CRYPTO WORDS

CY18 February

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

Contents

Goals and Scope 2
Support Crypto Words 3
Excited for Schnorr signatures 4
Rethinking Network Value to Transactions (NVT) Ratio 7
Bitcoin turning into a multi layered system is the most interesting thing in crypto in 2018 14
The Anatomy of Proof-of-Work 18
Crypto Innovation Spotlight: Schnorr Signatures 21
Disclaimer: 25

Goals and Scope

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

History

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

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

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

Support Crypto Words

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

Send Bitcoin | tippin.me | Send CashApp | Send PayPal

Spread the word

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

Follow us on social media

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

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

Twitter

Subscribe to our newsletter

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

Our pledge

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

Subscribe

Excited for Schnorr signatures

By Murch

Posted February 3, 2018

If you're keeping a finger on the pulse of Bitcoin development, you've probably already heard about Schnorr signatures and you probably won't find much new here. You might rather want to check out Pieter Wuille's recent talk at BPASE18, or Bryan Bishop's compilation of transcripts of Schnorr signature talks whom this article heavily leans on.

Bitcoin signatures are created using the Elliptic Curve Digital Signing Algorithm (ECDSA). Schnorr signatures are another form of digital signatures. The signatures are based on the same security assumptions as ECDSA and are compatible with the elliptic curve Bitcoin already uses (secp256k1). This means that Schnorr signatures can be created with the same private keys and are compatible with currently used key derivation schemes.

Schnorr signatures are smaller

ECDSA signatures vary in size, but almost all come in at a length of 72 or 71 bytes. A small portion will turn out smaller with a theoretical minimum of 8 bytes. [h/t Greg Maxwell]

Schnorr signatures are more efficient and compact than ECDSA signatures. The maximum length of each signature is 64 bytes. [via Harding] Bitcoin blocks include thousands of signatures, and I estimate from the top of my head that signatures make up more than a third of the blockchain data. Simply by being more compact, Schnorr signatures would reduce the blockchain data footprint by a few percent.

Schnorr signatures allow for compact multi-signature…

The multi-signature scheme in Bitcoin is straightforward but naïve. You first list the set of public keys of the authorized signers, and then provide a sufficient count of signatures by the former. E.g., in a 2-of-3 multi-signature transaction input, three public keys and two signatures are provided.

Schnorr signatures have a neat mathematical property that allows multiple signatures to be combined into a single signature. The combined signature has the size of a single signature, but provides the authorization of the original separate signatures.

This allows for a more compact multi-signature scheme, where you only list the authorized public keys and provide a single signature. This is even more efficient for bigger multi-signature transactions. For example, a 3-of-15 and a 10-of-15 transaction input could now have the same weight (if you don't care who signed).

…and aggregated signatures across a whole transaction!

While multi-signature transactions make up a solid portion of the blockspace, the real breakthrough is that signatures can be aggregated across multiple inputs of a transaction. Instead of providing one (or multiple signatures) for each input, a transaction with Schnorr signatures can have **a single signature for all inputs**.

For example at BitGo, we use 2-of-3 multi-signature transactions. Every transaction input therefore has two signatures. As we're seeing low fee rates on the network, some of our customers have started consolidating funds from low-value UTXO. With the current signature scheme, a 2-of-3 multi-sig transaction with 200 inputs would need 400 signatures or about 28.5 kB of signature data. With Schnorr signatures the same transaction could be signed with a single 64-byte Schnorr signature.

In his talk at BPASE18, Pieter Wuille estimated that purely from aggregating signatures for each transaction and leaving everything else the same, the Bitcoin blockchain would be between 25% and 30% smaller.

Scriptless Scripts, and… various black crypto magic

There is some interesting work by Andrew Poelstra lately which he calls "Scriptless Scripts" (see e.g. his talk at Real World Crypto 2018). The idea is that you can express conditions in a smart contract by requiring certain signatures to be provided for the payout. By means of the above mentioned signature aggregation, this could be used to compactly encode smart contracts. The terms of the contract would be hidden from other users and only transparent to its participants, yet enforced by the whole Bitcoin network.

