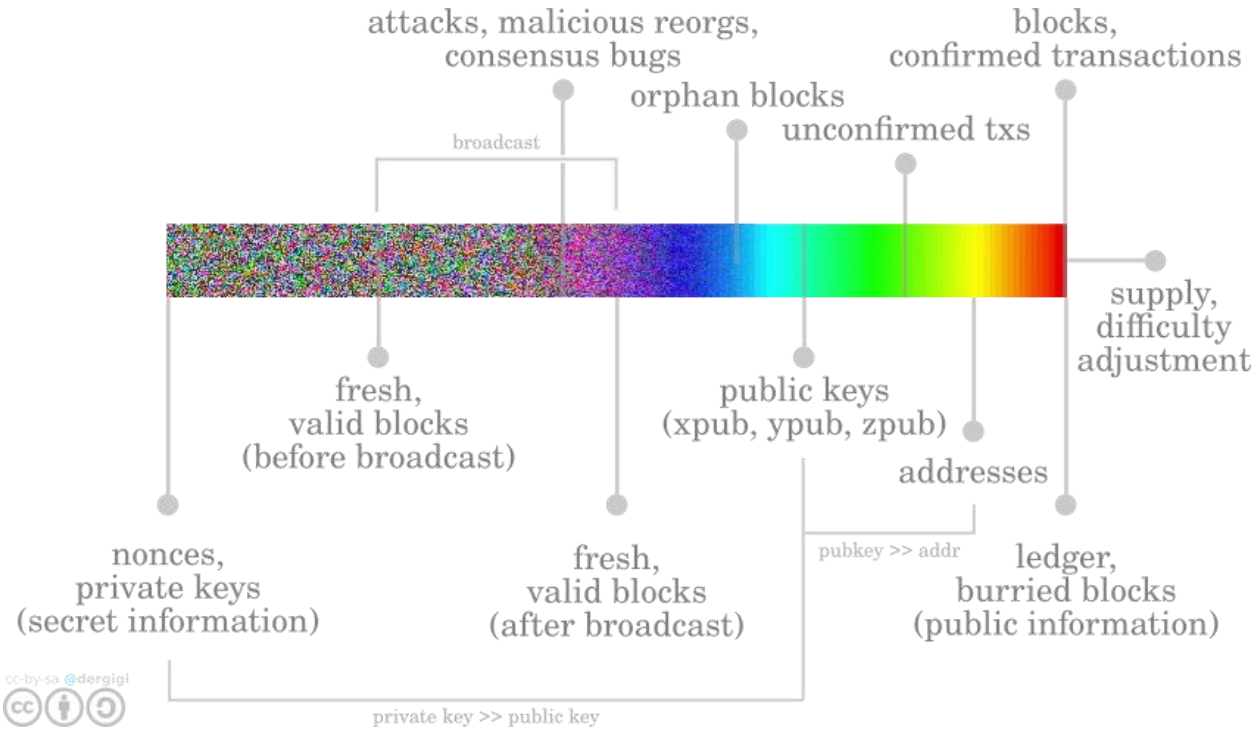
Of course, I expect something approximating hyperbitcoinization to have happened until this point. We will have a circular bitcoin economy, and bitcoin banks will globally settle vast amounts of value between them. What private citizens — or sovereign individuals, to use a more fitting term — will

use is yet to be seen. I doubt that the bitcoin base layer will be used by persons like you and me. And that's perfectly fine.

With the stage set, and concepts like order, information, randomness, and entropy in mind, let's take a look at some bitcoin concepts. We will distinguish them visually: from chaotic (left) to orderly (right).

Bitcoin grows between order and chaos.

While the framing of order and chaos is useful, it is neither precise nor universally applicable. However, I believe that thinking about the parts which make Bitcoin tick in this way is a helpful exercise, and I believe that the core point — that bitcoin lives, grows, and thrives on the edge between order and chaos — is profoundly true.



Let's ponder on these concepts for a bit.

- **Private key:** Chaotic information, very high randomness. Secret information which is best kept private. Maximum entropy for maximum security. If your private key is not random, you're gonna have a bad time.
- **Nonce:** Chaotic information, high randomness. A nonce is a specific number. Miners are in constant competition to find the next nonce which produces a valid block. Multiple numbers might fit the criteria, but the mining process is very much like finding one random number.
- **Fresh block (before broadcast):** Newly found blocks are the outcome of the chaotic process which is finding a nonce. Before blocks are broadcast, blocks can be understood as secret information. Fresh blocks can be ambiguous, since multiple blocks can form a valid chain tip at the same time. It is in your best interest to broadcast a fresh block immediately to everyone to reap the reward. Fresh blocks are only held back if you are an attacker, or very stupid, or both.
- **Chain tip:** Forming the chain tip is a process which is mostly orderly, but again, it is generated by a chaotic process. As mentioned above, the chain tip can be ambiguous. One version of the chain tip will survive, the losing versions will become orphan blocks. You can validate the correctness of all information in all blocks up to the chain tip. The chain tip reflects the current time in Bitcoin.
- **Orphan blocks:** Orphan blocks are part of the orderly, natural growth process of the Bitcoin block chain. Valid blocks are discarded on a

regular basis. If two valid blocks are found at roughly the same time, they fight a probabilistic battle for survival. In the long run, only one block can win this race. The losing block will become an orphan block and die a lonely death.

- **Unconfirmed transactions**: Orderly structure which can be easily validated. An unconfirmed transaction can be valid or invalid. Valid transactions are included in blocks based on economic incentives, which is — again — a probabilistic, market-driven process. Invalid transactions are discarded.
- **Buried blocks:** Orderly structure generated by a chaotic process, some time ago. The possibility of a *reorg* (re-organization of buried blocks) becomes exponentially unlikely because the probabilities against it multiply. Example: if every block has a 50% chance to reorg, the chance of a 6 block reorg would be 1.5%. Actual numbers are closer to 0.31% per block and 0.0000000000008875% for a 6 block reorg.
- **Confirmed transactions:** Orderly structure which can be validated very easily. Irreversibility is probabilistic and dependent on block height. Once a transaction is confirmed, it becomes more final the deeper it is buried in the block chain.
- **Public keys:** extended public keys (xpub, ypub, zpub) are generated by a deterministic process from a random seed — your private key.
- **Block time:** Valid blocks are found, on average, every 10 minutes. This is what makes the Bitcoin network tick. Bitcoin's heartbeat is extremely regular when measured in blocks. While still regular when measured in human time, mining is a fundamentally probabilistic process, and thus there is a real possibility that some blocks are found very quickly or comparably late.
- **Difficulty adjustment:** While the difficulty adjustment is a very orderly process, it can be a bit chaotic if hash power changes drastically (as it did in August 2017, because of the contentious bcash hard fork). Difficulty adjustment is based on block time, which is only probabilistically linked to human time.
- **Bitcoin supply:** Bitcoin's supply is fixed since its inception. The issuance of new bitcoin is embedded in Bitcoin's consensus code and is thus virtually impossible to change.
- **Whole ledger, deeply buried blocks (aka the Bitcoin block chain):** Orderly, sequential, structure which is pretty much unambiguous up to the chain tip and can be validated by everyone.
- **Ledger validation:** Validation is an orderly, sequential process. The outcome of this process is a simple boolean value for each block: true or false, valid or invalid. Every node arrives at the same block height independently, which is what forms Nakamoto consensus.

The fact that all of the above, the whole machinery, works in concert to provide a *yes* or *no* answer to the question *"Is this what actually happened?"* will never cease to amaze me.

Let me repeat the above. The whole purpose of the Bitcoin organism is to decide *what* happened *when* to *whom*. How much does everyone have, and how did this come to be? The *how* is important, because it allows everyone to audit everything, and come to the same conclusion.

In short, Bitcoin utilizes chaotic processes (mining, private key generation) and information asymmetry (public information which is widely shared, secret information which is not shared at all) to build up a structured, orderly, and permanent record, that can be audited and verified by everyone.

This is Bitcoin. This is Nakamoto consensus. This is the innovation, and this is also what makes bitcoin the best and hardest money that ever existed on planet earth.

You might call it open, permissionless, borderless, neutral, censorship-resistant, public, sound, antifragile, and a couple of other adjectives.

I call it Life. And we all call it Bitcoin.

The Bitcoin Times Ed 2 is the collaborative work of 8 writers & 1 designer with the intent to educate, inspire and spread ideas on bitcoin.

Each section will be released on Medium as a free long form article, and the full, compiled version of the Bitcoin Times will be available for free at the link below. In 2020, we'll release a limited edition hard cover collectible, for purchase, which you'll be notified of by email if you download the free pdf.

If you found value in this or any of the other essays and articles, please support each of the contributors by sharing it out & following their work.

Download the full guide at:

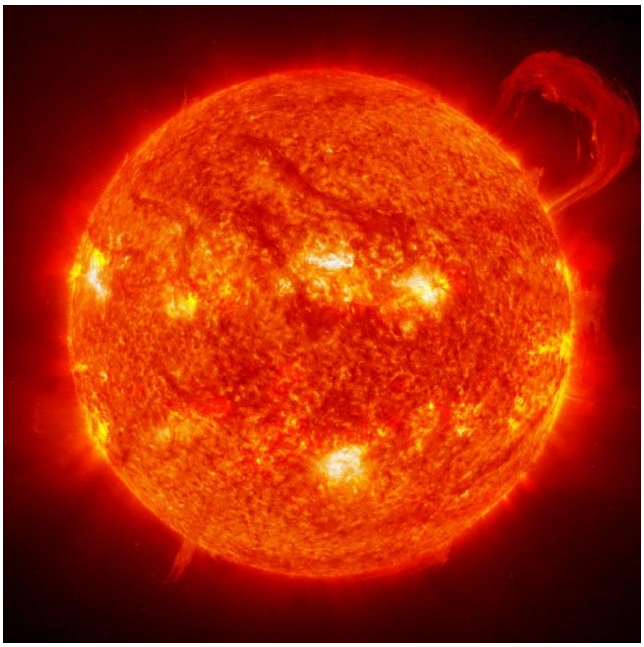
The Bitcoin Times

(Soon to be updated to: https://bitcointimes.news)

Proof-of-Work, The Fundamental Laws of Physics And Nature

By Rory Highside

Posted December 25, 2019



Almost since the dawn of Bitcoin, there has been a hot debate over the value of **Proof-of-Work** in cryptocurrency systems, and whereby the apparent ***wasteful*** use of energy by Bitcoin to secure its system will one day destroy the Earth. Unfortunately, there still remains a basic misunderstanding of the value of this Proof-of-Work, and the fundamental relationship to energy and work that makes up ***any*** and ***every*** system in the known universe.

One of the least understood and oft-cited technologies of this crazy universe is the emergent complex system called Bitcoin, and thus by extension, the intrinsically linked Proof-of-Work that drives the engine under its hood, metabolising raw energy as its life force.

There are many ways to describe **Bitcoin** the system, **bitcoin** the product, and the relationship to the underlying **Proof-of-Work**, but an overview of how the Bitcoin system functions at a high level is;

“The network timestamps transactions by hashing them into an ongoing chain of hash-based proof-of-work, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power.”

- Satoshi Nakamoto, The Bitcoin Whitepaper

The idea of Bitcoin was to create a reliable, decentralised network, upon which all transactions could be recorded & stored, that was able to be

validated by anyone. The issue was: how do you manage a ledger of transactions amongst a globally distributed database, entirely without a central point of failure, with a set of users who ***may*** or ***may not*** be known to each other, in a potentially adversarial environment, all the while ensuring that consensus is practically ***always*** achieved?

The answer to this equation fundamentally lies in a unique method of solving the "**Byzantine Generals Problem**", a thought experiment proposed while designing fault-tolerant consensus systems to accurately replicate the state of systems in aircraft.

Consensus & The Byzantine Generals Problem

Fundamentally, reliable computer systems must be able to handle malfunctioning components that can give conflicting information to different parts of the system.

This is exponentially harder when you begin to network multiple computer systems, across a distributed network, particularly when there is no "lead" or "authority".

"This situation can be expressed abstractly in terms of a group of generals of the Byzantine army camped with their troops around an enemy city. Communicating only by messenger, the generals must agree upon a common battle plan. However, one or more of them may be traitors who will

try to confuse the others. The problem is to find an algorithm to ensure that the loyal generals will reach agreement."

- The Byzantine Generals Problem, Leslie Lamport, Robert Shostak, and Marshall Pease

In distributed computing, consensus protocols are used to achieve accurate state machine replication. A state machine simply being a mathematical model of computation, and state machine replication is the general method of implementing a fault-tolerant process to replicate these computing 'states' globally in a distributed system.

The Bitcoin blockchain is simply a time-stamped record of ***all*** state transitions, and the network itself is a decentralised time-stamp server, stamping the first transaction to spend a coin to solve the issue of double-spending in a system without a central coordinator.

Nakamoto consensus,the protocol created by Satoshi Nakamoto, achieves its solution to the Byzantine Generals Problem by utilising Proof-of-Work to provide an economic cost to becoming the leader i.e. the network participant that may, providing all rules are followed and consensus is achieved, update the state of the Bitcoin blockchain.

To update the state of Bitcoin, miners must first compete via Proof-of-Work to find the solution to a cryptographic puzzle that abides by the rules of the system, with the winner of this race becoming the newly appointed leader. Once found, the leader must then update the state in a way that conforms to all of the consensus rules of the system, or else it will merely be rejected by all other participants.

Proof-of-Work and Competition

Proof-of-Work ultimately makes this process cost-intensive, and makes the mathematical odds of becoming the chosen leader _completely _random and indeterminable. Nakamoto Consensus follows the chain of work with the most accumulated Proof-of-Work as a key consensus rule, aiding in the self-organisation of the Bitcoin system. Participants are economically incentivised to be honest, as adversaries who attempt to create inaccurate states merely waste resources attempting to defraud the system.

Proof-of-Work economically incentivises Bitcoin to become the ultimate arbiter of truth.

By utilising Proof-of-Work for ***both*** the security ***and*** the issuance mechanism, the Bitcoin system leverages the "selfish gene" that all living species have, in

order to create a system that comes to collective agreement, whilst still working competitively. Bitcoin is the sum of its many subsystems, united to create a combinatory system; one that is led by Darwinian fitness in an elegant energy transforming race to secure its network, whereby in return for participation, miners are rewarded with (₿) bitcoin.

The product of this work, (₿) bitcoin, is exchanged for the trust and security that these miners deliver to the overall Bitcoin system, which becomes increasingly antifragile (and thus increasingly fitter) as these security network effects compound.

Miners, the warriors at the front line of Bitcoin's defence system are evolutionarily fit to protect its value. They work hard securing the network, the state of its ledger, and the distributed timestamp server via an energy intensive exercise, hence they deserve to be paid accordingly for providing this impenetrable wall of thermodynamic potential. That this work is increasingly hard makes it unlikely that an adversary could outcompete the cumulative work provided by the honest, cooperative majority.

The symbiotic relationship miners have with Bitcoin forms a system that's whole is greater than the sum of its parts; the apex Proof-of-Work collective.

Why Proof is Important

Work exists in every and all systems known to man, and the fundamental constant of the universe is that this work ***always*** requires energy. Energy is merely the ability to bring about change i.e. ***perform work***. The more energy

that exists in a system, the more thermodynamic potential, or simply put, the more useful work we can perform, hence the more value it can provide.

It is therefore a universal truth that all work has a measurable cost of energy transformation due to the very nature of the universe, and the laws of thermodynamics. It is with these laws that we underpin Bitcoin's Proof-of-Work.

Proof-of-Work is the unforgeable record of expended time and resources, therefore we can define Proof-of-Work as merely demonstrated **proof-of-time-and-resources**. This expenditure of time and resources subsequently give us a simple mechanism to measure production cost by, and whereby to secure and distribute the product of this work. It is through this procedure that we enact what we can describe as **unforgeable costliness**:

(1) find or create a class of objects that is highly improbable, takes much effort to make, or both, and such that the measure of their costliness can be verified by other parties. (2) use the objects to enable a protocol or institution to cross trust boundaries"

- Nick Szabo, Antiques, Time, Gold, and Bit Gold

Providing proof of this work creates an unforgeable record of expended energy utilised to secure, and to remove entropy from within the Bitcoin accounting system. Bitcoin metabolises this provided energy to make its heart beat roughly every ten minutes. Upon this beat, that is, the finding of a new block, Bitcoin broadcasts its latest state to all nodes in the network, flooding the system with the latest block like a virus, until all nodes reflect its current state.

The result of Bitcoin's redundancy in state being duplicated tens of thousands of times across the entire planet, is to make an almost completely impervious, and indestructible system. One that could survive even a nuclear holocaust. Bitcoin is the unkillable cockroach that may outsurvive mankind itself in some form. Wherever even a single copy of Bitcoin exists, the network can yet again be bootstrapped, however difficult the process may be.

Bitcoin: a self-expanding, self-replicating, self-organising, nuclear-proof, distributed accounting system for the digital-age.

Energy

Energy is the unit of all life, the constant that is utilised within all systems to perform useful work, it is the fundamental currency that all life transacts with. This energy is a necessary tool utilised in the act of rearranging matter and

information. All energy is bound by the unflinching laws of thermodynamics, meaning energy can never be destroyed, merely transformed.

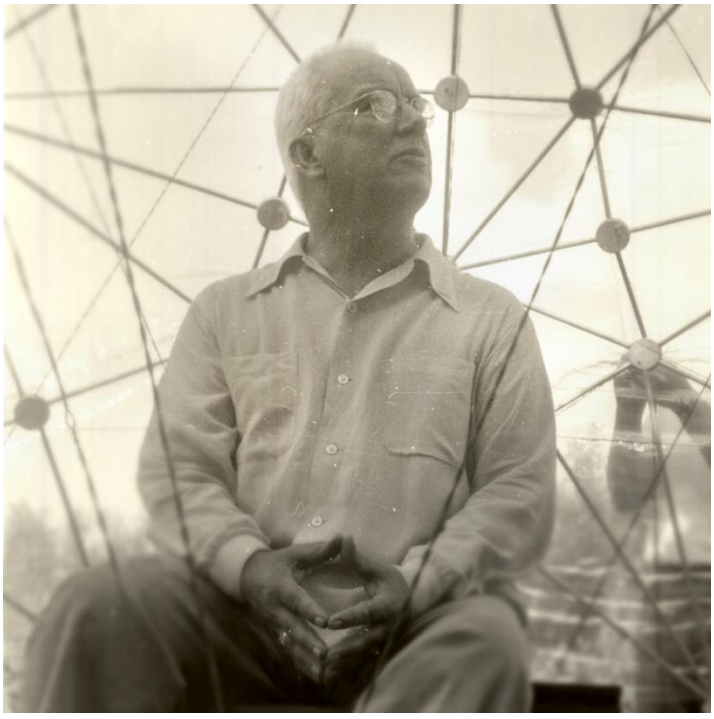
That work must have a measurable energy cost is due to these inherent laws of the universe, physics, and the laws of thermodynamics. These absolute, universal laws mean there is no such thing as a free lunch…ever. Therefore, we can demonstrate Bitcoin is secured via proof of the undeniable laws of thermodynamics that bind our universe, eating energy to sustain its metabolism, transforming information, proliferating, and self-organising its system.

“Bitcoin is the first example of a new form of life…It lives and breathes on the internet. It lives because it can pay people to keep it alive. It lives because it performs a useful service that people will pay it to perform. It lives because anyone, anywhere, can run a copy of its code. It lives because all the running copies are constantly talking to each other. It lives because if any one copy is corrupted it is discarded, quickly and without any fuss or muss.”

- Ralph Merkle

World Kilowatt Dollars

The great futurist and scientist Buckminster Fuller wrote of an energy backed currency in his novel Critical Path in 1981, with a prophetically accurate description of the DNA within the Bitcoin system.



“In this cosmically uniform, common energy-value system for all humanity, costing will be expressed in kilowatt hours, watt-hours, and watt-seconds of work. Kilowatt-hours will become the prime criteria of costing the production of the complex of metabolic involvements per each function or item. These uniform energy valuations will replace all the world’s wildly intervarying, opinion-gambled-upon, top-power-system-manipulatable monetary systems. The time-energy world accounting

system will do away with all the inequities now occurring in regard to the arbitrarily maneuverable banker-invented, international balance-of-trade accounting"

- Buckminster Fuller

Bitcoin Time-Energy Accounting and Thermodynamics

The Proof-of-Work under the hood of the Bitcoin security and rewards system provides one of the most powerful, *albeit novel* uses of modern cryptographic and computing technology; utilising modern silicon and consuming vast sums of energy to find a cryptographic needle in the haystack that can ***never*** be forged or simulated.

Miners race to find this exponentially difficult and unforgeable hash collision that is less than, or equal to the current target of the network. The subsequent rate of this computation effort we can define and measure is known as **hashrate**.

Hashrate (Hash per second, **H/s**) in Bitcoin is an SI-derived unit (i.e. derived from the base units specified by the International System of Units) representing the number of double SHA-256 computations performed in one second. The **H/s** unit is also part of a common measure of a Bitcoin miner's electric efficiency in the term watts**/TH/s**, denoted as **W/TH/s**.
One **watt** being exactly equal to one **joule/s** (more on this later), a measure that can also be expressed as **J/TH** i.e. **joules** per **trillion hashes**.

