CRYPTO WORDS

CY18 Q3 September

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

The Yin and Yang of Bitcoin

By LaurentMT

Posted September 3, 2018

This is post 2 of 3 in a series

- Gravity
- The Yin and Yang of Bitcoin
- Cliffhangers

"Countless words count less than the silent balance between yin and yang" - Laotzi

Hodling & Mining, the two dragons of Bitcoin (photo: Panels of Dragons Yin Yang)

In the second part of this series, we're going to define a new metrics called the Price-Performance Ratio of Bitcoin's PoW (PPR). Our goal will be to analyze the evolution of the actual efficiency of the system and to identify the factors driving its dynamics.

After having defined this new metrics, we will first witness its “surprising” correlation with the bitcoin’s market price. Going a bit further in our analysis, we’ll study the role played by hodling and mining. We’ll then focus on a “strange” pattern displayed by the metrics (resistance levels) before concluding with an observation about the existence of PPR cycles.

Prologue: Price-Performance Ratio of a product

The Price-Performance Ratio (PPR) is a metrics used in economics and defined as the ratio of the price of a product to its performance (expressed in any unit making sense for expressing this performance).

The PPR is often used to illustrate the difference between “classic” and “new technology” products. Indeed, it can often be observed that “classic” products display a constant or increasing PPR while each new iteration of “new technology” products come with a lower PPR.

This phenomenon can be explained by the fact that production of “new technologies” usually begins at an inefficient level but each iteration benefits from works and investments done for previous versions (R&D, etc). It’s this cumulative effect which allows to decrease the PPR.

Moore’s law is a famous example of this phenomenon. When I was a kid (i.e. before I learnt that Moore’s law was a thing), the Cray 1 was in my imagination a kind of mythical beast which would forever remain out of my reach. The first commercial version of the Cray 1A was sold in 1977 for the equivalent of $37M (in today value). Guess what… This beast was less powerful than your smartphone…

“Hello... Hello?”—Happy owner of a crappy smartphone

Price-Performance Ratio of Bitcoin’s PoW

Ok. Let’s define our new metrics. For this, we’re going to consider the UTXO set after each new block as a new iteration of a “product”. Its performance will be measured by the total number of bitcoins.days secured it has accumulated. At last, we’ll approximate the price of this “product” by the reward associated to the block.

The equation for the PPR is

$$PPR_b = \frac{R_b}{BDS_b}$$

with:

PPR_b: Price-Performance Ratio for block at height b

R_b: Reward associated to block at height b

BDS_b: Total number of BTC.Days Secured by the UTXO set after block at height b

which can be rewritten as

$$PPR_b = \frac{R_b}{\frac{\sum_{u \in U_b}(A_u \sum_{i=b_u}^{b} H_i)}{144\ H_b}}$$

with:

H_i: Expected number of hashes associated to block at height i

U_b: UTXO set after block at height b

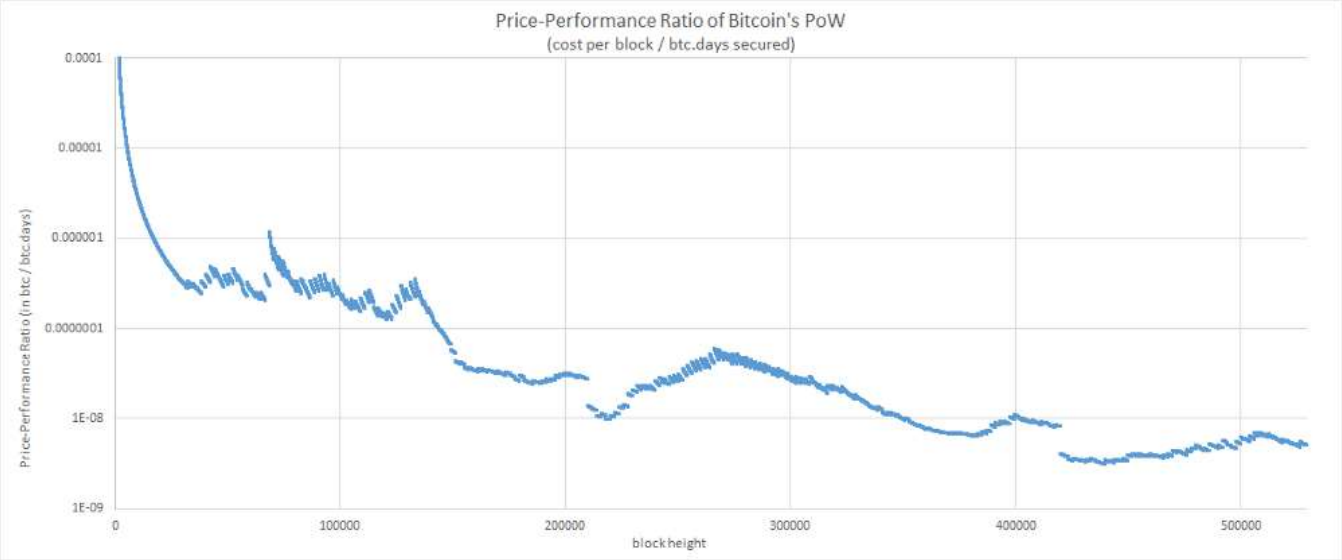
A_u: Amount of UTXO u

b_u: Height of the block containing the transaction creating the UTXO u

which is equivalent to

$$PPR_b = \frac{144\ H_b R_b}{\sum_{u \in U_b}(A_u \sum_{i=b_u}^{b} H_i)}$$

That gives us the following chart



The chart displays a decreasing trend (i.e. an improving price-performance ratio) which is consistent with what we might expect from a system having a cumulative effect. **And once again, the metrics suggests that the efficiency of the system has improved over time**.

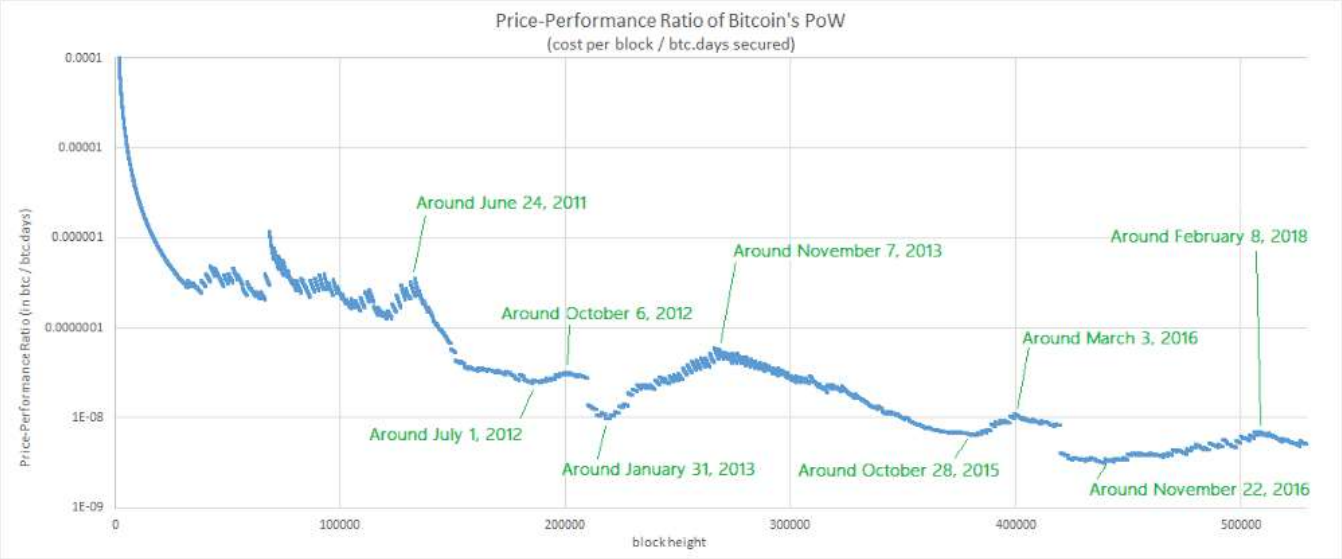
That being said, this curve is far less smooth than those obtained for our two previous metrics. It seems that the journey has been a bit rock & roll. Let's try to understand what is happening here.

Singularities

Let's begin with an easy task and let's try to identify the causes of a few singularities observed on the chart.

Bulls and Bears

All right. Now, let's focus on the multiple oscillations of the curve and let's add the dates associated to a few top and bottom values.



If you follow (even negligently) the multiple movements of the bitcoin's market price, these dates may remind you something...

Price-Performance Ratio & Market Price (market price data from bitcoincharts and blockchain.com with a linear interpolation used for missing data points)

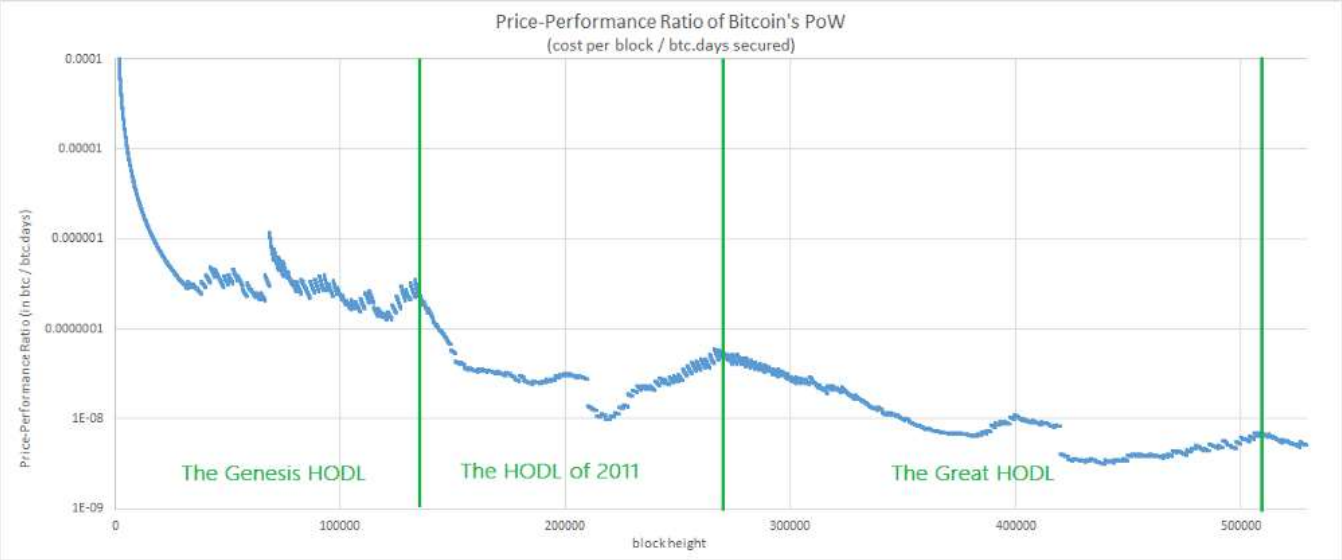
The chart suggests an interrelation between the PPR and the market price. At first, this might seem surprising since the market price isn't a factor used in the definition

of the PPR but it certainly makes more sense if we remind ourselves of multiple observations made in the past about the bitcoin's market price driving changes in hodling & mining behaviors, two components of the PPR.

Let's try to confirm this intuition with a deeper analysis of the relation existing between holding, mining and the PPR.

Yin (Hodling)

A few months ago, Unchained Capital published an excellent work about a phenomenon called the "Hodl Waves". The main finding of this study was a repeated pattern of increasing hodling after each rally in bitcoin's price. Considering that hodling is an integral part of the PPR, a convergence with the Hodl Waves model doesn't seem absurd. Let's check this hypothesis by plotting the dates associated to the three Hodl Waves.



The intuition seems good. We can already associate 3 "tops" with the Hodl Waves. Moreover, the chart suggests that the first phase of a new Hodl Wave (i.e. a period of increasing hodling) is correlated with an improvement of the PPR. It's then followed by a degradation of the PPR which is correlated to the new rally in bitcoin's price concluding the Hodl Wave.

Ok. Let's try to get a better picture of the influence of hodling by determining its lower and upper bounds (i.e. when hodling is maximized and minimized). For this, we're going to use a thought experiment and imagine two hypothetical versions of Bitcoin...

Upper bound: Bitcoin Steroïds

In the parallel universe of Bitcoin Steroïd, users seem gripped with a spending frenzy and they can't help but spend their coins as soon as they receive them. An UTXO never "accumulates" more hashes than the ones added by the block including the transaction creating the UTXO (notwithstanding that freshly created coins must wait for a 100 blocks period before becoming spendable).

The PPR for Bitcoin Steroïd can be defined by the following equation (for the sake of simplicity, we omit the constraint over the maturity of coinbase transactions)

$$PPR_b = \frac{R_b}{\frac{H_b}{144\ H_b}\sum_{i=1}^{b} R_i}$$

which can be rewritten as

$$PPR_b = \frac{144\ R_b}{\sum_{i=1}^{b} R_i}$$

Lower bound: Bitcoin Arctic

In the parallel universe of Bitcoin Arctic, store of value is all the rage. Basically, all users are miners trying to create new bitcoins that they'll never transfer. Their goal is just to transfer their wealth into this digital store of value and keep it there forever.

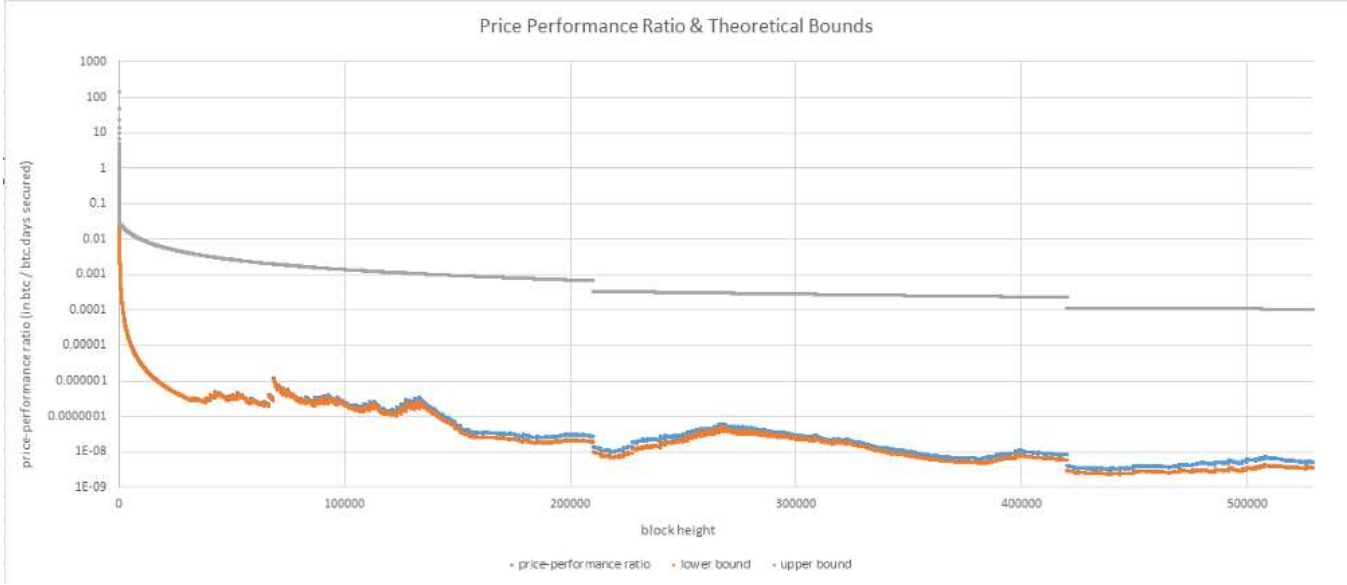
Thus, the PPR for Bitcoin Arctic can be defined by the following equation

$$PPR_b = \frac{R_b}{\frac{\sum_{i=1}^{b} H_i R_i}{144\ H_b}}$$

which can be rewritten as

$$PPR_b = \frac{144\ R_b H_b}{\sum_{i=1}^{b} R_i\ \sum_{j=i}^{b} H_j}$$

Now, let's plot our chart of the PPR with the two bounds defined by Bitcoin Arctic & Bitcoin Steroïd.



There are several observations to be made here.

First, it appears that **since its inception, Bitcoin has operated in a mode very close to the lower bound defined by Bitcoin Arctic**and their oscillations are quite similar.

On its side, the upper bound defined by Bitcoin Steroïd has a very different profile. Oscillations have disappeared. All we have is a smooth monotonically decreasing curve. This observation makes sense considering that in Bitcoin Steroïd, UTXOs don't accumulate hashes for longer than a single block. Here, the main drivers are the increasing number of coins and the decreasing rewards. But there's an expensive price to pay for this regularity; **the PPR of Bitcoin Steroïd is several order of magnitudes higher than the PPR of Bitcoin or Bitcoin Arctic**.

As a first conclusion, we can state that hodling has played an active role in the evolution of the efficiency of the system during the past 9 years.

Yang (Mining)

Let's now focus on the influence of mining. For this, we're going to plot a chart displaying the PPR and the expected number of hashes associated to the PoWs of past blocks.

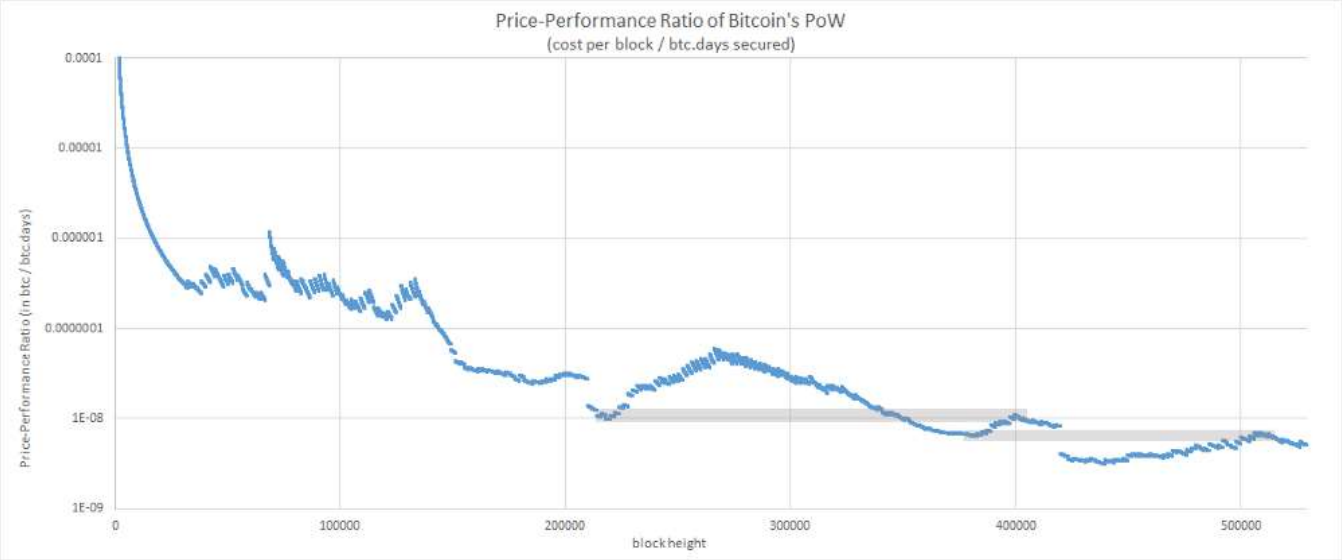
The chart displays a series of cyclic patterns composed of four phases:

- **A=>B / A'=>B' (a few months before a halving):** Hashrate growth and PPR start to increase.
- **B=>C / B'=>C' (around the halving):** Hashrate growth and PPR decrease.
- **C=>D / C'=>D' :** Market price starts to increase. Hashrate growth and PPR increase again.
- **D=>A / D'=>... :** A "bubble" pops. Hashrate growth and PPR decrease again... until a new cycle begins.

Once again, these observations aren't really surprising. They're consistent with past observations made about the dynamics of bitcoin's hashrate (anticipation of halvings, bull markets).

"Technical analysis"

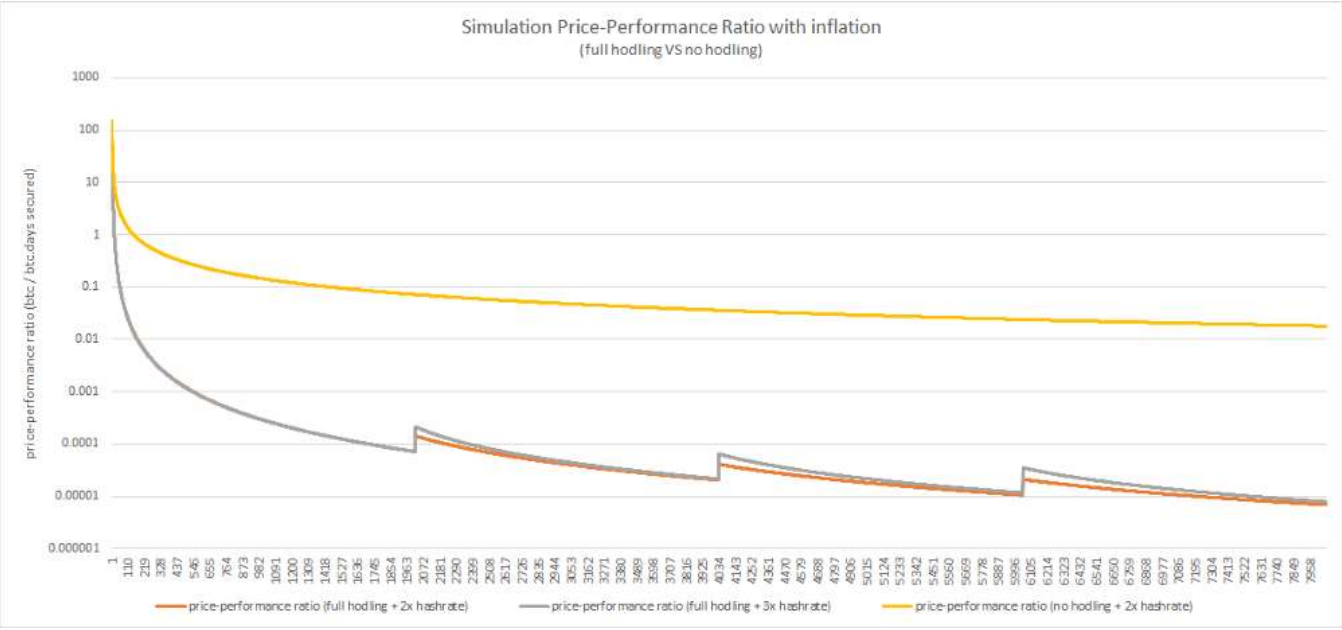
While looking at the PPR chart, you may have noticed something else which seems a bit "weird".



PPR “Resistance” levels

Yep. That’s it. Some bottoms seem to act as a “resistance” for the top coming later. This observation puzzled me for a while. To better understand what is happening here, let’s play with a simplified model simulating the system.

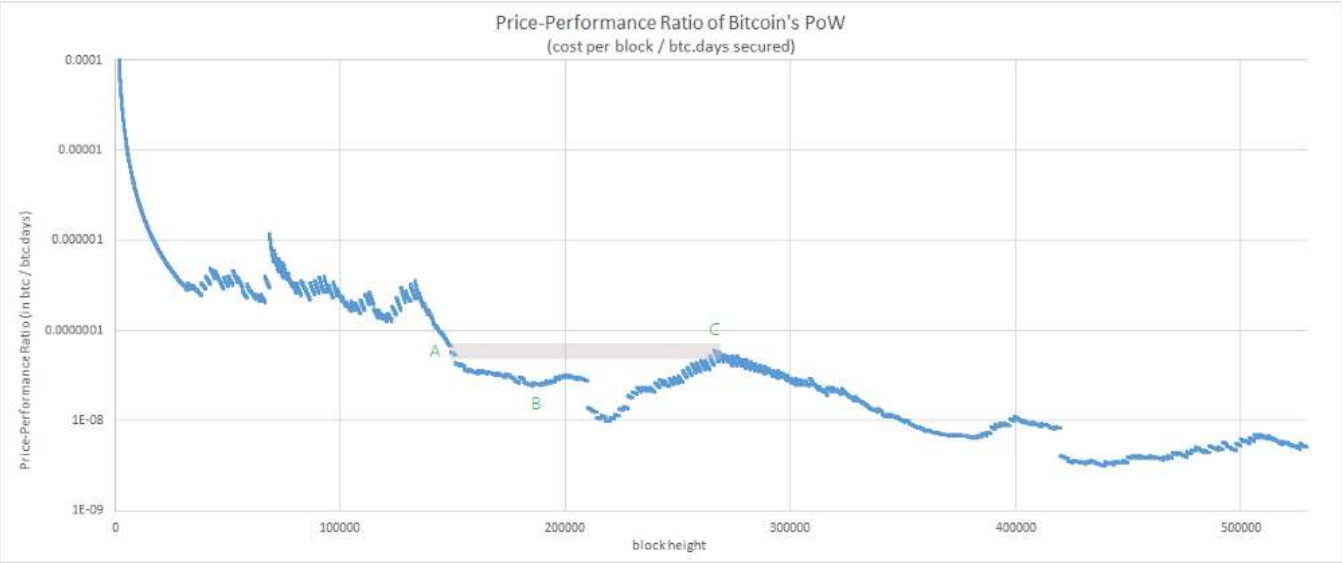
First, we’re going to remove the halvings and difficulty adjustments. Then, we’re going to state that each block is rewarded by a single coin and that the first mined blocks require a single hash. Every N blocks, we’re going to simulate an increased market price instantaneously driving up the hashrate by a given factor (x2 or x3 for our simulation). That gives us the following result:



As you can see, this very simplified model is enough to reproduce the main characteristics of the PPR observed in the wild. It confirms that the occurrence of oscillations is correlated with a hodling behavior and it also suggests that resistance levels are influenced by the multiplying factor (the lower the factor the more the previous bottom "acts" as a resistance).