You may have heard about the recent cross-chain atomic swaps. The basic idea is that two payments on two different blockchains are linked in a way that they either both go through or neither. This can be used to decentrally trade cryptocurrencies. Hereby, the traders first lock up funds in shared addresses on both chains, and then create two interdependent transactions. The second transaction depends on a hash preimage that is revealed by the first transaction. Either party can back out and wait for the lock to expire to reclaim their funds, but when the first transaction is executed, the other transaction becomes immediately valid.

By means of the same property that allows for the signature aggregation, all of the above cross-chain atomic swap can be expressed in a single Schnorr signature indistinguishable from a regular spending transaction.

A BIP for Schnorr signatures is in the works

The introduction of Schnorr signatures into Bitcoin requires a new OP_CODE for signature verification. Luckily, Segwit gave us versioning for Bitcoin script, so support for Schnorr signatures can be activated with a soft fork. I hear that multiple Bitcoin Improvement Proposals are in the works and forthcoming shortly. *Thanks to Pieter Wuille for review. Edit: Corrected the length of ECDSA DER-encoded signatures.*

Rethinking Network Value to Transactions (NVT) Ratio

Dmitry Kalichkin

Posted February 3, 2018

This is the first post in our series on cryptoasset valuation. Second one is " Rethinking Metcalfe's Law applications to cryptoasset valuation ".

Cryptoasset prices have been quite turbulent in the past few weeks. At times like this it's especially important to look at the fundamental foundations of cryptoasset prices, and quantitative metrics. Today I will share with you one of the main metrics we use in our investing decisions at Cryptolab Capital.

Emerging field of cryptoeconomic ratio analysis

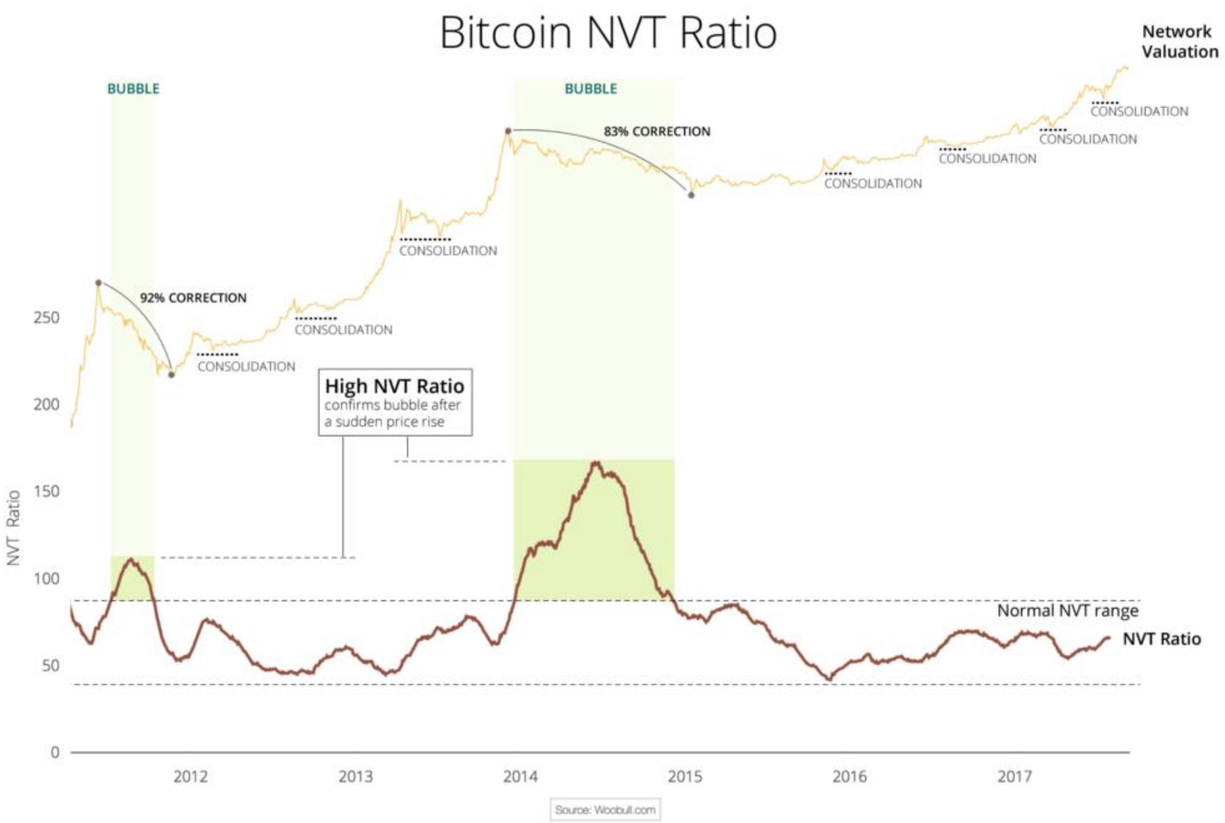
In traditional finance, ratio analysis is one of the most widely used valuation methods. Lacking the detail of other valuation approaches, such as DCF analysis, ratio-based valuation is much faster and is still a good proxy of fair value. It also allows one to easily track asset price dynamic over long periods of time as well as compare different assets to each other.