As of 2019, a current-generation Antminer S17 Pro has an efficiency of **49.5J/TH**, and this efficiency will likely continue to increase with time as technology progresses — although note that we are currently entering a maturation stage of ASIC design, whereby we begin to approach the law of diminishing returns, and the physical limitations of chip design due to electrical resistance approaching smaller nanometer scales.

In October 2019, the Bitcoin system was secured by a seven-day-average of **98 Exahash** of computation, that is a combined global hashrate of **98 Quintillion H/s**, or **98,000,000,000,000,000,000 H/s.** Although constructed for a very specific task, to put this in comparison to modern supercomputers, the fastest computer in the world is currently the IBM Summit at 200 Petaflops, while the Bitcoin network is currently hashing at a speed of 80,704,290 Petaflops, *more than **four hundred thousand** (400,000) times faster.*

SHA-256 hash results are pseudo-random, meaning they give the same result for the same input, but by changing the input even slightly, we will get a completely different and unpredictable (**pseudorandom**) result. Only by

miners finding a low enough hashed value in the pseudorandomness, and constructing a valid block meeting all consensus protocol rules, will your block be accepted by the Bitcoin system and net the product of the block reward; the sum of the current block subsidy (**nSubsidy**) and transaction fees(**nFees**).

The result is a new block containing transactions that are mined roughly every ten minutes, updating the global Bitcoin state, thereby returning the state to zero (or as close to) entropy. The artefact of this state change is the Bitcoin blockchain (**time-energy-chain**) and bitcoin(**time-energy**).

The whole is much greater than the sum of its parts, the self-reinforcing Bitcoin system of rewards is a conglomerate of subsystems ultimately responsible for creating and securing a self-replicating, self-organising, sovereign, **time-energy world-accounting-system**.

We can describe the complex self-organising Bitcoin system as such;

Bitcoin's network is secured by a process called Proof-of-Work more commonly known as mining. Mining is merely the computation of cryptographic hashes by specialised mining hardware to solve an unforgeable puzzle. The double SHA-256 hashing utilised for this function also underpins the Bitcoin block structure, with each transaction having a

corresponding hash that is itself hashed (sometimes several times) together to form the Merkle root contained inside the block header. This header is utilised within the cryptographic computational puzzle they seek to solve, and contains the header of the previous block, therefore linking each block together cryptographically, making forgery probabilistically impossible without employing the energy required to perform a full rewrite.

The produced hashrate results in the transformation of **energy** and **time**,*or* ***work***, at which cost we can measure in **joules**. Energy is transformed in Bitcoin's perpetual quest to remove entropy from, secure, and replicate its state in perpetuum.

In this entirely decentralised system there is no central-authority, instead the nodes form a decentralised agreement (consensus) through a protocol that hinges upon Proof-of-Work to secure it. The Proof-of-work functions as Sybil resistance for the network by making changes to the ledger artificially expensive, and creating a scenario where attackers would have to irrationally spend excessive amounts of time and resources to compete against the honest majority of miners.

Sybil Attack: is where an entity creates false identities (or nodes) within a system in an attempt to gain influence over the network. A network's vulnerability to sybil is determined by how cheaply you can create these identities.

Proof-of-Work secures and provides the energy to fuel the self-organising, self-replicating energy metabolising network, creating part of a feedback loop of network effects that sustains its proliferation.

The cumulative work process progressively hardens the system's security, building a digitally represented, impenetrable fortress of thermodynamic potential, that not only thwarts would-be adversaries, but converts them into supporters of the bitcoin **time-energy** accounting system.

As each successive block is found, the proof of this work compounds and crystallises into time, resulting in the artefact called the Bitcoin blockchain, the product of the miner's hash computations and the network's consensus rules; a secure, verifiably accurate, cryptographically-linked chain of blocks, transactions, and accumulated work dating back to the genesis block.

You can visualise this as a cryptographically linked **time-energy-chain** stretching back to genesis i.e. time zero, the creation of the first block. The Bitcoin system self-organises by determining that the correct chain is the one with the most cumulative Proof-of-Work meeting its inherent consensus rules, making a successful attack's requirement to meet this cumulative

work, and thereby becoming increasingly difficult as the network effects grow in mass and value.

Emission Schedule

The Bitcoin system from its inception at the genesis on 2009–01–03 was given an emission rate of exactly 50 bitcoins per block subsidy, delivered at roughly once *every* 10 minutes to miners via the block reward; the product of the block subsidy and transaction fees(**block reward** = **nFees** + **nSubsidy**).

The half-life cycle of the **nSubsidy** is once every 210,000 blocks (roughly 4 years), at which time **nSubsidy** emission rate is reduced by a factor of one half. This emission decay process continues each half-life cycle until no more bitcoin are produced at the absolute limit of 21,000,000 units.

At this point of maturation in the Bitcoin life-cycle, only **nFees** remain as the economic incentive to mine, and thus Bitcoin's gravity must increase accordingly to sustain this economic system, with only transaction fees subsidising hashrate by roughly 2140. This monetary policy is intrinsic to Bitcoin and hardcoded into the system to remain entirely immutable, and impenetrable to top-down control.

The Bitcoin Metabolism

The thermodynamic potential and the subsequenthashratesecuring the systemhas a direct relationship with the Bitcoin mining difficulty; as the hashrate rises or falls, thus does the security and difficulty to mine a block. This mechanism produces a stabilisation effect on block times, and creates a network that self regulates its metabolism *i.e.* ***the rate of which it produces blocks and consumes energy.***

Every 2016 blocks (roughly two weeks) the difficulty adjustment algorithm regulates based on the average hashrate of the prior 2016 mined blocks. This results in Bitcoin creating a predictable issuance of roughly ten minutes per metabolic cycle, or six cycles per hour i.e. when each subsequent Proof-of-Work puzzle is solved. The subsystem controlling this cycle could therefore be considered the internal Bitcoin metabolism, keeping its metabolic rate, or heartbeat, ticking along to roughly every ten minutes, regulating its production in perpetuum.

This halflife and metabolic rate creates a stock-to-flow of bitcoin that is entirely predictable, and with the subsequent hard limit to production, the bitcoin produced is the most verifiably scarce commodity to ever come into existence. The requirement of ever additional energy and timeto produce the same result as competition increases bolsters both the systems security, and its hardness_ i.e. _***the difficulty at which it is to produce***.

The sum of Bitcoin's mining difficulty system and its hardcoded monetary policy giving it an absolute scarcity combine to produce unforgeable-costliness.The culmination of this security and incentives model is Bitcoin, a cryptographically secured system of rewards that gives us an ability to abstract time and energy_, _thereby store, trade, or transport it through time and space securely in the digital-realm, forever along **the Bitcoin system's time-energy-chain**.

The product of this unforgeable thermodynamic energy transformation(or work performed) to secure the **Bitcoin** network is **bitcoin(₿)**: *a digital commodity that is granularly divisible, fungible, incorruptible, transportable, and counterfeit-proof, with an absolute scarcity of* ***21,000,000 ₿ units***.

Part 2

Why Thermodynamics Matter and Matter's Thermodynamic

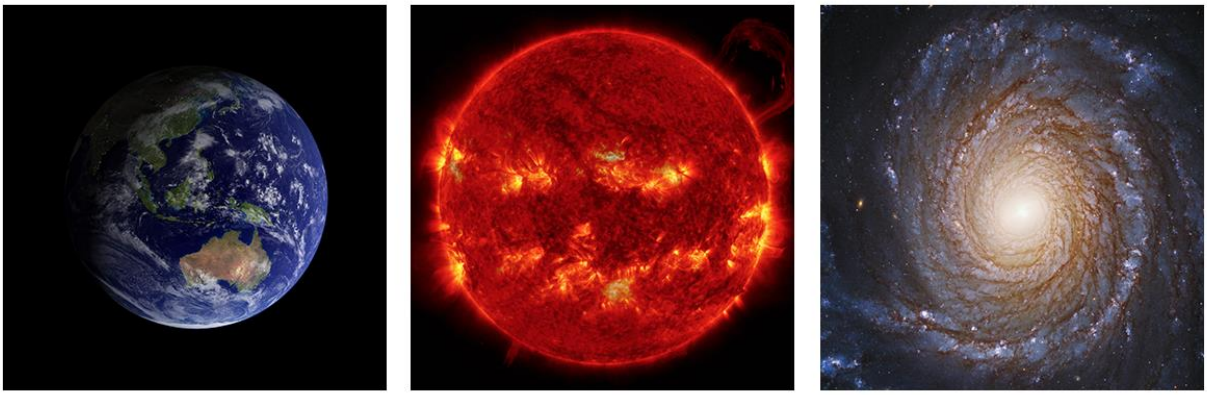
In the first half we covered the scientific processes in the Bitcoin system and its energy use, in this half we will relate this to physics, thermodynamics, and the universe around us...

Energy Of The Gods

Energy is the currency of life, the fundamental key to everything, at all scales of the universe. The macro progress of civilisation, the Kardashev scale, is merely a scale to measure a civilisations total potential **energy**capture. Therefore, it makes logical sense that the monetary system of a technologically evolved type I civilisation is fundamentally based on the construct of codifying **energy**, **time,** and **cooperation**. We cannot begin to approach a Type I civilisation without shifting our collective thinking to a universe of post-scarcity.

It's evolution baby...

Bitcoin, the apolitical time-energy-chain is the next logical step in human civilisations progression and social self-ordering, uniting the human race with self-interest and economic incentives by codifying **time**, **energy**, and **cooperation**, hardening Earth's resolve to act as one Spaceship. United we stand, divided we fall, destroying the earth with wanton destruction caused by burning fossil fuels.



TYPE I CIVILISATION
harnesses all the resources of a planet. Carl Sagan estimated that Earth rates about 0.7 on the scale

TYPE II CIVILISATION
harnesses all the radioation of a star. Humans might reach Type II in a few thousand years.

TYPE III CIVILISATION
harnesses all the resources of a galaxy. Humans might reach Type III in a few thousand to a million years.

Type I Civilisation: Is a civilization that can harness the entirety of the energy that falls on its planet from the parent star (for Earth-Sun system, this value is close to 7x1017 watts), which is more than five orders of magnitude higher than the amount presently attained on earth, with energy consumption at ≈4×1019 erg/sec (4 × 1012 watts)

- Wikipedia

What the hell has thermodynamics got to do with anything, especially Bitcoin…

To understand how these abstract concepts of thermodynamics, physics, Bitcoin, and Proof-of-Work gel together at the very genetic level, you need at least a cursory understanding of arm-chair physics and thermodynamics.

First, We Must Define Work

Work is merely the transfer of energy from one place to another, or from one form to another. To picture this, imagine that the universe is constantly at workaround us at the quantum, atomic, and even at macro scale. Energyis everywhere, and we can tap into this and harness ittoproduce useful work**,** products, information, or electrical energy (electricity).

The Joule of The Crown

One way we can measure the magnitude of this workis in joules_, *which is a derived unit of energy used in the International System of Units. _1*

kilowatt being *1000 watts _and _1 hour* being *3600 seconds*, therefore *1 kilowatt-hour* of electricity is equal to _3,600,000 joules _of energy.

1 joule is the energy dissipated as heat when an electric current of *1 ampere_passes through a resistance of _1 ohm _for _1 second*. This transformation of energy is can be described simply as the laws of physics and by extension thermodynamics.

First law of thermodynamics, or the law of conservation.

(Energy of a Closed System ΔU) = (Q / Heat) — (W/ Work)

Or

ΔU = Q — W

The first law of thermodynamics states the change in the internal **energy *ΔU*** of a closed **system** is *equal* to the amount of **heat** '***Q***' supplied to the **system**, *minus* the amount of **work** '**W**' done by the **system** on its surroundings.

The Second Law of Thermodynamics

In essence the second law states that *all* closed systems gravitate towards maximization of entropy (therefore is ever-increasing), energy ***must***be added to a system to overcome this natural tendency towards entropy.

Entropy = order and disorder

Entropy is simply the measure of the distribution of matter and/or energy, information, or, how spread out and disorganised it is. Energy is really only useful when it's ordered and clumped together, so the more concentrated and ordered(*or the lower the entropy*), the higher the potential energy output, therefore increasing its ultimate usefulness to perform potential work.

Yeah, Science!

Essentially thermodynamics means you can ***only*** ever get as much out as what you put in, and you can ***never*** get as much out as much as you put in**.**

One of the principles that guides the entire world around us is the law of conservation. This simply means the unflinching law of the universe is that energy cannot be created or destroyed, and that it is ***always*** conserved and transformed. If workis performed, energy is needed and heat is an ***obvious*** and ***necessary*** side effect (just think of friction), while the total energyof a closed system is ***always*** conserved.

One way to think about how these laws apply to our natural reality is; the universe is a closed system, and that the entropy of the universe is ***always*** increasing. The heat of the universe is dissipating, so the total energy stays constant. Therefore there is no such thing as waste in the universe system, only transformation.

We are all ***always*** in a constant fight with entropy, and the ultimate boss battle ends in the heat death of the universe. Heat is merely a form of kinetic energy we can measure in kelvins (K), *or,* heat is merely energy in transit. Absolute-zero (0 K, or −273.15 °C) is the lowest theoretically possible temperature on the thermodynamic temperature scale, where all thermal motion ceases, thus no heat energy remains.

The heat death of the universe is just such high entropy, that the energy is spread so far apart and is no longer useful for ***anything***. It's not absolute zero, but no more work, no more movement, no more life. Don't worry it's 10^{100} years away, but at this point in time there no longer remains enough heat energy to increase entropy. Time, the arrow that is the natural artefact of the universe's entropy stands *utterly* still. **Finito**.

Chaos And Order

Both energy and information are both infinitely more useful when neat and ordered ie. when it has low observed entropy. This is why the conversion of energy from sources such as fossil fuels has *radically* advanced our society, enabling the exponential expansion in networks of cities and economies.

Fossil fuels are burnt, transforming them into heat, this thermodynamic transformation of energy then powers giant mechanical steam turbines, the product of this mechanical work is in turn converted into electricity, and finally this electricity is delivered to your home as a useful product for your myriad of electronic devices. Science!

As this energy travels over long distances there is substantial amounts of entropy_, _this is due to the resistance and conductivity of metal creating heat and energy loss resulting in thermodynamic transformation. Electric energy (electricity) is merely useful energy that is transportable over _somewhat _long-distances.

Smashing The Coulomb barrier

Entropyis all around us and it requires vast energyto fight against its natural inclination to continually increase. This insane human fight against entropy to unlock thermodynamic potentialis what will catapult us into the future, as humanity begins to not only harvest vast ambient energy, but eventually also mass-produce fusion reactors.

In order to achieve nuclear fusion, particles must first be able to overcome the electric repulsion labelled "**The Coulumb Barrier**", named after physicist Charles-Augustin de **Coulomb.** In order for a nuclear strong force to take over and undergo nuclear fusion, particles must first break this barrier. This new frontier of energy production will provide the required energyto smash the Coulomb barrier en masse, capturing the Earth system's abundant stored clean thermodynamic potential, and scaling our energy production exponentially.

Spaceship Earth must work together as one if we are ever going to overcome the devastating pollution that we have created in the Earth's system, and to solve the immediate engineering challenges clean energyproductionposes. Scarce resource-based energy creates a vast number of security and scarcity issues plaguing the dove and hawk geopolitics of the world, not to mention the burning of these resources threatens our very long term existence.

We have to believe in a world of abundance and not one of scarcity. Earth needs to band together to tackle the socio-economic challenges our shared world is facing, and cooperate in the race to clean up a damaged planet that we have needlessly abused with fossil fuels and wanton destruction.

Energy use is not the root of the systemic problem, energy is the currency of life that fuels the advancement of all civilisation. The current unscalable, destructive, pollutant paradigm of scarce fossil fuel burning for energy creation is the multi-trillion dollar problem plaguing mankind. We must cooperate to solve it.

Energy + Time + Cooperation

Bitcoin is an apolitical monetary system that codifies **time**, **energy** *and* **cooperation**, incentivising the human race towards ***maximal efficiency*** of the potential capture and conversion of energy into usable forms. The act of harnessing the abundance of our universe, fusion energy, the power of the stars and the gods. Fusion energy harnessed will catapult us towards the heavens as a civilisation, aiding as humankind begins our rapid ascent to interstellar demigods.

There Is No Such Thing As Scarcity, Only Thermodynamic Potential and The Arrangement Of Matter And Information

In theory, all states and distribution of matter are replicable, at the atomic and subatomic level, all matter is merely information and energy distribution. The deconstruction and reconstruction of matter is a technological problem, once solved (we're working on it), there _will be _no longer a scientific absolute scarcity of any element in the universe. Through technological advancement, all matter will be able to be rearranged, therefore all matter and energy ***is abundant.***

Only unforgeable digital scarcity can be absolute, therefore, only time and energy and the sum of their product have any quantitative value. Digital scarcity, the ability to remain unforgeable is the only scarce product of creation known to man.

Cambrian Abundance

The competitive need forefficient energyconversion_, _and the markets insatiable demand to trade will create a Cambrian explosion of abundance and creativity. An apolitical '***energy renaissance***' driven by the free market demand to unlock thermodynamic potential.

Post-scarcity will bring about the cooperation of humankind as Spaceship Earth. The *entire* world should be radically increasing the efficiency of energy capture, and total consumption of energy to produce ***useful work***, not seeking the reduction of total energy consumption per capita through

draconian taxation measures. We ***can*** lean into a Type I civilisation and beyond without destroying ourselves in the process.

Advance humanity to the next level by cooperating, or burn the earth to the ground around us with fossil fuels.

The Self-Replicating, Self-Organising Bitcoin System

The Bitcoin system mechanisms are designed to self-replicate and self-organise, while its consensus protocol ensures replication is accurate, and that it's perpetually trying to remove entropy from the state of Bitcoin; the artefact being the resulting blockchain and the product bitcoin.

The essence of the complex systems singular role is to be an arbiter of trust and truth in the face of adversity, to create a singular distributed current and historic state and orderthat *all* nodes can reach consensus upon. Zero entropyis the ideal state of the system. This entropy is instead moving to the growing unspent transaction outputs (UTXO) stored in the blockchain.

In the digital realm, the cost to rearrange information generally trends toward decreasing on the macro scale as compute becomes more efficient, thus this process to remove informational entropy will become increasingly more efficient over time. The gravity of bitcoin is increasing over time, increasing its economic mass and density leading to an upwards trending efficiency in its system.

Much has been studied about Bitcoin's sustainability, though much is yet to be uncovered, but as Bitcoin's heartbeat rings out every 10 minutes from now until eternity, we will all be its students.

Satoshi Nakamoto in his infinite wisdom codified trustlessness, cooperation, energy, time, commoditised it, democratised its access, and made it transportable through space and time in perpetuum. The sovereign self-organising system is designed in such a way as to provide its own governance away from any top-down influence or corruption.

Bitcoin is the peak product of evolution in technology, pure capitalism, economics, and the beauty of thermodynamics, all working together in a state of perfect synergy. Bitcoin can bring about the apolitical time-energy world accounting system Buckminster Fuller prophesied, steering Spaceship Earth to a post-scarcity reality.

By Rory Highside Oct, 2019

The Bitcoin Times Ed 2 is the collaborative work of 8 writers & 1 designer with the intent to educate, inspire and spread ideas on bitcoin.

Each section will be released on Medium as a free long form article, and the full, compiled version of the Bitcoin Times will be available for free at the link below. In 2020, we'll release a limited edition hard cover collectible, for purchase, which you'll be notified of by email if you download the free pdf.

If you found value in this or any of the other essays and articles, please support each of the contributors by sharing it out & following their work.