Let's break some assumptions

There's a last observation to be made about this phenomenon. You may have noticed that this "resistance" effect doesn't seem to apply to all the tops.



Indeed, according to our previous observation, we might expect that blocks around C find a "resistance" at the level of B instead of A. The interesting part of this observation is that A marks the beginning of a very unique period in the history of Bitcoin. For the first time, the hashrate strongly decreased and remained at this "low" level for an extended period which ended... around B.

It seems that what we're witnessing here is the rare occurrence of a period breaking one of our assumptions (A5: "... the average amount of computing power dedicated to Bitcoin mining monotonically increases"). At this point, one of my hypotheses is that these top and bottom values might be associated to an equilibrium existing between hashrate, hodling behavior, mining rewards and market price. Anyway, the subject remains to be investigated further.

The PPR Cycles

The last observation that we can infer from all the previous points is that the **PPR follows a series of cycles which can be associated to bitcoin's market cycles** (anticipation of a halving or bull+bear cycle).

PPR Cycles

For each cycle, it can be observed that after a temporary period of degraded efficiency, the system has become more efficient. Specifically, each PPR cycle is composed of two phases:

- **Phase 1:** Market Price increases—Hodling decreases / Hashrate growth increases => PPR increases (the system becomes temporarily less efficient).
- **Phase 2:** Market price decreases / bubble pops—Hodling increases / Hashrate growth decreases => PPR decreases to a new low.

At last, it's worth noting that the PPR cycles are slightly more fine-grained than the Hodl Waves. My hypothesis is that it can be explained by the fact that PPR cycles associated to bitcoin halvings primarily result from the influence of mining, a factor excluded from the scope of the Hold Waves model.

Conclusion

We have defined a new metrics taking into account the effects of mining and hodling over the actual efficiency of Bitcoin's PoW.

Once again, the metrics suggests that the system has become more efficient over timebut the most interesting insights gathered from this metrics are certainly related to the analysis of its multiple oscillations. To my surprise, it remarkably synthetizes multiple past observations made about the interrelation between the market price and hodling & mining behaviors. It also highlights the **influence of the**

market price over the efficiency of the system through its influence over hodling and mining.

At last, we have witnessed the **existence of PPR cycles associated to market cycles** (anticipation of halvings, bull+bear cycles) and we have observed that under our assumptions, the PPR value at the top of each cycle seems to reach a "resistance" around the initial PPR value of the previous cycle.

(Next part)

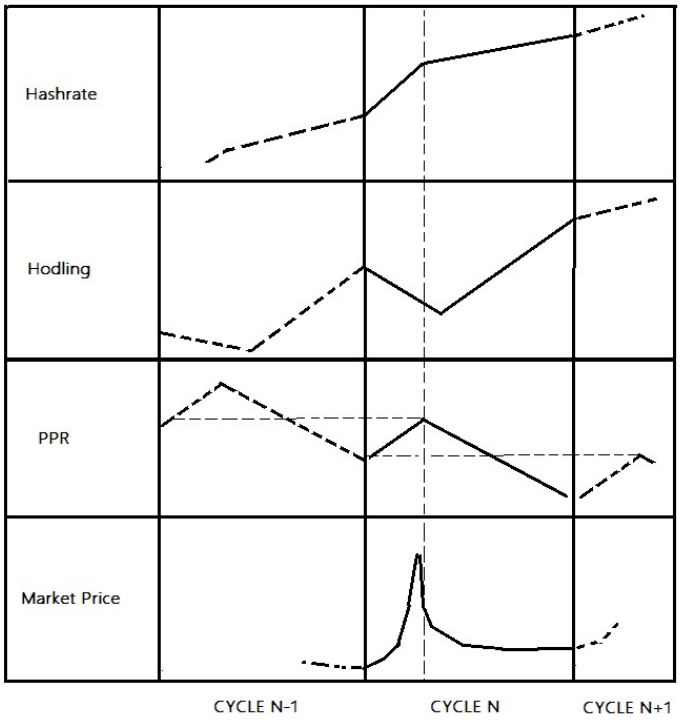
Acknowledgements

I wish to thank @Beetcoin, Pierre P. and Stephane for their precious feedback and their patience :)

A great thank you to @SamouraiWallet and TDevD for their feedback and their support of OXT.

At last, I wish to thank the team at Unchained Capital for their wonderful work on the Hodl Waves.

Annex A : Simplified schema of trends observed during a PPR Cycle



Cliffhangers

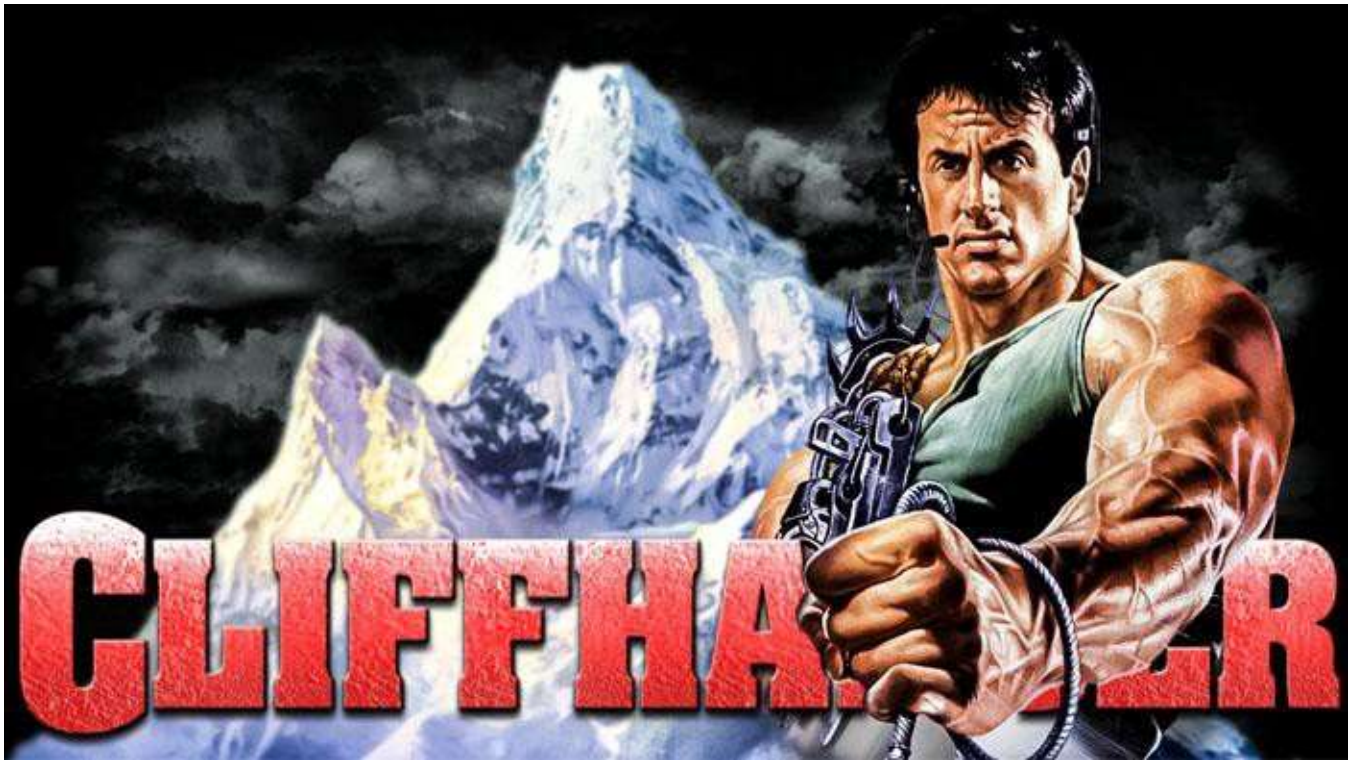
By [LaurentMT]

Posted September 10, 2018

This is post 3 of 3 in a series

- Gravity
- The Yin and Yang of Bitcoin
- Cliffhangers

"Be like the cliff against which the waves continually break; but it stands firm and tames the fury of the water around it." — Marcus 'Rocky' Aurelius, Meditations of a Bitcoin miner



In the previous parts of this series, we've started to investigate the efficiency of Bitcoin's PoW. In this third part, we're going to focus on a slightly different question: "Is the system running at its optimum ?".

For this, we'll first underline some points related to the effects of an increasing hashrate and we'll introduce the Satoshi's cliff, a 3D visualization illustrating the diminishing marginal security provided by older blocks. Then, we'll define what could

be considered as the theoretical optimum of the system and we'll wonder how far is the system from this optimum. At last, we'll conclude with a few thoughts about the diverging paths followed by Bitcoin and Bitcoin Cash.

Prologue: Bitcoin Steroïd and Bitcoin Arctic

We've previously discussed the influence of hodling over the efficiency of Bitcoin's PoW by imagining two hypothetical versions of Bitcoin. While caricatural, these two examples were useful for understanding the consequences of different trade offs. Bitcoin Steroïd sacrifices its efficiency for a maximized activity while Bitcoin Arctic sacrifices its activity for a maximized efficiency. Obviously, none of these solutions is very satisfying. Can we do better ?

Satoshi's Cliff

When I began to study the Bitcoin protocol, I was first amazed by the idea of new PoWs piling on top of old ones and providing an ever increasing security. But as often with Bitcoin, things aren't as simple as they seem. The truth is that with an increasing efficiency and availability of mining hardware, the security provided by old individual PoWs tends to decrease.

This phenomenon can be illustrated with a statistics provided by P.Wuille on this page. The chart displays the number of days which would be required for recomputing all PoWs since day 1 with 100% of the actual hashrate.

proof-of-work equivalent days (source: bitcoin.sipa.be)

In order to better visualize the evolution of the two phenomena (i.e. the cumulative effect of PoW and the effect of an increasing hashrate on old blocks) we're going to compute a 3D visualization generalizing the chart provided by P.Wuille. This visualization is going to display how many days (z axis) would be required to rewrite the history back to a past block (y axis) with 100% of the expected hashrate used to mine a more recent block (x axis).

I'll call this chart the "Satoshi's Cliff"

Satoshi's Cliff (simplified version, x and y axes are expressed in time periods between 2 adjustments of the difficulty)

Let's choose any value on the x axis and starting from the bottom, let's climb the cliff. As you can see, rewriting more blocks requires more and more time (and is more expensive). But at some point, we reach a plateau. Being older doesn't provide a significant additional security to an UTXO. This highlights why the approach followed by Bitcoin Arctic (i.e. a "naive" maximization of accumulated PoWs) isn't optimal.

Once the plateau has been reached, activity is sacrificed for almost no additional security.

On the edge of the cliff

Based on this observation, we're going to define the "edge of the cliff" as a theoretical optimum for the system. Indeed, beyond a certain point it doesn't seem very wise to sacrifice activity for the diminishing marginal security provided by older PoWs.

It's important to note that **the concept of an optimal age doesn't really make sense for an individual UTXO**. Indeed, as the "owner" of an UTXO you don't have a fine-grained control over its age. Either you hodl the UTXO and at some point it will reach the plateau or you spend it and it instantly goes back to the bottom of the cliff.

In my opinion, **this concept of optimal age is primarily useful when we consider the UTXO set as a whole.**It can be considered as a reference point for the distribution of existing bitcoins per age. The more existing bitcoins are concentrated around the optimal age, the closer the system is from its optimum.

Ok. Let's try to determine the evolution of this optimal age. For this, we're going to iterate over all the values on the x axis and plot a 2D chart for each value (a kind of transverse slice of the cliff).

A slice of the cliff

Then, we're going to use a very simple method based on vector arithmetic (see Annex A) in order to approximate the optimal age for the slice. We just have to repeat the same operation for each slice and that gives us the following chart.

Let's note that very different criteria might be used to determine what is the optimum at a given date. Which one is best remains an open question.

A lemming effect ?

SELLL !

You may remember some observations made about the Hodl Waves which suggest a "lemmings" effect occurring during rallies in the bitcoin's price, with many old UTXOs "jumping" from the cliff. As it was shown earlier, one of the consequences of this phenomenon (coupled with the increasing hashrate) is a temporary degradation of the efficiency of the system. Does it mean that the system is significantly moving away from our theoretical optimum during these events ?

As a first benchmark, we can try to use a few data points provided by the Hodl Waves analysis and plot the distribution of UTXO amounts per age. The selected data points

will be the last 4 four top and bottom values identified for the PPR. We'll then plot an interval identifying the position of the optimal age on top of these distributions.

Distribution of existing bitcoins per age (selected data points are the last 4 top and bottom values of the PPR)

We can observe that for most of these data points, a majority of the existing bitcoins (50–70%) are hanging on the cliff (i.e. below the optimum). But an indicator more important than the median is the concentration of existing bitcoins around the optimum. I must admit that I've been a bit surprised here. I was expecting a clear differentiation between the bottoms (07/07/2012, 31/01/2013, etc) and the tops (21/09/2012, 16/11/2013, etc) but it doesn't seem to be the case.

To be honest I don't think that we can infer anything definitive from so few data points. Unfortunately, I lacked time for computing an exhaustive fine-grained comparison and it remains a task to be done. [Yep. It's a really brutal cliffhanger]

Bitcoin and Bitcoin Cash

As a last thought on this subject, I'll say that it should be interesting to observe how Bitcoin and Bitcoin Cash evolve in the future. As you certainly noticed, the trade offs described for Bitcoin Arctic and Bitcoin Steroïd have some resemblances with the divergent visions followed by the two chains.

Concerning Bitcoin, it should be particularly interesting to observe how the Lightning Network impacts the efficiency of the system. Indeed, the idea of long lived channels (i.e. several months or years) may help to "naturally" aggregate more UTXOs around the optimum (which is currently oscillating between 18 and 24 months).

Concerning Bitcoin Cash, it should be interesting to observe if the effect of an ever increasing number of on-chain payments can be counterbalanced by hodlers and if it's enough to stay close from an optimal use of the security provided by its PoWs.

Conclusion

In this third part, we've discussed the idea of an optimal age of the UTXOs allowing to measure how far the system is running from its optimum. It's clear that this post has barely scratched the surface of the question. My hope is that this first foray into the subject will encourage more people to investigate it.

(Next part)

Acknowledgements

I wish to thank @Beetcoin, Pierre P. and Stephane for theirs precious feedback and their patience :)

A great thank you to @SamouraiWallet and TDevD for theirs feedback and their support of OXT.

Annex A — Approximation of the optimal age of an UTXO

We're going to use a method inspired from the Needle algorithm. For any value on the x axis of the 3d chart, we can define a 2d chart (a slice of the cliff) and compute a vector Vi (see chart below).

We can then iterate over each value of the x axis of this 2d chart and compute the vector Vo. From these two vectors, we can compute the vector Vd and its norm (dot product + vectors addition). We consider the point O maximizing the norm of the vector Vd as our optimum.

An interpretation of this method is that the segment IA is what we would observe if the hashrate was constant. Thus, O is the point maximizing the effect of an increasing hashrate (compared to a constant hashrate) while making a trade off between a maximized security and a maximized activity.

Expensive Privacy is Useless Privacy

By Paul Sztorc

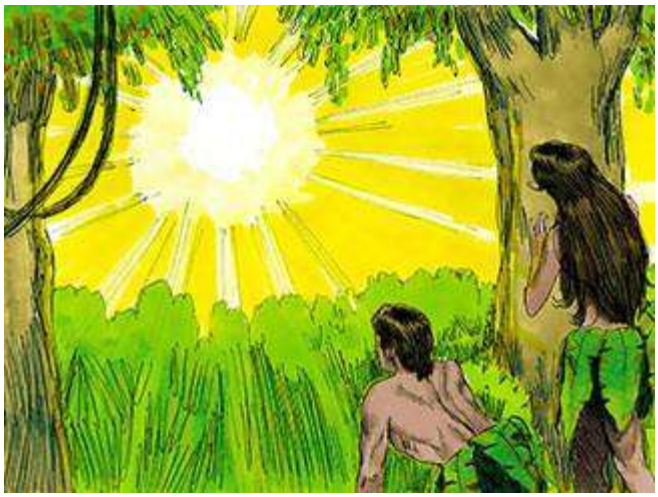
Posted September 11, 2018

Privacy is impersonation. To be useful, a privacy tech must be [1] cheaper, or at least [2] have costs which are themselves private.

1. Something to Hide

Sometimes, we need to keep a Truly Important Secret.

And I mean "important". Not a triviality or some piece of gossip – something that we *really* don't want anyone else to know.



Above: Adam and Eve hide from God. Taken from this website.

A. Resembling The Innocent

In such circumstances, we start **to take Secret-Keeping seriously**. We *need* the secret information to remain hidden. We simulate, in our minds, exactly what we think other people are like, and how [we think] that they learn things. We obsess over their ability to conduct which-kinds of research (and at-what-expense). We find ourselves absorbed by *their* interests and their distractions, over how they spend their "down time" (at parties, or at the dinner table), their expectations for engagement in conversation; which pretexts they will find believable.

For example: an early romance at around age 15.

Eg, the hackneyed "teenage crush". For example, Teenager 1 will "like" Teenager 2, but will keep this information dreadfully secret! Throughout modern history, many a popular children's television program has a main character or two burdened with this dire tribulation.

In this situation, we are equipped with this skin-in-the-game, and become much smarter than normal. We intuitively grasp something, that would otherwise pass for complex and arcane Baysian reasoning. It is an essential precept of both privacy and freedom.

It is that keeping **the secret** also involve **keeping a meta-secret**.

In other words, you are not only *keeping something hidden*. You are also *pretending that you have nothing to hide*. Teenager 1 has to pretend that 'talking about crushes' is exactly as boring or interesting as it was before.

B. The Meta-Secret

Once, my mother told me that she had “exciting news” to reveal (in other words, the news had henceforth been secret). But before she said another word, I had deduced immediately that my step-sister-in-law was pregnant – and I was right: this was, indeed, the secret.

I actually would never have just guessed it out of the blue, or assigned it to be likely (if, for example, I were presented with some sort of list of possible events, and asked to estimate their likelihood). But of the possible **secrets** that **my mother** could be keeping **from me** (and would then reveal), it ranked very highly.

If my father revealed that he had “exciting news” to announce, I would then know that he was about to explain that he intends to retire, sell his house in Connecticut, and move to Florida. I do not currently expect him to do this anytime soon. If my brother announced, I would know that he was about to say that he was getting engaged to his girlfriend. Again, I have no *current* expectations of either. I am *not* extrapolating from a set of “likely” events – it is only the “learning that a secret exists”, which makes me assume that they are imminent.

Similarly, if I had learned that “a secret exists between my brother and the CIA (or the KGB)”, I would –without knowing what the secret is, exactly– be forced to revise my opinion of him substantially. As I would if I learned that some secret were between him and a ballet school (or an alchohol rehab program, or an HIV clinic).

This concept I call the “meta-secret”. I make no pretense to have discovered it – it is ancient wisdom to all secret-keepers.

```
"..the most important part of any secret
 is the knowledge that a secret exists..."
-HPMOR, Chapter 48
```

C. Publicly Hiding Something

Imagine that Adolf Hitler shows up at your house, and asks you if you are hiding any Jews in your attic. He wants to send all of the Jews and the Jew-lovers into the furnace and burn them all alive, basically for no real reason.

And imagine that you are indeed sheltering some Jewish people in your attic. How should you respond?

But before you respond, ask yourself: what did my neighbors say, when asked this question?

You estimate that they said the following:

The Head of Household A says “No, I hate the Jews. I hope you find lots of them and burn them all.”

HoH B says the same thing.

But HoH C actually is hiding some Jews in his attic. Nonetheless, he imitates HoH A. (And so he and his Jewish guests live to fight another day.)

HoH D, being very naive, believes that "lying is wrong" (whatever that means). So he says "I admit there may be some Jews here. But all people have an equal right to share in th–" but before he can finish his poetic thought he and his entire family (and the Jews living in his attic) are arrested and killed.

Finally, consider HoH E: He says, "This question is objectionable. I have the right to use my house any way that I damn well please. None of your business!" and he slams the door. Of course, the Gestapo raid it that night, find the Jews in the attic, and kill everyone.

You see, if you are going to really keep a secret, you have to commit to it completely. **You need an entire second identity.** You are resembling an "innocent" person.

```
"...to keep a secret ...I must give no
sign that differs from the reaction of
someone truly ignorant."
-HPMOR, Chapter 70
```

Imagine that Modern Hitler comes next for the gays. He asks German Men, via survey, whom they feel most attracted to. The survey options are: [1] women, [2] men, and [3] decline to answer.

Option three is, really, not a serious option. All of the straight German men will be proudly checking option one, en masse. And *anything other than what they do* will look suspicious. **Admitting that you have something to hide is already a total defeat.** The only thing that you *could* hide, in this context, is a "shameful" thing. So hiding is not an option.

D. Block Explorers

Imagine that Hitler knows, using data from other countries, that around 3% of the male population is homosexual.

He then decides to use public surveillance, instead of a survey. He discovers that 98% of German 18-24 yr old males use public roadways to hit up the clubs, on Friday/Saturday, to get laid with women. But 2% are "staying home to read" or are "working on their careers". And he further discovers that, on Facebook/Twitter, 95% of good-looking bachelors freely talk to their friends/family about girls, but 5% instead become "irritated" and change the subject. Some percentage of the population is **aberrant**.

I don't know, it just seems obvious to me – if you really *need* to keep the secret [from someone], then you have to go *all the way*. You have to do what *they* expect a truly unsecretive person would do – go to bars with your friends, get married and have kids and all of that. You're either keeping the secret [again – *from* someone] or you aren't.

E. The Pretext

One of mankind's most powerful technological innovations is the **pretext**– a justification for doing something that is fake, but irrefutable. Pretexts act as a kind of "social shield" or "social encryption" that one can hide behind. Specifically, you can hide your *motivations*. Your **secret** motivations.

For example, imagine that Teenager 1 ("Alice") wants to spend more time with Teenager 2 ("Bob"). So Alice decides to join a drama club that Bob is in. While doing so, Alice will misdirect the audience's attention, to the non-Bob attributes of the club. In other words, she is sure to remark loudly that she loves acting (etc). And Alice may fool a few people with this ruse. But, much more importantly, Alice's claim [of interest in drama, vs an interest in Bob] *cannot be easily [dis]proven* by anyone. And therefore most people will be *disinterested* in the claim's truth or falsehood. Mission accomplished!

In fact, even those who are nearly certain that it is a lie (for example: Alice's rivals, or long-time members of the drama club), cannot prove their knowledge to anyone else, without appearing to be suspicious or dark-minded themselves. And so even the suspicious people are forced to self-censor their suspicion. The fact that Alice is up to something, goes un-discussed. (At least, not openly.)