Over the course of the last year, a new study of cryptoeconomic ratio analysis emerged. The main idea behind this new field is to study the relationship between price of a cryptoasset and its fundamentals. One of the most widely known ratios is **Network Value to Transactions**, or **NVT**. Introduced and popularized by Chris Burniske, Willy Woo, and the team behind Coinmetrics, NVT is often called "crypto PE ratio." Here's the definition of the ratio:

$$NVT = \frac{Network\,Value}{Daily\,Transaction\,Volume}$$

In a traditional PE ratio, the earnings metric in the denominator is used as a proxy for the underlying utility of the company created for the shareholders. While cryptoassets don't have earnings, one can argue that the total value of transactions flowing through the network is a proxy for how much utility users derive from the chain. It is worth highlighting that *Daily Transaction Volume* in NVT takes into account **only on-chain transactions**. All the trading activity that happens on exchanges and is, for the most part, speculative is not included in this volume.

This *Forbes* article argues that NVT can be successfully used to detect bitcoin price bubbles when valuation is not supported by fundamentals and differentiate them from consolidations. The chart below concisely illustrates this argument.



This chart also greatly illustrates what we at Cryptolab Capital don’t like about NVT in its current form. **The spike in NVT follows the bubble with a considerable lag of a few months.**Peak NVT coincides with the middle of a correction period. NVT is neither predictive (doesn’t precede the overvaluation), nor descriptive (doesn’t coincide with it). You can only detect the bubble a few months **after** it bursts.

Rethinking NVT ratio

Trying to dissect this issue and improve this ratio, we started by looking at the ratio definition:

“Ratio has been smoothed using moving averages, 14 day forward and 14 day backward facing…“

Mathematically speaking, this means the following:

$$(2) NVT_{Classic} = 28MA\left(\frac{Daily\ NV}{Daily\ TV}\right)$$

Hereinafter:

- *NVT_Classic* stands for *“Classic definition of NVT”*
- *28 MA_is “ _28-day Moving Average”*
- *NV* is *“ Network Value in USD”*

- *TV* is "*Transaction Volume in USD*"