Download the full guide at:

The Bitcoin Times

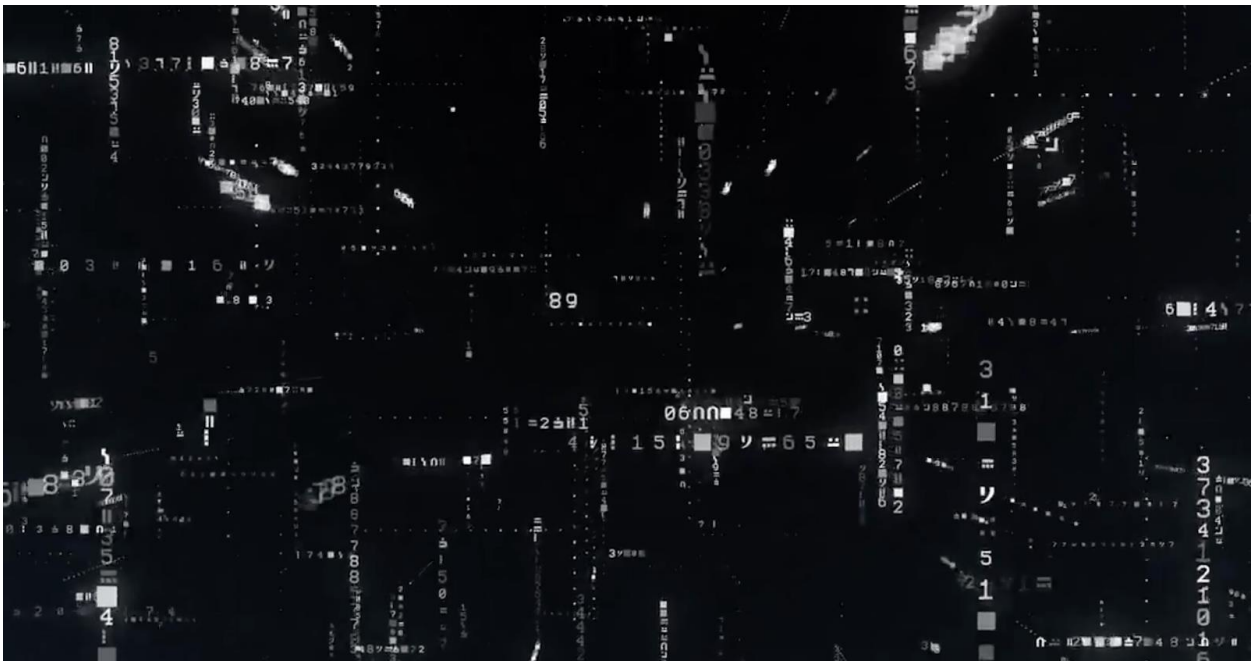
(Soon to be updated to: https://bitcointimes.news)

Information Theory of Money

By Dan Held

Posted December 27, 2019

Prices and the market are intricately intertwined



I recommend reading this article while listening to "Strix Aluco" by "Isan"

Prices reflect information

"In a free market economic system, prices are knowledge, and the signals that communicate information. Prices are not simply a tool to allow capitalists to profit; they are the information system of economic production, communicating knowledge across the world and coordinating the complex processes of production."

— Saifedean Ammous

Prices are the coordinating force of a free market system. Each individual decision-maker can rely on the prices of goods and services to help with their decision making, as the prices themselves are a distillation of all known market information into a single metric. In other words, the compression of all relevant data is ultimately manifested as price (for the more technie minded, it's a one-way hash function).

Each individual's buy and sell decisions, in turn, further shape prices that carry this altered information back out into the market. Some of you may

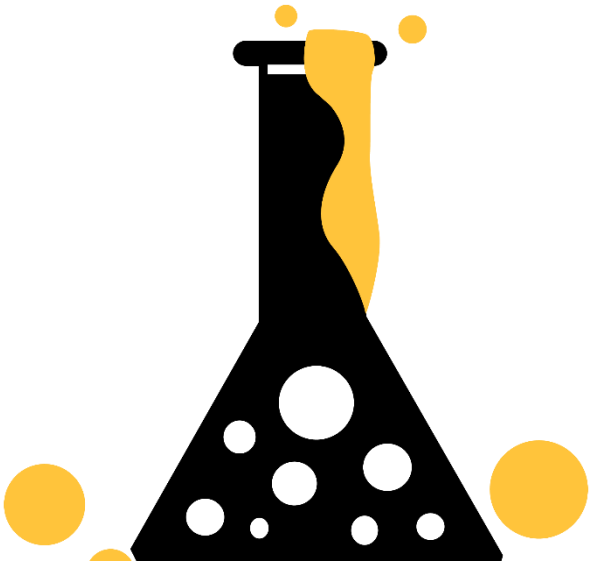
have heard of this from “Efficient market hypothesis” which is about how information in the market is reflected in the price of assets like equities.

Money is the measuring stick

“Money is the central information utility of the world economy. As a medium of exchange, store of value, and unit of account, money is the critical vessel of information about the conditions of markets.

Capitalist economies are not equilibrium systems but dynamic domains of entrepreneurial experiments. Money should be a standard of measure for the outcomes of entrepreneurial experiments.” — George Gilder

The essence of Capitalism is all about the efficient allocation of capital given the constraints of scarce resources and time. Companies are experiments on how to best allocate capital, and money is the standard measure for efficiency. Making money represents the efficient allocation of capital, losing money is not an efficient use of capital. And competition means decentralized planning by many separate companies and people to solve a problem in the market.



Capitalism, much like nature, is about experimentation

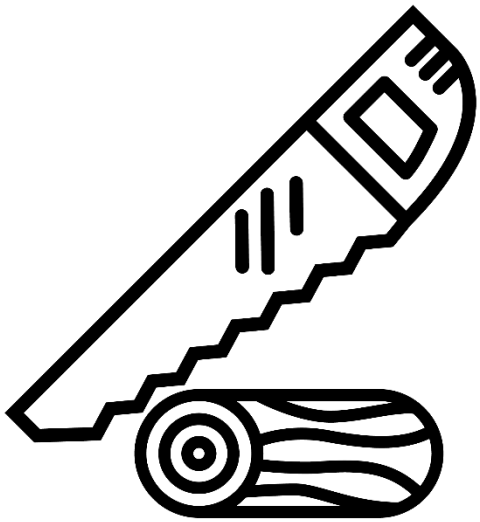
Information is Decentralized

“A centrally planned economy could never match the efficiency of the open market because what is known by a single agent is only a small fraction of the sum total of knowledge held by all members of society_” — Hayek (Hayek’s “Local Knowledge Problem”)

A decentralized economy thus complements the dispersed nature of information spread throughout society. Each company is an attempt to take the local knowledge that it has and create a good or service that ultimately is the correct capital allocation (aka profit).

To highlight how decentralized this information is, I’m going to give an example by Milton Friedman who made the statement: “There’s not a single person in the world who knows how to make a pencil:

- The wood comes from a tree
- To cut down that tree, it took a saw
- To make the saw, it took steel. To make steel, it took iron ore
- Graphite, comes from some mines in South America
- The eraser, which is rubber, probably comes from the tropics
- Or the yellow paint
- Or the glue that holds it together



There was no central planning office. It was the magic of the price system."

Praxeology. The study of Human Action.

Central banks have an unsolvable data problem

Central banks inherently have a data problem. There's an ingestion, processing, decision bottleneck — same as any electronic signal processing system. An economy cannot be planned by a central authority, because there is no way that a central authority can have all of the necessary knowledge to make the best decision at any single point in time, let alone all points in time.

"It is a problem of the utilization of knowledge which is not given to anyone in its totality" — Hayek

To operate effectively, central banks would have to ingest trillions of data points daily, and ingest those data points in a perfect manner which is impossible. Every single uber taken, every single sandwich purchased, every single in-app purchase.

"We need to believe we live in a predictable, controllable world, so we turn to authoritative-sounding people who promise to satisfy that need." — Philip Tetlock

We've created central banks because we want the world to make sense, and we want to feel that there is someone in charge. Even if we were able to ingest perfect data, it is hard to infer simple causality for this complex, chaotic system which involves billions of decision makers. While determining the relationship between weather and crops might seem easy, how do we determine the causality of burrito demand? Economics isn't like the sciences,

we are hamstrung by small or incomplete sample sizes. We can't re-run the Dot com bubble with a different central bank or a different President.

This brings us to how central banks measure impact and make decisions. There is a classic product saying that goes "If you can't measure it you can't manage it." It's hard to even measure a kilogram with extreme precision, so how could we possibly measure inflation properly? (ex: CPI excludes food and energy!)

"*Since big events come out of nowhere, forecasts may do more harm than good, giving the illusion of predictability in a world where unforeseen events control most outcomes (Aka black swan events)*" — Carl Richards

He goes on to say "*Risk is what's left over when you think you've thought of everything.*" Daniel Kahneman also has a great take on the dangers of using history as our guide:

"Hindsight, the ability to explain the past, gives us the illusion that the world is understandable. It gives us the illusion that the world makes sense, even when it doesn't make sense. That's a big deal in producing mistakes in many fields."

Here's a useful analogy: Essentially the Fed is driving the car, which is the economy, only using the rearview mirror which is foggy, and the front windshield is opaque (you can't see the future). How could the Fed possibly drive the car with any accuracy? What if we just let the car self adjust to the conditions of the road?

History cannot be interpreted without the aid of imagination and intuition. The sheer quantity of evidence is so overwhelming that selection is inevitable.

So what is our alternative?

Sound Money

"Sound money is the equivalent of scientific integrity: the system must not permit the manipulation of data after the experiment has taken place." — Adam Taché

Sound money keeps the ruler settings fixed so results cannot be altered by a centralized planning mechanism.

And Bitcoin is the perfect iteration of sound money. Bitcoin has a hard cap for several reasons: being a precise measuring stick, reducing political attack vectors, and encouraging speculative bubbles which act as a viral loop.

But why 21M? Why not 100M?

Here's the secret...***It doesn't matter!***It's precise length is irrelevant. What matters is just that there is a fixed amount. As economic activity moves from a primitive scale, it becomes harder for individuals to make decisions without having a fixed unit of account with which to compare value.

Regarding political attack vectors, Satoshi felt that setting a "proper" rate of inflation rate was impossible so he decided to remove human decision making from the process. Satoshi has two quotes regarding fixed supply that support this conclusion:

"Indeed there is nobody to act as central bank or federal reserve to adjust the money supply as the population of users grows. That would have required a trusted party to determine the value, because I don't know a way for software to know the real world value of things."

Satoshi also says

"If there was some clever way, or if we wanted to trust someone to actively manage the money supply to peg it to something, the rules could have been programmed for that."

Finally, Satoshi hypothesized that a fixed supply might create speculative bubbles.

"As the number of users grows, the value per coin increases. It has the potential for a positive feedback loop; as users increase, the value goes up, which could attract more users to take advantage of the increasing value."

Implications of Sound Money

Bitcoin is the ultimate safe haven asset. As more and more people buy into Bitcoin and that narrative, it becomes the de facto risk off asset.

Post hyperbitcoiniation, when Bitcoin is the SoV, MoE, and UoA, Bitcoin will reflect the most accurate "risk free" rate of return that we've ever had, which enables the economy and market participants to most efficiently allocate resources. Each market participant, both individual investors and corporations, make the risk on/risk off decision which is then manifested in Bitcoin's price.

And finally, when Bitcoin is the unit of account and used by every business, market participants can view the flow of funds of their suppliers and customers in real time via their publicly disclosed Bitcoin addresses. This transparency makes markets ultra efficient through the best processing of information.

Bitcoin rearchitects how capital is efficiently allocated in our economy, ultimately creating a world with more abundance and resources for all

By Dan Held, Nov, 2019

The Bitcoin Times Ed 2 is the collaborative work of 8 writers & 1 designer with the intent to educate, inspire and spread ideas on bitcoin.

Each section will be released on Medium as a free long form article, and the full, compiled version of the Bitcoin Times will be available for free at the link below. In 2020, we'll release a limited edition hard cover collectible, for purchase, which you'll be notified of by email if you download the free pdf.

If you found value in this or any of the other essays and articles, please support each of the contributors by sharing it out & following their work.

Download the full guide at:

The Bitcoin Times

(Soon to be updated to: https://bitcointimes.news)

Bitcoin Optech Newsletter #78: 2019 Year-in-Review Special

By Bitcoin Optech Newsletter

Posted DEcember 28, 2019

This special edition of the Optech Newsletter summarizes notable developments in Bitcoin during all of 2019. It's the sequel to our 2018 summary. This summary is based heavily on our weekly newsletters from the past year for which we reviewed almost 9,000 commits (nearly 2,000 merges), over 1,500 mailing list posts, many thousands of lines of IRC logs, and numerous other public sources. It took us 50 newsletter issues and over 200 printed pages worth of content to summarize all that amazing work originally. Even then, we missed many important contributions, especially from people fixing bugs, writing tests, performing reviews, and providing support—work that's critical but not necessarily "newsworthy." In summarizing even further and trying to compress the entire year into this article's handful of pages, we've now also omitted a great many other important contributions. So, before we continue, we want to extend our heartfelt thanks to everyone who contributed to Bitcoin in 2019. Even if the following summary doesn't mention you or one of your projects, please know that we at Optech—and probably all Bitcoin users—are more grateful than words can express for all that you've done to help Bitcoin.

Contents

    - OP_CHECKTEMPLATEVERIFY
- June
    - Erlay and other P2P relay improvements
    - Watchtowers
- July
    - Reproducible builds
- August
    - Vaults without covenants
- September
    - SNICKER
    - LN vulnerability
- October
    - LN anchor outputs
- November
    - Bech32 mutability
    - Bitcoin Core OpenSSL removal
    - Bitcoin Core BIP70 removal
- December
    - Multipath payments
- Featured summaries
    - Major releases of popular infrastructure projects
    - Notable technical conferences and other events
    - Bitcoin Optech
    - New open source infrastructure solutions

January

In January, Steven Roose proposed a standardized format for *proof of reserves* pseudo-transactions that bitcoin custodians can use to generate evidence that they control a certain number of bitcoins. No tool of this type can guarantee that depositors will be able to withdraw their coins from a custodian, but it can make it more difficult for a custodian to conceal the loss or theft of coins. Roose would go on to produce a tool based on Partially Signed Bitcoin Transactions (PSBTs) for creating reserve proofs and would follow through to see the specification published as BIP127.

February

In February, Bitcoin Core's master development branch saw the merge of the final set of PRs necessary for using it with the Hardware Wallet Interface (HWI) Python library and command-line tool. HWI would later see its first stable release in March, see Wasabi Wallet add support for it in April, and see BTCPay add support for it via a side package in November. HWI makes it easy for hardware wallets and software wallets to interact using a combination

of output script descriptors and Partially Signed Bitcoin Transactions (PSBTs). The increasing support in 2019 for standardized formats and APIs makes it easier for users to choose the right combination of hardware and software solutions for their needs rather than having to choose one solution or another.

Also in February, Pieter Wuille gave a presentation during the Stanford Blockchain Conference on miniscript, a spin-off from his work on output script descriptors. Miniscript provides a structured representation of Bitcoin scripts that simplifies automated analysis by software. The analysis can determine what data a wallet needs to supply in order to satisfy the script (e.g. a signature or a hash preimage), how much transaction data will be used by the script and the data that satisfies it, and whether or not the script passes known consensus rules and popular transaction relay policies. In addition to miniscript, Wuille, Andrew Poelstra, and Sanket Kanjalkar also provided a composable policy language that compiles down to miniscript (which itself converts to Bitcoin Script). With the policy language, users can easily describe the conditions they want to be fulfilled in order to spend their coins. When multiple users want to share control of a coin, the composability of the policy language makes it easy to combine each user's own signing policies into a single script. If widely adopted, miniscript could make it easier for different Bitcoin systems to work together to sign a transaction, significantly reducing the amount of custom code that needs to be written in order to integrate wallet front-ends, LN nodes, coinjoin systems, multisig wallets, consumer hardware wallets, industrial Hardware Signing Modules (HSMs), and other software and hardware. Wuille and his collaborators continued working on miniscript through the year, subsequently requesting community feedback and opening a PR to add support to Bitcoin Core. Miniscript would also be used by LN developers in December to analyze and optimize several new scripts for upgraded versions of some of their onchain transactions.

March

In March, Matt Corallo proposed the consensus cleanup soft fork to eliminate potential problems in Bitcoin's consensus code. If adopted, the fixes would eliminate the time warp attack, lower legacy Script's worst case CPU usage, make caching transaction validation status more reliable, and eliminate a known (but expensive) attack against lightweight clients. Although parts of the proposal (such as the time-warp fix) seemed to interest a variety of people, other parts of the proposal (such as fixes for the worst case CPU usage and validity caching) received some criticism. Perhaps it was for that reason that the proposal didn't make any obvious progress towards implementation in the second half of the year.

March also saw Kalle Alm request initial feedback on signet, which would eventually become BIP325. The signet protocol allows creating testnets where all valid new blocks must be signed by a centralized party. Although this centralization would be antithetical to Bitcoin, it's ideal for a testnet where testers sometimes want to create a disruptive scenario (such as a chain reorganization) and other times just want a stable platform to use for testing software interoperation. On Bitcoin's existing testnet, reorgs and other disruptions can occur frequently and for prolonged lengths of time, making regular testing impractical. Signet would mature throughout the year and eventually be integrated into software such as C-Lightning as well as used for a demonstration of eltoo. A pull request adding support to Bitcoin Core remains open.

Additionally in March, Lightning Labs announced Lightning Loop, providing a non-custodial solution for users who want to withdraw some of their funds from a LN channel to an onchain UTXO without closing the channel. In June, they would upgrade Loop to also allow users to spend a UTXO into an existing channel. Loop uses Hash Time Locked Contracts (HTLCs) similar to those used by regular offchain LN transactions, ensuring that a user's funds are either transferred as expected or that the user receives a refund of all costs except for any onchain transaction fees. This makes Loop almost completely trustless.

2019 summary Major releases of popular infrastructure projects

- C-Lightning 0.7 released in March added a plugin system that would see heavy use by the end of the year. It was also the first C-Lightning release supporting reproducible builds for increased safety through improved auditability.
- LND 0.6-beta released in April included support for Static Channel Backups (SCBs) that help users recover any funds settled in their LN channels even if they've lost their recent channel state. The release also featured an improved autopilot to help users open new channels, plus built-in compatibility with Lightning Loop for moving funds onchain without closing a channel or using a custodian.
- Bitcoin Core 0.18 released in May improved Partially Signed Bitcoin Transaction (PSBT) support and added support for output script descriptors. The combination of those two features allowed it to be used with the first released version of the Hardware Wallet Interface (HWI).
- Eclair 0.3 released in May improved backup safety, added support for plugins, and made it possible to run as a Tor hidden service.
- LND 0.7-beta released in July added support for using a watchtower to guard your channels when you're offline.

- LND 0.8-beta released in October added support for a more extensible onion format, improved backup safety, and improved the watchtower support.
- Bitcoin Core 0.19 released in November implemented the new CPFP carve-out mempool policy, added initial support for BIP158-style compact block filters (currently RPC only), improved security by disabling protocols such as BIP37 bloom filters and BIP70 payment requests by default. It also switches GUI users to bech32 addresses by default.
- C-Lightning 0.8 released in December added support for multipath payments and switched its default network to mainnet from testnet. It was also the first major C-Lightning release to support alternative databases, with postgresql support available in addition to the default sqlite support.

April

In April, James O'Beirne proposed AssumeUTXO, a method for allowing full nodes to defer verification of old block chain history by downloading and temporarily using a trusted copy of the recent UTXO set. This would allow wallets and other software using the full node to start receiving and sending transactions within minutes of the node being started instead of having to wait hours or days, as is the case now for a newly started node. AssumeUTXO proposes that the node download and verify the old block chain history in the background until it eventually verified its initial UTXO state, allowing it to ultimately obtain the same trustless security as a node that doesn't use AssumeUTXO. O'Beirne would continue working on the project throughout the year, incrementally adding new features and refactoring existing code on the path towards a goal of ultimately adding AssumeUTXO to Bitcoin Core.

Also in April, Pierre-Marie Padiou proposed the idea of trampoline payments, a method for allowing lightweight LN nodes to outsource pathfinding to heavyweight routing nodes. A lightweight node, such as a mobile app, might not keep track of the full LN routing graph, making it unable to find routes to other nodes. Padiou's proposal would allow the lightweight node to route the payment to a nearby node and then have that node calculate the rest of the path. In essence, the payment would bounce off the trampoline node on the way to its destination. To add privacy, the original spender might require the payment bounce off several trampoline nodes in sequence so that none of them know whether or not it was routing the payment to the final recipient or just another trampoline node. A PR adding features for trampoline payments to the LN specification is currently open and the Eclair implementation of LN has added experimental support for relaying trampoline payments.

May

In May, Pieter Wuille proposed a taproot soft fork consisting of bip-taproot and bip-tapscript (which both depend on last year's bip-schnorr proposal). If implemented, this change will allow single-sig, multisig, and many contracts to all use the same style of scriptPubKeys. Many spends from multisigs and complex contracts will also look identical to each other and single-sig spends. This can significantly improve user privacy and coin fungibility while also reducing the amount of block chain space used by multisig and contract use cases. Even in cases where multisig and contract spends can't take full advantage of taproot's privacy and space savings, they still may only need to put a subset of their code onchain, giving them more privacy and space savings than they have today. In addition to taproot, tapscript brings small refinements to Bitcoin's scripting capabilities, mainly by making it easier and cleaner to add new opcodes in the future. The proposals received significant discussion and review throughout the rest of the year, including through a series of group review sessions organized by Anthony Towns that had more than 150 people sign up to help review.

Towns also proposed in May two new signature hashes to be used in combination with tapscript, `SIGHASH_ANYPREVOUT` and `SIGHASH_ANYPREVOUTANYSCRIPT`. A signature hash (sighash) is the hash of a transaction's fields and related data to which a signature commits. Different sighashes in Bitcoin commit to different parts of a transaction, allowing signers to optionally let other people make certain modifications to their transactions. The two new proposed sighashes function similar to BIP118's SIGHASH_NOINPUT by deliberately not identifying which UTXO they spend, allowing the signature to spend any UTXO whose script it can fulfill (e.g. that uses the same pubkey). The primary suggested use for noinput-style sighashes is to enable the previously proposed eltoo update layer for LN. Eltoo can simplify several aspects of channel construction and management; it's especially desirable for simplifying channels involving more than two participants that can significantly reduce onchain channel costs.