F. Dis-Entanglement

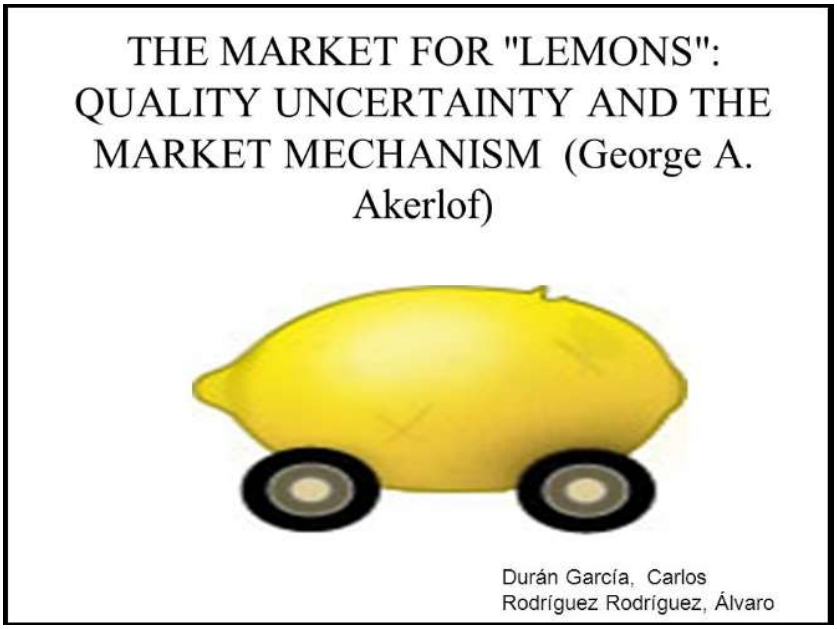
The pretext works because some people *really do* enjoy drama club, and *really are* interested in joining it for the first time. Since "interaction with Bob" is **entangled** with "participation in drama club", we can't know for sure which event Alice is after.

But, like Hanson's Clothes, the pretext starts to break down as it becomes more expensive. Drama Club is one thing, but what if it met on *Sunday mornings*? Or two hours away from the school? (Or what if it were just objectively not fun at all, a terrible experience.)

A sufficiently Bob-motivated Alice would still join drama club, and invent the appropriate pretext. And it will still be impossible to prove her state of mind, or to talk about it without seeming nosy or obsessive.

But, alas, things for Alice are about to go horribly wrong! Say that the school has two drama clubs, identical in all ways except two: Bob is in Club 1 [but not Club 2], and Club 1 costs $5 to join [but Club 2 costs nothing]. Choosing Club 2 is effectively "buying Bob" for $5.

Since the clubs are identical in every other way except Bob, there are now no pretexts available for Alice to use. Even if Alice is super-super-wealthy, it makes no difference. There is only one reason for Alice to pay that five dollars: to be with Bob.



Above: “Market for lemons” title slide image, from this presentation.

Alice can try some new pretext, ie that Bob and Alice are “friends” and want to hang out together. But only if they are already friends. If Alice is trying to make a new friend it will not work[^n] – it will be obvious, and possibly desperate.

Aside: this may shed some light on the puzzling but incontrovertible claim that “making friends” requires there to be “unplanned interactions” among potential-friends.

2. Bitcoin Privacy Technologies (ie “Fungibility”)

Now...

...with all that you’ve just learned...

...I would like you to tell me, what the key difference is, across the following Bitcoin Technologies:

Column 1	Column 2	Column 3
Reusable (“stealth”) addresses, The lightning network, Non-interactive CoinJoin w/ Schnorr signature aggregation, TumbleBit, Dandelion, Taproot	Sending your own BTC to yourself N times.	Ring Signatures, zk-SNARKs, Confidential Transactions, Confidential Assets, Interactive CoinJoin

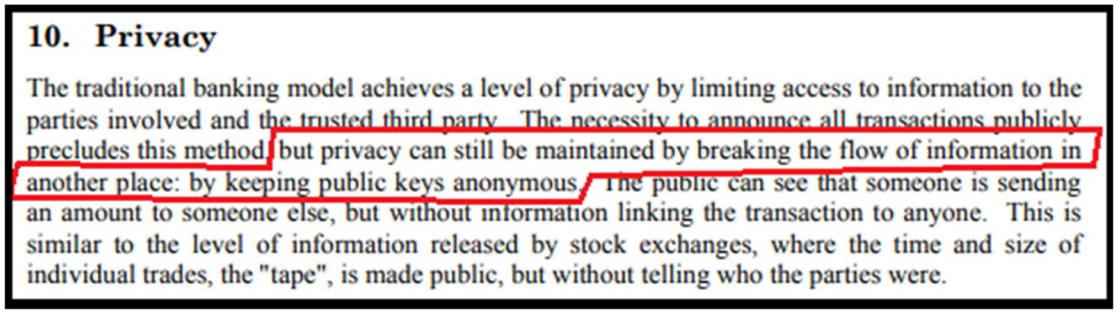
Column 1 contains technologies that are more private, **and also cheaper** or more convenient for the user. Reusable addresses are much more user-friendly than our

current process [of awkward interaction, over an endlessly mutating list of gibberish][1]. LN and Schnorr-CoinJoin are literally cheaper to use – they consume fewer on-chain bytes. And developers [we can assume] will eventually make TumbleBit, Dandelion, and TapRoot the standard or default behavior[2] for clients/LN-hubs/MASTs, at which point doing anything else will be inconvenient (and suspicious).

Column 2 contains one item: "sending your own BTC to yourself". This is certainly not "free", because each txn costs one tx-fee. However, the costs are *themselves* 100% private[3]– no one knows, for sure, that you are going out of your way to pay-for-privacy. So the cost-differential is itself private, making it unobservable.

This is, incidentally, why it does not matter that TumbleBit and Dandelion are "more expensive" in that they require more CPU cycles (relative to "basic" LN-hubs or node-txn-rely). No one observes CPU cycles directly, and even if they could, observers couldn't *prove* their observations to third parties. The CPU cycles, just like self-sending cycles, are done in private.

In fact, any fake txns that you broadcast will not only mix your coins, but they will also make the chain as a whole more incomprehensible. It is even (speaking very roughly) the privacy model advocated by Satoshi himself:



10. Privacy

The traditional banking model achieves a level of privacy by limiting access to information to the parties involved and the trusted third party. The necessity to announce all transactions publicly precludes this method, but privacy can still be maintained by breaking the flow of information in another place: by keeping public keys anonymous. The public can see that someone is sending an amount to someone else, but without information linking the transaction to anyone. This is similar to the level of information released by stock exchanges, where the time and size of individual trades, the "tape", is made public, but without telling who the parties were.

Column 3 contains privacy technologies that are more expensive to use. Thus, they will tend to be exclusively used by "the guilty", as any innocent person has no reason to pay up[4].

I am sorry to trod on other people's hard work, but I don't see any hope for the members of Column 3. While those techs certainly have academic value, and while they could certainly be stepping stones to greater technological improvement, they are unserious and should be discarded. Any talk of their use or implementation is perplexing at best. They are in the situation I outlined above, of Alice paying $5 to join the Bob-drama-club. These techs make no attempt to achieve **the goal of privacy**: to allow the Guilty to resemble The Innocent.

3. Applied to Bitcoin Itself

This critique –that expensive privacy unravels, Market-for-lemons style– can be easily applied to Bitcoin itself.

In fact, it's so easy that a sitting US Congressman has already done so, on camera no less!

I give you the comments from Congressman Sherman on July 18, 2018, emphasis added:

"[Bitcoin] seems to be a solution looking for a problem. What can an honest citizen *not* do... I can be in the smallest hamlet in rural India, and use my VISA card. I've never had a problem paying somebody. ...we have pretty efficient, mostly digital, transfers of dollars every day... So what's the problem [that Bitcoin is] trying to solve? ...unless I'm a tax evader or narco-terrorist. ... **I'm trying to illustrate that it [Bitcoin] is a solution, only to the problems of tax evaders, criminals, and terrorists**. ... the currency whose **sole** value is helping the before-mentioned ne'er do wells."

As you can see, he lays out exactly the argument that I have been making. That Bitcoin will tend to be used "sole"ly by "ne'er do wells", because it is marginally useful to them and marginally inconvenient[5] for innocent people. And therefore that Bitcoin should be completely suppressed.

If we are interested in defending against this argument, then Bitcoin must *do something else* for 'the Innocent'.

The obvious choice is for Bitcoin txns to be cheaper, because everyone prefers having more money to having less money. Unfortunately, this choice has become needlessly controversial with the rise of the Great Scaling Dispute.

Another choice would be to emphasize Bitcoin's use in anything hitherto-impossible, such as "smart contracts". Unfortunately, any "smart contract" could be turned into a more-straightforward dumb contract, using the formula "smart_contract = dumb_contract + (brand_name OR judicial_system). And so these transactions

would not truly be “hitherto-impossible”, and so Sherman’s critique [that Bitcoin is useless for Innocent people] would still apply.

Footnotes

1. Especially after they are merged with blockchain identity technology. ⮌
2. In my upcoming Introduction to Game Theory, I will describe the surprisingly extreme power of the “status quo” or “defaults”. ⮌
3. Assuming, of course, that you take appropriate internet privacy precautions when physically *broadcasting* the transactions. For example: broadcasting these transactions while connected to a VPN, or to TOR, or while behind several proxies, or at the public library, etc. (I say “physically” because electromagnetism is physics.) ⮌
4. Other than idealism. In other words, these privacy techs may be used by a few almsgiver privacy-advocates. But this simply cannot scale. Oover time, regular users will defect to the cheapest and easiest-to-use technologies (as they should), and so the use of awkwardly-expensive technologies will look more and more suspicious. ⮌
5. We can see that Innocents today place a high premium on convenience, as many use the Venmo app and maintain its default “everything public” privacy settings. ⮌

PoW is Efficient

By Dan Held

Posted September 14, 2019

Foreword

Most people think #Bitcoin’s PoW is “wasteful.” In this article, I explore how everything is energy, money is energy, energy usage is subjective, and PoW’s energy costs relative to existing governance systems. This article is a collection of direct thoughts from many individuals in the space—my value-add was in the aggregation, distillation, and combination of narratives.

Work is Energy

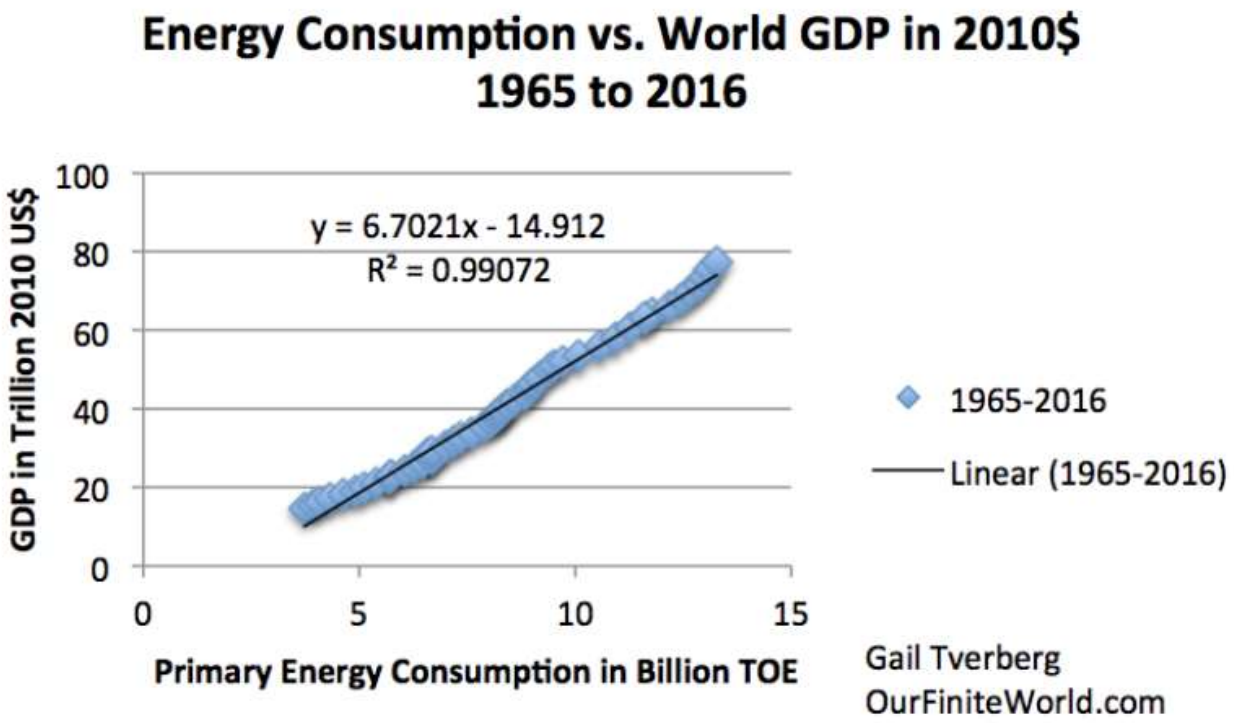
The idea of “work” being energy started when the French Mathematician Gaspard-Gustave de Coriolis introduced the idea of energy being “work done.” A long time ago, the work done in the economy was entirely human. That work was powered by food.

About a million years ago, humans stumbled across fire. As a result, the energy available to us increased because now we could keep warm not just from what we ate but also from burning. So this added energy usage improved our standard of living.

Some thousands of years ago, our energy usage increased still further when we domesticated animals. Animals could labor in our place. Those new laborers also had to be fed. Large amounts of food were required to meet the energy demand, and our prosperity increased alongside.

In the last few hundred years, we built great machines. Those mechanized machines produced work, first from sources like water & wind, and then the cheaper sources like coal and gas, and now from nuclear sources (fission/fusion). Both machines and nature produce work through the utilization of energy. We have an economy based not on money, but on work and energy.

All things in our lives are closely linked to the price of energy. Purifying water requires energy. Transporting products requires energy. Manufacturing products requires energy. Cooking requires energy. Refrigerators and freezers require energy. In a free market, the cost of any good largely reflects the energy used in producing that good. Because free markets encourage the lowest priced goods, the energy used in producing any good is minimized. Money, which is the representation of the work required to generate goods and services, can also be viewed as stored energy.



World GDP in 2010$ compared (from USDA) compared to World Consumption of Energy (from BP Statistical Review of World Energy 2014).

In the early 20th century, industry leaders like Henry Ford and Thomas Edison were interested in replacing gold or the dollar with "the energy dollar" or "units of energy" (commodity/energy currency). The concept was popular due to its sound money characteristics, including: a well-defined unit of account, easy measurement/not easily counterfeited, divisibility into smaller units, and fungibility (that these units would be equivalent to any other unit). However, energy money was flawed—it could not be transmitted or stored easily.

"that in order to make a man/woman covet a thing, it is only necessary to make the thing difficult to attain." — Mark Twain

Fast forward to October 31, 2008—Satoshi publishes the Bitcoin whitepaper. Bitcoin's Proof of Work (PoW) was originally invented as a measure against email spam. Only later did Satoshi adapt it to be used in digital cash. What PoW mining does under the hood, is use dedicated machines (ASICs) to convert electricity into Bitcoins (via block reward). The machine repeatedly performs hash operations (guesses/votes) until it solves a cryptographic puzzle and receives Bitcoins (block reward). The solution to the puzzle proves that the miner spent energy in the form of ASICs and electricity, a proof that a miner put in work. Bitcoin has a capitalistic voting mechanism, "money risked, votes gained" through the energy/ASICs used to generate hashes (votes).—Hugo Nguyen

When Satoshi designed PoW, he was fundamentally changing how consensus between humans is formed from political votes to apolitical votes (hashes) via the conversion of energy. PoW is proof of burn, or the validation that energy was burnt. Why is that important? It's the most simplistic and fair way for the physical world to validate something in the digital world. PoW is about physics, not code. Bitcoin is a super commodity, minted from energy, the fundamental commodity of the universe. PoW transmutes electricity into digital gold.

The Bitcoin ledger can only be immutable if and only if it is costly to produce. The fact that Proof of Work (PoW) is "costly" is a feature, not a bug. Until very recently, securing something meant building a thick physical wall around whatever is deemed valuable. The new world of cryptocurrency is unintuitive and weird—there are no physical walls to protect our money, no doors to access our vaults. Bitcoin's public ledger is secured by its collective hashing power: the sum of all energy expended to build the wall. And through its transparent costly design, it would take an equivalent amount of energy to tear it down (unforgeable costliness).

Energy Consumption

The cryptopocalypse is coming—Bitcoin's (PoW) is so bad that it's going to destroy the world in 2020! You may have noticed that most of the "doomsday" articles were based on the results of an analysis provided by Alex De Vries, a "financial economist and blockchain specialist" working for PWC Netherlands and author of the site Digiconomist. His estimation has already received a fair share of criticism due to its poor energy consumption calculation. But the KPI of his choosing was intentionally misleading: "the electricity consumption per transaction" for several reasons:

- The energy spent is per block, which can have a varying number of transactions. More transactions does not mean more energy
- The economic density of a Bitcoin transaction is always increasing (Batching, Segwit, Lightning, etc). As bitcoin becomes more of a settlement network, each unit of energy is securing exponentially more and more economic value.
- The average cost per transaction isn't an adequate metric for measuring the efficiency of Bitcoin's PoW, it should be defined in terms of the security of an economic history. The energy spend secures the stock of bitcoin, and that percentage is going down over time as inflation decreases. A Bitcoin "accumulates" the energy associated with all the blocks mined since its creation. LaurentMT, a researcher, has found empirically that Bitcoin's PoW is indeed becoming more efficient over time: increasing cost is counterbalanced by the even greater increasing total value secured by the system.

Now that we know what the right KPI is for ROI on energy consumption, let's take a look at how energy costs are trending for Bitcoin's PoW.

The rate of ASIC efficiency improvement is slowing. As efficiency gains slow we can expect an increase in manufacturer competition as margins narrow.

https://cseweb.ucsd.edu/~mbtaylor/papers/Taylor_Bitcoin_IEEE_Computer_2017.pdf_

	2009	2010	2011	2012	2013	2014	2015	2016	2017	2018
Hash Rate (Gh/s)	0.003	0.575	0.550	0.650	63	878	4,255	9,750	11,500	22,550
Watts	55	241	271	250	445	509	1,145	1,200	1,450	1,786
Price (Release)	104	540	369	550	1,299	460	1,553	1,494	1,100	1,709
Efficiency (Gh/W)	**0.00005**	**0.002**	**0.002**	**0.003**	**0.16**	**1.7**	**3.7**	**7.9**	**7.9**	**12.4**
y/y		*4749%*	*-14%*	*27%*	*6190%*	*923%*	*121%*	*112%*	*1%*	*56%*
Hash Rate Cost ($/Gh)	**$39,808**	**$938**	**$671**	**$846**	**$21**	**$0.5**	**$0.4**	**$0.2**	**$0.1**	**$0.1**
y/y		*-98%*	*-28%*	*26%*	*-98%*	*-97%*	*-30%*	*-58%*	*-38%*	*-21%*

https://research.bloomberg.com/pub/res/d3bgbon7nESTWTzC1U9PNCxDVfQ

All-in mining cost will shift from the upfront accessibility cost of ASIC hardware (capex) to the ongoing energy costs to operate (opex). Since the physical location of mining centers is not important to the Bitcoin network (they are movable), miners flock to areas generating surplus electricity for the lowest marginal costs. In the long-run, this has the potential to produce more efficient worldwide energy markets with Bitcoin miners performing an arbitrage of electricity between global centers. The cost of Bitcoin mining becomes the lowest (excess) value of electricity. This may solve a problem with renewable energy sources that have predictable capacity that is otherwise wasted, like hydro and flared methane. In the future, Bitcoin mining could help with renewable energy sources that have variable output—energy producers can plug in miners, and store the excess power as bitcoin.

Aluminum was a popular means of "exporting" electricity from a country with abundant renewable energy resources that are stranded (ex: Iceland). Smelting bauxite (aka aluminum ore) has huge energy requirements, and converting that into aluminum is a one way function (just like a hash). The same concerns around "unfair" energy consumption existed for aluminum nearly 40 years ago—1979 (including concerns of centralization). All of these companies constantly scoured the planet for cheap power and other concessions. As aluminum manufacturing matured over the decades, the kWh per Kg of aluminum produced became more efficient.

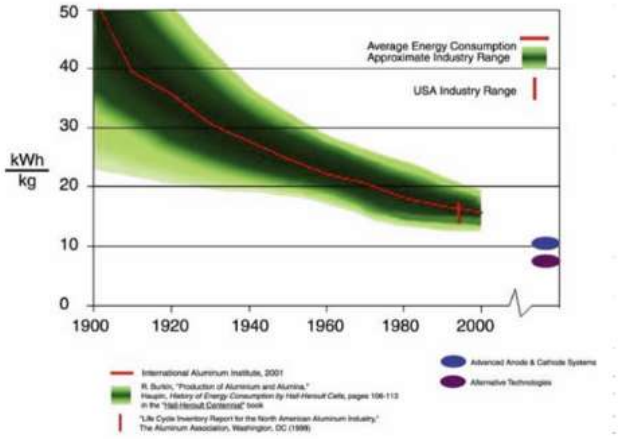


Figure 5.2: Primary Aluminum Electric Energy Consumption 1900 to 2000

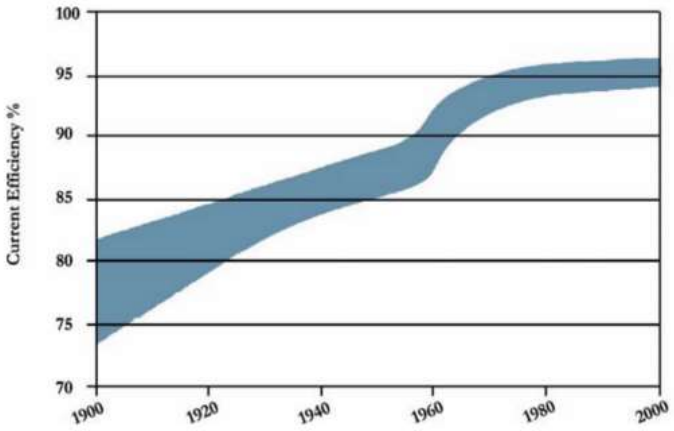


Figure 5.3: Primary Aluminum Current Efficiency 1900 to 2000

https://www1.eere.energy.gov/manufacturing/resources/aluminum/pdfs/al_theoretical.pdf

"This global energy net liberates stranded assets and makes new ones viable. Imagine a 3D topographic map of the world with cheap energy hotspots being lower and expensive energy being higher. I imagine Bitcoin mining being akin to a glass of water poured over the surface, settling in the nooks and crannies, and smoothing it out."—Nic Carter

Bitcoin's PoW is the buyer of last resort for all electricity, creating a floor that incentivizes the building of new energy producing plants around disparate energy sources that would have otherwise been left untapped.

"When will the energy used for PoW *stop* growing? Precisely when enough energy producers have started doing PoW directly that the marginal return from burning a kWh of energy through PoW = the marginal return from selling that kWh to the grid—when the "premium" on PoW is reduced to zero. I call this equilibrium the "Nakamoto point." I suspect PoW will use between 1–10% of the world's energy when this equilibrium is reached."—Dhruv Bansal

Some complain that Bitcoin mining doesn't accomplish "anything useful" like finding prime numbers. While introducing a secondary reward for doing the work might seem like a virtuous idea, it actually introduces a security risk. Splitting the reward can lead to a situation where "it's more worthwhile to do the secondary function than it is to do the primary function." Even if the secondary function was innocuous (a heater), instead of an expected $100 per x hashes, we'd move to $100 + $5 of heat per x hashes. The "Mining Heater" is just another increase in hardware-efficiency, resulting in a higher difficulty and an increase in (energy used/block). Luckily, Bitcoin

will never have this problem as its security is guaranteed by the purity of its proof-of-work algorithm.

Note: Bitcoin is already doing something immensely useful for society (mining wouldn't be profitable if it wasn't), and it isn't rational to ask miners to perform a function that is altruistic without incentives.

Relative Costs

Everything requires energy (first law of thermodynamics). Claiming that one usage of energy is more or less wasteful than another is completely subjective since all users have paid market rate to utilize that electricity.