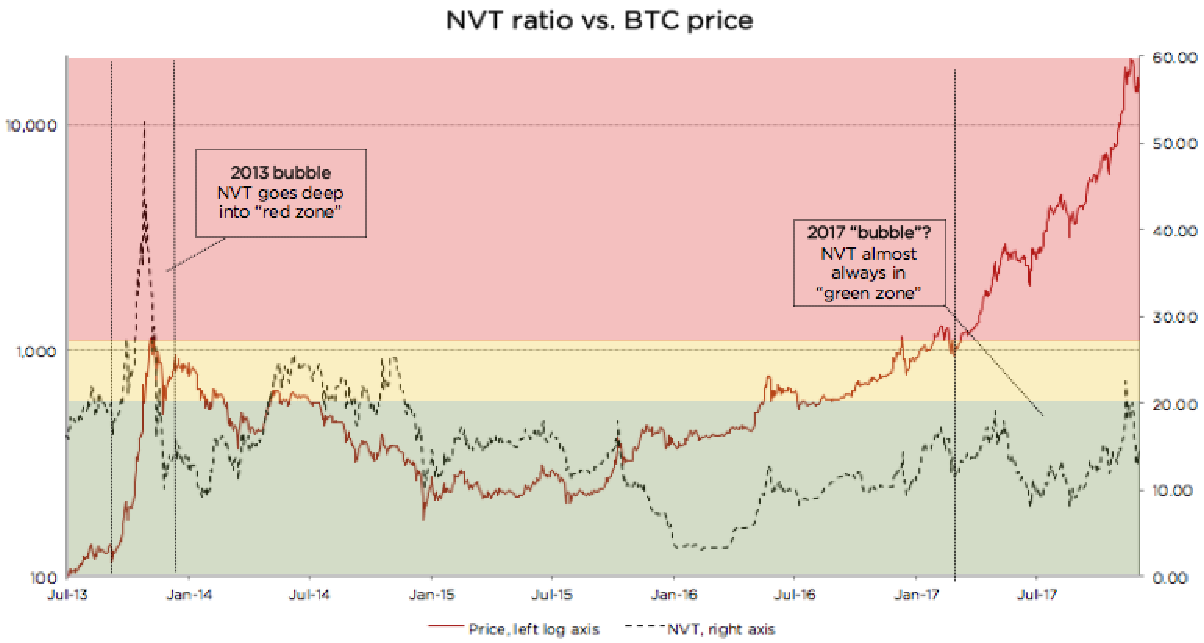
Let's pause here and look back at the conceptual meaning of NVT. In this ratio, *Transaction Volume* is used as a proxy for fundamental network utility value. When you look at *Transaction Volume* on a daily basis, there is a lot of noise, so I completely agree with the decision to smooth it by using a 28-day Moving Average. But we asked ourselves a few questions:

- Why 28 days, and not 10, 30, 90, or 180? A 28-day average might be not enough for a truly fundamental metric.
- Why 14 days forward and backward? If we are trying to develop a predictive, or at least descriptive, indicator we shouldn't rely on future data.
- Do we need to smooth both parameters—ratio as a whole—or just the denominator?

We then experimented with different Moving Average periods, and came to an empiric conclusion that the optimal solution is to **divide daily Network Value by 90 days Moving Average of Transaction Volume**. So here's a definition of our new NVT ratio:

$$NVT_{new} = \frac{Daily\ NV}{90MA\,(Daily\ TV)}$$

Comparing old and new NVT for bitcoin



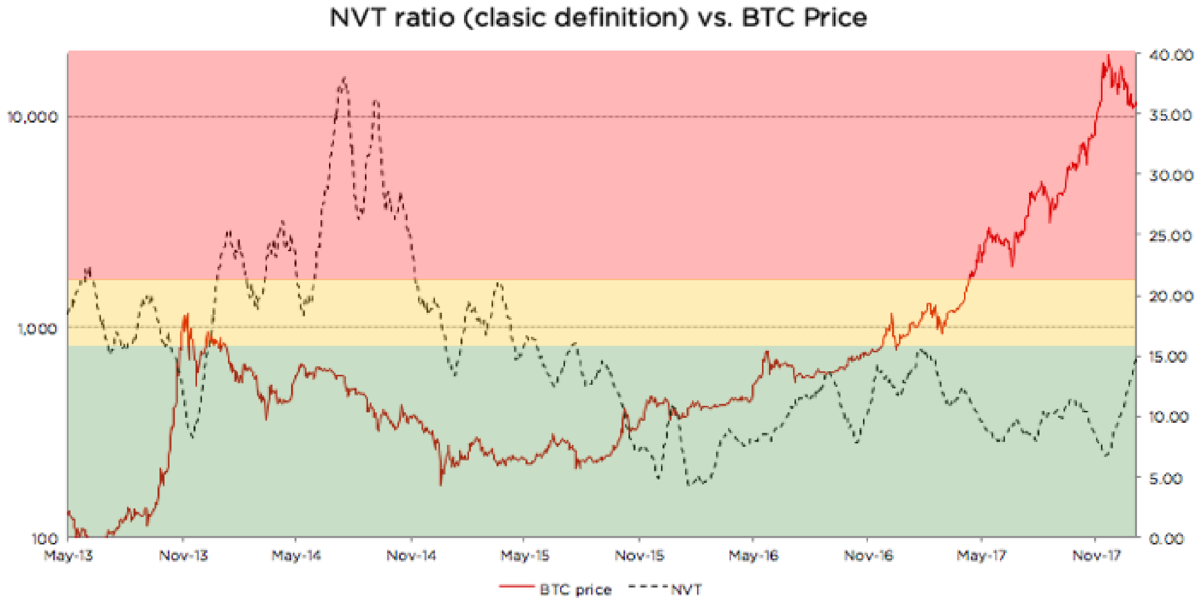
Source: author's calculations

As can be seen from the chart above, when we move from a 28-day Moving Average to a 90-day Moving Average NVT definition, we get rid of the time lag issue described above. We can also see that every time NVT went to the Yellow or Red zone (autumn 2013, spring 2014, December 2017), a price correction followed.

We claim that this refined NVT ratio is a better descriptive metric of bitcoin bubbles. Conceptually, this makes sense. Given that Transaction Volume in NVT is a proxy for fundamental utility value of the network, a 90-day Moving Average is a better proxy for long-term fundamental value than a 28-day Moving Average.

Let's now look at the recent bitcoin price performance using the refined NVT ratio in more detail. From January until mid-December 2017, bitcoin has appreciated almost 20x. For the most part of this rally, though, NVT ratio has stayed in the Green Zone. However, in December when price reached almost $20,000, NVT went into the Yellow for a few days. This rapid appreciation was shortly followed by a 30% price correction, and another even steeper price correction in the last weeks. After the correction, NVT has returned to the Green zone. This is another empiric evidence in support of 90 MA NVT.

Looking at the chart below, it is much harder (if at all possible) to foresee the December 2017 correction. Quite the opposite, during late 2017 price rally, NVT went down! How can it be?