A third soft fork proposed this month came from Jeremy Rubin, who described a new opcode now called `OP_CHECKTEMPLATEVERIFY` (CTV). This would allow a limited form of covenant where an output of one transaction would require a subsequent transaction spending it to contain certain other outputs. A suggested use for this would be committed future payments where a spender pays a single small output that can only be spent using a transaction (or a tree of transactions) that later pays dozens, hundreds, or even thousands of different receivers. This could enable new techniques to enhance coinjoin-style privacy, support security-enhancing vaults, or manage spender costs when transaction feerates spike. Rubin would continue

working on CTV for the remainder of the year, including opening PRs (1, 2) for improvements to parts of Bitcoin Core where optimizations could make a deployed version of CTV more effective.

2019 summary Notable technical conferences and other events

- Stanford Blockchain Conference, January, Stanford University
- MIT Bitcoin Expo, March, MIT
- Optech Executive Briefing, May, New York City
- Magical Crypto Friends (technical track), May, New York City
- Breaking Bitcoin, June, Amsterdam
- Bitcoin Core developers meetup, June, Amsterdam
- Edge Dev++, September, Tel Aviv
- Scaling Bitcoin, September, Tel Aviv
- Cryptoeconomic Systems Summit, October, MIT

June

Gleb Naumenko, Pieter Wuille, Gregory Maxwell, Sasha Fedorova, and Ivan Beschastnikh published a paper about erlay, a protocol for relaying unconfirmed transaction announcements between nodes that makes use of libminisketch-based set reconciliation to produce an estimated 84% reduction in announcement bandwidth. The paper also demonstrates that erlay would make it much more practical to significantly increase the default number of outbound connections that nodes make. This could improve each node's resistance to eclipse attacks that can trick it into accepting blocks not on the most proof-of-work block chain. More outbound connections also improves node resistance against other attacks that could be used to track or delay payments originating from the node. Work on erlay would continue through the year with additional research and the proposal of BIP330 for the set reconciliation protocol. Other improvements made in P2P relay this year included Bitcoin Core's privacy improvements for transaction relay (eliminating a problem described in the TxProbe paper by Sergi Delgado-Segura and others) and the addition of two extra outbound connections used only for the relay of new blocks, improving resistance against eclipse attacks.

After a significant amount of prior work, June also saw the merge of altruist LN watchtowers into LND. Altruist watchtowers don't receive any reward via the protocol for helping to secure their client's channels, so a user needs to run their own watchtower or depend on the charity of a watchtower operator, but this is enough to demonstrate that watchtowers can reliably send penalty transactions on behalf of other users—ensuring that users who go offline for significant amounts of time don't lose any money. Altruist

watchtowers would eventually be released in LND 0.7.0-beta and would see additional development through the remainder of the year, including a proposed specification and discussion about how they could be combined with next-generation payment channels such as eltoo.

July

In July, the Bitcoin Core project merged Carl Dong's PR adding support for reproducible builds of Bitcoin Core's Linux binaries using GNU Guix (pronounced "geeks"). Although Bitcoin Core has long provided support for reproducible builds using the Gitian system, it can be difficult to set up and it depends on the security of several hundred Ubuntu packages. By comparison, Guix can be much easier to install and run, and builds of Bitcoin Core using it currently depend on a much smaller number of packages. In the long term, contributors to Guix are also working on eliminating the trusting trust problem to make it easy for users to verify that binaries such as `bitcoind` are derived solely from auditable source code. Work continued on Guix build support throughout the year, with some contributors hopeful that Guix will be used for the first major version of Bitcoin Core released in 2020 (perhaps in parallel with the older Gitian-based mechanism). Independently, documentation was added this year to both the C-Lightning and LND repositories describing how to create reproducible builds of their software using trusted compilers.

August

In August, Bryan Bishop described a method for implementing vaults on Bitcoin without using covenants. *Vaults* is a term used to describe a script that limits an attacker's ability to steal funds even if they obtain a user's normal private key. A *covenant* is a script that can only be spent to certain other scripts. There's no known way to create covenants using the current Bitcoin Script language, but it turns out that they're not necessary if users are willing to run code that performs a few extra steps when depositing their money into the vault contract. Perhaps more notably, Bishop described a new weakness in previous vault proposals as well as a mitigation for the weakness that would limit the maximum amount of funds that could be stolen from a vault by an attacker. The development of practical vaults could be useful for both individual users and large custodial organizations such as exchanges.

2019 summary Bitcoin Optech

In Optech's second year, we signed up six new member companies, held an executive briefing during NYC block chain week, published a 24-week

series promoting bech32 sending support, added a wallet and services compatibility matrix to our website, published 51 weekly newsletters, saw several of our newsletters and blog posts translated into languages such as Japanese and Spanish, created a topics index, added a chapter to our Scalability Workbook, hosted two schnorr/taproot workshops with publicly released jupyter notebooks, and published field reports from BTSE and BRD. We have big plans for 2020, so we hope you'll continue to follow us on Twitter, subscribe to our weekly newsletter, or track our RSS feed.

September

Adam Gibson proposed a novel form of non-interactive coinjoin for the existing Bitcoin system. The protocol, called SNICKER, involves a user selecting one of their UTXOs and a randomly-selected UTXO from the global UTXO set to both be spent in the same transaction. The proposing user signs their part of this transaction and uploads it in the Partially Signed Bitcoin Transaction (PSBT) format to a public server. If the other user checks the server and sees the PSBT, they can download it, sign it, and broadcast it—completing the coinjoin without both users needing to be online at the same time. The proposing user can create and upload as many PSBTs as they want using their same UTXO until some other user accepts the coinjoin. SNICKER's major advantages over other coinjoin approaches are that it doesn't require the users be online at the same time and that it should be easy to add support for it to any wallet that already has BIP174 PSBT support, which is an increasing number of wallets.

Also in September, the maintainers of C-Lightning, Eclair, and LND disclosed a vulnerability that affected previous versions of their software. It appeared that, in some cases, each of the implementations failed to confirm that channel funding transactions paid the correct script or the correct amount (or both). If exploited, this could result in channel payments being impossible to confirm onchain, making it possible for nodes to lose money by relaying payments from an invalid channel to a valid channel. Optech is unaware of any users who lost money before the first public announcements of the vulnerability. The LN specification was updated to help future implementers avoid this problem and there's an expectation that other proposed changes to LN's communication protocol will help avoid other failures of this type.

October

LN developers made significant progress in October and November towards addressing a long-standing concern about ensuring that users can always close their channels without excessive delays. If a user decides that they want

to close one of their channels and they're unable to contact their remote peer, they broadcast the latest *commitment transaction* for that channel—a pre-signed transaction that spends the channel's funds onchain to each party according to the latest version of their offchain contract. A potential problem with this arrangement is that the commitment transaction was potentially created days or weeks earlier when transaction fees were lower, so it may not pay a high enough fee to confirm quickly before any security-essential time locks expire. It's always been known that the solution to this problem is to make it possible to fee bump commitment transactions. Unfortunately, nodes such as Bitcoin Core have to limit the use of fee bumping in order to prevent Denial of Service (DoS) attacks that waste their bandwidth and CPU. In trustless multi-user protocols like LN, your counterparty might be an attacker who could deliberately trigger the anti-DoS policy in order to delay the confirmation of your LN commitment transaction, an attack sometimes called transaction pinning. A pinned transaction may not confirm before its time locks expire, allowing an attacking counterparty to steal funds from you. Last year, Matt Corallo suggested carving out a special exemption from the part of Bitcoin Core's transaction relay policy related to Child-Pays-For-Parent (CPFP) fee bumping. This limited exemption ensures that two-party contract protocols (such as current-generation LN) can guarantee each party the ability to create their own fee bump. Corallo's idea was named CPFP carve-out and his implementation of it was released as part of Bitcoin Core 0.19. Even before that release, other LN developers worked on the revisions to the LN scripts and protocol messages necessary to start using the change. As of this writing, those specification changes are awaiting final implementation and acceptance before seeing deployment on the network.

2019 summary New open source infrastructure solutions

- Proof of reserves tool released in February allows exchanges and other bitcoin custodians to prove they have control over a certain set of UTXOs using BIP127 reserve proofs.
- Hardware Wallet Interface released in March makes it easy for a wallet already compatible with Partially Signed Bitcoin Transactions (PSBTs) and output script descriptors to use several different models of hardware wallets for secure key storage and signing.
- Lightning Loop released in March (with loop-in support added in June) provides a non-custodial service that allows users to add or remove funds from their LN channels without closing existing channels or opening new channels.

November

Discussion in November about using bech32 addresses for taproot payments brought additional attention to an issue discovered in May. According to BIP173, mis-copied bech32 strings are supposed to have a worst-case failure rate of about 1-in-a-billion. However, it was discovered that bech32 strings ending with a `p` could have any number of preceding `q` characters added or removed. This doesn't practically affect bech32 addresses for segwit P2WPKH or P2WSH addresses, as at least 19 consecutive `q` characters would need to be added or removed in order to transform one address type into another—and any other length change for v0 segwit addresses would be invalid. But that's not the case for v1+ segwit addresses, such as those proposed for taproot, where a single added or removed `q` character in a vulnerable address could lead to a loss of funds. BIP173 co-author Pieter Wuille performed additional analysis and found that this was the only deviation from bech32's expected error correction ability, so he proposed limiting the use of BIP173 addresses in Bitcoin to only 20 byte or 32 byte witness programs. This will ensure that v1 and subsequent segwit address versions provide the same reliable error correction as v0 segwit addresses. He also described a small tweak to the bech32 algorithm that will allow other applications using bech32, as well as next-generation Bitcoin address formats, to use BCH error detection without this problem.

Also in November, Bitcoin Core removed its dependency on OpenSSL, which had been part of its codebase since the original 2009 release of Bitcoin 0.1. OpenSSL was the cause of consensus vulnerabilities, remote memory leaks (potential private key leaks), other bugs, and poor performance. It's hoped that its removal will reduce the frequency of future vulnerabilities.

As part of the OpenSSL removal, Bitcoin Core deprecated its support for the BIP70 payment protocol in version 0.18, and later disabled support by default in version 0.19. This decision was supported by the CEO of one of the few companies that continued to use BIP70 in 2019.

December

In December, LN developers achieved one of their major goals from last year's planning meeting: the implementation of basic multipath payments. These are payments that can be split into several parts, with each part being routed separately through different channels. This allows users to spend or receive money using more than one of their channels at a time, making it possible to spend their full offchain balance or receive up to their full capacity in a single payment (within the limitations of certain safety restrictions). It's expected that this will make LN significantly more user-friendly by

eliminating the need for spenders to worry about the balances of specific channels.

Conclusion

In the summary above, we see no revolutionary proposals or improvements. Instead, we see a flurry of incremental improvements—solutions that take cases where Bitcoin and LN are already successful and build on them to make the system even better. We see developers working to make hardware wallets more accessible (HWI), generalize communication between wallets for multisig and contract use cases (descriptors, PSBTs, miniscript), strengthen consensus security (cleanup soft fork), simplify testing (signet), eliminate unnecessary custody (loop), make it easier to start running a node (assumeutxo), improve privacy and save block space (taproot), simplify LN enforcement (anyprevout), better manage feerate spikes (CTV), reduce node bandwidth (erlay), keep LN users safe when offline (watchtowers), reduce the need for trust (reproducible builds), prevent thefts (vaults), make privacy more accessible (SNICKER), better manage onchain fees for LN users (anchor outputs), and make LN payments automatically work more often (multipath payments). (And those are just the highlights for the year!) We can only guess what Bitcoin contributors will accomplish next year, but we suspect it will be more of the same—dozens of modest changes that each make the system better without breaking it for anyone who's already satisfied. *The Optech newsletter will return to its regular Wednesday publication schedule on January 8th*.

Bitcoin As a Startup

By Hass McCook

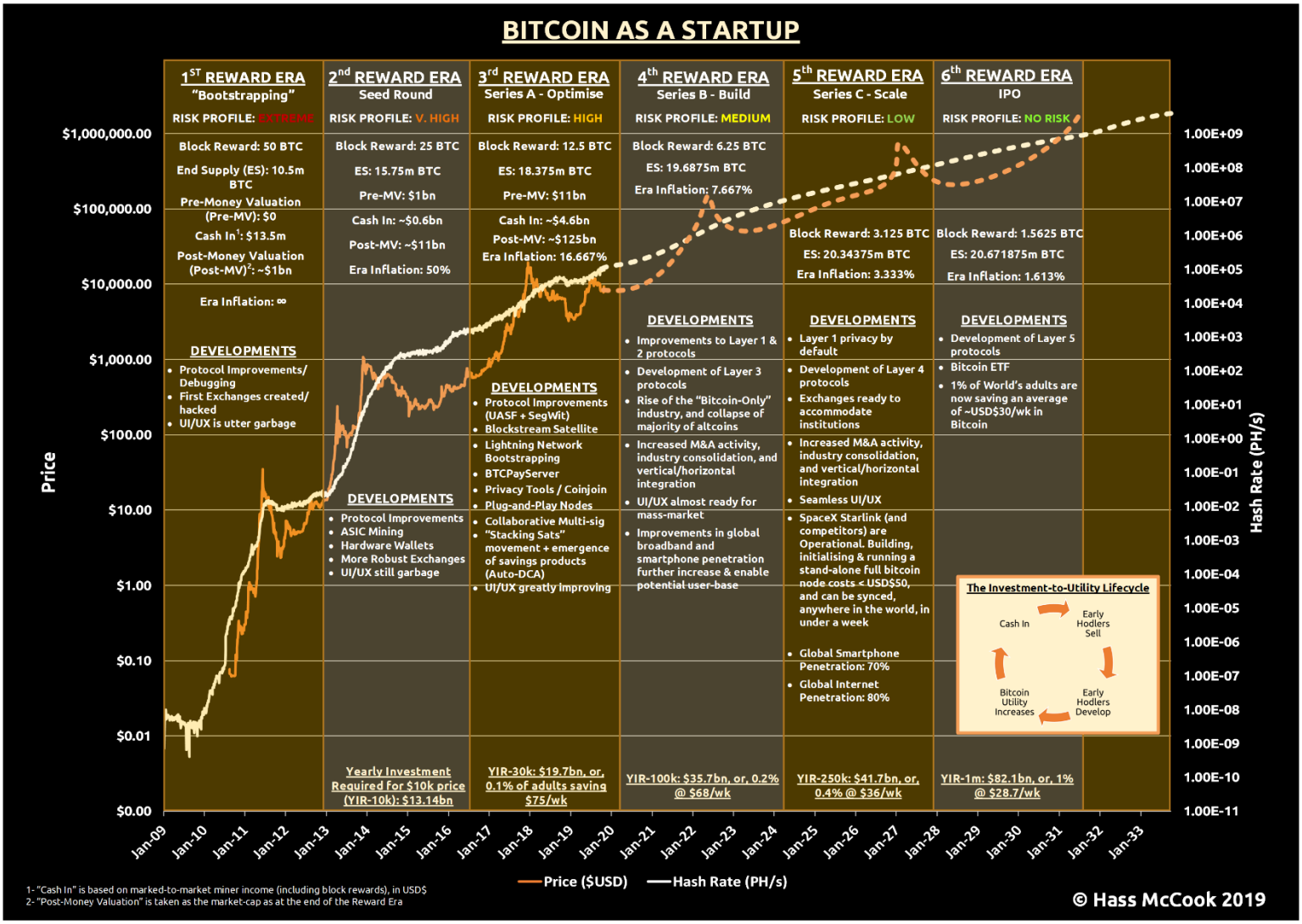
Posted December 29, 2019

Original Presentation of Framework from November 2019

People hate Bitcoin analogies. But Bitcoin is so hard to understand for so many, concessions need to be made.

VCs are a group of people demonized in the Bitcoin industry for not understanding Bitcoin's value proposition. Well, how do you expect a VC to value Bitcoin if they're only used to valuing startups?

Here is a framework that will hopefully help. It tracks the development and evolution of the Bitcoin ecosystem in discreet "fundraising rounds", which coincide with Bitcoin's Reward Eras. An organization is defined as "an organized group of people with a particular purpose". If that's the case, then Bitcoin is a well-oiled "un-organisation" with founders but no CEOs, many volunteers but no employees, and provably non-diluting equity, available to anyone who is willing to trade their energy for it.



Bitcoin As A Startup

I will be borrowing heavily from Nathan Reiff's piece "Series A, B, C Funding: How It Works"

Pre-seed Round *(1st Reward Era, 3/1/2009–28/11/2012)*

The earliest stage of funding a new company comes so early in the process that it is not generally included among rounds of funding at all. Known as "pre-seed" funding, this stage typically refers to the period in which a company's founders are first getting their operations off the ground. The most common "pre-seed" funders are the founders themselves, as well as close friends, supporters, and family (Reiff, 2019)

The "Bitcoin Company" was founded by Satoshi Nakamoto, with its single product offering being an open-source monetary system project, known as Bitcoin. 2,100,000,000,000,000 shares were to be issued on a predetermined

schedule, and anyone was free to buy or sell these shares. The founders initially held no initial equity, but equity was easy to build in those days, and rightly so. Just like any startup, it is the founding team and initial bootstrappers who should get the biggest rewards down the line for putting the most skin in the game.

Due to the nature of Bitcoin's incentive mechanisms, many early "equity holders" were encouraged to use their time, skills and money to evangelise or develop the product, and hence increase the value of their equity. The company manages itself, in a zero-overhead environment.

During the first stage of "the company's" life, traditionally the "the first bugs appeared and were ironed out, and this was an iterative process for many months. After proving to be robust and reliable, a market developed, and the first exchanges started to emerge. User experience, both from a software point of view, and a financial point of view, were a disaster. Bitcoin was virtually unusable without a PhD in Computer Science, and when you could use it, you'd be robbed by an exchange that had been "hacked". Volatility was extreme, and the risk was unpalatable for the majority of onlookers. Whether or not "The Bitcoin Company" would remain "in business" was still a very dubious proposition.

This Era, the early equity holders were blessed with a parabolic bubble, and many divested some equity to give themselves runway to work on Bitcoin full time. It's just like a fund-raise: get a big cash injection, and then burn it relentlessly until the next funding round. Coincidently, each round has exhibited at least one of these massive injections and equally massive drawn-out draw-downs.

During this Era, miners were rewarded with USD$13.5m in total block rewards and transaction fees. Assuming that, on average, cost to mine a bitcoin is equal to the market price, we can consider the mining reward to be miners buying bitcoin at-spot. Therefore, we can take the "money-in" for the round to be the cumulative miner's revenue. Money-in is never consistent, and even a small injection is enough to make the price fly and form a bubble.

With all the above said, fortune favours the bold, and Bitcoin entered its seed round at a $1bn pre-money valuation (i.e. Bitcoin's Market Cap was $1bn at the end of the first reward era).

Seed Round *(2nd Reward Era, 28/11/2012–9/7/2016)*

You can think of the "seed" funding as part of an analogy for planting a tree. This early financial support is ideally the "seed" which will help to grow the business. Given enough revenue and a successful business strategy, as well as the perseverance and dedication of investors, the company will hopefully eventually grow into a "tree." (Reiff, 2019)

Risk of short-term ecosystem death did not substantially decrease until the end of the Secord Reward Era. You could say that the risk profile dropped from “Extreme” to “Very High”. In terms of PR/Optics, this was arguably the worst and most dubious “round” of Bitcoin’s existence. In the face of these FUD-inspiring superficial problems, Bitcoin did what it does best — got on with it.

This era saw the first Bitcoin bubble to be featured in Mainstream Media in some way shape or form. Going from catastrophe to catastrophe; from the numerous exchange hacks, scams, asset seizures, 51% attacks (GHash.io) and China bans, those who invested in the mania of 2013 would not break even until the Third Reward Era. Inflation made things worse, with the market having to absorb the 5.25 million Bitcoin producing during the Era. However, those who divested during the mania provided themselves with many years of runway to give back to Bitcoin and make their equity more valuable.

In this Era, we started to see the emergence of user-friendly plug-and-play hardware wallets; the age of ASIC mining was in full swing, with miner fabrication done at a huge scale. The gamblers had a field day — with the majority of “fiat-onramps” providing toys for the traders, but not for the savers. For better or worse though, this added much needed liquidity and means for price-discovery. That said, liquidity was quite low, and for the first half of the era when the exchanges were just so sketchy, you couldn’t even really trust what the advertised market price was.

The first VCs entered the game; some investing in Bitcoin companies, and others, like Tim Draper, investing directly in the underlying.

Miners were not put off by the prolonged bear market, with the network hashrate growing by orders of magnitude mostly due to competition-driven innovation among ASIC fabricators. In the Second Reward Era, miners earned a total of USD$600m for their efforts. This USD$600m “investment” resulted in an $11bn post-money valuation at the end of the Round.

Despite failing to reclaim the heights of 2013, Bitcoin closed this round on the upswing — one that wouldn’t end for another year and a half.