"If people find that electricity worth paying for, the electricity has not been wasted. Those who expend this electricity are rewarded with the bitcoin currency."—[Saifedean Ammous]

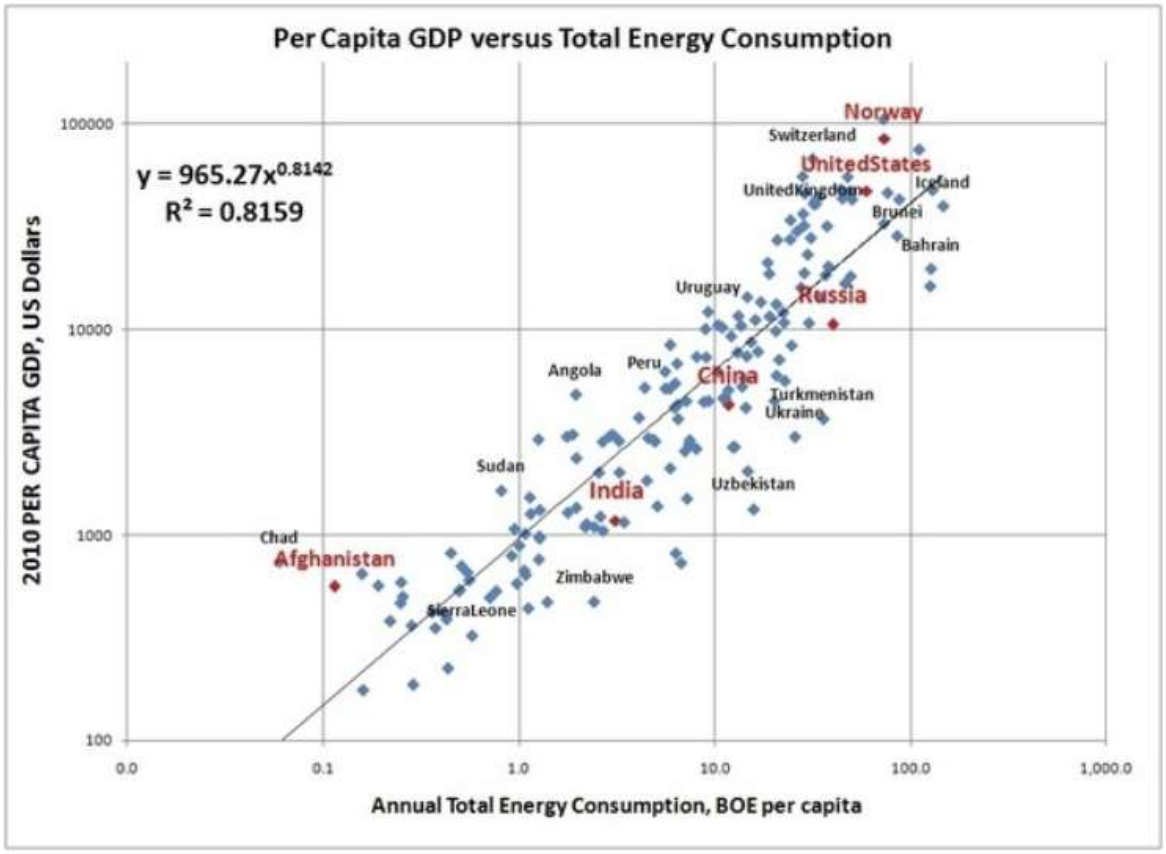
In thermodynamics, the universe is the ultimate closed system. Bitcoin's utilization of the excess electrical capacity consumes magnitudes less electricity than existing fiat systems which not only have power requirements banking infrastructure, but the military and political machina. The energy tradeoff for the utilization of that electricity to secure the financial system backbone is a "net positive" outcome. Below I make a rough comparison to the existing financial, military, and political systems (notes are at the bottom of the article)

	Yearly Cost	Energy Used (GJ)
Gold Mining	$105B	475M
Gold Recycling	$40B	25M
Paper Currency and Minting	$28B	39M
Banking System	$1,870B	2,340M
Governments	$27,600B	5,861M
Bitcoin Mining	$4.5B	183M

Type I Civilization

In the hunt for cheap energy sources, we will unlock greater economic abundance in the real world. Bitcoin, through the harnessing of these new or disparate energy sources, not only moves us forward to a Kardeshev Type I economy but may bring us closer to a Kardeshev Type I energy civilization (We're ~ 0.72 on the Kardashev Scale). With Bitcoin mining as an incentive, it may shrink the time we get to T1 from 200

years to less than a few decades. After reaching Type I status, there is less of a need to restrict the growth of energy consumption, which increases the standard of living for everyone.



The pressure to find cheap electricity sources will accelerate the effort to build fusion reactors. Nature is showing the way, powering the whole universe with nuclear fusion (stars). Humans are in the process of emulating nature by building fusion reactors. It is estimated that it will take ~ $80B in research over decades to finally unlock nuclear fusion. The fuel for fusion (primarily deuterium) exists abundantly in the Earth's ocean which could potentially supply the world's energy needs for millions of years. Fusion power has many of the benefits of renewable energy sources, such as being a long-term energy supply and emitting no greenhouse gases or air pollution. Fusion could provide very high power-generation density and uninterrupted power delivery. Another aspect of fusion energy is that the cost of production does not suffer from diseconomies of scale. The cost of water and wind energy, for example, goes up as the optimal locations are developed first, while further generators must be sited in less ideal conditions. With fusion energy, the production cost will not increase much

even if large numbers of stations are built, because the raw resource (seawater) is abundant and widespread.

“Water, water, everywhere, Nor any drop to drink.”—Samuel Taylor Coleridge

Fusion power and other cheaper energy sources will solve major problems for humanity like fresh water shortages. We are surrounded by seawater, but desalination stations, which remove salt from the seawater, require large amounts of energy. Costs of desalinating seawater are currently higher than freshwater, groundwater, water recycling, and water conservation.

Humankind’s will to explore, up the mountains, down to the sea floors, to the heart of the atom, to the very fabric of space-time; to grow, not be stifled by a limit to energy. We will reach for the stars.

Is the trustless settlement of $1.34T between counterparties annually with the added benefit of cheaper energy for all, worth the $4.5B in current mining costs? I think the answer is a resounding yes.

If you enjoyed reading this please:

1/ Follow me on Twitter.

2/ Sign up for my weekly newsletter which contains my distilled thoughts of the week

3/ Check out my other articles 👇

- **Planting Bitcoin** *Sound Money (sanum pecuniam)* medium.com
- **Bitcoin’s Distribution Was Fair** _ Debunking FUD _ blog.picks.co
- **Hodlers are the revolutionaries** *My reflections on the important role hodlers play in developing Bitcoin’s network (and other cryptocurrency networks).* tokeneconomy.co

Notes:

- All costs are in USD
- “Governments” are the total annual expenditures including military spending
- In 2006, the DoD used almost 30,000 gigawatt hours (GWH) of electricity, at a cost of almost $2.2 billion
- Global military spending annually is ~ $1.7T
- Initial research this analysis was based on
- Gold mining, banking system, gold recycling costs are all estimates from 2014
- Banking system and government estimates are a combination of annual expenses which includes electrical cost
- US energy usage as % of world

- US federal government energy expenditures
- Bitcoin Mining Costs
- $63.8B a year is spent on electricity alone for the banking system
- Bitcoin has had 0 recorded worker deaths, whereas gold has had 50,000 recorded deaths over the last 100 years
- Inflation for fiat currency has been approximately 2–3% annually which is a stealth tax that erodes savings. The costs are enormous to calculate and are not included
- Bitcoin isn't issued by a government, there is little to no corruption involved in distribution

---

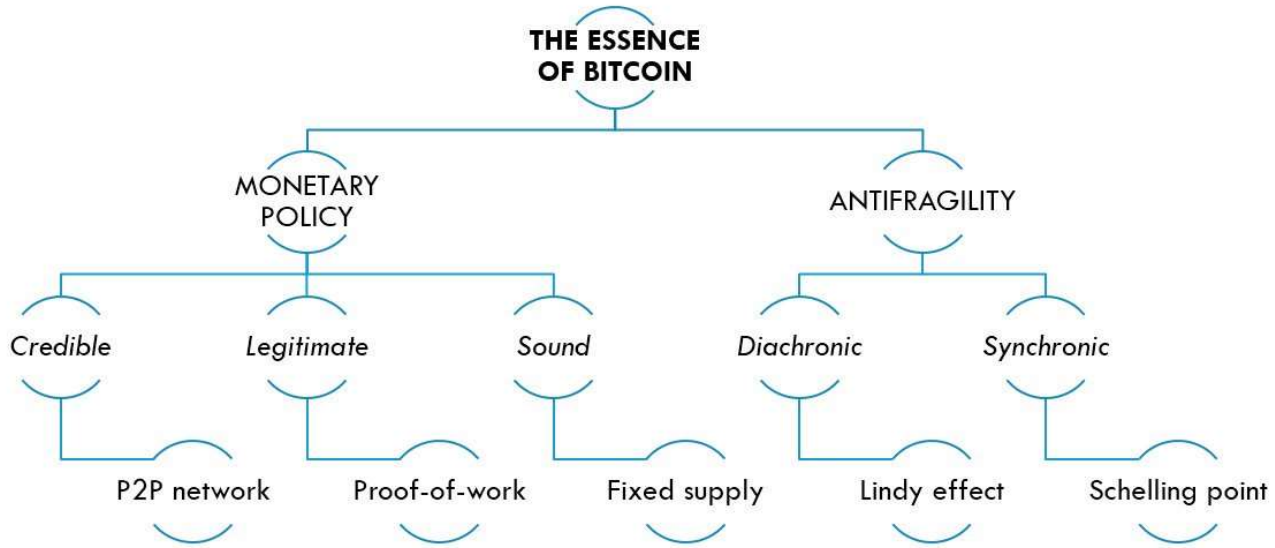
The Essence of Bitcoin

By David Puell

Posted September 14, 2018

For the newbs or the shitcoiners, the essence of Bitcoin in a simple graph.

(Based on @pierre_rochard.)



Bitcoin as a store of energy

By JP Thor [₿ ⚡]

Posted September 15, 2018

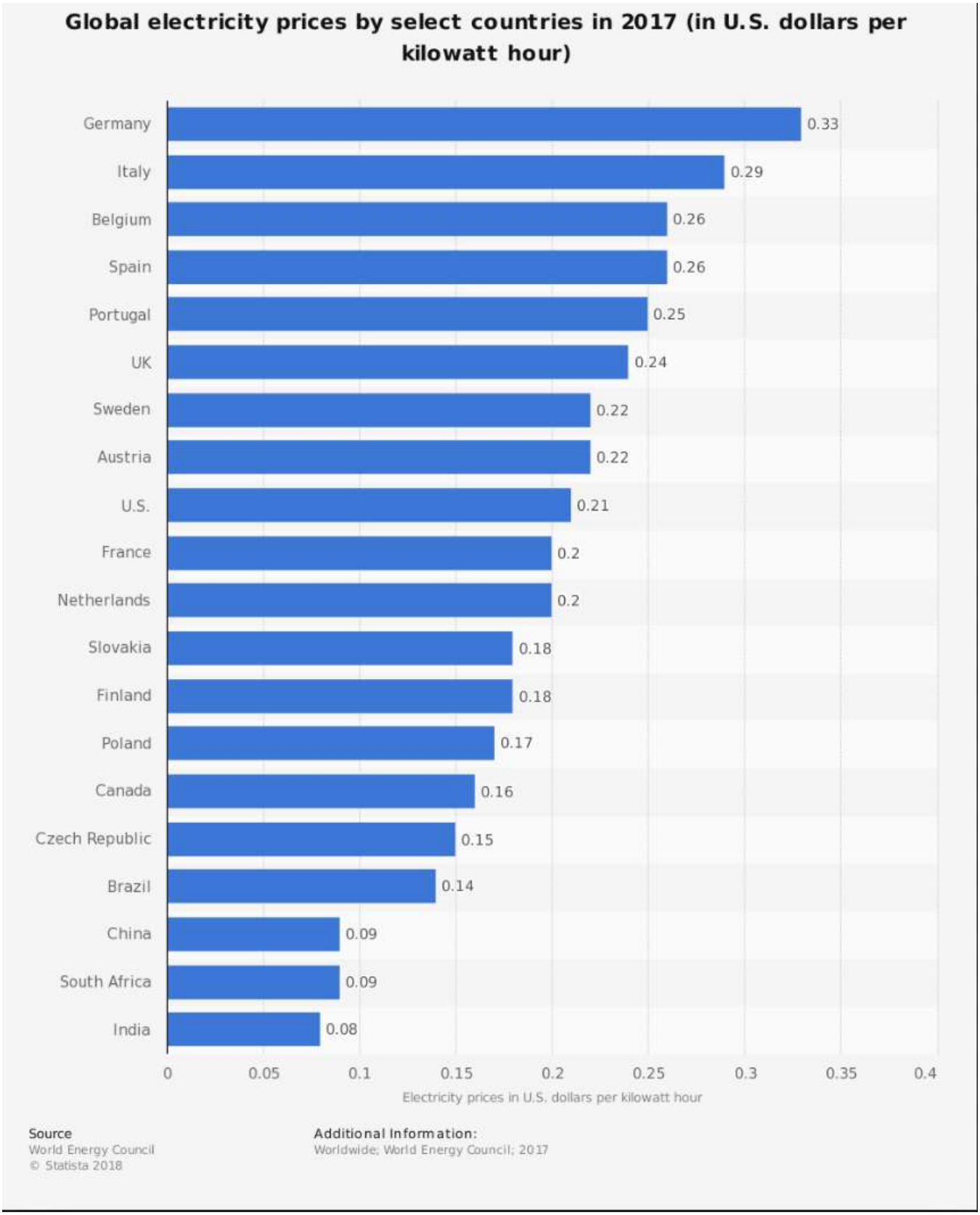
Bitcoin is a fascinating new asset class that we are only just barely beginning to understand. This article is one of a multi-part series that I want to explore about how the world can transition to the Bitcoin Standard; where BTC is used as the liquidity of the global economy instead of the current status quo (USD).

I'll discuss Bitcoin as a Store of Value and how that relates to energy. I'll then outline global energy production trends and problems. I'll then do an analysis on how Bitcoin can be used to compliment and augment energy production as a means to transmit energy from low cost regions to high cost regions, and what it may look like for Australia's energy grid.

We are beginning to see how Bitcoin can be used as a store of value (SoV). For almost a year now BTC has maintained a value higher than $5000 a unit, and 18 months for higher than $1000 a unit. Going deeper we can see that Bitcoin is actually a store of *energy*, as it consumes electricity in the most efficient manner possible via the actions of self-interested profit-seeking mining operators. As Bitcoin is created from coinbase rewards that can only be performed by miners, the value of that Bitcoin is invariably related to the amount of work that was performed in creating the Bitcoin, which requires energy expenditure. The combination of mathematically defined supply and proof-of-work is the strongest case of Bitcoin's SoV argument.

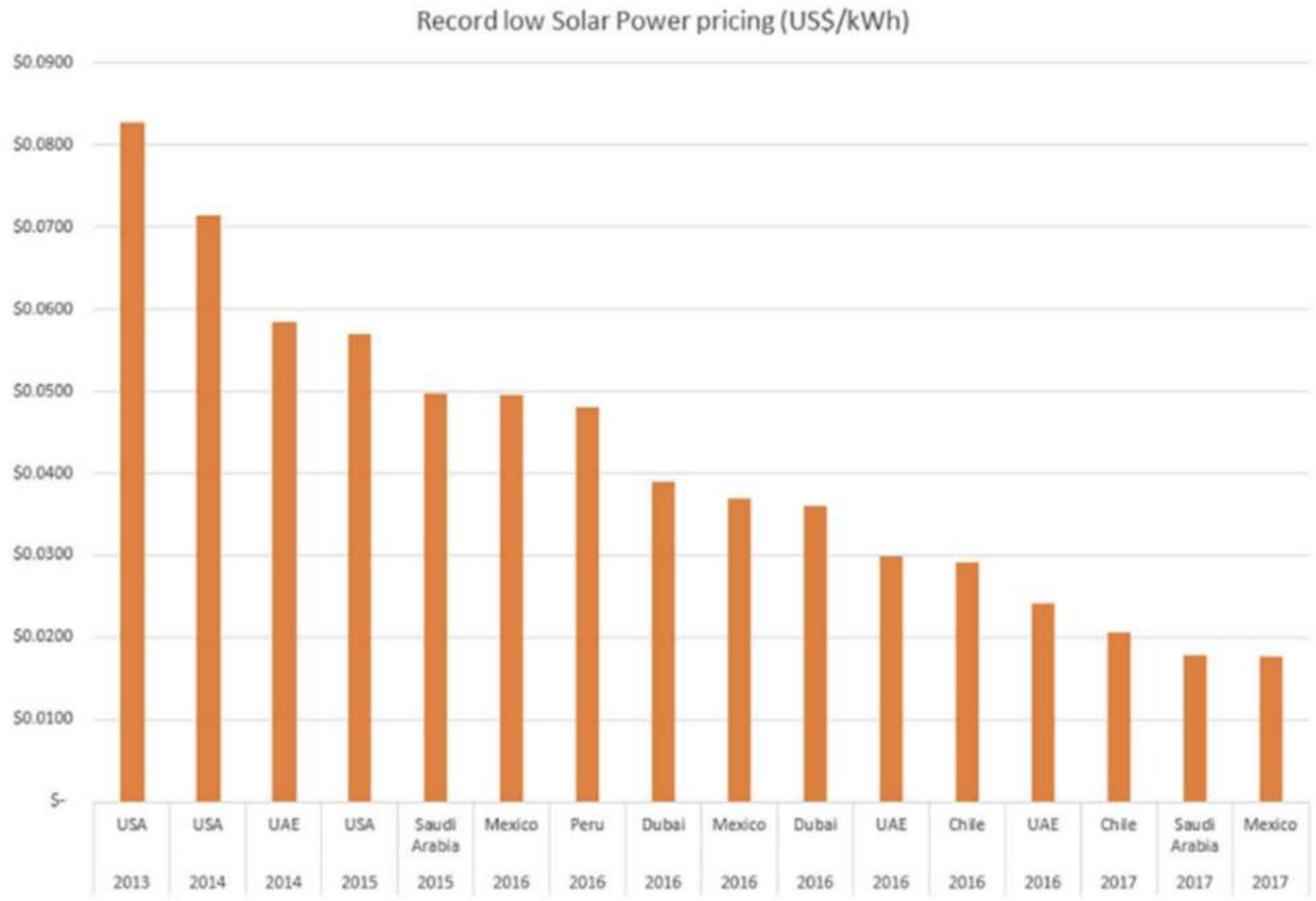
Global Electricity Prices

There is a massive disparity in global electricity prices, ranging from less than 10c kwh in some countries, to over 40c kwh in others. This can all be attributed to the differences in regional electricity production costs, exacerbated by the cost of transmission.


Global electricity prices by select countries in 2017 (in U.S. dollars per kilowatt hour)
Germany 0.33
Italy 0.29
Belgium 0.26
Spain 0.26
Portugal 0.25
UK 0.24
Sweden 0.22
Austria 0.22
U.S. 0.21
France 0.2
Netherlands 0.2
Slovakia 0.18
Finland 0.18
Poland 0.17
Canada 0.16
Czech Republic 0.15
Brazil 0.14
China 0.09
South Africa 0.09
India 0.08
0 0.05 0.1 0.15 0.2 0.25 0.3 0.35 0.4
Electricity prices in U.S. dollars per kilowatt hour
Source
World Energy Council
© Statista 2018
Additional Information:
Worldwide; World Energy Council; 2017

[Link]

However, these prices are far higher than what can be achieved through renewable sources, in particular Solar PV:

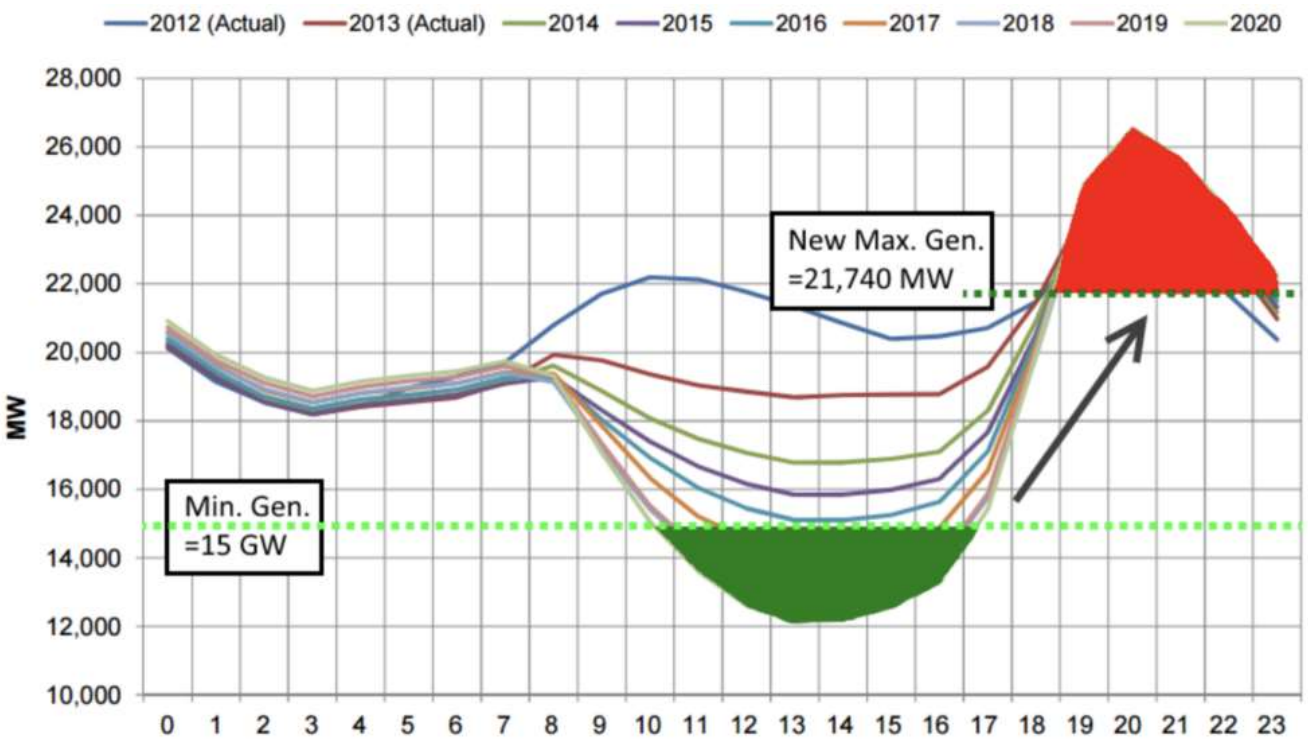


Link

In 2018 ACWA Power won a bid to deliver a 300MW Solar plant at a cost of $300m with energy production pegged to 2.34c kwh. A bid by Enel for a similar sized plant in Mexico was at a pegged price of 1.77c kwh.

Energy Production and the Duck Curve

Energy production follows the "duck curve", where the variable generation of energy across a day does not match the variable demand. Without some way to store, energy production must be adjusted to match demand, resulting in very expensive infrastructure such as peaker plants to compliment peaks of demand and load banks to shed energy when demand is below baseload. The baseload is the minimal amount of energy a grid must generate "at idle" to prevent infrastructure being turned off, which is expensive and damaging.