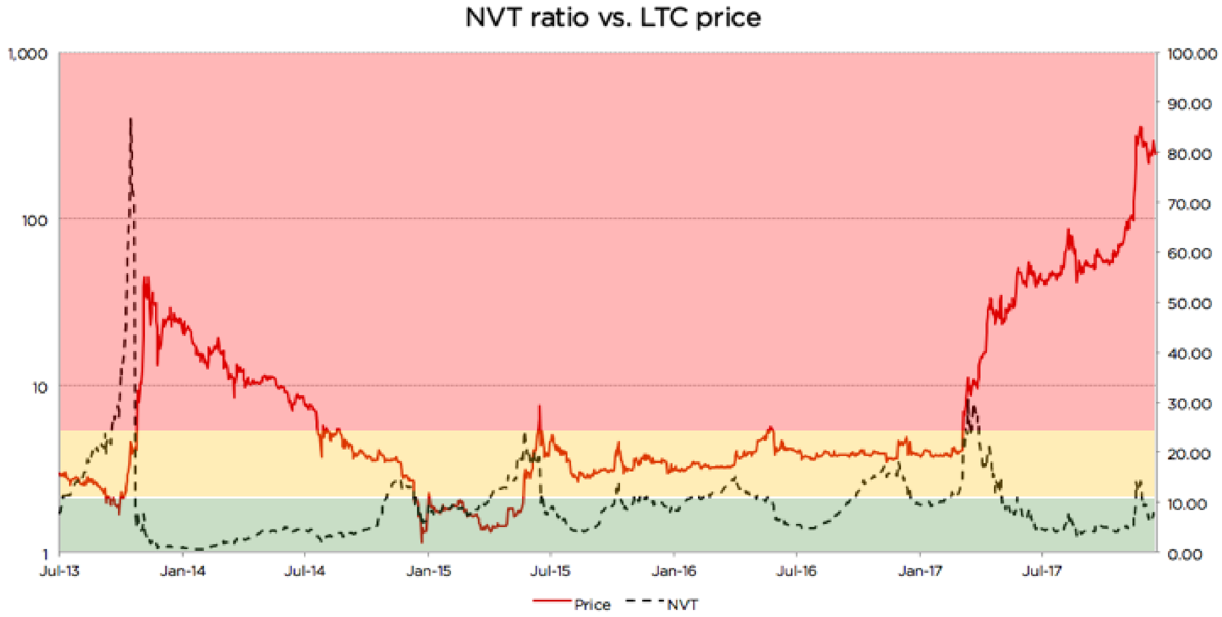
Source: author's calculations

There is a non-static non-linear relationship between the numerator and denominator of NVT. Every time there's a sharp increase in price, there's growth in trading activity (off-chain transactions) that is shortly followed by on-chain transaction volume growth as investors liquidate their positions. Exchanges and wallets trade with each other to provide liquidity to their users. All this activity increases on-chain transaction volume, even though it is fully speculative.

In other words, the cryptoassets exhibit reflexivity. **In the short run, the price changes the fundamentals.** In this case, **transaction volume follows price**. I don't want to go into much detail on this, but I can refer you to an excellent article on the topic by the Coinmetrics team: " *Mean-reversion and reflexivity: a Litecoin case study* ".

So why does a longer period average result in a better indicator? Intuitively it makes sense. By definition, the role of Transaction Volume in the NVT denominator is to be a proxy for fundamental utility that users get from using the network. A longer smoothing period helps to get rid of the reflexivity effects described above—spikes in transaction volume that follow sharp price increase. These irregularities are speculation-driven and are bad descriptors of fundamental intrinsic utility of the network. When we remove these irregularities, we end up with a better proxy for fundamental value in NVT denominator, and, as a result, the new NVT ratio becomes a better descriptor of price level.

Analyzing Litecoin using the refined NVT



Source: author's calculations

Looking at the chart, we can see that there were at least 3 cases since 2013 when the same logic applied: price spikes coincided with, or in some cases were even preceded by, spikes in 90-day NVT