Series A — Optimise *(3rd (and Current) Reward Era, 9/7/2016 — May 2020)*

Once a business has developed a track record (an established user base, consistent revenue figures, or some other key performance indicator), that company may opt for Series A funding in order to further optimize its user base and product offerings. (Reiff, 2019)

With “traditional” startups, their Series A round is used to fund the optimization of the offering, and to lay a solid platform to build further during

the next round. Several experts and industry stakeholders were split on how to best optimize Bitcoin to increase transaction throughput. The Establishment took the view that achieving this through an increase in block size was the answer, The People took the view that this was a slippery slope, and that scaling be achieved with protocol optimisations, i.e., Segregated Witness (SegWit). The People were victorious, which was a huge positive indicator that centralizing Bitcoin would be a Sisyphean task. As a result, and in combination with a supply halving, the money flowed in, and Bitcoin achieved a valuation in the hundreds of billions at its all-time-high.

The Third Era also featured "The Scambrian Explosion", with thousands of cryptocurrencies being spawned, sending Bitcoin's dominance of the cryptocurrency to a paltry 35% at one point in time. While most of these altcoins now having lost over 95% of their value (hundreds have lost >99% of their value), the only result was the wasting of hundreds of thousands of hours of development time and hundreds of millions of dollars which should have been directed at Bitcoin. The fact that Bitcoin now accounts for 75% of the cryptocurrency market (and rising) is a testament to why people should have just stuck to Bitcoin.

The huge influx of money in this Era allowed early equity holders to further divest to focus on development — and my oh my, was there a lot of development. In terms of scalability, The Lightning Network successfully came out of beta and is being extensively used. Privacy and coin-joining solutions emerged and became easier to use. There are literal satellites in space broadcasting the network. The rise of the "run your own node" movement gathered serious momentum and was bolstered by a host of companies offering "plug-and-play" nodes. With your own node, you can also be your own payments provider through BTCPayServer. Multi-signature security has never been easier. This paragraph could go on for pages — so if you want a full technical recap of just 2019, the Bitcoin Optech Newsletter will give you everything you need to know.

At time of writing, Era miner revenue is USD$4.6bn, and the valuation has risen from $11bn to over $125bn.

Despite all the progress made, Bitcoin is still a high-to-very-high risk investment at this stage, as the market price can still move in excess of 30%, in either direction, in one week, regularly. This will ultimately remain the case until both the liquidity pool grows, and the mining reward (inflation) shrinks.

Series B — Build *(4th Reward Era, May 2020 — Apr 2024)*

Series B rounds are all about taking businesses to the next level, past the development stage. Investors help startups get there by expanding market reach. Companies that have gone through seed and Series A funding rounds

have already developed substantial user bases and have proven to investors that they are prepared for success on a larger scale. Series B funding is used to grow the company so that it can meet these levels of demand

With the necessary protocol upgrades happening during Series A and early in Series B, the focus will shift to the building of products and services on top of the slowly ossifying Bitcoin base layer. This Era will see the replacement of the "Old Guard" by a newer generation of more business-savvy Bitcoin entrepreneurs and through merger and acquisition activity.

There will also be a lot of vertical and horizontal integration, as companies aim to achieve a "full-stack". One example of all this is Layer1 mining, in what is effectively an electricity utility that also mines, and designs and fabricates ASIC miners.

It is impossible to predict what's specifically going to happen during this 4 year era, let alone in the first year of it, but if the past 18 months are anything to go by, security, privacy, and most importantly going forward, UI/UX, will improve dramatically. I'd expect that running a full-sovereignty stack (your own VPN, node, electrum & BTCPay servers, multi-sig setup, etc.) will be easy enough for **almost anyone** to do at the end of The Era. Effectively, Bitcoin's infrastructure will be developed enough to handle some proper scale.

What will be most interesting thing to see will be the technological, economic and political developments during this Era. In this regard, everything is "Good for Bitcoin". Internet access, computers and smartphones become cheaper and more accessible? This is good for Bitcoin. Never ending quantitative easing and negative interest rates? This is good for Bitcoin. Increased political turmoil, censorship, or surveillance? This is good for Bitcoin.

Should Bitcoin "stay in business", risk level at this point would be medium-to-high, and you could expect to be exposed to weekly swings of +/-15%, but maybe not as regularly as in Series A.

When looked at in conjunction with some economic models like the Stock-to-Flow model, there is little reason to think a 10x growth in market cap will not be seen in this series, as per the 3 series preceding it. This would mean a series-end market cap of about USD$1 trillion, or, around USD$50k per bitcoin. Chances are that the All-time-high price achieved during this series will be dramatically higher than the end price, as this is the main driver of the "investment-to-utility" loop.

Series C — Scale *(5th Reward Era, Apr 2024 — Mar 2028)*

Businesses that make it to Series C funding sessions are already quite successful. Series C funding is focused on scaling the company, growing as quickly and as successfully as possible. (Reiff, 2019)

Inflation is finally starting to drop, with only ~650,000 BTC needing to be absorbed by the market over the 4-year period — the inflation rate is now lower than that of Gold. Scarcity is becoming a more dominant element of Bitcoin's value proposition.

With basically all the infrastructure largely built, and UI/UX continuing to improve, this Era is "The Era of The Evangelist". Bitcoin is ready for prime time; somebody just has to go out and tell everybody. This Series' fund raising round made all the right people very wealthy (if they weren't already wealthy from the Series B raise), and these people will begin to use their influence (i.e. money) to promote Bitcoin, and increase the "saver-base", i.e., the number of people who buy bitcoin on a weekly basis, or, earn their living in Bitcoin.

At this stage, to maintain a USD$500k price, about 10 million people are each saving USD$150/wk in Bitcoin. This represents 0.2% of the world's adult population. Considering the level of utility and the seamlessness of the UI/UX in the late stages of this series, only 10 million active savers may even feel like a failure of sorts! From here, it is simply an exercise of marketing.

Discussion of The Framework on The Total Connector Podcast with Keyvan Davani

IPO *(6th Reward Era, Mar 2028 — Feb 2032), and beyond...*

At this point, if Bitcoin is still alive, it is effectively unkillable. Major banks have now made big acquisitions, and are offering bitcoin services to their customers. Most power utilities have skin in the Bitcoin game. People won't know that they're using Bitcoin — and we'll probably have 4 (or even 5) layers on top of Bitcoin now. On-chain base-layer transactions are reserved for high value transactions, all people adopting Bitcoin going forward won't be onboarded via the base layer. The Bitcoin ETF has FINALLY been approved after an 18 year effort. Price per coin is in the millions, and fairly stable (to the downside, at least). Number still go up — just as designed.

It's improper to say that it is "zero risk" in 2032, but the risk is extremely low. That said, if it gets to a 7th Era, I'd be comfortable enough to say that Bitcoin may become the first ever truly risk-free asset, with inflation rapidly approaching zero. I'll be 50 years old by the end of Era 7, so I'm literally betting my career that this will be the case. Talk about skin in the game!

The cat is out of the bag

By Nic Carter

Posted December 29, 2019

Bitcoin is everyone's problem now

Evey: Remember, remember, the Fifth of November, the Gunpowder Treason and Plot. I know of no reason why the Gunpowder Treason should ever be forgot... But what of the man? I know his name was Guy Fawkes and I know, in 1605, he attempted to blow up the Houses of Parliament. But who was he really? What was he like? We are told to remember the idea, not the man, because a man can fail. He can be caught, he can be killed and forgotten, but 400 years later, an idea can still change the world. I've witnessed first hand the power of ideas, I've seen people kill in the name of them, and die defending them... but you cannot kiss an idea, cannot touch it, or hold it. Ideas do not bleed, they do not feel pain, they do not love...
– Evey Hammond, V for Vendetta

An exorbitant privilege

Bitcoin is first and foremost a monetary phenomenon. The social climbers and false prophets who proclaimed it is a payments revolution have either come around or been repudiated by the market and washed out, embittered.

Most who understood it that way are now moving on to new things. The world did not need another Paypal. **The world needed a new monetary institution**.

As Bitcoin went from a proof of concept, to a toy, to a joke, to a collectible, and then to a movement, a few policymakers came to realize that it posed a threat to the established system. Not because of its present form, but because what it represented: a profane insult to the carefully calibrated monetary system. All done in a mocking, insouciant fashion — a band of nerds and ne'er-do-wells insolently challenging the state's monopoly on seigniorage. Satire is what despots fear most, and the rise of Bitcoin made our present monetary system look patently absurd.

Critic: Nothing backs Bitcoin.

Bitcoiner: What backs the dollar?

Critic: Nothing intrinsically — our ability to compel foreign nations to accept our currency as the numeraire of international trade, our ability to force citizens to pay taxes in dollars, and our military assets required to enforce both conditions.

Bitcoiner: How persuasive!

The visceral hatred elites feel about Bitcoin? Perfectly justified. How else would you react to a upstart aimed at usurping your sacred monetary privilege?

Such is the potency of Bitcoin that it compels the high priests of U.S. imperialism to reveal the unwritten rules about the role the dollar plays in power projection abroad. In May of this year, U.S. Representative Brad Sherman (D-CA) spoke out against cryptocurrency on the floor of the house. His statement laid bare the normally veiled post-Bretton Woods doctrine in which the dollar is employed not only a monetary tool but a strategic one, too.

An awful lot of our international power comes from the fact that the dollar is the standard unit of international finance [...] and it is the announced purpose of the supporters of cryptocurrency to take that power away from us [...]. Whether it is to disempower our foreign policy, our tax collection, or our traditional law enforcement [...]. the purpose of cryptocurrency [...] is solely to aid in the disempowerment of the United States and the rule of law.

Representative Sherman is practically a soothsayer. He understands *precisely* where the world is going.

His mistake is not in the diagnosis, but in the cure. He mistakenly believes that Bitcoin can be reckoned with. But Bitcoin is an idea, not a product. The

notion of a weightless, virtual commodity was productized for good in 2009 (although the idea long predated Bitcoin), and it has been eroding the state's monetary monopoly ever since.

It could not have been created at a better time; one wonders how Bitcoin would have fared if it had been created in the 1980s or 90s when the US economy was fairer, the monetary system was totally unquestioned, and the US was the sole dominant global superpower. Against today's backdrop, Bitcoin insists on itself. It has *urgency*. In the halcyon days of Pax Americana, Bitcoin would have mattered much less. In the twilight of the American empire, however, it is more relevant than ever.

Our monetary system is disastrously redistributive

The wealth of political elites derives primarily from privileged access to the monetary spigot. This is no longer a secret. The heavenly mana of seigniorage has opened, first a trickle and now a flood. The world is grappling with inequality, and the dozens of populist revolts active in the world today are patent evidence of this. Yet the resurgent socialist parties misdiagnose the situation. The enemy is not a nebulous form of capitalism, but rather a form of socialism itself — a low-rates fueled perma-bailout to the owners of financial assets. It's no coincidence that asset prices have steadfastly risen in the last decade, as the Fed has embarked on a ludicrously unshackled period of money creation.

Many ask: against the backdrop of monetary issuance, where did the inflation go? It went of course into financial assets. But this benefits the paltry few. Did you know that the decade-long rally in the S&P500 has been characterized by historically low participation from retail investors? The riotous gains in asset prices have sidelined mom and pop. They accrue instead to institutional investors and corporate insiders who returned capital to themselves through buybacks. In the 90s, Wharton MBAs convinced investors that the ideal mode of corporate governance was making large equity and options grants to corporate directors to create incentive alignment. Well, the grants were made, and the directors rewarded the shareholders by spending corporate earnings on buying back the stock, thus juicing earnings per share and triggering options payouts for directors. They just so happened to forgot to generate corporate value along the way. That pesky real economy... that was secondary.

Why are politicians so rich? Why do they become rich *after* leaving office? Why do regulators go work in industry? Why is the Secretary of the Treasury a former Goldman banker and hedge fund manager?

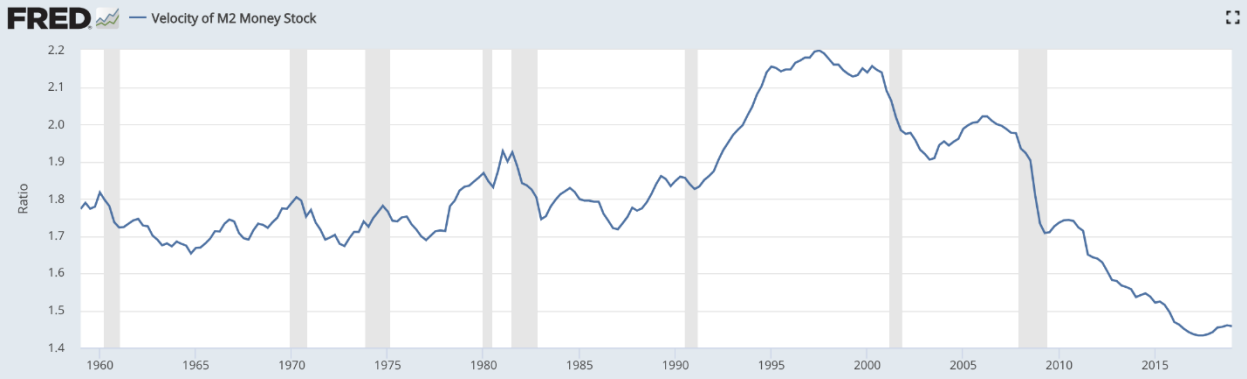
The Cantillon effect pictured

Why are renters historically disempowered, whereas landowners are historically privileged? Why has the cost of higher education and healthcare outpaced inflation by orders of magnitude? Why is the CPI a sad, pathetic joke? Do consumer goods account for most of your expenditures, or does rent, healthcare, and education?

What are you more exposed to? The cost of a TV, or property values?

Even if you didn't know what the Cantillon effect was, you felt it vividly in the last decade. The hopelessness felt by many in today's society is the consequence of this monetary misalignment; the introduction of eye-watering money into the economy, but an uneven distribution. Who benefited from historically low rates? Normal folks dealing with predatory credit card loans, or owners of financial assets who were able to put historically cheap capital to work? And no, cheap financing didn't help the middle and lower class get a foothold in property… because property values were horrendously inflated in the first place! Property, treated as a store of value for the rich, is precisely where so many of the Fed's newly-minted dollars settled. Reflect on those hollowed-out city centers in Vancouver, New York, and London — full of empty homes used as capital warehouses for absentee millionaires.

If there's a single graph that evidences the impact of a decade of freewheeling monetary stimulus on the economy, it is the following:



Monetary velocity in the U.S. is at its lowest since modern records began. If you think about the equation of exchange (MV = PQ), a decline in V is sufficient to offset an increasing money supply (M) to keep prices (P) stable. And that's just about what happened: the purchasing power of the dollar has remained relatively stable even as supply has expanded dramatically. "Where is the inflation?" is the common refrain, but the question should instead be "where has the new money supply gone?" It is clear that it has settled, inert and unproductive, in financial assets mostly owned by the ultra-rich, bidding them up to century highs in relative valuation terms.

This is why our perverse form of zombie capitalism is often referred to as socialism for the rich. If you can position yourself close enough to the money spigot and arrange to share in the spoils of the monetary redistribution, you can profit handsomely. If you have access to financial assets and can benefit from a low cost of capital (whether you are an investor or a corporate director with discretion over buybacks), you can make low rates and quantitative easing work for you. If you cannot, you are utterly frozen out of the system, and indeed disadvantaged, as pricier capital assets immiserate the non rentier class.

Bitcoin is a system that explicitly rejects identity

Critics often ask who, exactly, Bitcoin is for. This perhaps a misspecified question. Bitcoin does not serve a "who," or a subset of whos. It just serves, indifferent its end users. Bitcoin, by design, does not require identity data to work. Your counterparty could be on the OFAC sanctions list, they could be a sentient toad, or a few lines of code. Bitcoin has no way of knowing, nor does it care. The only requirement to send a payment is to provide a valid signature which meets the criteria sufficient to unencumber a UTXO.

Traditional payment and credit relationships, on the other hand, enshrine identity. My credit card company is *very _interested in knowing that it is me*

who is using the card. If I inform them that a stranger has absconded with my card, they consider all the spends post-theft _totally invalid. The call with the fraud department goes like this:

- 'Can you vouch for the $10.51 purchase on 2/24 at Chipotle?' Yes, that was me. Extra guac.
- 'Can you vouch for the $463.39 purchase on 2/29 at Lululemon?' No, I don't habitually buy athleisure gear.

Identity data is inextricable from traditional payment networks. This is because they are many layers between payments and final settlement. An incredibly large and profitable business exists to assess the credibility of transactors and facilitate deferred-settlement transactions between them. This is because credibility and mutual trust enables massive efficiencies. You can lend your neighbor a lawnmower without demanding he provide a bond to cover its value because you *trust him*. Credit card networks just scale this up: they are trust underwriters, determining quantitatively how trustworthy I am, and passing along those assurances to merchants with whom I transact.

If they get it wrong, and it turns out I'm the kind of person who racks up a $10,000 credit card bill with no intention of ever paying, they swallow the cost! It was their bad. They should have done a better job assessing my trustworthiness.

The compact you implicitly agree to when you use Bitcoin is between you and the protocol, not between you and all the other users of Bitcoin. The only trust required is users trusting that the cryptographic and economic assumptions hold. So far, they have.

It has become trendy to denounce popular Bitcoiners as uncompromising, unreasonable assholes, and imply that there is something wrong with Bitcoin as a consequence, too. But Bitcoin is indifferent to this. It is a protocol for encoding and conveying value through a communications medium. Bitcoin isn't even aware of what the price of Bitcoin is, let alone the political trends of the day. It knows very, very little about itself.

As stated above, Bitcoin is attractive and useful precisely because it *rejects* any identity data from the conditions required for a spend. The only thing that has to be furnished is knowledge of a private key corresponding to a public key. When you receive Bitcoin, you do not need to be aware of the identity of the sender, because Bitcoin settles probabilistically. You can simply define your own threshold for finality — say, requiring $500,000 of work to be done before you consider a transaction final. That would correspond to waiting, at current rates, for 4–5 blocks under which your transaction should be buried.

This is what allows me to accept funds from people that I mistrust, and why Bitcoin is carving out a niche in these frontier transactions. Think of a ransomware hacker and his victim. These people mutually mistrust each other. They victim has been wounded and attacked. But the hacker still trusts that the $500 sent to them for the ransom in the form of BTC is a valid, unlikely-to-be-reversed payment. You may not like this. But Bitcoin flourishes on the margins of society. These are increasingly widening, as banking becomes politicized and used as a political tool, as the U.S.-driven settlement system is coopted for strategic objectives, and as identity requirements for payments networks become ever more rapacious.

Transacting with people you have no reason to trust is precisely why Bitcoin exists. The internet allowed us to transact with people on the other side of the globe, but internet commerce is beset by fraud. The reason credit cards are expensive is because the costs of remediating fraud and chargebacks are socialized.

If you aren't comfortable with evil people using Bitcoin, you should abandon it now

Of course, the jettisoning of counterparty trust (and risk) comes with some perceived drawbacks. Principal among them, you cannot evict someone from your network. This is very uncomfortable to people who believe that money ought to be a political tool, to be exploited to disempower political foes of the day.

There is a particular paradox in demanding that the members of a network you have inserted yourself into adhere to a certain moral code of conduct. As stated above, Bitcoin, and fast-settling hard money more generally, exists to facilitate commerce between individuals that do not have a pre-existing bond of trust. What did inter-continental traders use to transact in the 17th century? They certainly didn't use IOUs, wampum, collectibles, or credit relationships. They knew that they might never see each other again, so they used the hardest money they had available — gold and silver. Monetary metals speak for themselves; they are no one's liability.

In this same way, Bitcoin is a means to transfer wealth between individuals who both have an interest in final settlement. It is not a means to establish a credit relationship (although Lightning is an early move in this direction). Bitcoin is deliberately amoral, it has no requirements to entry and asks nothing of the user aside from a valid signature. It facilitates commerce

between people who explicitly disagree with each other. Thus trying to impose a moral code on Bitcoin is contrary to its very nature. If everyone who used Bitcoin agreed with each other, then no one would need Bitcoin — they could all exchange IOUs backed by their mutual trust in each other. But because the world is messy, and people disagree with each other, hard money is warranted. Our chaotic world practically demands it.

So if you are the kind of person that rejects a useful transactional medium because someone you dislike is using it as well, it wasn't suited for you in the first place. Bitcoin is edgy precisely because the world needs a payment and savings system which cannot be interfered with on moral or political grounds. To repudiate these transactional constraints is to violate the carefully poised moral setting that has seized the West. If stepping out of line isn't for you, stick to Paypal instead.

Bitcoin is an apocalyptic death cult...

As Bitcoin hater-in-chief David Gerard so elegantly puts it, Bitcoin is in fact an apocalyptic death cult. Apocalyptic, because Bitcoiners recognize the futility of the current monetary system, and appreciate that it is likely to end in tears. Death, because States won't give up their monetary privilege easily. Bitcoin is veiled in eschatological overtones. Cult, because you have to be somewhat deranged to take a pill this black.