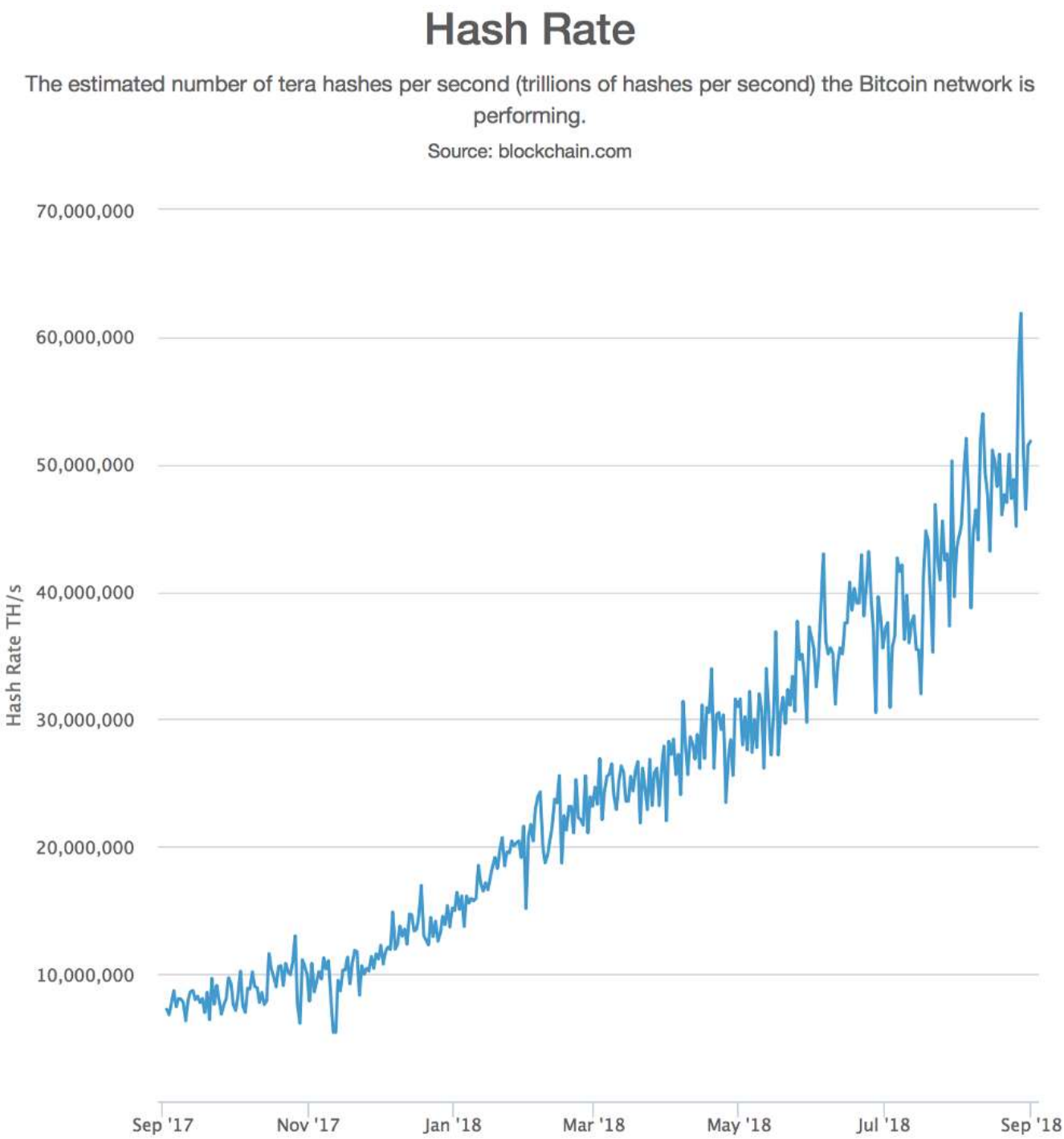


A Stanford study into Californian Energy Generation and Demand cycles

It is clear that energy can easily be produced in very large quantities for very cheap prices in the right regions. However, the issue is in transmitting this energy to the regions where it is needed. Enter Bitcoin.

Bitcoin Hash Rates

There is a continual increase in Bitcoin hash rate; which is an indirect metric of how much infrastructure is invested into and maintains the network at any given moment. Over the last year, despite any price volatility, the hash rate has increased 6 times, from 10 exa-hash to 60 exa-hash.



For every day that it is more profitable to mine a single Bitcoin and sell it than the amortized cost of infrastructure and the cost of electricity that goes into mining it, hash rate will be added. It is a very simple equation.

$$profit.Day = valueBTC.Day - (\frac{fixedCosts}{daysHashing} + Electricity.Day)$$

Equation

Analysis

The question is whether Bitcoin can be used to effectively absorb energy in one location and transmit it to another region to release that energy. We will do an analysis around a $300m energy contract with two scenarios:

1. Spend $300m on a Gas Power Plant in Australia.
2. Spend $100m on a Bitcoin mining farm in a low cost solar plant and $200m on an initial solar plant with storage, then using Bitcoin energy revenue to continue augmenting the growth of the plant.

Using existing data, the following are real-world numbers:

$300m Gas Power Plant yields 210Mw of peak power.

$150m on Solar yields 100Mw of power, with $50m in storage to store 60MW.

For this analysis we will use the following assumptions around the Antminer S9 with a realistic wholesale cost of $1000/unit (Bitmain are currently selling them off in a firesale less than $400):

- Bitcoin: $7000 USD
- Average cost of Antminer S9:$1000
- Output of Antminer: 14.5Th/s
- Daily Energy Consumption: 32kwh
- Daily Bitcoin produced: 0.000542

We will also use the following assumptions around a mining farm that would be built to consume energy from a low cost solar plant:

- Total farm cost: $100m
- Mining Equipment: $90m
- Fixed infrastructure: $10m
- Years of operation: 3 years
- Daily amortized infrastructure cost: $90k
- Total Antminers: 100,000
- Total Bitcoin produced a day: 50 BTC
- Total Daily Revenue: $170k

- Total mining reinvestment: 50% Profit
- Total Daily profit realised: $80k
- Total Daily electricity consumption : 2,948,400 kwh
- Total Daily Hash Rate: 2% of total hash rate
- Farm Size: 122 MW
- Electricity Cost Break-even: 5c kwh

Over 3 years, half of the daily profit from the farm is used to reinvest back into more mining infrastructure to prevent dilution against increasing hash rate. This leaves $80k of daily profit to be immediately transmitted back to Australia. This profit can then be used to either reinvest in the growth of the Australian solar plant, or by reducing the retail cost of electricity by over half.

1. Reinvesting into growth of solar plant

If reinvested, a total of $100m more is collected over 3 years (assuming no further increase in Bitcoin value). This would allow the solar capacity of the plant to be doubled.

1. Reducing cost of electricity

Assuming that solar energy can be retailed at 10c kwh in Australia, a profit-generating farm would allow the retail cost of electricity to be reduced by more than half by subsidising the cost of retail electricity.

Summary

These are significant figures in a world of marginal improvements. It was shown that energy cost can be arbitraged between two different regions by simply using Bitcoin mining to consume it in one area, and produce it in another via liquidation to local currencies and investment into infrastructure.

Currently Bitcoin mining consumes around 40,000,000 MWh, which is roughly 0.2% of the world's energy production. In the future it may consume around 10–20% of the world's energy production, at least a 100x multiple from here, at the same time as supporting the world's $80tn global economy, which is also a order of magnitude of 100 from where we are today.

In the next part I will discuss how the Lightning Network can be used by a self-sovereign country to completely power their economy and still collect consumption-based taxes fairly to run essential services. It will also be a look at how an economy can work in a low-inflation environment.

Electric Money

By LaurentMT

Posted September 17, 2018

"Do states dream of electric money ?" — Philip K. Dick (Reloaded)

So Electricity. Many Efficiency. (Blade Runner)

No equation, no chart in this fourth part. Just a short discussion about the total cost of Bitcoin's PoW. It will offer us the opportunity to introduce another fundamental property of PoW which makes it truly unique.

Is it really worth it ?

While our previous posts suggest that the efficiency of Bitcoin's PoW has improved over time, they don't address another source of concerns which is the total cost of the system.

Indeed, it seems legit to ask ourselves if this cost is really worth it. After all, we already know that alternate models (centralized systems, federations, etc) can be used for

implementing monetary and/or payment systems and it's often said that these models come with a lower environmental cost. If it's really the case, why should we bother with a such expensive system ?

Centralized and federated systems

Let's first focus on alternate models relying on centralized or federated parties acting as block builders. The details will depend on the exact model but it's easy to understand that in these systems, the centralized party or a large enough fraction of the federation is always able to prevent a new actor from joining the system. **By design, these systems allow incumbents to indefinitely maintain their dominant position and to enforce arbitrary decisions.**

Proof of Stake

Since they are often touted as serious challengers of Proof of Work, let's now consider alternate models based on Proof of Stake, Delegated Proof of Stake, etc.

At first sight, they seem better than the centralized or federated versions. Indeed, participation to the consensus is pseudonymous and it only requires that you have a stake in the currency. But here lies the issue with these models. With PoS and DPoS systems, a majority of incumbents is still able to prevent a new actor from becoming a leading player.

It means that in PoS and DPoS systems, a majority of incumbents still has the ability to indefinitely maintain its dominant position.

Proof of Work

With Proof of Work, the game is different. A lot has been written about the shortcomings of Proof of Work (cost, concentration of mining, suspicions of incumbents "playing dirty", etc) but a fact remains:

PoW is intrinsically an open system.

It means that no coalition of incumbents can prevent a new actor from entering the game or even from becoming a leading player. Not even a coalition of 100% of the participants. Your position in this "competition" is always dynamic and it primarily depends on the energetic, financial and technological resources invested.

Because of this truly unique property, **Bitcoin's Proof of Work creates on the long term an open and dynamic playing field** far more immune to unilateral political decisions (blockades, lock-out, etc) than any other existing digital system.

After 50 years of "hegemony" of the US dollar, if the ideas of digital gold and of a truly global currency must become a reality, it's not unlikely that the ability to provide an open and dynamic playing field will increasingly be considered as a fundamental property for a globally acceptable system. I don't expect that this conclusion will be natural for most governments and it's likely that their first instinct will be to create national cryptocurrencies relying on a "Proof of Authority". But as always, it's hard to predict the future. Time will tell.

A last word about "efficiency"

Since the term efficiency is often used to explain how "X is more efficient than PoW", it's seems important to remind a few things about it.

Efficiency isn't an absolute metrics. It isn't something that you can define without a context. When we state that "X is more efficient than Y", it's implied that both X and Y produce the same expected results/properties but X wastes less resources. But it doesn't make sense to state that "X is more efficient than Y" if it requires that X sacrifices important properties of Y.

And it's precisely my issue with the trending assertions that "PoS (DPoS or whatever) is more efficient than PoW". These statements conceal that this efficiency "gain" is the result of a trade-off sacrificing the intrinsically open nature of PoW.

On my side, I consider this property as a fundamental aspect of Bitcoin (if not the most important) and removing it from the system would clearly change the value proposition of the cryptocurrency. It doesn't mean that there's no room for alternative consensus and anti-sybil systems in the context of different specific use cases but these alternatives should clearly state the trade-offs being made.

I guess that the conclusion will be somewhat shocking for some people but the fact is that to date Bitcoin's PoW is the most efficient solution in its category because it's the only existing digital solution providing this property. It's simple as that. Pending a breakthrough in Computer Sciences, our best roadmap for building a truly open and dynamic playing field is to continuously work on improving the utility of Bitcoin's PoW, to encourage the use of renewable energies and to make sure that the positive feedback loop at the heart of the system is counterbalanced by negative feedback loops avoiding a runaway which might have very negative consequences.

Conclusion

This fourth part marks the end of this series dedicated to the properties and the efficiency of Bitcoin's Proof of Work.

These articles have barely scratched the surface of the subject. To be honest, they're mostly the result of an intellectual curiosity mixed with a high propensity to choose weird hobbies. **I have little doubt that it should be easy to improve and generalize the model proposed in the first parts (just remove a few assumptions) or to come up with a better model.**

My only wish is that this series has convinced you that many aspects of Bitcoin's Proof of Work are still greatly misunderstood, be it by ignorance or on purpose. This subject is a greenfield remaining to be explored. Don't be scared to go down the rabbit hole.

Acknowledgements

I wish to thank Yorick de Mombynes , @Beetcoin, Pierre P. and Stephane for theirs precious feedback and their patience :)

A great thank you to @SamouraiWallet and TDevD for theirs feedback and their support of OXT.

Bitcoin's Inflation Adjusted NVT Ratio - An UpToDate Assessment

By cryptopoiesis

Posted September 18, 2018

Noon. Herd in the steppe by Arkhip Kuindzhi c. 1895

This analysis aims to take a closer look at the NVT Signal/Ratio adjusted for Bitcoin's inflation in circulating supply, in the light of recent price developments and comparing it to the original **NVT Ratio/Signal** developed by **Willy Woo** and **Dimitri Kalichkin**. The data of these ratios, provides a good insight regarding the current market cycle, as well as a better understanding of the wider perspective in regard to the relevance & applicability of these metrics going forward.

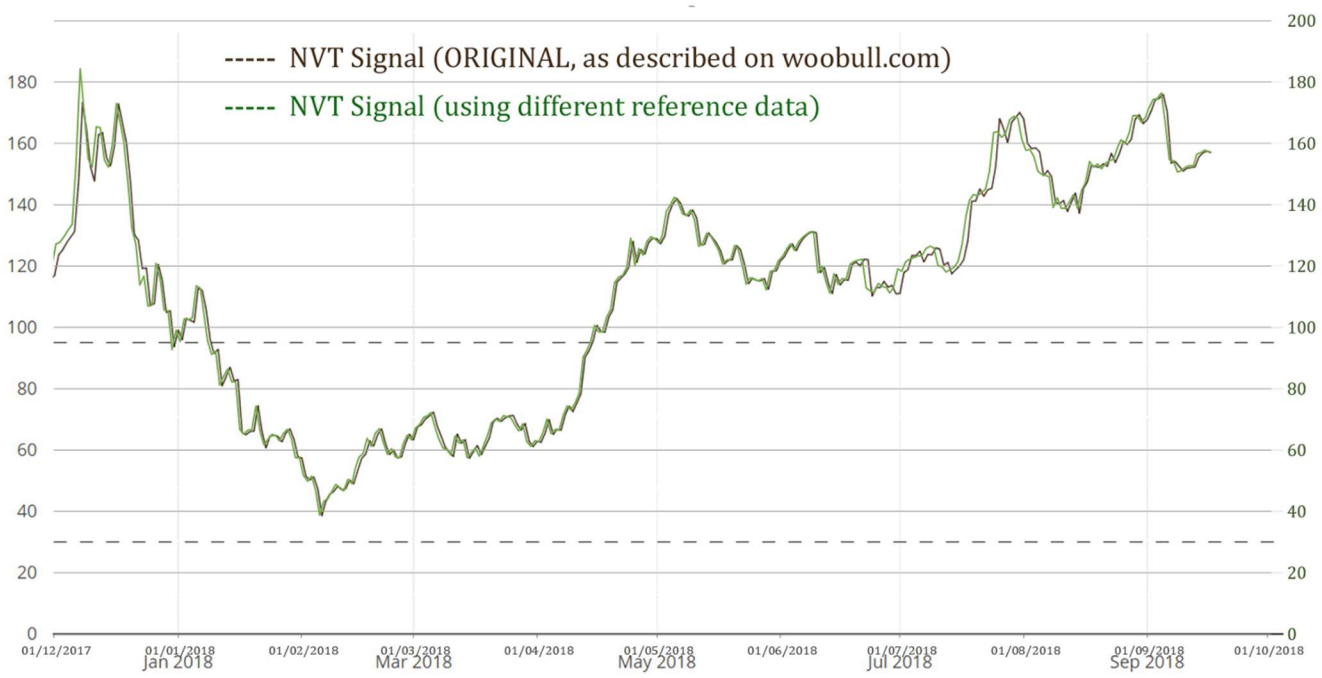
" **Bitcoin's NVT Ratio Normalised for Inflation in the Circulating Supply**" will be referred to as: ***Wookalich Ratio*** for short and as credit to the developers of the original NVT Ratio & Signal. Whether that will be welcomed or disapproved off, remains to be seen.

The rationale for adjusting the ratio was put forward in the article ***Bitcoin's NVT Ratio Normalised for Inflation in the Circulating Supply*** .The ***Wookalich Ratio*** charted in this article differs slightly in methodology by further "normalising" / flattening the trend line: a denominator factor of **3.75** replacing the 4 in the equation bellow:

$$"dilution\ factor"\ (df) = 1 - \frac{\text{coins in circulation} - \ coin\ supply\ at\ t_0}{3.75 \times coin\ supply\ at\ t_0}$$

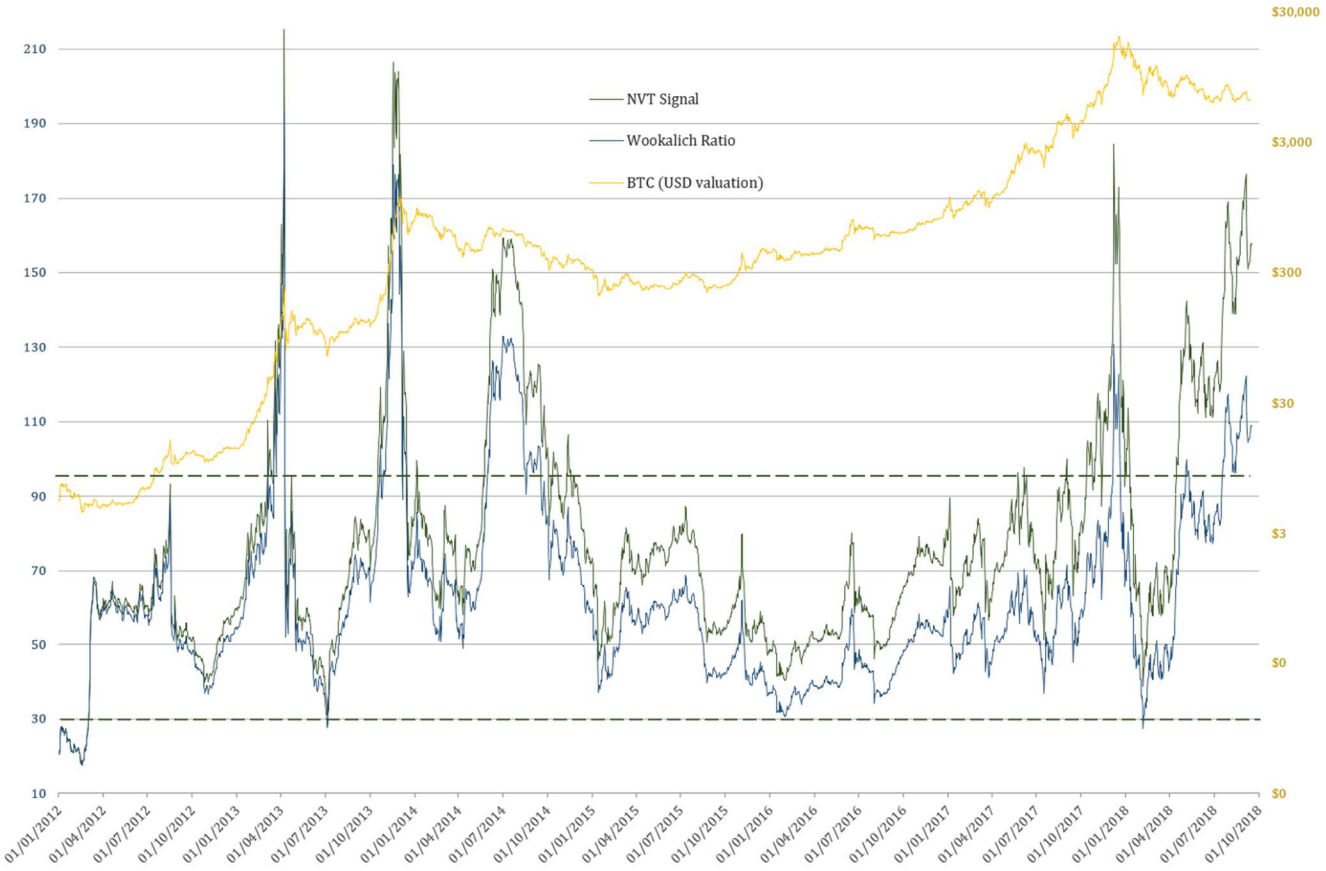
$$Wookalich\ Ratio = \mathrm{df}\frac{\mathrm{MC}}{MA_{90}(TV)}$$

Furthermore, the Wookalich Ratio had been charted in this article using a different set of price, coin supply and market cap data. The graph below assesses the reliability of this data in comparison to that used to calculating NVT Signal on **woobull.com** :



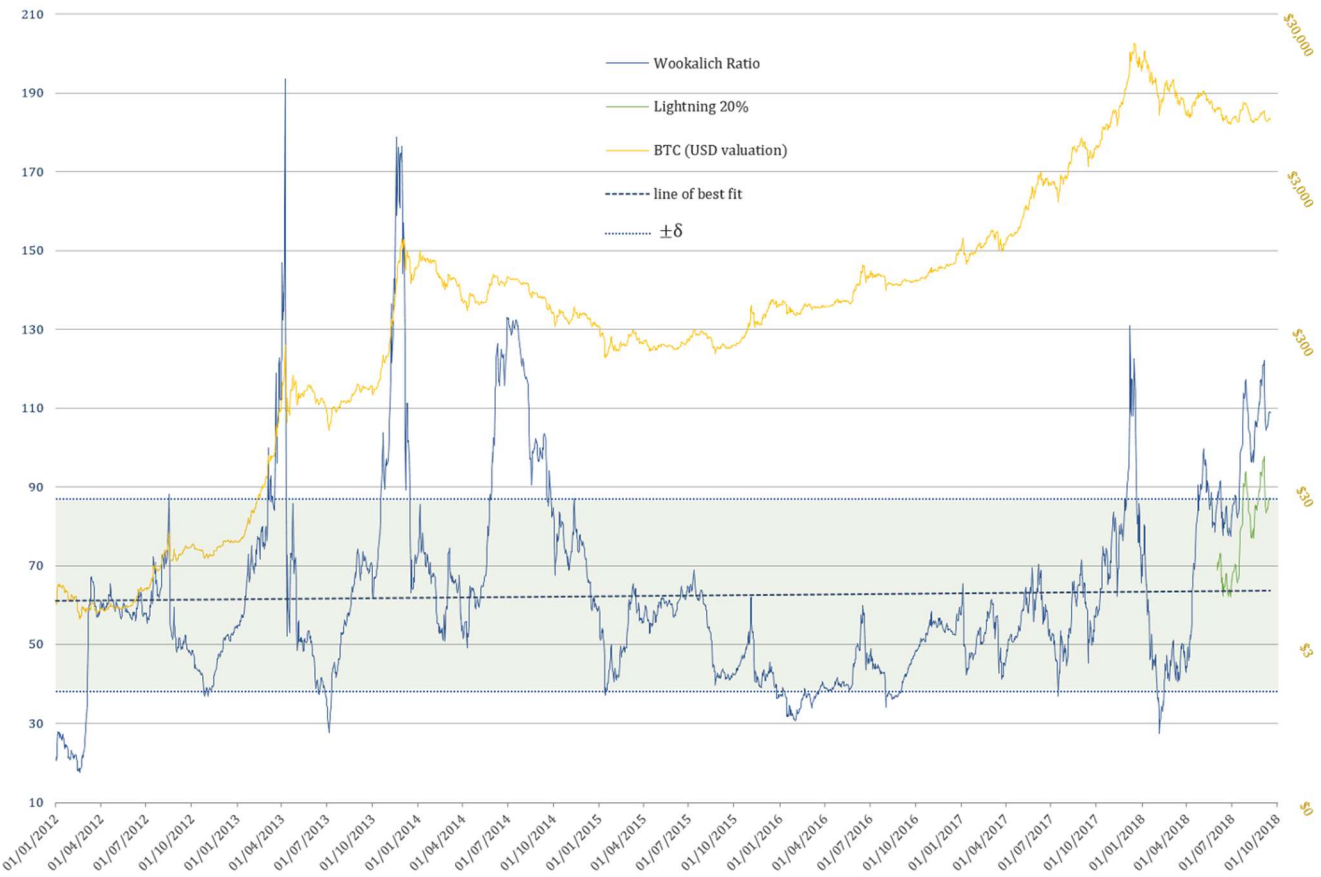
From the above chart, it can be concluded that the data is compatible, giving a virtually identical NVT Signal. The one subtle, nevertheless constant, difference is the slightly (1 day) leading "bias" generated by this data. The rationale and the methodology used for this reference data are succinctly described in the article: ***What is the Price of Bitcoin, or its Market Cap…. exactly?***

NVT Signal & Wookalich Ratio Overview



The Wookalich & NVT Ratios in all charts have been plotted against BTC dollar valuation instead of those of the Market Cap for the purpose of being more “user friendly”.