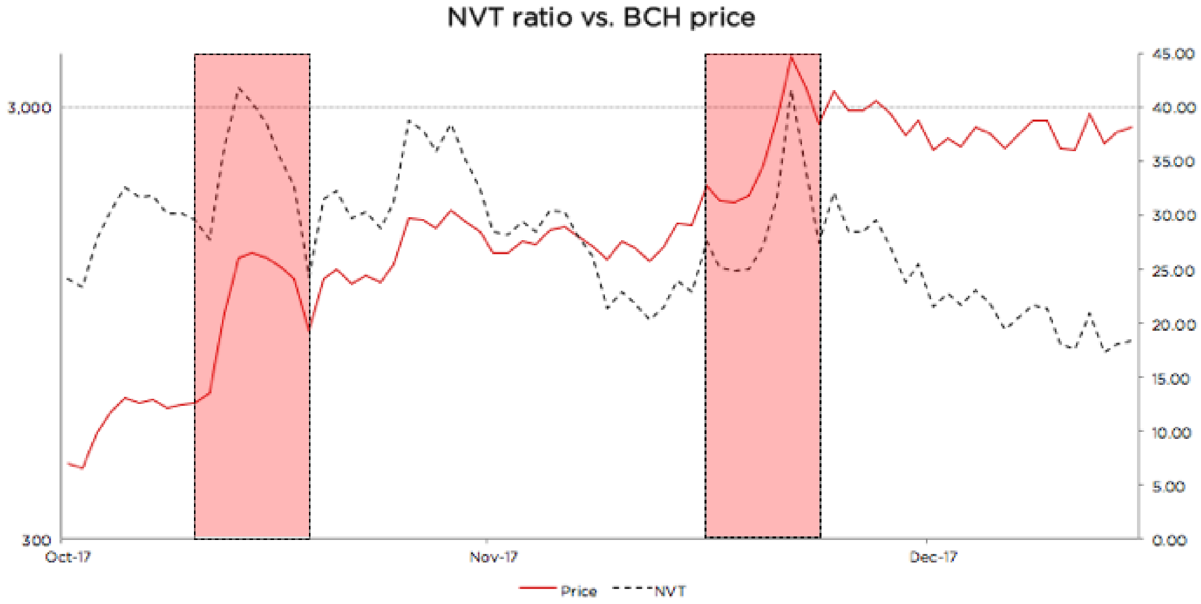
- Autumn 2013
- Summer 2015
- Autumn 2015
- Late 2017

However, in a few cases it didn't work as well. Those cases are usually explained by a strong trend or some big external news:

1. In late 2014, an NVT spike happened during a one-year-long price correction, and the price just kept going down. A similar dynamic can be seen on the BTC graph above during the correction of the second half of 2014. NVT spiked a couple of times while BTC price was steadily declining.
2. Most interestingly, in April 2017 NVT spiked really high, but price actually went up! Here there were a couple of strong external factors: (1) SegWit adoption speculation, and more importantly, (2) listing on Coinbase in May that propelled asset price to a whole new level and moved LTC to another league. The price did increase significantly, but the fundamentals shortly followed.

Despite these exceptions, the descriptive power of the refined NVT for detection of overvaluation is still quite strong. It is definitely stronger than that of the currently used NVT.

Using new NVT for BCash



Source: author's calculations

BCash is quite new, and its history has been full of breaking news, hostile attacks on bitcoin, and other exogenous events. Given this, it is hard for us to define the limits of the Green, Yellow, and Red zones for this currency. If we were forced to state Cryptolab Capital's opinion, we would likely say it is rather overvalued at the moment, the NVT might still be in the Red zone, and the fundamentals have to catch up for the price to make sense.

But one thing that can be seen from the chart above is the sharp NVT spikes coincide perfectly with local price maxima. Yet another win for redefined NVT.

Summary

For every investor it is of crucial importance to understand what is going on in the market right now. As a result of Cryptolab Capital research, we have designed a metric that describes price bubbles well and without a time lag across different time periods and assets.

There is, however, another more fundamental weakness of NVT. **It only takes into account total value of on-chain transactions, but it doesn't factor in the number of transactions or the number of addresses** (wallets) participating in these transactions. Let's call this metric **Daily Active Addresses (DAA)**.

For internet companies, especially marketplaces, social networks, and other businesses with strong network effects, the analogous Daily Active Users (DAU) indicator is one of the most important performance and valuation metrics. This and other metrics that now make up the language of valuing internet companies didn't exist in the 1990s. It has been developed by technology investors over the last 20+ years. Similar valuation framework for cryptoassets is yet to be developed and is only starting to form.

In our next post, we will try to contribute to this framework and propose a way to use Daily Active Addresses (DAA) in cryptoasset network valuation.