Freedom is not "Free".

So spare a thought for the Bitcoiners. They are fully awakened to the pending grief and strife that await us, Cassandras warning governments and citizens alike to the disruptive effects of truly sovereign currency (sovereign, as in free, not as in State-owned). But unable, most of the time, to convince their fellow man that the State's monetary machinations may not be sound. Most people are content to surrender all freedom and autonomy to the Leviathan, as long as the pot they are in boils slowly.

... but it's open to all

The exact reason that Bitcoin is despised by so many— identity, creditworthiness, and trust are irrelevant in this system, making it a fertile ground for criminals — is the exact reason why it's so inclusive. Unlike Paypal, Venmo, or traditional payment processors, it cannot deplatform you for

wrongthink, holding subversive political views, being a sex worker, or legally selling cannabis. Ours is the biggest possible tent. Don't be distracted by the online discourse. Bitcoin is utterly indifferent to the political views of its users. Its core developers, the high priests of the protocol, can barely change it: (implementing a fairly routine upgrade, SegWit, took them _years _of cajoling and pleading). Getting it to do anything other than produce blocks, accept valid spends, resolve forks, and relentlessly march onward is virtually impossible.

Whether Bitcoin will challenge the State, or whether that task will be left up to a successor, is yet to be determined. That the State's monetary privilege has been permanently eroded is evident though.

It died a little that day in January 2009 when the *Chancellor [was] On the Brink*, and it has been shrinking ever since.

By Nic Carter, Oct, 2019

The Bitcoin Times Ed 2 is the collaborative work of 8 writers & 1 designer with the intent to educate, inspire and spread ideas on bitcoin.

Each section will be released on Medium as a free long form article, and the full, compiled version of the Bitcoin Times will be available for free at the link below. In 2020, we'll release a limited edition hard cover collectible, for purchase, which you'll be notified of by email if you download the free pdf.

If you found value in this or any of the other essays and articles, please support each of the contributors by sharing it out & following their work.

Download the full guide at:

The Bitcoin Times

(Soon to be updated to: https://bitcointimes.news)

Bending Bitcoin — The Principle of Hard Money

By Ben Kaufman

Posted December 30, 2019

Hard money is one of the most well-known monetary terms used in practical discussions. From political discourses on policy decisions to the commentary debates of the financial sector, the term can be heard often enough to make even the ordinary citizens familiar with it. However, and despite its substantial use, while the concept of hard money has a very clear connotation to traditional fiscal responsibility with the monetary system, its exact definition is still quite vague. While for many, it is merely a practical term almost synonymous to a gold-backed system, its conceptual meaning clearly goes beyond that. For theoretical discussions then, it should be evident that, despite gold being for centuries the most accurate practical representation of the concept, it cannot be its very definition. Until today, in spite of the theoretical merits of adequately defining the term, such exact definition seems to have been quite unnecessary. For a long time, it has been

established that assuming it as simply meaning a gold system is sufficient for all practical purposes.

In recent years, however, the term has started being applied to the newly emergent system of cryptocurrencies, and most notably, to Bitcoin. The new employment of the term to describe the new-born monetary system causes an evident confusion as to its exact meaning, and the question of what it is that makes money "hard" has become of practical significance. This current state of affairs has left us with multiple questions. First, what indeed, would be a satisfactory definition for the "hardness" of a monetary system. Then secondly, whether this term could be appropriate to describe Bitcoin. And lastly, if other cryptocurrencies also merit such classification. The rest of this article is thus an attempt to deal with the problems just presented above. As a last note, this article will solely deal with the question of what hard money is. The broader question of whether a hard money system is even desirable in the first place is out of scope for this piece. On that matter, interested readers may find my answer in my previous article.

What is hard money?

While, as said above, no precise and consistent definition seems to be prevalent in discussions on the subject, we must first provide such a definition if we are to investigate the matter seriously. The definition we shall use from this point forward is as follows:

The hardness of money is in reverse relation to the monetary inflation, and the consequent dilution of the value of the existing stock, which can economically be inflicted on it.

Now, there are a few notable points to clarify in order to avoid common misunderstandings regarding the above definition. First and foremost, we shall note that, like many economic terms, the hardness of money is a subjectively perceived factor, subjected to constant changes by various events (such as technological improvement in production, effective counterfeiting, etc.). In this sense, it is similar to discussing the purchasing power of money, which, while can be generally understood, is a rather subjective and ever-changing metric. While this consideration certainly does not invalidate its importance and usefulness, we shall keep in mind these limitations and uncertainties which necessarily accompany its use.

The second point to notice is with regards to what exactly does "can economically be inflicted" mean, and what are the subsequent implications. In simple words, the question is how much of the money can be produced until its value drops (or production costs rise, or both) to such an extent where production is no longer profitable. Here we can notice a sharp distinction between "commodity money", of which the market determines

the supply, and fiat money, of which legislation determines it. As the supply of commodity money is determined by the market demand for it (its price), the costs of its production will always tend to match its market price, as producers will quickly rush to produce more if the margin is larger, and stop production even faster if that becomes unprofitable. On the other hand, the supply of fiat money, such as the government paper we have today, is regulated not by the demand for it, but rather by bureaucratic processes of arbitrary decisions. The main difference concerning us here between the two monetary systems is that, with the former, the risk of dilution of wealth is to be found mostly with technological progress in the production process. While for the latter, there always exists a risk of massive dilution for any arbitrary cause. Thus, while money from the former category is worth the extra effort of looking into its hardness, the latter leaves us no doubt as for its "easiness". It might be worth mentioning that this monetary easiness is not at all accidental, but rather the intended result of conscious policies aimed mainly at government financing through seigniorage — the monopolistic profits made by the issuer of a currency which is protected by law from market competition. A discussion on the economic and ethical issues of fiat money in general, and seigniorage in particular, is out of the scope of this article. However, interested readers can find such discussions in "The Ethics of Money Production" by Jörg Guido Hülsmann.

A (Very) Brief History of Hard Money

So far, we provided an exact definition for the concept of hard money and saw why it must be commodity money produced through open competition on the market. Now, we will continue investigating the principles of hard money by looking into some historical monetary systems, and the gradual shift from easier monies to a harder one.

The history of money, including such notable examples as salt, seashells and glass beads, is full of cases where the advancement of production processes or even the improvement in trade connections for a certain money, along with its inferior monetary properties (durability, divisibility, etc.) compared to another money, caused it to depreciate quickly and eventually to lose its monetary role altogether. Such a process is perhaps best illustrated through the famous case of the Rai stones of Yap island. These stones, ranging in size (and value) from small beads to some massive 3.6 meters tall ones, were for hundreds, if not thousands, of years used by the native population as money. As the methods for producing them did not improve much for the long time of their monetary use, their production remained quite stable for many years, establishing their local status as hard money. However, with the arrival of Europeans around the end of the 19th century, and with the advanced tools and production methods they brought with them, production became increasingly cheaper and the stones started depreciating rapidly until they

eventually lost their monetary role to the Western money system. Similar cases were witnessed at many times and places throughout history, such as glass beads and cowry shells in Africa and America, salt in Europe, and so on.

Since the beginning of their use as money from about 1000 BC, precious metals were probably the most prominent money of all. Used mostly through Europe and Asia as the most common monetary system and later spreading rapidly to all other continents after the discovery of America and under the strong influence of European colonization efforts, the entire world started converging towards a unified monetary system of precious metals, namely copper, silver and gold. The growth in the use of such metallic monetary systems was much due to their relatively excellent physical monetary properties, such as their durability, portability, and divisibility. No less influential, or even more so, was the monetary hardness they demonstrated in comparison to all other monetary goods throughout history. This age-long trend towards the use of metal currency arguably reached its peak around the middle of the nineteenth century. Flourishing as the Gold Standard, which prevailed during La Belle Époque, it has declined since the end of this period around the beginning of WWI. Since then, there has been a strong tendency in the direction of irredeemable fiat money, mainly in the form of paper, "token" coins, and later also its digital representations of today.

This transition from metallic to a purely fiat standard has its origin with the Chinese invention of banknotes, a paper (or similar material) note which the bearer could redeem for specie, on-demand, from a reserve maintained by the producer of the note. The use of such banknotes as a circulating media of exchange began around the 11th century, with the Jiaozi paper currency, and has continually spread around the world ever since. The peculiarity of the practice was of course not with the new physical form which the instrument of payment has taken, but the fact that, although all notes were redeemable on demand, the reserve maintained only a fraction of the funds needed for the redemption of all notes — what is commonly known today as fractional reserve banking. While these paper forms of money were initially privately issued and used mostly for their easier portability (as carrying metal coins became heavy), they were quickly nationalized and served as a new form of a government financing scheme, namely seigniorage, enabled by their cheap production costs and the use of such fractional reserve techniques. A full examination of the history of banking is out of scope for this article. For our purposes the important thing to note is that while the physical form of money started shifting towards paper long ago, today's concept of permanently irredeemable paper money constitutes a purely modern "invention". While it is similar in form and probably owes its existence to such ancient practices as described above, it lacks any historical precedent.

It is true that the global convergence towards metallic money, and especially the later transition from metallic to a gold standard, owes a significant part of its emergence to the political influence of governments. However, the massive scale of interventionist measures taken to implement this latest transition to a completely irredeemable fiat standard is entirely unprecedented. Arguably starting with WWI, consolidating with the end of WWII, and ripening with Executive Order 11615 of President Nixon in 1971, the transition from a metallic to a pure fiat money has nationalized and politicized the global monetary system in any conceivable aspect. The consequence is a regression in the evolutionary tendencies of money from that of international convergence on the hardest money to a degradation towards the cheapest production methods, which will generate the highest seigniorage profits possible to extract for each national government. Thus, we are not surprised to find out that the last hundred years have experienced over 50 cases of hyperinflationary economic collapses. What used to be an extremely rare event has become an epidemic of modern economies, and is now virtually the only check which deters governments from excessive money production.

To briefly summarize, the history of money shows us a tendency for international convergence of monetary standards towards the hardest money. This tendency likely reached its peak with the nineteenth-century gold standard, and has been suppressed for the last hundred years by political forces compelling the use of the easiest money — that which can be infinitely created at their whim. While the trend towards hard money seems to have completely reversed, the great economic distress and instability arguably caused by this reverse in trend may indicate its mere temporary nature. Thus, there appears to be a strong reason to believe that these last hundred years will be but a short regression in the long trend towards harder money.

Nevertheless, this last century left us little hope that such a return to progression could manifest itself as a return to a gold standard. With the transition to global online payments, the need for a centralized trusted reserve for the smooth operation of such a system has grown more evident than ever. Yet this very need for a centralized reserve system is precisely the flaw that allowed the political capture and eventual demise of gold in the first place. Also, taking into account the immense expansion in the power of governments worldwide during the last few decades, the risks inherent in such a centralized reserve system make a return to gold seem like an impractical option, however theoretically desirable it may be. Despite the obstacle posed by the closing of this past option, the advancement of technology has opened up a new alternative in the form of Bitcoin, a digital adaptation of hard money. If it indeed provides a secure alternative, such a system has a true potential for becoming the next evolution in monetary

standards, continuing the old trend towards harder forms of money. It is investigating this premise to which we will now turn.

Bitcoin as Hard Money

In a nutshell, Bitcoin was built to have a final and limited supply, produced by open competition for expending computational power. It is by design limited to a total supply of roughly 21M bitcoins to be produced according to an estimated time schedule. The production of new Bitcoin requires solving a cryptographic puzzle, with each competitor having the probability of solving it in direct relation to its expended computing resources. We see that, by theoretical design, Bitcoin was designed to be hard money, with an eventual hardness allowing for no further production, in a sense, creating absolute scarcity. While we now have the basic understanding needed of the theoretical guarantees of Bitcoin in regards to its monetary hardness, we must proceed to look at how those guarantees are to be secured in practice, and what possible threats may arise for them.

The monetary hardness of Bitcoin is guaranteed by its consensus rules — the code that either accepts or rejects transaction history (in the form of blocks) according to their validity with this predetermined set of rules. These rules include, among other things, the requirement for a solution to the cryptographic challenge (the proof of work), a verification ensuring no transaction spends more bitcoin than its sender has, and a check that no bitcoins were issues over the supply limit or before the predetermined schedule. Every machine which has verified all the transaction history up to the present, and which maintains as the result of this verification the present UTXO set (the current set of owners of bitcoins), is called a *full node*. The entire "Bitcoin network" is the sum of all full nodes communicating by the same protocol rules and propagating information about new data (mainly blocks and transactions). By following identical rules of verification, and by passing all data between themselves, all nodes are expected to reach the same view of the current state — a consensus.

There are two possible ways by which nodes may reach a disagreement over the present state — by having different (or partial) data or by verifying according to different consensus rules. The former case is usually not an issue. It includes mostly nodes in the process of joining the network (in IBD), nodes which have not yet received a new block, and on rare occasions, the case where two conflicting blocks are solved independently of one another and are propagated at the same time. This area of data propagation, while being highly critical, does not concern the monetary hardness of Bitcoin per se, and thus we'll ignore it for the present discussion. The second possible case — the establishment of different consensus rules — is where the risk of inflation lies and is what we will now examine.

Strictly speaking, there are no "definitive" rules for Bitcoin. There are, for example, the original rules of the first version of the Bitcoin software, and the rules of the current Bitcoin Core software, but since Bitcoin is an entirely decentralized project, there are no rules one *has to* follow. This essentially means that (for convenience, taking the most unlikely yet still technically possible case) if all participants in the Bitcoin network were to unanimously modify their rules, for example, as to have permanent inflation, these would become the new rules. There exists no controlling authority which could stop users from running whatever version of the software they desire. This characteristic of Bitcoin, which is inherent in its nature as a man-made digital asset, is probably its most significant difference from the natural commodities, such as gold, and thus requires great attention in assessing the practical hardness of Bitcoin.

To understand what guarantees the hardness of the monetary policy and other consensus rules of Bitcoin, we should start by analyzing the network, not as a whole, but starting from the very individual nodes comprising it. As far as a full node is concerned, its control over the rules — the "definition" of Bitcoin — is absolute, there is no procedure to compel a node to use a particular set of rules. On the same token, it is also the case that no node can force another to accept its rules. Thus we arrive at a situation where, starting with the initial consensus rules laid out in the first Bitcoin software as base guidance, all nodes in the network must either converge on the same set of rules or lose the ability to transact with the rest of the network. If a node decides, for example, to mint itself new bitcoins "out of thin air", he may change his own rules as to allow that, but at the cost of losing the ability to transact his "Bitcoin" with the rest of the network. If we assume two people have modified their rules in that way, they give up the ability to transact with all but one another. The same thing happens if we now imagine that 10% of the participants changed their nodes to the new rules, the network can be said to have split into two distinct networks, each defining Bitcoin in a different way.

While such cases as described above are of little interest, they beget the question of what happens if 50%, or even say 99% modify their rules. In other words, what happens if the majority changes the rules, and what would define a majority in the first place. With Bitcoin, being essentially a communication network, the most appropriate manner to determine a "majority" is to consider the extent to which participants can communicate (transact) with others. Contrary to common fallacies, it does not matter how much hash rate, market cap or total transaction volume a network may have and even less so does it matter how many nodes run its rules (as anyone can deploy as many nodes as he wishes). The only metric which is relevant for the determination of which rules a node joining the network "should" run is to what extent it can transact with others. In simpler terms, how many of those

with which he wishes (or expects) to transact with will accept his bitcoins as valid.

The threat of being unable to transact with others (running incompatible rules) is what deters participants (both other nodes and miners) from arbitrarily modifying the rules. The need for such extensive coordination is what makes changes to Bitcoin, from trivial bug fixes to the most controversial changes, so difficult to implement. Any modification means risking losing the ability to transact with the rest of the network (or part of it). Thus the theoretical ability to exercise such modifications is rarely used. To get back to our subject of monetary hardness, what is most important to understand is that the hardness of Bitcoin for each participant depends on the ability and likelihood of a sufficiently large portion of the network to coordinate and successfully perform a consensus rule change which will inflate the supply of Bitcoin. It is important to emphasize that "sufficiently large" means such a large portion with which losing the ability to transact would render Bitcoin useless. This measure, like the rules of Bitcoin themselves, is by necessity subjective, but it should not be hard to have a rough agreement on what such a case would look like.

Bitcoin's Soft Spot

As we have seen by now, since each user of Bitcoin can run his own node, the power of a participant in the influence over the enforcement of the consensus rules is solely with regard to the transactions he is personally involved in. A node must verify all transactions not for the sake of enforcing the rules for others on the network, but for being able to determine whether a payment he receives himself is valid or not — this is the economic activity of a participant, and it is the only manner by which he may influence the decision of others to use certain rules. Whenever one accepts payment in Bitcoin, it's akin to asserting what the definition of Bitcoin is by enforcing the consensus rules under which the payment is accepted.

However, while in our analysis until now we have (intentionally and implicitly) assumed that every participant is actively setting his own rules by running certain code with his full node, and using it to verify the validity of incoming payments, this is not necessarily (and indeed is often not) the case. It is completely possible for anyone to delegate the responsibility of this active rule setting by passively trusting another entity with validating transactions for him. By doing so, the receiver of payment in a sense delegates his economic activity on the network, thus the influence over the consensus rules, to another which in turn may use it with whatever rules he likes. For example, assuming I am using an online Block Explorer to verify that I have received a transaction, whenever I accept a transaction in such a manner, I delegate the influence my economic activity may have over the rules to the

operator of that service. If, for example, the operator would decide to use rules allowing larger blocks, new signature schemes or (more worrisome) changing the rate of inflation, I am not only susceptible to passively accept these changes against my consent, I am in fact actively endorsing them by signaling my willingness to accept transactions using these specific rules.

In the previous section, we have concluded that in order to impair the monetary hardness of Bitcoin, it is necessary to coordinate (convince others to perform) a consensus rules modification causing such a change with a sufficiently substantial portion of the active economic participants of the network, a task we can consider quite impractical in light of both theoretical considerations and practical (although short and insufficient) experience. This difficulty in coordination is not merely due to the decentralized structure of the Bitcoin network, but specifically due to the decentralized, or more correctly self-sovereign, enforcement of rules over individual economic activity. When each participant is actively validating his transaction, it is necessary to convince a very considerable part (if not almost all) of them to accept the new set of rules modifying the hardness of Bitcoin. However, the fewer participants actively validating their transactions, the more centralized does the verification of economic activity becomes, and thus the easier it is to carry out such a change.

Although, in theory, nothing prevents the use of a full node by each participant, there are various practical obstacles for running and using a full node. Probably the most significant of these obstacles is the technical complexity of operating such a node, which for many is still a very non-trivial task. Moreover, there are the issues posed by the size of the transaction history data, which when increased affects both the initial time needed to join the network, while also raising the hardware requirements needed for an active node, making it increasingly more expensive to maintain. These issues (and potentially various others), while probably manageable, can, if left unhandled, lead to such dangerously large centralization of payment verification which could potentially nullify the monetary hardness guaranteed by the theoretical design of Bitcoin.

The greatest risk to the hardness of Bitcoin lies therefore in the centralization of payment verification. We see that in theory, if a sufficiently large part of the network is using just a few service providers for validating their transactions, there is a chance that these service providers will coordinate a change to the supply of Bitcoin while having the unaware but nonetheless economically active support of everyone using them to accept Bitcoin payments. It is true that as long as you run your own full node you are able to stick to the present “hard money rules”, but if such a large part of the network has moved (aware of the change or not) to an inflationary set of rules, you will lose the ability to transact with them and thus the utility of using Bitcoin. Before reaching our

conclusions on the hardness of Bitcoin, we should address the question of whether other cryptocurrencies may be termed hard money, and what differentiates Bitcoin from all of them.

What about "Shitcoins"?

Contrary to constant claims from almost any "blockchain-based" shitcoin, none of them can be considered as hard money. While there are many different implementations for how a decentralized blockchain may work (PoW/ PoS, etc.), they must all rely on the same client-side payment verification model discussed above. However, unlike Bitcoin, they all either merely pay lip service or even disregard completely the importance of self-sovereignty in determining the consensus rules. That is, they all tend towards centralizing the formation and enforcement of the consensus rules. Some projects have some sort of central authority, to which, with little exception, most decisions on the rules are delegated (whatever explicitly or implicitly). Others disregard the necessity of keeping the ability to run a full node as accessible as possible and thus lead to centralization in payment verification. And yet others which try to set up a "governance" process — making arbitrary changes to the consensus a matter of formality.

I should emphasize that I'm not speaking of all "blockchain projects" or projects with decentralized governance. What I'm speaking against is the often-heard claim of various tokens that they should be considered as hard money, while in practice, their supply can and regularly is arbitrarily altered. As defined above, the hardness of money is in reverse relation to the monetary inflation which can economically be inflicted on its holders. With such digital assets that either rely on a centralized (or semi-centralized) payment verification or have some clear and simple process for modifying the consensus rules, there cannot be even the pretense of being hard money. The potential inflation which could be inflicted upon them is infinite — once you can modify the "monetary policy" of a digital asset, there is virtually no limit to how much you can create from it, and it cannot be considered a harder money any more than any of the fiat monetary systems.