The Wookalich Ratio



2012—Present

Wookalich Ratio properties:

- Average value (since 2012): 62.24
- Standard deviation from the mean (±δ): 24.48
- Upper bound (+δ): 86.72 & Lower bound (-δ): 37.77

Taking into consideration the levels at which the line of best fit is currently at the following approximate key levels can be determined:

- **Wookalich Ratio average: 63**
- **Upper "overbought" bound: 88**
- **Lower "oversold" bound: 39**

Discussion

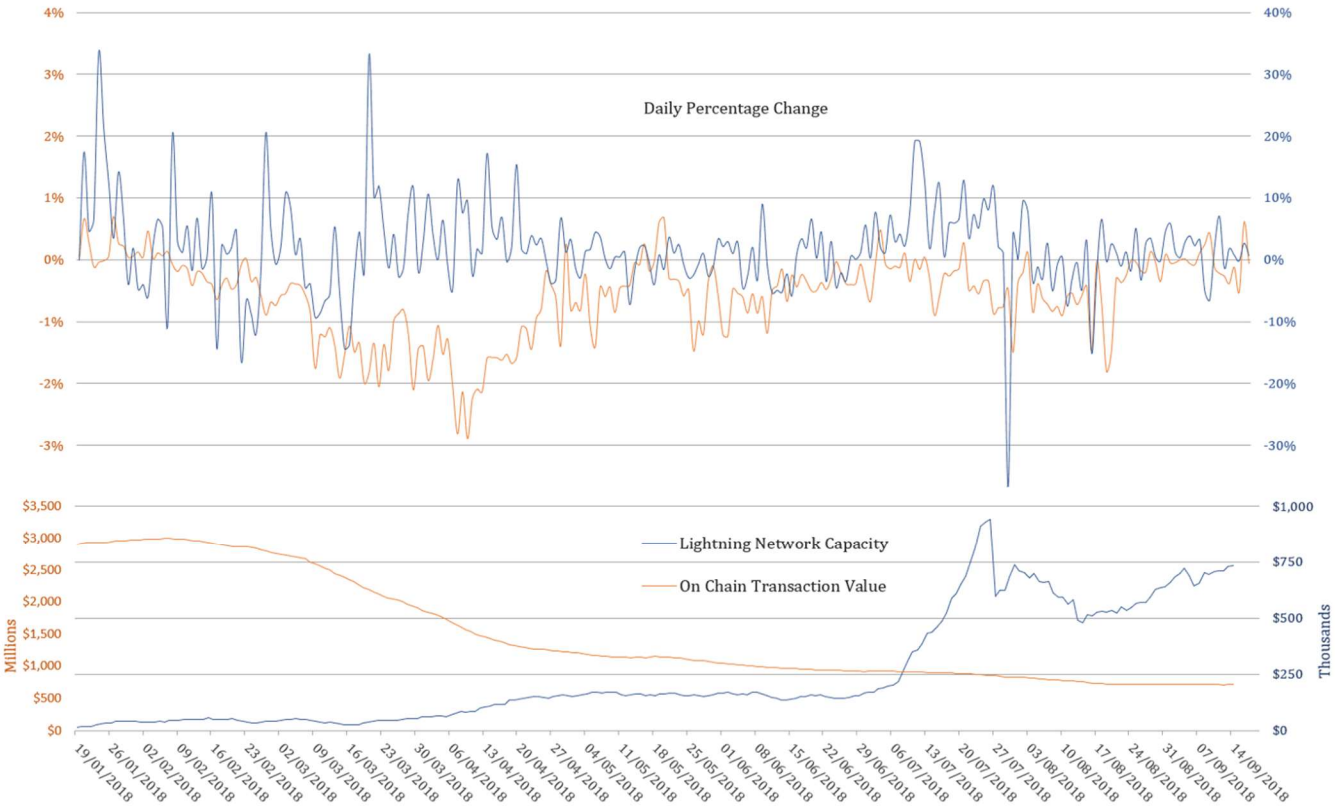
If one is to expect an **oversold condition**, close to an **NVT Signal level of 30**, similar to the **2015 capitulation**, the price would have to drop to c. **$1239**, tomorrow, as would be the case in the coming few weeks.

However, if an **oversold condition** is expected to mirror the **NVT Signal levels of 40,** as was the case in the **first 2017 "capitulation",** the price would "only" have to drop to c. **$1653**.

As for the denominator side of equation, the value transferred over the network has been steadily declining for a while. Furthermore, the fact that a 90 day moving average is used in calculating the NVT Signal & Wookalich Ratio ensures that this trend is not bound to change in the near future.

Another reason that no considerable uptick is to be expected in the on-chain TV is the increasingly adoption of Lighting Network, which, so far, remains an unknown quantity in terms of its measurable effect on the overall TV.

If the large values are transferred by rich investors, speculators and exchanges, which until very recently would have had to be solely settled on-chain, now they have the option and every incentive to make use of the Lightning Network. The "smart money" can afford being smart, thus be managed with competency on the technical part as well.



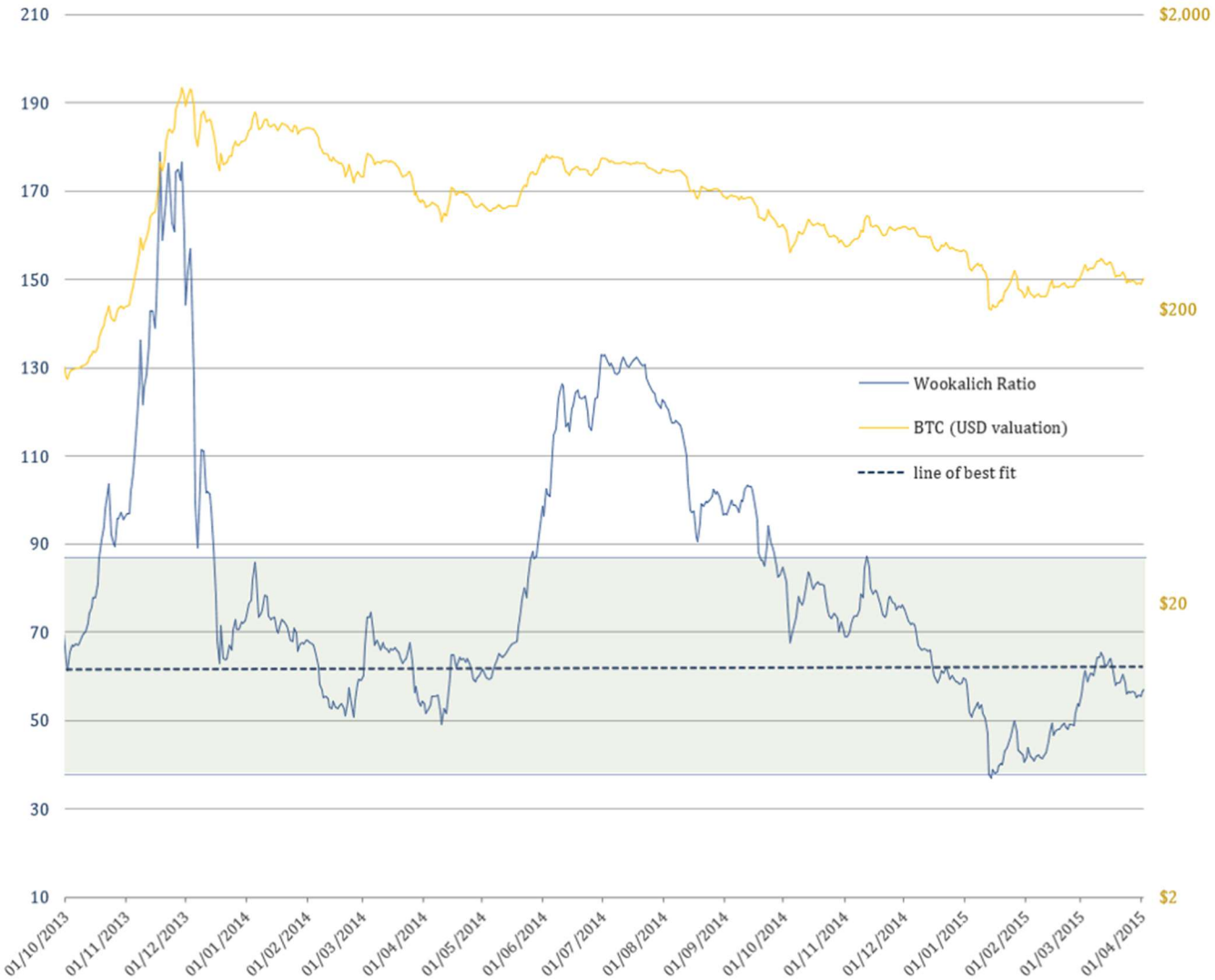
Note: On Chain Transaction Value and it's percentage change refer to the smoothed 90d MA (as the one used in the ratios)

As highlighted in ***Brief Observations and Questions on the Lightning Network's Effect on Bitcoin's NVT Ratio***, the Lightning Network Capacity is continuing to grow

and does correlate with the on-chain TV (using percentage change). This can only be seen as proof that it is very much alive and kicking, mimicking the "on-chain behaviour". Hence it has the potential to serve as proxy in estimating a more inclusive / overall transaction volume.

The Wookalich Ratio despite being "fudged" / normalised, it does not, however, offer any significantly less of a dire / bearish outlook. If one is expecting the metric to go into **"oversold" territory** (e.g. 1 standard deviation below the mean), tomorrow or in the coming weeks, the price would require taking a deep **dive to**c. **$1615**. If we are to assume that **Lightning Network** capacity handles **20%** of the overall value transfer, the same **"oversold" threshold** would be reached at c. **$2918**.

Looking back for clues into a more volatile past



2014 Bear Market

The Wookalich Ratio could, however, signal an “oversold” level in the coming weeks, without a dramatic free fall in price, only if we are to **assume the possibility that the lightning network takes care of approx. half of the overall value transfer**. In this scenario an oversold level would be reached by dropping to a value of c. $4671 as of today.

Looking down a cliff or across the plains in the middle of nowhere?

2018 Bear Market

Conclusion

If the Wookalich or NVT Signal /Ratio are to serve any purpose in the future, a method of quantifying and incorporating the transaction value over the Lightning Network would be essential.

Settling just for the on-chain transaction will increasingly make this metric less relevant, much like trying to assess combustion engines in terms of horsepower and continuing to attempt to match it against that of an actual horse.

The Lightning Network Capacity could serve as a proxy metric in estimating a more inclusive TV. To what extent however, remains to be answered.

Acknowledgements

- **Willy Woo**
- **Dmitry Kalichkin** & Cryptolab Capital

Disclaimer

The content is only to be take as my personal observations and opinions for the purpose to be further considered, answered or discarded, hence this article is far from exhaustive and IS NOT and CANNOT serve as basis for any financial / investment / trading advice.

The Bitcoin Analyst Brain: A Primer

By Christopher Bendiksen

Posted September 19, 2018

The industry is in building mode and I love it. It almost even smells like a giant construction site. I kinda want a Bitcoin hard hat.

Institutions are building too, but they are huge, slow-moving beasts whose motions can seem imperceptible against the fury of the Bitcoin anthill. Don't be fooled though, there is activity happening and their (not to mention their clients') thirst for information is ever growing. Which brings us to the very topic of this post.

One of the next developments we foresee is the initiation and increased frequency of Bitcoin coverage by financial research desks. This will in turn necessitate the hiring or

re-training of a new wave of Bitcoin analysts to fill these new requirements of skills and knowledge.

That is why we are creating a Bitcoin Analyst series geared at training interested readers and the next wave of budding Bitcoin analysts. Our intention is to help readers "level up" in all the areas that are critical to understanding this emerging digital asset class and the technology on which it is built.

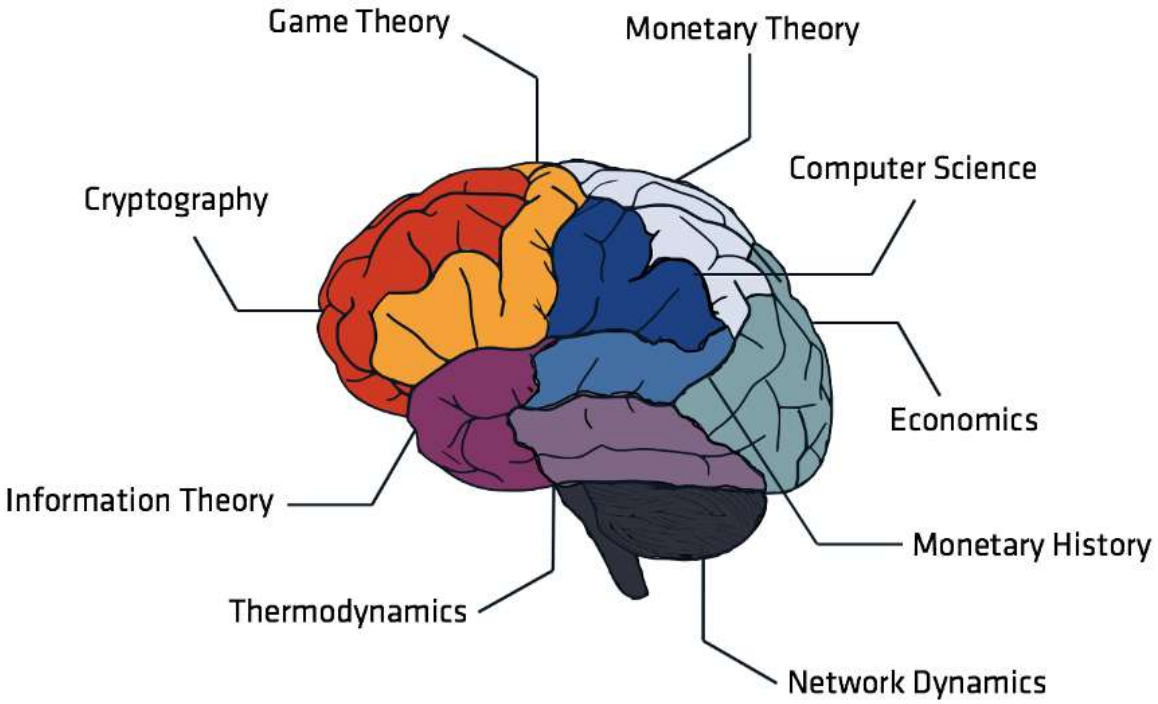
Perhaps you will become one of these new analysts. Or maybe you're just *really* interested in going deep into Bitcoin so you can humble that insufferable blockchain guy at your next dinner party. In any case, finding this article means you're already on the right track. It's a levelling up of sorts in its own right.

But before you get too excited, I feel obliged to let you know that Bitcoin is one of those games where *no one can ever truly complete or "beat" it._It's almost like Chess in that the more you learn, the more there is _to_learn. And if you ever hear anyone claiming to be a Bitcoin (or worse, _blockchain*) expert, turn your scam sensors to eleven. The real experts never claim to be such, because as soon as you actually start getting deep into Bitcoin, it immediately dawns on you *just how little you actually know*.

Over the next few months, I will do my best to guide readers towards the appropriate skills, knowledge and resources needed to succeed in our business through a series of articles. The goal is not to teach you everything, I wouldn't know how, but to point you in the right directions for applying your own efforts without wasting too much time on the way. I will also be hosting interactive events in London and Stockholm

(and NYC if the demand is there) where we'll cover selected Bitcoin topics in more detail. But I digress..

The Bitcoin Analyst Brain



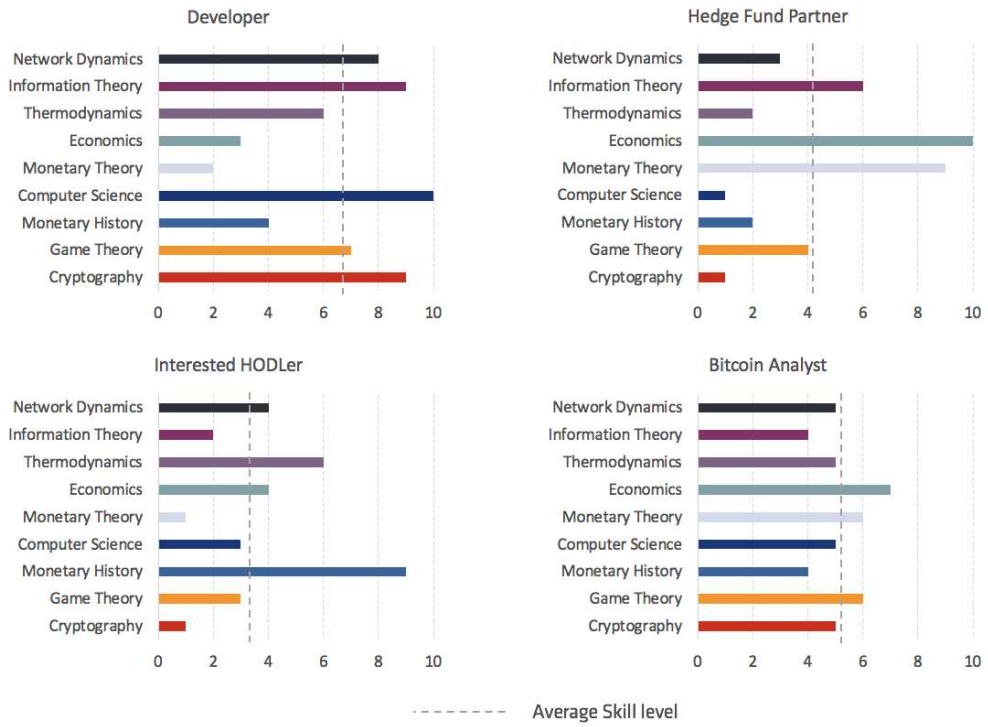
This is a brain. I used to work with them but they weren't complicated enough so I got into Bitcoin instead.

Behold the Bitcoin Analyst brain in all its phrenological glory. It precisely maps nine important (but non-exhaustive) fields of Bitcoin knowledge to their exact corresponding neurological structures in a colourful and approachable manner while simultaneously illustrating the diverse domains of knowledge required to understand and analyse Bitcoin.

This anatomical masterpiece demonstrates how a successful Bitcoin analyst must be competent across a wide array of topics. Full-blown specialisation is no longer really feasible, or even desirable, particularly as a first-wave analyst (though specialisation may well become more sought-after in time). At least at the moment, Bitcoin analysis is a game reserved for women and men with certain renaissance-like inclinations.

I am not aware of any single person worldwide who can be considered an expert in all of these domains. While such persons might conceivably exist, it is also not necessary to be one in order to understand Bitcoin and add value to those in need of thorough, insightful analysis.

To illustrate further, allow me to pick a few perceived archetypes in the Bitcoin community; heavily prejudice them based on my own jaded perceptions; shamelessly reduce their perceived faculties to our nine colourful metrics; and finally, chart out what their skill distributions might look like:



Just so we're clear, I made all these numbers up. As far as I know they do not actually represent any real person(s).

It is your overall score that will serve you as a Bitcoin analyst, not whether you are a world-class specialist in a single domain or not. As you can see, there is really no right or wrong domain to attack in order to increase your overall skill level, some will suit you well, others you will find more difficult.

Work first on the ones that come easy, this way you can trigger that amazing feeling of increasing mastery, but do not shun from the ones that are hard, if your neglect them they will end up limiting your ability to fully grasp the whole picture.

Think about it this way: You can be a strong developer without knowing much about economics, but it's tough to be on the development side without expertise in computer science. Similarly, you can have a deep understanding of the economics and monetary theory behind Bitcoin's success without having to know your way around an elliptical curve.

But working towards being a Bitcoin analyst is probably best served by adapting a generalist approach. It is not sufficient to be a world-class cryptographer, nor is it

necessary. Your job will be to break down a complicated large-picture phenomenon into more easily digestible components. That necessitates broad knowledge, or you might risk missing significant pieces of the puzzle, jeopardising your entire analysis.

The Next Level

We will kick this series into full gear in our next post where we look at the current state of Bitcoin analysis output; who is doing it right and how you can learn from them; some historic parallels to coverage initiation of emerging industries; and thoughts on how this might play out in the Bitcoin space.

Until then, you should continue reading about Bitcoin and learning as much as you possibly can. I was going to compile the best introductory resources on Bitcoin as an addendum to this piece, but to my express delight, Nima Tabatabai already made an excellent one, published only a couple weeks ago. There's no need to re-invent the wheel here so I refer you to his work instead.

Read his introduction, follow him on Twitter, and in addition to ***all*** his other recommendations, add the following handles on Twitter and Medium:

Twitter:

@danheld, @StopAndDecrypt, @giacomozucco, @LaurentMT, @cburniske, @therealSherwinD, @aantonop, @TraceMayer, @MustStopMurad, @BitMexResearch, @twobitidiot, @jlppfeffer, and @nic__carter.

Medium:

Andreas M. Antonopoulos, StopAndDecrypt, Nic Carter, John Pfeffer, LaurentMT, Murad Mahmudov, Ryan Selkis, Dan Held, Giacomo Zucco, Sherwin Dowlat, Chris Burniske, and Trace Mayer

These lists are nowhere near complete and I'll add more recommendations as we go along, but starting with too many voices in the room can be confusing so let's leave it at these for now. Know that what these people write is *the real deal.* Don't take my word for it though—thoroughly examine their work and try to punch holes in their arguments (they are obviously not *always* right about everything).

Before I end this piece, though, I want to repeat one of Nema's points, as it is probably the best single piece of advice I can offer at this moment of your journey:

I cannot stress enough how important it is that you follow his suggestion and **stop reading the news** *. It is almost entirely worthless and will teach you little to nothing about Bitcoin. In fact, it is virtually certain that* **they will teach you a bunch of incorrect stuff** *which you will painstakingly have to un-learn later, costing you valuable learning time.*

So... drop out of the mainstream media, get on Twitter and Medium, and enjoy the journey as your Bitcoin knowledge grows.

And that's another level up. See you at the next checkpoint.

Disclaimer

Please note that this Blog Post is provided on the basis that the recipient accepts the following conditions relating to the provision of the same (including on behalf of their respective organisation).

This Blog Post does not contain or purport to be, financial promotion(s) of any kind.

This Blog Post does not contain reference to any of the investment products or services currently offered by members of the CoinShares Group.

Digital assets and related technologies can be extremely complicated. The digital sector has spawned concepts and nomenclature much of which is novel and can be difficult for even technically savvy individuals to thoroughly comprehend. The sector also evolves rapidly.

With increasing media attention on digital assets and related technologies, many of the concepts associated therewith (and the terms used to encapsulate them) are more likely to be encountered outside of the digital space. Although a term may become relatively well-known and in a relatively short timeframe, there is a danger that misunderstandings and misconceptions can take root relating to precisely what the concept behind the given term is.

The purpose of this Blog Post is to provide objective, educational and interesting commentary. This Blog Post is not directed at any particular person or group of persons. Although produced with reasonable care and skill, no representation should be taken as having been given that this Blog Post is an exhaustive analysis of all of the considerations which its subject matter may give rise to. This Blog Post fairly represents the opinions and sentiments of its author at the date of publishing but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and the blog post may not necessarily be updated to reflect the same.

Nothing within this Blog Post constitutes investment, legal, tax or other advice. This Blog Post should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, 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.

Bitcoin as a Store of Value

A note on Bitcoin's SoV characteristics

By JP Thor

Posted September 22, 2018

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

F. A. Hayek, 1984

Bitcoin innovates from the edges

In a coral reef the most diversity, life and evolution happens at the edges, whilst the centre, the most stagnant and least exposed to external change, dies the first. This may seem counter-intuitive as the centre receives the most protection from the marine environment; but in reality it's because it *is* protected and thus receives critical environmental information the last. The edges flourish in evolution, diversity and resilience.

The greatest innovation and disruption in industries so too will happen at the "edges" where the disrupter is continually exposed to attack vectors, must be resilient, adaptable to change and intrinsically diverse. The greatest innovation in money, arguably one of the most important aspects of society, will happen from the edges. And it's Bitcoin. Legacy money will die obliviously in the "centre", whilst Bitcoin seeps in at an accelerating rate from all sides.

This blog is a quick look at Bitcoin Store of Value (SoV) characteristics, some comparisons to other cryptocurrencies and how Bitcoin will continue to "seep in from the edges".

Stored Value

For almost a year now BTC has maintained a value higher than $5000 a unit, and for 18 months higher than $1000 a unit. Going deeper we can see that Bitcoin is actually a store of *energy*, as it consumes electricity in the most efficient manner possible via the actions of self-interested profit-seeking mining operators. As Bitcoin is created from coinbase rewards that can only be performed by miners, the value of that Bitcoin is invariably related to the amount of work that was performed in creating the Bitcoin, which requires energy expenditure. The combination of mathematically defined supply and proof-of-work is the strongest case of Bitcoin's SoV argument.

A naive counter-argument to this is arguing that digging a hole in the ground takes a lot of energy, but the hole is not valued by anyone except the digger, so the hole has no market price and was a worthless exercise and waste of energy.

However, if there can only be 10 holes dug in a common courtyard, and only 1 dug at each time, *and* the holes are permanent forever, *and* everyone can own part of the hole as a hole-coin, *and* everyone can access the hole-coin in a permissionless way, *and* everyone can transport their hole-coin anywhere and transact with it, *and* everyone recognises it, then it becomes much different. This in fact bears close resemblance to the Rai Stones of Yap; where proof-of-work was captured in large, carved and immovable limestone rocks as value.

Another perspective is that a $100 hole-coin cannot possibly retain $100 in value if it only cost $0.10 to make. The closer the marginal cost of production of a hole-coin to the market value of that coin, then the more it is likely to retain that value.

The Bitcoin Cycle of Life

Bitcoin is secure -> because miners spend a lot of time and money mining for it -> because Bitcoin is valuable -> because people acquire and hold it as an asset -> because Bitcoin is secure -> ...