There is no claim here that the current state of Bitcoin is perfect, or anywhere near that. There is of course much undesirable centralization of verification in the space of Bitcoin as well, and even more concerningly, there is a great sentiment of ignorance of the importance of such self-sovereign verification. However, the main difference is the insistence of Bitcoin "activists" on promoting the use of full nodes, such examples being the Core developers' efforts on keeping nodes usable on even such weak and affordable machines as a Raspberry Pi, and the many projects which provide various options for running a full node, from a plug and play machines to a completely DIY solutions. The ecosystem dedicated to promoting and simplifying the use of

Bitcoin full nodes is both very significant and rapidly growing, and the community's emphasis on this subject is unmatched by any other project.

Furthermore, and no less important, is the fact that, being the "first of its kind", Bitcoin serves as the base consensus rules not only of a single asset but of general digital value transmission. As Bitcoin is in principle a protocol, or even (in its most basic sense) an idea, for "A Peer-to-Peer Electronic Cash System", and since its rules are, as we have seen, determined individually and independently by its users, it means that in some sense, all other implementations of such a system could be seen as versions of Bitcoin, but with a completely modified set of rules. With that taken into account, the mere fact that these other "Bitcoins" have such a different set of rules and a substantially different monetary policy, signals the relative malleability of their rules — which have disconverged from the original base rules in a very incompatible manner and for no real (monetary) reason (such as an emergency change due to a bug). We may say that these other coins, being a mere replication of Bitcoin's model, at least in the monetary field, have already proven their lack of hardness by their mere creation as an arbitrary divergent from the main Bitcoin protocol. All those coins might very well have significant differences from Bitcoin and various other "use-cases", but with regards to being a hard money system, they have all started at a loss against "The Bitcoin Standard".

On Bugs

Before concluding our discussion, there are few remarks which still need to be made. First, while until now we have discussed the hardness of Bitcoin as derived from enforcing its coded rules, we must note another caveat. Bitcoin is a software, and like any software, it can and did (and possibly still does) have bugs. While it's true that such bugs could cause unexpected inflation, they are unlikely to have any serious impact on the hardness of Bitcoin.

To understand why, we may divide the possible inflationary bugs into minor (1, 10 or even 100,000 bitcoin — like could happen with CVE-2018–17144) and major ones (like a 184 billion coins inflation). Minor bugs may indeed introduce some inflation, which technically would undermine the core tenet of limited supply, but since they can be quickly fixed, their effect on the total supply will be effectively inconsequential in the long run. In more popular terms, they may increase the stock of Bitcoin to a small extent, but they do not undermine its guarantees as for the upcoming expected flow of new coins.

As for major bugs, while potentially undermining the interim confidence in the success of Bitcoin, the retroactive countermeasures which could be implemented to nullify the effects of such a clear violation of the constitutional precedent of limited supply would be successful in preserving

Bitcoin's creed. Such measures would be absolutely necessary to preserve the value of the coin-holders and the utility of the network itself. In fact, this is precisely the course of events that transpired in the wake of such a catastrophic bug in 2010. As we have concluded previously, the lack of malleability of the rules of the network contributes to its hardness as a monetary medium. However, here, it is apparent that the literal opposite is true as well; it is the ability of the network to evolve to protect users by way of them each acting individually in their own self-interest that defends the 21 million hard cap.

Conclusions

Throughout the article, we have discussed the basic principle of hard money and how it relates to Bitcoin. We saw that from the theoretical aspect, the usual description of Bitcoin as "the hardest money ever" is well deserved, but from the practical perspective, the soundness of this statement is to a large extent dependent on the exercise of their self-sovereignty by its users — the use of full nodes for validating and accepting transactions.

Run a Full Node!

For the hardness of Bitcoin, it is necessary that as many economic participants as possible use their own full node. However, far more important than this "collective" necessity of self-sovereignty, there are the "individual" reasons to run a full node.

As said above, when you don't verify your own transactions but trust another party to do so, you blindly accept whatever definition that party may use for what Bitcoin is. It may very well be that they verify transactions by rules incompatible with most other network participants. Furthermore, they might not be truly verifying anything at all, and just arbitrarily present to you fake data. It is of course very unlikely, at least at this stage of Bitcoin, for established service providers to risk losing their customers by providing them with incorrect or misleading data (although we have already seen such cases, mostly with the Bitcoin Cash and Segwit2X cases). It may very well be fine to occasionally use the assistance of such services, especially for small payments.

The main thing to remember is that by delegating verification of payments, you open yourself to significant risks, while also potentially weakening the hardness of the rules of Bitcoin. I would not discourage the use of such services altogether, but for those using Bitcoin either frequently or with large amounts, as well as for anyone who cares about their privacy and wants strong security, I would highly recommend to make this effort and find a self-sovereign full node solution which suits their needs. (See below for guidance for that).

Although commonly heard, the advice to use a full node cannot be stressed strongly enough, it is a crucial part of using Bitcoin — as without using a full node, you cannot even know if you're really using Bitcoin.

How to Run a Bitcoin Full Node

Up to this point, we dealt with the fundamental question of *why _run a full node. Now, it is time for us to move to the no less important question of _how* to run a full node. But first, let's start by clearing a few popular misconceptions as to the requirements needed for running a full node. As for today, the minimum disk space required to operate a Bitcoin full node is no more than 10GB. For an illustration of how small that is, you can find a 16GB SD card for less than 4$. Most smartphones today already come with at least 32GB, and for many, it is possible to add more with such SD cards. It is true that storing the entire history (~300GB as for today) is much preferable, but this is not necessary for running a secure and fully verifying full node, and should not be an excuse not to use one.

Another important misconception is an alleged need for strong computing power, this misunderstanding usually comes from the confusion between a Bitcoin miner and a full node. It is true that in order to run a (profitable) Bitcoin mining operation, it is necessary to have some expensive specialized hardware, but this is not necessary at all for running a full node. To run a full node you can use as little as a mere Raspberry Pi, or simply your personal computer or smartphone.

The last thing to note here is the alleged complexity of running a full node. It must be admitted that for now, running a full node is probably not something your grandma will be able to do, but so wasn't, and still isn't for many, using a smartphone or a web browser. While in the present time it is certainly easier to use a web browser than running a full node, we should remember that for now Bitcoin is a not only new, but brings a completely new paradigm for using money. The invention of implementing Bitcoin itself was for decades considered an impractical challenge. Compared to that, the challenge of building an ecosystem of user friendly full node solutions is exceedingly minor. The fact that we've gotten so far makes me quite confident that the challenge of creating a user-friendly full node will not be a true obstacle. It is also conducive to look at how greatly the simplicity of using a full node has already improved during these last 10 years. Without having any budget whatsoever, depending on the voluntary contributions of people alone, dozens of solutions have already been created for various different audiences.

Here, I will list a few of the present options. As I cannot guarantee otherwise, I must note that this list might contain imperfect options, and does not

substitute for doing your own research in regards to the quality and integrity of the services.

Probably the simplest solution for anyone familiar with the basic use of a computer is to use the Bitcoin Core software. While its interface is not the best, it is simple to install and use, and is the most common Bitcoin software. For more information see the links below:

- Bitcoin Core official Download page
- bitcoin.org Full Node Guide

Another option is to use Bitcoin Core through another app. There are few such services which will install and set up Bitcoin Core for you. These might not necessarily be simpler than the normal Bitcoin Core install, but they all offer more features, such as Tor support/ Lightning Network setup/ Coin mixing and other useful features.

- Node Launcher — Bitcoin and Lightning one-click setup tool, including useful Lightning tools and guides.
- Wasabi Wallet — Bitcoin wallet with built in Bitcoin Core automatic installation, CoinJoin mixing, and hardware wallet integration.
- Bitcoin-Standup (warning: still in early beta) — MacOS (possibly Linux soon) tool for setting up Bitcoin full node and includes tools for remotely connecting through a mobile app over Tor.

For the less tech savvy users, a “plug and play” full node might be the best solution. These cost generally between 200$ to 500$, but they come with all the hardware, many great features, and generally much more user-friendly design.

- Nodl — Includes a Bitcoin full node and one-click support for various features such as Lightning node, Tor and BTCPay server (also available with Samourai Dojo support here).
- Casa Node — Bitcoin full node which comes with a user-friendly UI, full Lightning support and built in integration with other Casa products (such as a lightning mobile wallet and membership for their multi-sig wallet).
- RaspiBlitz — Raspberry Pi based Bitcoin full node with Lightning integration.
- MyNode — Similar to the Raspiblitz with a slightly more user-friendly interface and integrated features like a Blockexplorer and Electrum Server for Hardware Wallet support.
- Lightning In A Box — Bitcoin and Lightning node with BTCPayServer pre-installed and configured.

- BTCPi — A cheaper version similar to and sold by Lightning In A Box.
- BitBoxBase (not yet released) — Bitcoin full node includes a hardware wallet secure element, user friendly wallet, a Lightning node and Tor support.

For those technical users who likes to get their hands dirty (or just want to save money building their own node):

- RaspiBolt — A step-by-step guide for creating a Bitcoin full node with Lightning support using low-cost components.
- RaspiBlitz — The DIY version of the RaspiBlitz. Should cost about ~150$ for the hardware parts while giving the same results as the pre-built option.
- MyNode — Similar to the RaspiBlitz again which lets you build your own node from ordered parts. The basic software is provided for free but can be upgraded to paid premium with one-click upgrades for more features.
- RoninDojo — DIY Samourai Dojo with Bitcoin full node, Tor, and Whirlpool coinjoin support.

There are also several mobile Bitcoin full node options:

- ABCore — Android app with a Bitcoin full node, uses Bitcoin Core and provides an interface for using it as an Android app.
- HTC Exodus — An HTC Android phone with a built in Bitcoin full node, a hardware wallet TEE element and more related features.
- As for today, there is no iOS compatible way to run a full node Bitcoin. However, the app Fully Noded allows you to connect to your node remotely and use it on iOS.

A note on key management:

It is important to note that while many of the solutions presented here provide the user with a Bitcoin wallet, many are using (either only or by default) a “hot” wallet, i.e. a wallet stored on a machine connected to the internet. This is considered a relatively insecure practice. Many users therefore opt to use hardware wallets (such as Trezor, Ledger, and ColdCard). Though (at least considered) much more secure for key management, the benefit derived from using such hardware wallets is significantly impaired if they are not used along with a full node. While most hardware wallets don’t provide a (simple) integration with a user’s full node, there are complementary solutions developed to provide such support.

- Bitcoin-Core HWI — A UI for interacting with many types of hardware wallets while connecting them to Bitcoin Core for verification.
- Electrum Personal Server — Allows the integration of Electrum wallet with a Bitcoin full node. Supports various features including hardware wallet integration, multisig wallets etc.
- YetiCold — (warning: still in beta) A self-sovereign, easy to use, multisig setup protocol aimed at minimizing trust and various attack vectors.

Special thanks to Ben Prentice (mrcoolbp), Bezant Denier (bezantdenier), Daniel Wingen (danielwingen), The Bitcoin Observer (festina_lente_2), Thib (thibm_), Simon Lutz (simonlutz21), and Stefanie von Jan (stefanievjan) for all the feedback I received from their reviews, comments, and suggestions which helped me shape this article.

The rise of the individual

By Aleksander Svetski

Posted December 31, 2019

The Fall of the State

"The greatest danger to the state is independent, intellectual criticism"

- Murray Rothbard

Dedicated to those who stood up to Tyranny. Today the people of HongKong, tomorrow, all of us.

Why does Bitcoin matter?

I wrote an article on Hacker Noon about a year ago now, which is entitled "Why Bitcoin Matters".

I explored Bitcoin from first principles, starting with an examination of the societal stack, money's role in society, how it evolved over time, it's fundamental attributes & functions, and finally culminating into an analysis of why Bitcoin is superior both as a monetary unit & a monetary network (aka; a monetary operating system).

Winston Smith's sub-conscious cry

For this piece, I'd like to take a more, perhaps, 'revolutionary' approach to why Bitcoin matters.

It's that "thing" which the protagonist (Winston Smith) of Orwell's seminal piece, 1984, was unknowingly calling out for, and inherently describing, whilst O'Brien was torturing him.

The "force" of good that exists in all humans, and the desire for Freedom was and always will be there, but a tool via which it could manifest in spite of the oppressive power of an authoritarian state, just did not, and could not exist at the time.

But it's no longer 1984. Times have changed.

Bitcoin matters, because Bitcoin is that tool. It's what we, the revolutionaries have been missing this entire time.

We had the human spirit, we had the will, we knew there was something wrong, but we lacked the tool with which to stand up to Big Brother.

Bitcoin is that tool.

Whilst getting rich because you're in the game early is cool and all (greed drives me as much as it does the next person), it's this revolutionary aspect of Bitcoin that should get you most excited about it's prospects.

Not since the gunpowder revolution were ordinary men & women able to stand up to those who chose to oppress or rule them unjustly. Only this time, it can be done in a non-violent method, whereby one can peacefully opt out — as John Galt and the 'men of the mind' did in Atlas Shrugged.

This, above all else, is why Bitcoin matters, and why the legend of Satoshi will go down in history as the most profound story since the beginning of time (or whichever significant religious event / story you'd like to reference instead).

This fact also just reinforces why megalomaniacs like Craig Wright, and his band of deranged cool-aid drinking followers are simply the antithesis to Satoshi and Bitcoin.

Revolutionaries & Renegades

Bitcoin is the stand we take, this decade, this century, this millennium. **Bitcoin** is the tool we use to separate money & state. **Bitcoin** is the lightning rod that will bring together the renegades & the revolutionaries.

Bitcoin is of and for the liberators, the missionaries & the visionaries.

The men & women who won't accept suppression, oppression, or the dictates of a world in which we're subjugated to the whims of central planners, bureaucrats, rent seekers, attention whores, corrupt politicians, crooked bankers, backdoor dealers, creeping socialism and crony capitalism.

There has never been a tool so incorruptible yet so inherently powerful & accessible.

With it we can reimagine the "state". We will transform society.

We will redefine the very essence of what it means to be a modern, collaborative human.

Have I gone off the deep end? Of course.

But there's an entirely new world over here — and at some point, I know you'll join me.

May this essay be a start....

The separation of Money & State

Make no mistake about it, this century will be defined by the separation of money & state.

It has already started, and nothing can stop it.

It's inevitable, assuming of course, we plan on surviving. The alternative is a parasitic dystopian future in which society feeds on itself until it collapses.

So...if we err on the side of humanity's continuation, we must be honest with ourselves and realise a paradigm shift is nigh.

Even Ray Dalio is coming around. He's just missing the word Bitcoin from his most recent articles — although I would guess that's a wise move in his shoes, for if he mentions it in a positive light, it may cause a stampede and drive the god damn price up to $1m a coin prematurely and fuck up the S2F model!

Furthermore, it will mean my shitty fiat will buy less Bitcoin — and we can't have that (yet).

So Ray, if you're reading this, keep buying Bitcoin *privately*. Please.

_...._Back to separating money & state.

The Paradigm is shifting. Economically, politically, technologically, socially, ethically and in every other way imaginable.

Davidson & Rees-Mogg, in their seminal pre-2000 work, "The Sovereign Individual", posited that this shift started in the 90s, with the fall of the Berlin Wall, the end of communism, and the beginning of the information age.

I would tend to agree with them.

Communism was the peak of the parasitic, centralised state, at least measured in terms of brute violence & broad incompetence.

The crony-capitalism & quasi socialism we in the West live with today are very much improvements on the communism of the USSR, and to some degree so is the Communism in China (thanks to the benefits of capitalism that helped enrich their rulers), but the inherent concentration of the unit through which society is measured (ie; money) has led us to a point of diminishing returns, where peak stupidity, peak stimulus, and peak economic distortion mean the government, aka; "the state" can no longer squeeze more out of the system and has begun to feed on itself.

Note that I omitted peak 'outright' violence — but I guess that depends on who you ask. The people of Hong Kong, or the Falun Gong would probably disagree with me.

This shift in "feeding on itself" is evident in the comments made by megalomaniacs such as Bernie Sanders or AOC, for example:

"The billionaire class is scared, and they should be". Bernie Sanders

Comments as such can only come from parasites who have never produced anything, and can only subsist via the expropriation of the production of another.

This is only possible in a system where the instrument through which we measure economic value is the sole privilege of the state.

But this is now changing.

The separation of money & state is being driven by the individual who now has the technological capacity AND the monetary ability to become more autonomous, independent, sustainable and yes, more sovereign, than they have ever before been.

The period will mark the rise of the sovereign individual

Whilst the peak of the state may have come 20yrs ago, the shift is on-going.

It will not happen overnight.

Prior shifts have taken multiple generations, if not multiple centuries to occur, and although today, progress much faster, we still have a ways to go.

And it's not going to a smooth ride.

Paradigm shifts happen in a tumultuous fashion. They are *by definition* both constructive AND destructive, simultaneously! Change, in the real world, is a complex process.

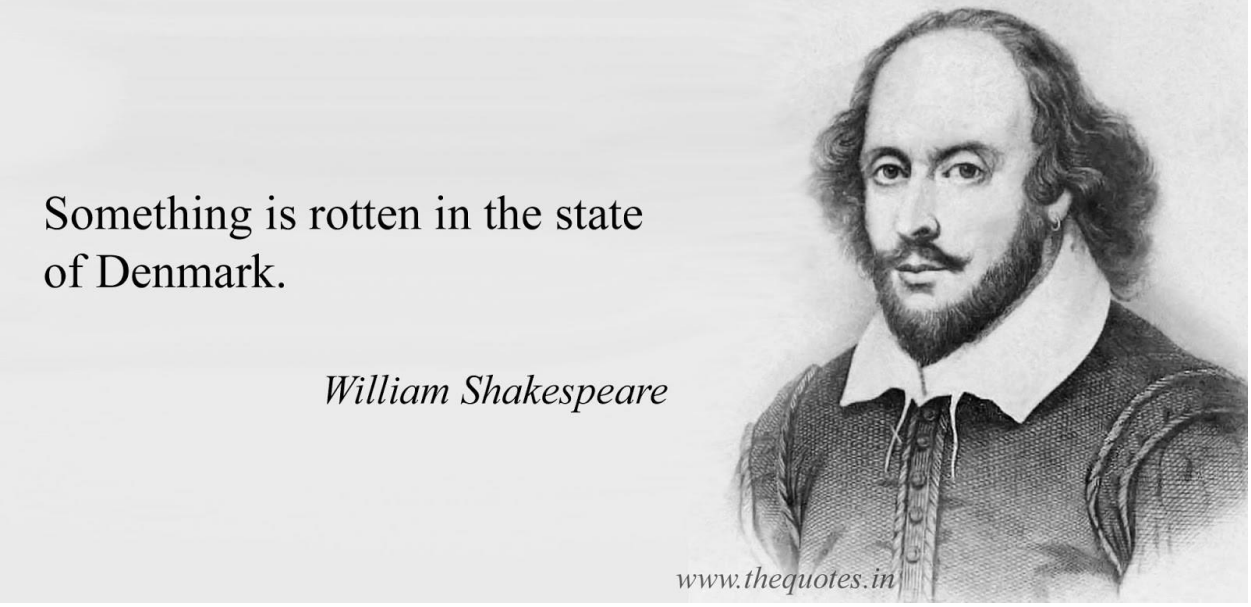
Whilst new structures are being built, old structures are coming down, and it will not be smooth. It will not be orderly. It will not be "fair", and it will not be "equal", that's for damn sure.

Your bullshit Keynesian / neo-classical economic & social theories cannot forecast shit, and can do less to make for a "smooth landing" or "elegant deleveraging" (sorry Ray, not likely).

Those who will be most rewarded will, as always, include the lucky (the world abounds with fools of Randomness, eg; Roger Ver), along with the prepared, curious and those hungry for knowledge.

It's those who get off their asses and dig deeper than the surface who will be best positioned to be on the constructive side of this shift, whilst the lazy, incompetent, ignorant, arrogant and of course, unlucky, will likely find themselves on the destructive.

“Something is Rotten in the state of Denmark”



The Romans experienced it. So did the Church. Shakespeare wrote a play about it, almost 500 years ago.

There comes a point when the “state”, or the “empire”, or the “collective” simply starts to rot.

When corruption, rent seeking, politics and all form of non-organic bureaucratic meddling begin to define the function of the very structure that was initially designed for its constituents’ prosperity, you know the end is nigh.

In modern times, the beacon of prosperity has been capitalism.

In fact, ruthless, free-market capitalism is the mechanism of human collaboration that most closely resembles nature.

Power laws, recursive network effects, complex inputs & outputs that are allowed to reach equilibrium of their own accord, rewards & punishment through inherently system-based incentives and of course; luck.

One can draw parallels to these attributes in all natural systems that have evolved over thousands, millions & billions of years.

So what went wrong with capitalism? How the hell did we wind up with a crony version of capitalism that has rot to the core?

I’ll explain below, but it can be summed up in the following quote by Michael Hopf.