A fundamental difference between Proof-of-Work and Proof-of-Stake is that PoW involves an indiscriminate sunk-cost for every coin. Miners will spend energy that can never be recovered directly during the mining process. PoS has almost negligible sunk cost, therefore the value behind each minted coin does not accumulate cost, and is unlikely to retain value.

Valuable assets become ossified

An asset must retain SoV characteristics before it can become a Medium of Exchange—the latter can not be achieved prior to the former as people will store money as *money* prior to making a purchase decision. This is part of the [double coincidence of wants] problem; where people need to desire the same common thing in order to make a transaction. If a transaction is made with a money that is not desired by one party, they will immediately transact out of it. Thus people need to want money in the first place, as opposed to storing value in other asset classes, and if that money does not retain value then it will not work.

This is where I think Vitalik is fundamentally wrong about Ethereum's SoV characteristics; highlighted in a recent tweet:

If Ethereum is a useable, decentralised and censorship-resistant world computer, then it will succeed at utility. This is correct, but since Ethereum is open-source; then there is nothing stopping a different team forking away Ethereum with more useable, decentralised or censorship-resistant features, and developers moving to that platform.

In fact, Ethereum developers are currently asking their community to do exactly that.

Bitcoin on the other hand has some characteristics that can never be forked away:

- an anonymous founder
- 9.5 years of a single chain, always backwards compatible
- 5 years as a $1bn+ asset class

The most important characteristics of Bitcoin make it the most convincing as a SoV. Bitcoin is what it is because its main virtue is that it *does not change* and is becoming ossified. One can still validate all blocks to today using the same software client Satoshi released almost 10 years ago.

Other cryptocurrencies on the other hand do not have this; and in fact regularly schedule in hard forks making change a cornerstone of their protocols. Let alone the presence of founders and CEOs.

If Bitcoin were to fail (it recently almost could have) then all cryptocurrencies will fail, and the entire notion that value can be stored digitally will go down with it. We have one chance to make this work.

From the Edges

Every day a new hodler of last resort enters the ecosystem, and every day the timer to the last minted Bitcoin ticks down. Every day another Bitcoin is irreversibly lost, and every day another attack vector is countered and fails. Bitcoin is innovating from the edges and the old money at the centre will never see it in time. Growth will happen in waves, and each time will advance upon the centre faster.

I've been part of two Satoshi cycles; the first in 2013 and the second in 2017. The next Satoshi cycle IMO will occur sometime around the next halvening in 2020; a scenario very clearly described by LaurentMT and most likely brought on by large institutional money. The final cycle will probably occur four years later in 2024, set off by the entry of sovereign countries adding Bitcoin to their balance sheets.

Why would they do this? For many reasons including checking out of the US-controlled monetary economy, resetting all their debt to zero, avoiding hyper-inflation of their own currencies, gaining a large surplus of Bitcoin before their own purchasing power goes to zero, countering trade wars and economic oppression, etc

Most strikingly to me is that everyone's debt goes to zero at the same time as we transition to a sound-money global economy with a single currency with no single person, company or country in charge; the Bitcoin Standard. In a perfect storm of self-interest (think prisoner's dilemma), we will rush to exit the monetary mess that the last 60 years has put us in.

Don't be caught in the centre of the reef. Get yourself to the edges and be part of the innovation.

Much can be said on this subject. I highly recommend Saifedean's latest book on The Bitcoin Standard: Saifedean Ammous — The Bitcoin Standard; summary by Craig Jaquish. Also read LaurenMT's series on Bitcoin PoW—a facinating look at PoW efficiency.

Lastly make sure you pre-order a CASA Lightning box; next up will be an article on moving an entire nation's economy to the Lightning Network. ⚡

Tweetstorm: Mass adoption of Bitcoin is inevitable

By Misir Mahmudov

Posted September 25, 2018

- 1/ Mass adoption of Bitcoin is inevitable
- 2/ Bitcoin is first perceived as an internet toy by cypherpunks.
- 3/ Its rapid price increase makes a small group of people rich and brings media attention.
- 4/ The media, the financial and tech establishment (Wall St. and SV), having failed to buy Bitcoin early and capture the growth, denounce it as a Ponzi scheme/bubble/MySpace of blockchain etc.
- 5/ A large number of scammers jump onto the Bitcoin hype-train and create their own cryptocurrencies claiming to be superior though lacking critical qualities including decentralization, security, credibility of monetary policy, immutability, distribution, infrastructure & others
- 6/ The retail, VCs, HFs, lacking understanding of monetary economics and applying inappropriate valuation models, invest into the shams that all other cryptocurrencies are, creating more noise and confusion as the prices of these altcoins increase at a rate higher than Bitcoin.
- 7/ Well connected VCs/HFs are given discounts on the investments only to then dump much of what they bought onto the retail.
- 8/ The world watches as the bear markets continue to wipe out more and more altcoins as these fail to deliver any useful product and constantly show cracks with regards to all crucial properties of a "cryptocurrency".
- 9/ Bitcoin, meanwhile, is able to retain its value best and its price continues to increase steadily in the long run.
- 10/ People, burned in the altcoin craze, witness and learn about Bitcoin's undisputed superiority across all characteristics.
- 11/ On the eve of and during the next bull markets, Bitcoin's unshakable and antifragile record exacerbates the chronic fear of missing out.

- 12/ Hyperinflating fiat currencies are further contributing to the adoption of Bitcoin as it becomes the only means of preserving wealth for many people.
- 13/ Investors and high net-worth individuals are convinced to allocate a portion of their portfolio (1-5%) to Bitcoin to capture further growth, as well as increase Sharpe ratio of their traditional portfolios.
- 14/ Such speculation facilitates a 'speculative attack' on ""stable"" fiat currencies as the increase in demand for Bitcoin necessarily involves a reduction in demand for fiat currency causing higher expected fiat inflation (see @pierre_rochard Speculative Attack article).
- 15/ Central banks, in an attempt to adapt to the new conditions, start to accumulate Bitcoin (somewhat similar to gold today) causing the price to increase more and "legitimize" Bitcoin even further.
- 16/ Bitcoin's market capitalization is now in the tens of trillions. One of the greatest monetary wealth transfers in human history has occurred. Most of the investors are reaping large profits and are willing to part with some of their Bitcoin to pay for their purchases.
- 17/ Bitcoin's volatility subsides as both the market cap and the liquidity are larger than ever.
- 18/ More and more people demand to be paid in Bitcoin now that it has proven to be a good store of value given its disinflationary (later deflationary) nature.
- 19/ Bitcoin's use as a medium of exchange becomes a widespread practice.
- 20/ Bitcoin is now also increasingly used as a unit of account.
- 21/ Due to the emergence of a superior, uninflatable, new monetary standard, people increasingly store their wealth in Bitcoin rather than fiat currencies. Central banks' power is reduced and previous local monopolies on money are described by historians as a relic of the past.

A Modest Privacy Protection Proposal

How to reclaim your privacy in the surveillance age

By Jameson Lopp

Posted September 29, 2018

Photo: Bernard Hermant/Unsplash

It's hard to retain much privacy in the information age—the internet has a nearly perfect limitless memory and we're placing a ton of sensitive data onto it. After being swatted in 2017, I set out on a mission to start my life over with a renewed focus on privacy. While I was motivated by changes in the Bitcoin ecosystem (an increased rate of physical attacks), this guide is meant to be comprehensive for people living in the USA and generally helpful for other citizens of the world. The journey has been long and arduous because there simply aren't many resources out there for how to achieve what I wanted.

Why protect privacy?

You may be thinking "I'm not doing anything wrong—why should I be concerned about privacy?" It's important to over-invest in privacy because once it's lost, it's really challenging to recover. Consider this: you may not be a target right now—but you may become one in the future as your wealth increases, you endorse unpopular political or religious perspectives or... you make a single post on social media in poor judgment.

In December 2013, Justine Sacco, a woman with 170 Twitter followers, posted a very bad joke as she was boarding a plane. Sacco slept during her 11-hour plane trip and woke up to find out that she was the number-one Twitter topic worldwide, with celebrities and bloggers all over the globe denouncing her and encouraging all their followers to do the same. Sacco's employer, New York internet firm IAC, declared that she had lost her job as director of corporate communications. At least one Twitter user showed up at the Cape Town airport to photograph her arrival. Point being: In the Information Age, it doesn't take much for you to attract the ire of millions of people.

If an unforeseen event such as this happens to you, do you really want to have to move to a new address for safety? It turns out there's no one-size-fits all solution to this problem—it has to be customized to suit each person's needs and be appropriate for the jurisdiction in which you reside. With that said, I'll cover high-level privacy threat vectors and as many of the details as possible for mitigating them in this post.

Privacy goals

It's important to note the goal of this guide: It's not "how to completely disappear." If you want perfect privacy, then just close all of your online accounts and move to the middle of nowhere. Rather, my goal is to show you how to achieve the best possible privacy while still retaining your existing reputation.

Also, some of the following are specific to your jurisdiction. Most privacy guides are written for Americans because they are under more attacks with frivolous lawsuits, tracked by more private investigators, targeted for more asset seizures, and jailed for more homeland security charges than any other country.

There are four major levels of privacy protection:

1. Protection against the average person who knows how to search the web
2. Protection against someone with resources to hire a cheap private investigator
3. Protection against someone willing to indefinitely fund a top-tier private investigator
4. Protection against agents of nation states with nearly unlimited funds

Most folks are concerned about none of these potential attackers, while some may only be interested in protection against the first level. I can only speak about the first few levels; if you want to hide from governments you'll have to search elsewhere.

Pricing people out of privacy

Before we begin, I want to be clear that many of the techniques come at a cost. I had to fill out hundreds of pages of paperwork, spend around $30,000 in legal/banking/service fees, and endure a four-month process in order to achieve my goals. I estimate annual recurring costs of over $15,000 for my extreme setup. I had to speak to half a dozen attorneys before I found one that was even comfortable helping me. Once I did have an attorney, this made it easier for me to work with bankers because they were more assured that my intentions were legal and I wasn't trying to cover up criminal activity.

And it's not just about money—the amount of time and effort required even to perform the financially "cheap" aspects of this guide are sufficient to turn most people off from attempting them. If you're willing to dedicate a weekend and a couple hundred dollars, you should at least be able to substantially improve your online privacy, which will put you in the top one percent of internet users.

Again, everyone should customize their privacy plan according to their individual needs and resources. Some of the below suggestions are moderate in nature, while others require far more commitment. Learn about them, anyway. The truth is, surveillance has become the norm. Most people are willing to sacrifice privacy in return for convenience, and swimming against the tide makes for a challenging journey.

My primary takeaway after countless hours of research is that we give a lot of personal information to many different merchants and service providers that are vulnerable to hacking and social engineering. You should assume that over a long enough period of time, any data you give to third parties will be made public—whether or not it happens intentionally is irrelevant. The general solution to many of these data leaks is to use proxies of all kinds: electronic, legal, and human. Let's dive into specifics.

Mitigating real-time location tracking

The best thing you can do is stop carrying around a portable surveillance device (mobile phone), but they're so darn convenient! At the very least, though, you can disable location history whenever possible such as with Google-based services. You should turn off GPS on your phone, though apps may still be able to get rough location data via cell triangulation. Though you may not even want to trust that the tracking is actually turned off. It's probably best not to log into Google services using an account that can be tied to your real identity. Consider creating a throwaway account for mobile use. More details on protecting your phone are in the next section.

A much harder threat to defend against is the rise of CCTV with facial recognition, tattoo recognition, and even gait recognition. You can opt-out of some facial recognition with online services such as Facebook and Google, but not others such as Amazon and Apple. And of course, who knows if that data may still be getting resold and used elsewhere, even if you opt out? Since walking around with a mask is often illegal or will draw unwanted attention, it seems that there is no great solution to CCTV at the moment. The optimal solution would be some sort of wearable device that blinds cameras, though all of the incarnations thus far emit infrared and are only capable of blinding infrared nighttime surveillance cameras that don't have IR filters installed.

You could try a product such as the Justice Cap, though it's only going to work well during low light conditions against cheap cameras that don't have infrared filters. If you do go this route you'll want the highest powered LEDs you can find and if you can get them to pulse, that would likely be even more effective.

Along a similar vein was this privacy visor that emits infrared light in order to defeat facial recognition, though it's probably not a great way to blend into a crowd.

Reflectacles, on the other hand, don't emit IR light—they reflect it. This seems like a more low-key and low-tech solution.

A recent study showed that perhaps going the other way will work well: projecting infrared onto your own face may defeat most facial recognition software. With sophisticated calibration, the researcher showed that you could even fool face detection software to get false positives and effectively make it think you are a specific person.

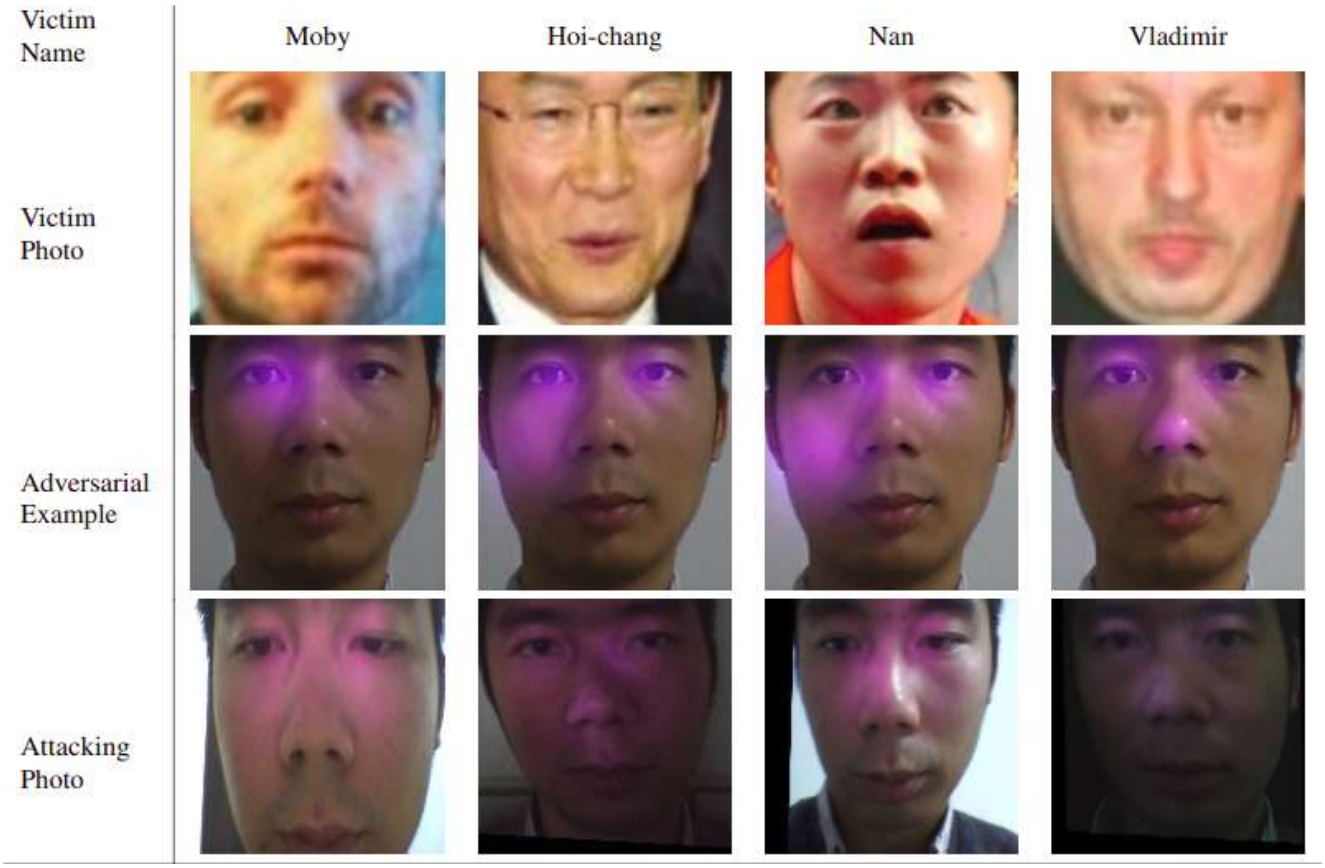


Image: Zhe Zhou, Di Tang, Xiaofeng Wang, Weili Han, Xiangyu Lui, and Kehuan Zhang/Fudan University via arXiv

You can also try wearing a photorealistic mask. However, note that in some jurisdictions it's illegal to wear a mask in public. And you'll once again just end up attracting attention from other members of the public.

The most practical solution seems to be low tech: wear a hat with a large brim such as a baseball cap, along with large dark or mirrored sunglasses that cover a significant portion of your face.

Failing all else, you can always go Juggalo...

Protect your phone

Many services require you to provide a phone number when you sign up and they may even validate that you control it by sending a unique code via SMS. If you don't want to give away information such as your phone provider or area code, you should buy a virtual phone number that forwards to your real phone number. You could use a service like Tossable Digits, though they only accept credit card payments so you'd need to use a prepaid card or virtual credit card to retain your privacy. For even

stronger privacy, consider using a service that accepts cryptocurrency, such as NumberProxy. Note that virtual phone numbers/proxies may have issues receiving 2FA SMS codes from web services. They also tend to be unable to send and receive group SMS messages.

For maximum privacy, you should only use a prepaid phone service so that they don't know your name. You should assume that every phone service provider not only knows your location (by triangulating cell tower pings) but also resells that information. What they don't know can't be used against you.

It turns out this is harder than you might expect! From my extensive experience watching *The Wire* multiple times, I figured I'd be able to walk into any store selling prepaid phone SIMs, plunk down some cash, and walk out with a burner. Turns out brick and mortar stores like Best Buy will often require ID in order for you to buy a phone plan, even if it's prepaid! I ended up having to go online and buy a SIM with a prepaid plan that I purchased via a prepaid debit card and had delivered to a private mailbox.

At the software level, the operating systems and apps on phones tend to have abysmal privacy. If you want top-notch privacy, your best option at the time of writing is RattlesnakeOS, which is taking the reins from CopperheadOS (no longer maintained). Something to keep an eye out for is Purism's Librem phone, which will hopefully be released in 2019.

Protect your residence

In order to achieve privacy that will protect you from a variety of attacks upon your home, you need to break any ties between your name and your residence. To be clear, you must consider your current location compromised—these techniques only work if they are used on a residence that has never been tied to your identity. This means either having official documents listed in someone else's name or in the name of a legal entity that can't be linked to you.

In the U.S. there are a few states with especially strong privacy protection for Limited Liability Corporations—New Mexico, Nevada, and Wyoming. You can read one comparison of legal differences here and another here. To get an idea of a high-end privacy protection setup, check out the "Ultra Asset Protection Package" from Wyoming Corporate Services:

The Ultra Asset Protection Trust Package provides bullet-proof asset protection. This package includes a 1,000 year Wyoming Spendthrift Trust wrapped with three LLC's, gives you a physical presence in Wyoming with a phone line for the trustee, and two hours of time with the attorney to draw up the Trust.

Includes:

- **Wyoming 1,000 year Spendthrift Trust designed for your needs by an attorney**
- **Corporate Mail Forwarding and Physical Address Package for Trustee and the Trust**
- **Allows for use of a Wyoming address on the Articles and the State's website**
- **Special Trustee LLC**
- **LLC for the Beneficiary**
- **LLC for the advisor**
- **An Attorney for two hours of consultation**
- **Phone Service answered by computer for Trustee**
- **Plus everything that is included with our Basic Incorporation Package.**

As we can see, more sophisticated setups basically use the "shell company" paradigm to wrap the actual ownership of assets with a variety of legal entity layers that are difficult, if not impossible, to peel away. Once these legal entities are formed, you should use them to purchase / rent / lease property and pay for any services such as utilities and deliveries at your residence.

One helpful thing to keep in mind when setting up new services is to remember that there are plenty of "address-challenged" people who don't have a permanent address because they live in recreational vehicles / live a nomadic lifestyle. There seem to be a lot more of them than people trying to protect their privacy. As such it may be easy to find practical advice by reading forums and websites devoted to nomadic lifestyles. It's also useful when explaining your situation to others. That is, you're less likely to be questioned if you just say "my RV doesn't have a fixed address" than if you say "I'm trying to protect myself from data leaks."

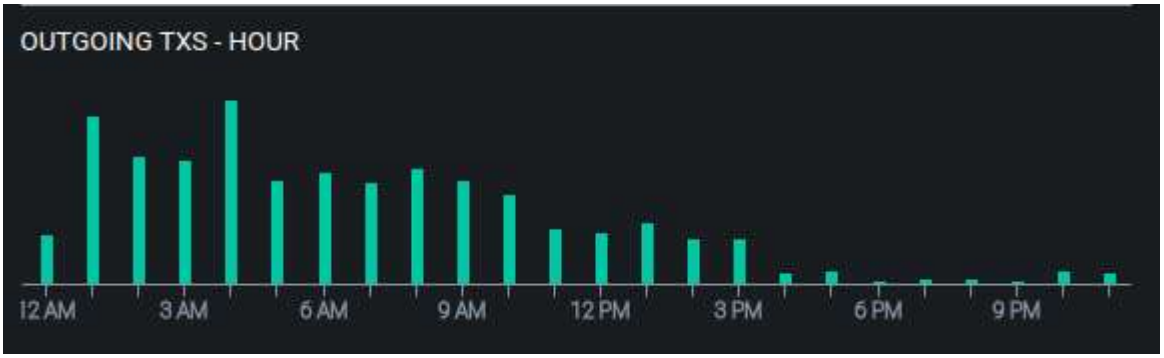
Once you are settled into your new location, you may want to take it to the next level when you are on phone calls or video chats. You'll want to ensure that you don't leak information via ambient noise or visuals. In this case I'd recommend setting up your camera to have a blank wall behind you or just buy a collapsible screen. For noise, place the microphone in a small isolation booth or build one by lining the sides of a

cardboard box with noise absorbing material. For the ultra paranoid, be aware that something as innocent as a storm outside could help attackers to pinpoint your location.

Are you worried about surveillance from laser microphones? If you complete the rest of this guide, hopefully no one can find your residence in the first place—but if you want to be extra safe, consider a noise generator.

Another issue to consider is EXIF data in photos. You shouldn't post photos that you have taken near your physical location as they may very well include embedded GPS coordinates, especially if the photo was taken with a smartphone. The only way to be sure about this is to use an EXIF cleaner (Windows/Mac) or ExifTool (Linux) to scrub metadata before posting such photos online.

Yet another edge case concern is related to your time zone. If you are making public posts that get timestamped then it doesn't take a ton of your post data to narrow down which longitude you're living near via temporal analysis. This may not matter much if you live along a well-populated longitude, but if you're living somewhere more (longitudinally) remote such as Hawaii, New Zealand, or Greenland, it could be a dead giveaway.



Temporal analysis of spends out of 336xGpGweq1wtY4kRTuA4w6d7yDkBU9czU via BitInfoCharts

Above is an example of temporal analysis on a bitcoin address that holds quite a few BTC. The times listed are in GMT and we can see that daily activity begins at 12 a.m. GMT and drops off after 3 p.m. GMT. These times happen to line up with 9 a.m. and midnight, Tokyo time. It turns out that this is the cold wallet for a Japanese exchange called CoinCheck.

This should be obvious, but you shouldn't make public posts about physical businesses because it gives away your location. This includes "checking in" on FourSquare, tagging photos and status updates on Instagram/Facebook/etc, and even posting business reviews on Yelp/Google/Facebook. One caveat is if you do so

for misdirection by making posts about places that aren't near your residence. (More on misdirection later.)

You may think some of the above is overkill, but remember when 4chan found Shia LaBeouf's secret art location in a little more than a day? First, they used planes seen overhead to narrow down via public flight path info, then they used positions of stars to narrow further. The final piece of info that gave it away was when a user drove around the area honking their car horn. Don't underestimate the power of the internet to crowdsource investigations.

Protect your snail mail

You should never receive *any* mail or deliveries in your own name at your address. Little known fact: All mail that goes through the US Postal System gets scanned and put into a database. Is that database secure? Best to assume it's not...

Optimal ($$$): Rent the cheapest apartment you can find just to receive mail. Since it's a "real address" it won't raise any red flags with services to which you give it.

Decent ($$): If you have a good relationship with an attorney, they may be willing to accept mail on your behalf. You can also use a "ghost address" via JJ Luna's contacts.

Decent ($): Buy a virtual address/remailing service. You can even combine several of these together to create a sort of "onion routing" for your physical mail. Each "hop" will only know about the hop before and the hop after it. Some options are EarthClassMail and TravelingMailBox.

Better than nothing ($): Buy a Post Office Box/mailbox in a UPS Store.

Once you have your proxy address(es) set up, you'll want to use them for every service that doesn't require proof of residence. This includes:

- Credit cards
- Domain names
- Bank accounts
- Subscriptions and memberships
- Online services

Protect "real property"

"Real property" is a category of items for which you are taxed on a recurring basis simply for owning, which creates public records, a.k.a. privacy leaks. Most commonly this will be a house, any vehicles you own, though in some jurisdictions it can also cover pets! On a related note, income taxes are not public record, but over 75,000 IRS employees in the US have access to them... they're not *exactly* private.

Once again, you'll need to register these assets under an LLC/legal entity that can't be tied to your identity. For liability and privacy purposes you will likely want separate LLCs to own real estate versus owning vehicles. This is to reduce the number of links to your residence: If an attacker manages to find one of your vehicles and sees that it's owned by "NoName LLC," the first thing they will do is search for all publicly registered property owned by "NoName LLC"—if this same LLC owns your residence, your privacy has been compromised.

Another thing to note with regard to vehicles is that if you don't want your name on the insurance policy, you'll need to get commercial fleet insurance and in my experience, this can be about twice as expensive as personal insurance.

Protect your real name

Since you will inevitably end up interacting with people as you go about your life, you'll want an alias that can't be connected to you. A first name and last name that is common to your area (but not suspiciously common) should suffice, as it will be more forgettable. If you need help thinking of a common name, look up census data from your region. If you're in the US, you can use this name generator service.

It's not like folks are going to be asking for your government ID unless you're purchasing age-restricted goods and services. Just make sure that you keep it simple and consistently use the same pseudonym; otherwise, you're likely to forget which 'nym you gave to which service provider.

Keep a low profile

Another common privacy strategy other than using proxies is to "hide in the crowd." As such, when you're out in public you should strive to be unnoticeable and unmemorable. Don't wear flashy clothes, don't make exotic body modifications, blend in with local styles and customs. Don't drive a rare car, don't make any noticeable exterior modifications such as wheels, stickers, or vanity plates.

Protect your internet privacy

Your ISP, various government agencies, and who knows who else may be monitoring your internet traffic.

Many popular web services are chock full of various tracking software, much of which is simply trying to correlate your internet browser with your interests in order to better target advertising at you.

You'll also want to protect yourself from various online activity trackers such as advertisers and social networks. I recommend installing these browser extensions:

- Privacy Badger
- uBlock Origin
- HTTPS Everywhere

You can also provide protection for all devices on your network including smart TVs and mobile apps by configuring your router to use a local DNS server that is running Pi-hole. It will block any network requests for known advertisers and trackers.

While you're at it, change the default search engine for your browsers to be one that is pro-privacy.

You should also switch to a pro-privacy email service. Similar to choosing a VPN, there's no clear "best" provider. There's a good comparison guide here.

If you want to take it to the extreme, consider quitting the use of all Google services. There's a great guide here:

How I Fully Quit Google (And You Can, Too) *My enlightening quest to break free of a tech giant* medium.com

You can secure a decent amount of your web browsing from snooping third parties by installing browser extensions, but it's not foolproof—the aforementioned entities can still see which domains / IP addresses you're visiting, even though they can't peer into the data packets that are going back and forth.

VPNs are quite important for protecting your internet privacy. When you're at home they prevent the websites and other online services from knowing your real IP address, and thus your geographic location. When you're not at home and using WiFi access points operated by untrustworthy third parties, it prevents them from snooping on your traffic. It's really hard to decide on the best VPN, because there are many factors at play, so I'll leave you to research that. There's a great guide here.

What I definitely recommend is setting up your home network to automatically use your VPN—you can accomplish this by buying a router that has a built-in VPN client. By having the VPN configured at the router level, any device that connects to your router will automatically be protected by your VPN without requiring configuration on the device itself. There's a lot of good info here.

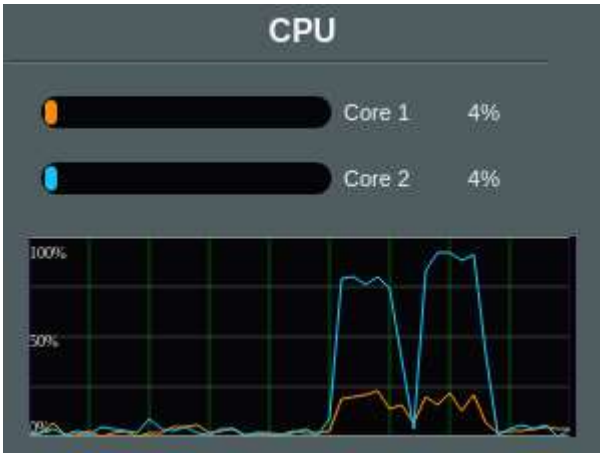
I'm a fan of the AsusWRT Merlin firmware which provides a lot of additional functionality on top of the stock ASUS firmware, including more complex routing policies. By using the Merlin firmware you can specify certain devices (like video streamers) to not use the VPN and you can configure a kill switch with just a few

minutes of tinkering. After running VPNs at the router level for several months I noticed that, from time to time, the VPN connections would fail. If you don't have a kill switch enabled, you won't know if your VPN fails until perhaps you notice that you aren't getting as many CAPTCHAs as usual when logging into web apps. A kill switch is a must so that you instantly know when you are no longer protected by a VPN.

Also note that you won't be able to put video streaming services behind a router that is configured to send ALL traffic through a VPN; they'll lock out your account because they assume you are trying to bypass regional content restrictions. The solutions to this are to either use one with firmware that supports selective routing as linked above (and create an exclusion rule for streaming devices) or to use a two-router setup that's chained from your modem (where the first router is) for non-VPN devices, and the second router for VPN devices. If you're not a networking expert, you may need a hand from a geeky friend to help set that up.

You can purchase some VPNs anonymously with a throwaway email account and cryptocurrency. For next-level purchase privacy here, note that any bitcoin-accepting VPN provider can be purchased with monero via xmr.to.

Using a router with VPN support is the most user-friendly way to protect all of your devices, but it comes at a cost. The CPU(s) on the router will likely become your bottleneck with regard to bandwidth. In my testing with a top of the line multi-CPU router, it wasn't possible to achieve over 50 Mbit/S speeds due to the CPUs maxing out while performing the encryption and decryption operations.



First spike: maxing out downstream at 43 Mb/S. Second spike: maxing out upstream at 48 Mb/S. Screenshot: Jameson Lopp

A downside here is that if you have a very fast ISP that's over 50 Mb/S, an off-the-shelf consumer router, even a high-end one with multiple processors, is going to be bottlenecked by its CPU. If this bottleneck is a concern for you then you'll need to

invest more effort into building a Linux-based router on beefier hardware. Here's a good guide, though you'd want to invest more than $50 in the hardware.

The above is great for your at-home devices, though note that you'll also want to configure VPNs manually on your mobile devices that are going to leave your home network from time to time. In my experience, VPNs that support OpenVPN are the easiest to configure on various devices.

Finally, you'll want to make this setup more robust. Routing all of your traffic through one server creates a single point of failure, and sometimes a VPN server can get overwhelmed and become unresponsive for a lengthy period of time. What to do? Configure *multiple* active VPN connections! The tricky part that took a fair amount of research was how to do this in a way so that the kill switch doesn't activate if any of the servers go down, which would make your setup even *less* robust.

For AsusWRT Merlin firmware, the answer is explained in this forum post. TL;DR: you should define four or five VPN clients, set them all to start on boot, but only enable the kill switch on the last VPN client. That way, if any of them fail the routing rules for a lower priority client will kick in, while if the last VPN client fails AND all of the other clients have failed, the kill switch will activate and block all traffic.

A note on DNS leaks—if you're protecting all of your traffic with VPN tunnels then it ought to also be making DNS queries through the VPN. However, if you aren't protecting all of your devices with VPNs then consider running a Pi-Hole DNS server on your home network. It will block DNS queries to advertising domains and reduce your overall query volume by caching results. You can configure the upstream DNS server that it uses to be a pro-privacy server such as Cloudflare's 1.1.1.1.

Protect your PC

In order to prevent data leaks due to malware, install covers over your webcams. I'm a fan of the magnetic SpiShutter for MacBooks, otherwise you can just buy a simple adhesive sliding shutter.

At the software level, you can take back some control of what various processes in your computer are accessing by running a firewall such as Little Snitch. You can also run antispyware apps such as Micro Snitch, which will alert you when processes try to access your microphone or camera. If you want the best privacy and security, you really shouldn't run OS X or Windows, but rather a privacy-focused flavor of Linux.

If you're at Edward Snowden-levels of paranoia then you'll want to break out the soldering kit and physically remove the hardware connections for cameras and microphones. As Edward states, this is a "pain in the ass."

If you're a Linux nerd and you want extreme privacy without destroying your hardware, buy a Librem laptop. They run on open source hardware with hardware switches to enable/disable the webcam/microphone and the wifi/Bluetooth. It also runs a stripped-down version of Debian with no proprietary closed source software packages.

Protect online accounts

This is good advice for anyone in general, but you should do what you can to keep unwanted intruders out of your online accounts—*especially* your email account. The average person uses the same password or three across all of their online services and they just memorize them. This is a single point of failure and when a single one of those services suffers a data breach, you can be sure that your username and password will be sold on the black market and fed into bots that try to use them to log into every popular online service. You've probably already been "pwned" and don't even know it.

This means using a good password manager such as LastPass/1Password/KeePass to generate strong random unique passwords for every online service you use and to add second-factor authentication to every online account that supports it. While you're at it, protect your password manager with a hardware 2FA device such as a Yubikey, Trezor, or Ledger.

The prior listed password managers are convenient and reasonably secure, though they put your privacy in the hands of a third party. They also have design flaws that can potentially expose your entire password database to malware. The ultimate security and privacy (but less convenient) password managers let you control your own data and use a hardware token for decryption. Lance Vick, lead security engineer at BitGo, has a great guide here.

Pay special attention to your email account—most people only have a single email address that likely has a ton of sensitive information in it, and if an attacker gains control of your email account they can probably use it to reset passwords to most of your other online accounts. This is a single point of failure; consider using different email accounts for different purposes, and protect them with hardware 2FA.

Protect communication channels

Any email, phone call, or text message you send can be intercepted because they're sent across public networks without being encrypted. Trying to fix email with PGP encryption is pretty much a lost cause; consider using a secure email such as Cisco's Registered Envelope Service. You can pretty easily improve phone call and text message security by buying a burner phone and using end-to-end encrypted apps

such as Signal, Whatsapp, and Telegram on it. You can use other services such as Send Safely to transfer larger documents.

For the ultra privacy conscious it's worth noting that Signal, Whatsapp, and Telegram are all closed, centralized walled gardens that can still sell your metadata even though they can't read the content of your messages. Signal and Whatsapp require a phone number, making it much more work for you to have a private account. They can find out who you are talking to and when you are talking to them. More private but slightly less user-friendly alternatives are decentralized open communications systems like Riot, XMPP with OTR, and IRC with OTR.

Protect your financial data

Most mainstream financial services are highly insecure and have poor privacy. You can protect those services using standard online account strategies as mentioned earlier—strong passwords and hardware 2FA. And certainly don't input your real address with any of those providers.

Credit reporting agencies have created huge targets by centralizing tons of sensitive information, thus they get hacked from time to time, resulting in rampant identity theft.

Many Americans are familiar with "the big three" credit bureaus, but it turns out that there are quite a few more!

You should freeze your credit reports; this will prevent anyone from requesting a copy and potentially finding sensitive data. Here are links to freeze your credit report for major providers in the U.S.:

- TransUnion
- Equifax
- Experian
- Innovis
- SageStream
- Advanced Resolution Services
- Clarity Services
- CoreLogic

I also recommend submitting forms to opt out of as many data brokerages as possible—you can find an extensive list here.

You should also stop using normal credit cards except perhaps while traveling—more details on that in the next section.

Protect your purchases

Cash is still the king of financial privacy, though it's less convenient than plastic and downright unusable for online purchases. Another downside I've encountered recently is that it is becoming more common for merchants to not be able to provide sufficient change. I can only assume this is because far fewer customers are using cash.

A more convenient and still highly private option is to carry prepaid debit/gift cards you purchased with cash. The next best privacy option is to use a debit/credit card in the name of your LLC. Make sure it doesn't have your real name or address on it; the billing address should be the billing address of your LLC (the address of the registered agent or of a private mailbox). This can be tricky because card providers tend to require a real name on every card they issue. I don't have a specific solution I can share here other than to recommend making some banker friends who will work the system on your behalf.

Virtual disposable credit cards are great for privacy and security. You can limit your attack surface by giving unique card details to each merchant and setting spend limits on each card.

Entropay

- Up to 10 virtual prepaid Visa cards at a time
- Some fees apply

MyCard2Go

- Prepaid physical Visa card
- Limited to €100 without identity verification
- Some fees apply

Netspend

- Create virtual prepaid Visa cards or Mastercards
- Some fees apply

Privacy

- Create unlimited virtual Visa cards
- Supports custom card spending policies
- Must provide checking account details
- Free

SpectroCard

- Create virtual or plastic prepaid Mastercards
- Some fees apply

TangoCard

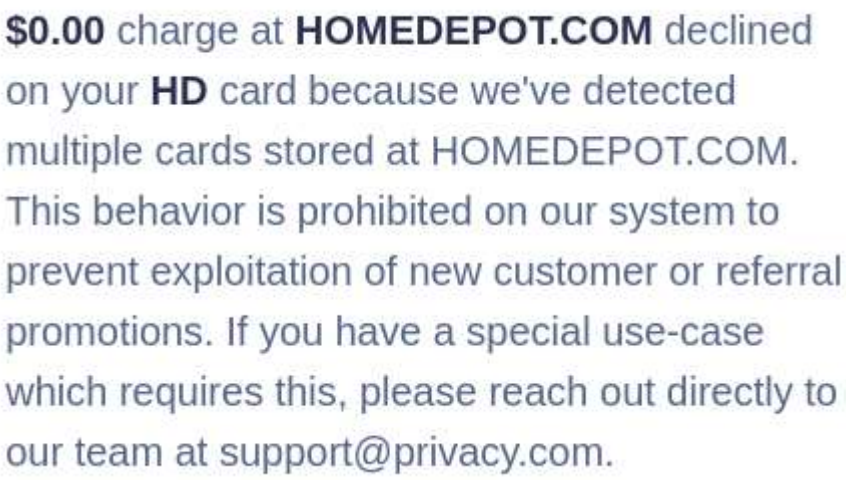
- Create virtual gift cards for participating merchants
- Free

For folks with a U.S. bank account, the most convenient option seems to be Privacy.com. However, by default, they will ask for the login info to your online checking account. For the best privacy, you should ask them to enable your account via ACH integration to ensure that they can't read all of your bank account's activity.

Note: What Privacy.com doesn't tell you is that there are global limits for maximum daily/monthly usage. I'm not sure what the defaults are, but the daily limit seems to default to less than $2,000. If you email support, they'll increase your limits, though your limit will depend upon your usage history.

Also note that you may encounter issues with single-use Privacy.com virtual cards. It turns out this is because a number of merchants actually make multiple charges to your card. Often this is because they make a pre-authorization charge at the time of sale, then cancel it and make the real charge upon shipping the product. I've also run into issues with merchants such as Home Depot where they have multiple delivery services (local vs. shipping carriers) and they make separate card charges for each one even if you created a single order. Also, some services may not accept these virtual cards at all because they get identified as prepaid cards and some merchants consider those to be too risky to process.

Also worth noting is that Privacy.com has a policy against creating multiple cards for the same company, which isn't clear when you're setting up your account. This can result in charges being declined on the Privacy.com end.



Screenshot: Jameson Lopp

Finally, if you want even stronger privacy, you can create what equates to a double proxy on your purchases by creating a Privacy.com account that is linked to your LLC bank account. Note that Privacy.com likely won't approve your account immediately because it's geared toward personal checking accounts, but it should be reviewed and approved within a few days of signing up.

Protect your driver's license data

This one is tricky because DMVs in the U.S. must comply with the REAL ID Act, which requires proof of residence. Generally, this means showing bills or financial statements that are mailed to your residence. Of course, if you've followed the above procedures then you shouldn't be receiving any mail at your residence that has your name on it! And unfortunately, commercial remailing addresses (such as the private mailbox services discussed earlier) are kept in databases and you will often be prevented from using them for anything requiring a residential address.

In terms of threat models, the average person probably can't access the DMV data to see what address is on your driver's license, but licensed private investigators have access to tools that often do have this data. There are also likely thousands of government employees who can access this data, and countless incidents of abuse have been cataloged over the years. And in fact, many states make tens of millions of dollars a year by selling DMV records to third parties. Thus it's important to decide what you need protection against—if you think that someone may go to the trouble of hiring a PI to track you down, you should consider going to the effort of protecting your driver's license.

As mentioned previously, you may find some helpful information on RV forums. It seems like many nomads find a friend nearby to use their address as a registered residence. Of course, this requires that you trust the person with your mail and that

there are no issues with their address being associated with your name—you don't want to make your friends a target!

I can't offer specific advice here because it varies from jurisdiction to jurisdiction, but there should be alternative forms that you can submit in order to provide certification of your residence address. This was an area where I needed help from an attorney. If you have sufficient resources then you should consider renting a cheap apartment that you use as your official residence, but don't actually spend much time there.

Regardless of what you end up doing with your driver's license, you should consider having a "passport card" issued if your country offers them. You can carry this card around and use it as proof of identity without exposing your physical address, as your address is not listed on your U.S. passport.

Traveling and crossing borders

If you drive a car, there's a high likelihood that cameras will capture your license plates, scan them, and connect them to your identity. There are various products you can buy to help obscure the plate from cameras, though it's unclear how effective they are.

This is another data leak that you can somewhat protect against by only registering vehicles to an anonymous LLC. For the ultra paranoid, note that many newer vehicles come with built-in GPS tracking in the form of a service such as OnStar. You may wish to take extra steps to disable this hardware or simply not purchase a vehicle equipped with it.

If you want to take vehicle privacy to the extreme, one option may be to not own one at all. This is easy in high-density urban environments, though nearly impossible in rural areas. If you're in a semi-densely populated area then you can create accounts with ridesharing services that are registered with your anonymous LLCs and use them to order cars as needed.

When you cross the borders of nation-states, you are subject to extremely high levels of scrutiny. There are two schools of thought for protecting your privacy here:

1. Carry your data with you, encrypted at rest A. Pro: convenience B. Con: no plausible deniability
2. Carry no data, just fresh unencrypted devices A. Pro: border agents can have access and find nothing B. Con: must transfer the data by other means

If you don't want to cross borders with data then you can ship an encrypted drive to your destination ahead of time, or you can take a snapshot of your hard drive and

upload an encrypted disk image that you download upon reaching your destination. Another option is to keep data on an always-running computer at your home that you then download your files from via SFTP/SCP/a more user-friendly tool such as Syncthing. Or you can just run your "real" computer on a private server somewhere and use your laptop as a thin client, using protocols such as RDP and SSH to remote into the server.

Johnathan Corgan wrote a tool to create fully encrypted live boot Ubuntu images with custom content. It outputs ISO images you can either burn to DVD or make a bootable USB stick out of. You can also run the images in a virtual machine.

For international travelers, you have probably noticed the installation of automated border control machines that scan your passport and take your photo. You probably don't have much choice but to use them when entering a country for which you are not a citizen, but if you are entering your own country you should be able to opt out and avoid having your photo taken.

When traveling you will probably end up staying at hotels. If it's known that you will be in a certain city (such as for a conference) then you should protect yourself from being found at a specific hotel by using a pseudonym. This used to be a lot easier because you could give any name you wanted to a hotel and pay with cash. But these days most hotels are going to want ID and a credit card. JJ Luna recommends that you get around this issue by adding an "authorized user" to one of your existing credit cards in the name of your desired pseudonym. You can make the reservation and payment in that name, and while you will give your real ID to the concierge at check-in, they generally don't care if it matches the reservation. This is a common thing for authors, actors, and musicians—if you are questioned then just state that the reservation is under your professional name rather than your legal name because your credit card was issued under your professional name.

Voting

Registering to vote is high risk (it creates a public record).

Crime

Obviously, you shouldn't commit crime; if you get caught it's going to create a set of very public records. However, there's a flip side: becoming a *victim* of crime can have a similar negative impact upon your privacy due to the public records that are created by the justice system! Good opsec means being aware of the company you keep and staying out of sketchy situations that could cause you to become collateral damage. It also means that if you witness something that makes you call for

emergency responders, you should consider doing so from a burner phone and not leaving any identifying information.

Protect your family

This one's tough. The larger the size of your family that's living at your residence, the larger the attack surface on your privacy. Anyone who can be tied to you needs to have the same level of privacy protection—your privacy is only as strong as the weakest link.

Marriage: This creates a public record and ties you to someone. As far as I'm aware there is no requirement for a county-issued marriage license—that form of registration is voluntary. Given that weddings tend to be fairly public events, you should probably get married in a location other than where you reside.

Children: Create birth records, health records, and school records. The school records are difficult to work around; the best options seem to be either homeschooling or private school, which are both expensive in different ways.

Stretch goal: Leave false trails

If you have the resources to do so, consider using misdirection as another tactic. If someone is hunting you down, they probably have limited resources. By purposefully leaking incorrect data, you can leave trails of breadcrumbs that lead to dead ends and frustrate folks who are trying to penetrate your privacy shield.

How might you do this?

- Choose a location that is plausible you may be moving to.
- Tell friends and acquaintances who are never going to actually visit you that this location is where you're moving.
- Change your location data on social media profiles to say you're there.
- Set up cheap accounts in that area that may show up on public reports.

No one has unlimited time; most attackers will give up after spending a certain amount of resources and failing to find you.

Data cleanup and protection

Depending upon your jurisdiction you may have different options available to you to ask for personally identifiable information to be removed from various services. Though depending upon your desired level of protection this may be a waste of time—once data has been leaked you can never be SURE that it is deleted.

If you take the most extreme route of burning your old life and starting anew then you shouldn't bother with data removal, because leaving your old data out there can serve as misdirection/false trails.

Limitations

You're not going to be able to hide from government agents by using these tactics—there will be a legal trail of breadcrumbs. Also, given the pervasiveness of networked surveillance cameras this day in age, you can't completely avoid the eyes of Big Brother in urban environments. It's safe to assume that various entities are sucking up these data streams and applying various facial/tattoo/gait recognition algorithms to them.

One weak point certainly becomes the third parties with which you are communicating. There were several points along the way when clueless folks with whom I was interacting leaked data that could be used to correlate the entities I formed with my identity; I plugged the ones that I could and just have to hope that the others went unnoticed. In order to protect against this, don't even open the possibility for someone who is helping you set up a new service to screw up and correlate the new service with your identity. Don't give them your real email address or your real phone number.

You also have to be very careful about reviewing what your service providers are doing. I had several points at which I had to direct a service provider to stop what they were doing. For example, I had a banker send me an authorization form to issue a credit card for my LLC that had my real name on it as the cardholder. That would have been a massive privacy leak to the credit card provider and every merchant with whom I interacted, as they'd now be able to make the association between the LLC and myself.

Stress-test your setup

The only way to be sure that you have achieved the level of privacy that you desire is to hire experts to try to break through the shields you have erected. Find an experienced private investigator or two and ask them to dig into your life. At this point it will come down to how much digging you are willing to pay for, which you should decide based upon how motivated you expect your attackers may be.

An experienced PI should start by doing various database searches, trying to find trails you may have left behind. If this initial search fails to find any leaks, you may wish to take it a step further and ask them to try to socially engineer your friends and family to see if any of them could be tricked into leaking information about you.

Are you an expert in this field? Can you find holes in my proposal? Can you help me improve my privacy? If so, send an email to opsec@lopp.net and let's chat.

Educational resources

The following are some educational resources that I used to jump start my research that were not linked in the main body of this guide:

- Jolly Roger's Security Guide for Beginners
- How to Disappear
- How to Protect Your Financial Privacy and Keep Your Accounts Secure
- JJ Luna — International Privacy Consultant
- Intel Techniques by Michael Bazzell
- How to Vanish

Disclaimer:

THANK YOU, CREATORS.

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 members of the any specific business, that means any business I am associated with. Bitcoin, shitcoins, and related technologies can be volatile, Don't fuck around with this stuff because you might get burned.

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.

This Blog Post fairly represents the opinions and sentiments of its author at the date of publishing but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and the blog post may not necessarily be updated to reflect the same.

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.

DYOR | BTFD | HOLD