"Hard times create **strong men**. **Strong men** create good times. Good times create **weak men**. And, **weak men** create hard times." Michael Hopf

Over time, we humans seem to repeatedly stray from founding principles. Our forebears, growing up in better times, forget why some decisions were initially made.

It's worse when those forebears realise they can also run a monopoly over the core resource of the time.

The Church had a monopoly on the written word & education (information). ***Capitalism & Science broke that.***

The State today, has a monopoly on Money. ***Bitcoin is breaking that.***

So....why the rot?

Productive or Parasitic

In life, likely on planet Earth & anywhere else there may be life, there are two ways to earn a "living".

1. Production. To produce, one must trade their time & energy, in the form of effort, talent, skill and labour, and be rewarded with property, either in the form of currency (money) or in the form of another instrument you deem valuable & commensurate to your work.
2. Theft. To steal, you make someone else's property your own, without their permission. You take what you want, whether through lying, cheating or most often (as evidenced throughout history), the act of violence.

German sociologist, Franz Oppenheimer calls (1) the "economic means" by which we build wealth.

Economic because there is an additive & multiplicative effect that occurs as a result of the collaborative efforts of the constituents of a society who produce, and then trade their property, and thus both prosper.

Oppenheimer call the other, mutually exclusive method, the "political means". Political because it is not concerned with the production of new goods or property, but exists and persists through the seizure, appropriation, taxation and theft of said goods & property in the "name" of the collective.

Once again, this fundamentally parasitic nature seems to come to a head every 500yrs if you accept the analysis of Davidson & Rees-Mogg's work in "The sovereign individual".

So where are we now?

Understanding which system is dominant in the paradigm within which we're currently operating is important + useful.

Modern Times

I recently had a conversation with a friend, who I would consider centrist, or moderately conservative in nature (if those labels even mean anything anymore).

She pointed out that centrally managed states such as the Scandinavian countries are the "happiest" in the world today, based on the latest statistics & surveys.

Now — whilst those surveys are laughable at best, let's just assume that there is a grain of truth in there — the problem with this 'fact' is that the "happiness" is being measured during the largest monetary inflation in the history of humanity.

It's a facade!

1 The cycle of humanity

And those who are high on this fake happiness are going to feel it the worst as their world crumbles thanks to the bloated social structures that cannot subsist in a new economic reality that is fast approaching.

Furthermore, these 'happy' people sacrifice their liberty & personal Sovereignty for the illusion of peace via the benevolence of their leaders — who would very quickly justify behaving more like dictators should dire economic circumstances warrant such actions.

And don't for a minute think "it will never happen", because it is happening, ***NOW.***

My decree thou shalt yield to, for thy savings are mine...

Former IMF Managing Director, and now head of the ECB, Christine Lagarde recently came out with the following gem:

"Isn't it true that ultimately we have done the right thing to act in favour of jobs and of growth rather than the protection of savers?"

Implying that people should be grateful for their jobs, whether their savings protected or not.

Translation:

"you should be grateful, for your master gives you the right to be a slave"

Are you kidding me?

The very notion of paying an institution just to store your money (well, not really 'your' money), or being paid to borrow money is utterly absurd — but is slowly being pushed upon us in the west as not only necessary to "stimulate" the heroin-junkie of an economy we now have, but it's being called "normal".

Even Dalio is waking up:

"As a result rich capitalists will increasingly move to places in which the wealth gaps and conflicts are less severe and government officials in those losing these big tax payers will increasingly try to find ways to trap them."

Ray Dalio

And it's not just economic madness.

Bernie Sanders, whom I mentioned earlier, is a brilliant example of an old fool espousing a nice-sounding veneer of an ideology with incredibly dangerous roots.

Maybe he was inspired.....

"It is difficult for me to imagine what "personal liberty" is enjoyed by an unemployed person, who goes about hungry, and cannot find employment.

Real liberty can exist only where exploitation has been abolished, where there is no oppression of some by others, where there is no unemployment and poverty, where a man is not haunted by the fear of being tomorrow deprived of work, of home and of bread. Only in such a society is real, and not paper, personal and every other liberty possible."

Sounds nice right?

That same person went on to say:

"When we hang the capitalists, they will sell us the rope we use"

Yep. That same person went on to rule the regime that gave us gulags, famine, deportations, massacres, forced disappearances, extrajudicial killings, torture and and was responsible for not only the deaths of millions of people, but the utter oppression of tens of millions more over the ensuing decades.

That person was **Joseph Stalin.** (although you may for a moment have thought it was Bernie)

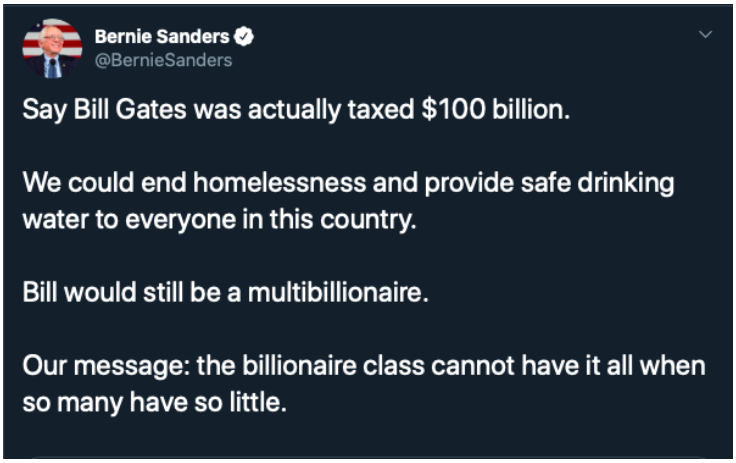
Stalin was, in the early days, viewed as the man who would help the lower class & poor people fight back against the so-called 'oppressive capitalists'.

Little did those poor people (pun very much intended) realise they would be accepting a modern form of serfdom. Little did they know how dire the ramifications of such an ideology would be.

And here we are, barely a generation since the god damn Berlin Wall came down, at it again.

This time, from the likes of Bernie Sanders, AOC and Elizabeth Warren — all who want to walk in the shoes of Chairman Mao, Lenin or Stalin himself.

This tweet came out just as I was finishing up this piece, and I had to include it:



Of course. Bernie would surely know how to deploy that capital...to his cronies, to the military, to bullshit social programs that don't work and in every other non-functional, mal-invested, mis-appropriated fashion. Bernie's next book: How to burn $100bn and achieve nothing.

Bernie Sanders is merely the modern day equivalent of

prior socialist leaders, who embodies the political means of wealth [confiscation] via the power to rob whomever he deems as unworthy.

Welcome to the slippery slope that leads to ***communism & enslavement.***

The only way to maintain such a system is via violence or the threat of said violence.

That's not freedom. *That's slavery.*

And no man, woman or child should have to live in a world like that.

This the path of collectivism

One of my favourite lines from Ayn Rand's Atlas Shrugged surmises Hamlet's quote (the headline of this section) perfectly:

Money is the barometer of a societies virtue. When you see that in order to produce you must seek permission from those who produce nothing. When you see money is flowing to those who deal not in goods, but in favours, When you see that men get richer by graft & by pull, not by work, When your laws protect the looters more than the consumer, You will know, that your society is doomed.

- Ayn Rand

Piercing the Veil

Bitcoin's promise to help bank the unbanked was not to do so by giving them a payments technology. It was to do so by giving them a money via which they have property rights.

Those who live in nations that don't respect, recognise or value personal property are those who have the most freedom to gain.

Those of us in the west, who are watching the state ever so slyly repeal our property rights have a two-fold motivation to participate in this revolution.

(a) We are able to escape the grip of a modern, technologically empowered iron fist which continues to squeeze, and

(b) We ride a rocket ship to the proverbial 'moon' because we had the balls, foresight, insight, vision or dumb luck to get in early.

It's (a) that I'm personally more interested in though, perhaps due to my personal libertarian bent, or because it's something I derive a greater sense of "meaning" from (likely both).

Now, you might say that:

"Hey, you're exaggerating. We're pretty good here in the West. We have stable social structures, good property rights, and yeah while taxes might be high, that money goes to use. We live a pretty good life".

By & large I would agree. But I would urge you to look beyond the veil.

The central banking cartel & crony capitalist governments of the west have reached a point in history where they can no longer sustain their structure without squeezing their subjects harder. And they know it.

The signs are evident, as described above. Furthermore, look around!

These same "stable" governments continue to strip away our freedoms via absurdities such as the Anti-Encryption laws in Australia, anti-cash laws, draconian follow-you-everywhere tax laws, inability to travel freely, panopticon surveillance, increased 'law enforcement' powers, speeding ticket optimisation frameworks (you can't drive around for 10min in Sydney without seeing a cop hiding around the corner ready to book you for blinking) and even new laws empowering their 'agents' to force you divulge your private information (eg; decrypting your drives coming into NZ).

It's madness.

Ayn Rand was so poignant, once again:

Laws are designed to be broken, not observed. When you're after power, There's no way to rule innocent men. The only power any government has is the power to crack down on criminals. And when there isn't enough criminals, one makes them. One declares so many things to be a crime that it becomes impossible to live without breaking laws. Who wants a nation of law abiding citizens? There's nothing in that for anyone. But pass the kind of laws that cannot be observed, followed or objectively interpreted and you

create a nation of criminals & law breakers. Then you cash in on guilt. That's the system.

Cogitos Ergo Sum

I think, therefore I am.

- Descartes

Descartes said this almost 500yrs ago, during the last major transformation in human history; the fall of the dominance of the church & the rise of the merchant-and-science-enabled state.

Much has been said about this recently, particularly in the Bitcoin circles.

I'm sure all the "crapto" people are going to try hijack this soon too, but let it be known here that Bitcoin has been about this from the beginning.

The parallels drawn between the events of the gunpowder revolution, the renaissance, early banking, the rise of the merchant and the fall of the prominence of the church to today's technological revolution, private, self-sovereign banking, the rise of the sovereign individual and the fall of the state are eerie.

I think, therefore I am.

Descartes' words have never been so profound.

The words "I think" and "I am" are the genesis of the self.

Yes we are all made of the same stuff, but it's that unique combination of stuff that makes us who we are.

The sanctity of the individual is paramount. Tony Robbins has a profound quote:

"the most powerful force in the human spirit is the desire to stay consistent with its identity".

To say "I am" is a claim to one's identity & independence.

It's a claim to one's personal sovereignty — which we can now do so like never before, thanks in large part to Bitcoin.

How you may ask?

Our work is our labour. Our labour is our time & and our energy.

When we boil it down, they are all we we have, and all we are truly made up of.

To live, to love, to work, to travel, to experience, to remember, to plan, to do anything requires two things: **Time & Energy.**

We can only effectively measure these through a unit that we can all agree best represents time & energy.

As you'll learn in this publication, "money" is that unit, and for the first time in history we have a version that can do the job, without being compromised.

It is why Bitcoin is the ultimate tool for personal sovereignty, and the catalyst that leads us to a future more like Star Trek, and less like Terminator.

Incorruptible Property Rights

Bitcoin provides a stable system of property rights without reliance on the State

With it, individuals can be truly self sovereign

The mathematical primitive of strong, open source, modern day cryptography gives us for the first time in history, a method whereby the sanctity of personal property and the act of sacrificing for the future can be maintained WITHOUT the requirement for the protection (or oppression) of the state, the church, the monarch, the feudal lord nor the tribal leader.

In modern times, and in the future that lay before us, Human beings (and potentially machines alike) will be able to save the product of their labour and delay gratification (the very building blocks of society) on their own terms.

As this multiplies, and we are collectively empowered to take back our personal sovereignty (via what is likely the greatest gift to humanity since we became conscious), we have the rare opportunity to define a new form of local & global cooperation that is voluntarist, and non-violent in nature.

Bitcoin's core "opt in" or "opt out" nature, its open access & its absolute nonchalance / disregard of who or what you are is the basis of this new era we now embark on.

Bitcoin has chosen to not only forego the requirement of the state, but has chosen to do this via the irrefutable conversion of time & energy into a visible, verifiable network and unit.

Through Math, it will help us reinvent the notion of what we humans define as 'state'.

Cash is the ultimate tool of the sovereign individual.

And in an increasingly digital world, the apogee is a peer to peer electronic cash.

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the double-spending problem using a peer-to-peer network.

Cash is the ability to transact ***freely.*** And by freely I mean "to do so in a manner uncensored, direct & final".

That was traditionally only able to be done physically in the real world. Now it's able to be done digitally.

Ineptitude on display in the crypto community, for example Roger Ver and his BCash cronies, think free means no cost. They're unable to understand that costlessness can only mean one of two things:

1. It has **no value**. ie; the very definition of costlessness is something with no value.
2. It has value, in which case cheap & free means there is a cost elsewhere. A cost that is most likely draconian in nature.

They think trending toward a centralised payment system for free internet transactions is what was meant by cash. That's not the freedom cash gives.

Roger clearly got lucky buying bitcoin. Dumb luck, for the ultimate fool of randomness.

Bitcoin, and banking the unbanked was ***never*** about cheap payments.

It was about giving everyone an incorruptible, uncensorable tool for economic prosperity.

Bitcoin was, is and always will be a tool for personal sovereignty.

That's what was meant by "cash" — which of course Satoshi could not be so blatant & brazen about it back in 2008, lest Bitcoin be left in the dustbin of history alongside other crazy ideas.

He let the protocol and its inherent nature do the talking.

He then chose to walk away, and in doing so let loose something no amount of violence can destroy and no amount of tyranny can control.

The rest is history....and it's in the making.

Conclusion

We live in a world where our rights are slowly being encroached upon, our privacy is slowly being repealed, and our freedom to truthfully express ourselves is being censored, whether due to deranged "political correctness" on one side or maniacal authoritarian rule on the other (eg; China).

May the brave people of Hong Kong continue to inspire us

Bernie, and those of his ilk, whether due to incompetence, stupidity, or just being a part of what Taleb calls the "intelligentsia", believe in treating the symptoms by introducing more interventionist inputs into an already complex system that's slowly spinning out of control.

This will never work, and will only serve to send society to a real-world hell.

The ONLY way to fix up the fuckery of the current system is to start again. We must embrace the essence of Kali, cut out the cancer & burn it all down.

The time for negotiations has come to an end.

Libertarians have tried this to no avail, for playing within the confines of the old paradigm is no way to bring about a new one.

The battle for the future is now, and the front lines are where Bitcoin meets the fiat denominated state.

This is a war, and the stakes are higher than they've ever been.

Money is the lifeblood of society. It is wealth, at the very core of what the word means. He who controls it, controls all of society.

The introduction of free markets was the catalyst for the separation of church & state. The creation of free money is the catalyst for the separation of money & state.

And more than that, it's also a stake in the heart of today's state, which has decayed to the point that it's primary function is to leech, take, suck dry and confiscate your wealth.

Today, it exists no longer to protect you & serve you, but to subdue you. You are once again it's subject.

You can see this just by looking at the language used for a group who are supposed to be protecting you: "Law Enforcers".

When did I agree to pay someone to "enforce" laws upon me which I neither agreed to in the first place?

The state's control of money is its locus of power. Through this tool, it is able to enforce its will over every facet of our lives.

We, the Bitcoiners of last resort, on the front line, are here to destroy that.

Freedom is not Free

Bitcoin is our chance.

It allows us to take the most important tool of human collaboration, ie; money, aka; the ultimate resource, and make it:

- Un-inflatable
- Un-censorable
- Un-confiscatable

and all in all, **un-fuck-with-able.**

By removing it from the purview of the state, we:

1. Starve the state of its ability to perpetuate it's parasitic existence
2. Get a chance to design a new form of collective collaboration in which personal sovereignty comes first, where the constituents of a society are treated like customers and the "state" or "social collective" is organised by means of POLA (principle of least authority).

According to Locke, we ought to part with no more of our rights to life, liberty, or property then is necessary for government to preserve those rights from each other. "The right to do whatever one thought fit to preserve oneself is given up to be regulated by society so far forth as the preservation of himself and others shall require. When any rights are given up, it is only with an intention in every one to better preserve himself, his liberty, and his property."[6] A corollary is that government officials ought not to be given more power to take away those rights than is necessary for government to fulfill its role of the preservation of those rights addressed by the statute.

At a constitutional scale, the principle of least authority is reflected in the enumeration of powers and in the Tenth Amendment[7]. Under a Lockean interpretation, the federal government was given certain enumerated powers only in order to protect life, liberty, and property. These enumerated powers gave the federal government no more authority over life, liberty, or property than it needs to protect life, liberty and property. Other powers, where more local decisions protect rights better, should be retained by the states, or by smaller groups, or by individuals, the ultimate source of all such authority. The Ninth Amendment[8] is a mirror-image of the Tenth. Whereas the enumeration of powers should restrict the federal government to the least authority required to execute those powers[9], the enumeration of individual rights is open-ended -- to coin a phrase, a *principle of most rights* against governments consistent with protecting the life, liberty, and property of others.

I saw this excerpt a few weeks ago. Pretty sure it's attributed to Nick Szabo

The cornerstone of all of this is personal sovereignty & liberty, and this is ***only*** possible with Bitcoin.

It's only possible when the economic unit has personal, private property rights built into its very being.

To paraphrase Winston from 1984 once again, the only thing Big Brother didn't have control over was what goes on in your head & your heart.

Bitcoin transforms money into a unit that is fundamentally information, and information is both nowhere & everywhere.

It's both inside of us, and all around us — and when we ourselves know the combination that gives us personal access to that information (money), it's ours, in the deepest sense of "private property".

Libertarians, Austrian economists and the natural economists before them had it right — only it was never practical in a world in which the unit of economic measurement could be owned or managed by an organisation, government, collective or state of any kind.

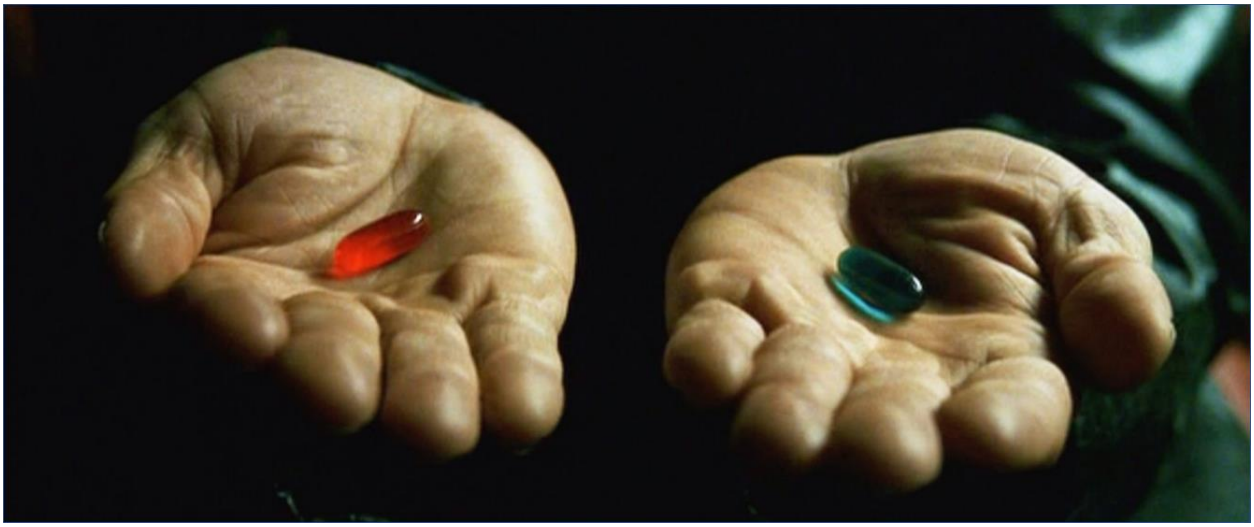
but....

Money has now become an unforgeable form of data, that nobody can control or manipulate — built on a network which nobody needs permission to build products & services on. This foundation allows us to build an entirely new world — not just a financial one, but a new form of society.

So...let us come together...

Bitcoin is now here.

Money is THE battlefront. This is where the battle lines are drawn. Not fucking "blockchain". Money. It's THE resource. And we're all going to have to pick a side.



Join us, & we'll show you how deep this rabbit hole goes....

Bitcoin is now here.

This is the new counter culture. This is what it means to be ***your***self. To be who ***you*** are. To do what ***you*** were born for.

To be truly sovereign. *It's scary — but it's liberation, in all its glory.*

By Aleks Svetski Oct, 2019

The Bitcoin Times Ed 2 is the collaborative work of 8 writers & 1 designer with the intent to educate, inspire and spread ideas on bitcoin.

Each section will be released on Medium as a free long form article, and the full, compiled version of the Bitcoin Times will be available for free at the link below. In 2020, we'll release a limited edition hard cover collectible, for purchase, which you'll be notified of by email if you download the free pdf.

If you found value in this or any of the other essays and articles, please support each of the contributors by sharing it out & following their work.

Download the full guide at:

The Bitcoin Times

(Soon to be updated to: https://bitcointimes.news)

Disclaimer:

WORDS

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

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

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

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

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

DYOR | BTFD | HODL

I hope you enjoy this project. I'm on a mission to archive the great works from todays Bitcoin thinkers. There's tons more work to be done!

- @_joerodgers