Acknowledgements

I wanted to thank a few people who contributed to my understanding of cryptoasset investing, and gave valuable feedback in the process of this research:

- Professor Susan Athey from Stanford
- Professor Christian Catalini at MIT
- Chris Burniske from Placeholder.vc
- Willy Woo

Bitcoin turning into a multi layered system is the most interesting thing in crypto in 2018

By Bèr Kessels

Posted February 2, 2018

When you use Tinder, and you swipe someone, you probably don't sit there thinking "Let's create some TCP packages and send them over IP, hoping they reach the phone of that nice looking fellow there". You probably just think in terms of "lets swipe this nice fellow, Leo"

I'm bringing Tinder into this story to show the power of a layered architecture. You can swipe Leo because the Internet is made out of layers that You, Tinder, your phone, apps, your browser, can use for "free". Disclaimer: I don't actually have a Tinder, so I actually don't know if "swiping" is the right term. But, well, this is a story about Bitcoin.

So, TCP/IP is made up out of four layers: Link layer, Internet Layer, Transport Layer and Application Layer. For this story, only the last two are interesting. On the internet, data is transported in the transport layer. Applications such as your browser, Tinder, your email-client or even the security camera at your front-door, use the transport layer to transport data. The power of this design becomes apparent if you turn it around: Applications don't need to invent, maintain or run their own network, cables, or protocols. They can just tell the Transport layer "Hey, I've got a swipe, for Leo, can you deliver it to the Tinder servers? (so they can send it along to Leo)".

Now, back to Bitcoin. The Bitcoin community is rolling out this thing called "Lightning Network ". It is a layer on top of Bitcoin, in which value can be transported between people (aka "make payments"). It is *one* of the possible layers that can run on top of Bitcoin, but it is the first, and an important one: making payments is one of the most important features of Bitcoin today, so logically that this is the first thing to be moved into an application layer.

This Lightning Network can be used today. Sure, Leo needs to have a Lightning Network enabled client as do you, you might need to compile some stuff, might need to run your own server and so on, but it *is* possible. Today.

Essentially Lightning Network is the birth of an application layer on top of Bitcoin. This might seem uneventful, but the birth of this second layer gives Bitcoin a new purpose: it "degrades" Bitcoin to a mere transport layer for value. This is not some "Pop! And we're done" event, but a long process. Right now, Bitcoin is that transport layer, but is also, still an application layer: you can buy pizza, or buy beekeeping-gear through this transport layer, just fine. So it isn't very layered *yet*.

This new layer is going to be so much better at this “paying” thing, that it will take an important feature “away” from Bitcoin: payments. But, before you get all angry: like with TCP/IP, one can use a layer directly, if you wish. You can just skip the transport layer, and deliver data directly over one of the lower layers, if you insist. You application can skip all the application layer stuff and interact with the transport layer directly, which happens a lot, actually. You’ve probably seen these “Use TCP/IP use UDP”-toggles in some settings of some app. Here an app can bypass, say, HTTP, TCP and so on, and use a much more raw way of delivering. You can still interact with Bitcoin, in order to transfer or manage funds, just fine. It’s just that with this new Application layer, it will become much easier to just use that instead.

If you want to buy takeway, or beekeeping gear, today, both you and the recieving party interact with the Transport layer directly. Tomorrow, we both will interact with an application layer; probably the Lightning Network, to settle that payment instead.

There will be more layers on top of Bitcoin, there will be layers on top of layers on top of layers, but deep down below, Bitcoin is the Layer that ensures value is transferred from you to Leo.

To me, this proves, again, that Bitcoin, as a project, “Gets It”. Bitcoin does not need to be everything: it only needs to be a system to store and transfer value. Nothing more!

It does not need to invent, develop and maintain all the layers, just like Tinder does not need to maintain and invent everything from cables to how-to-get-a-swipe-to-Leo-protocols. Bitcoin needs to be a very secure, very solid, very stable layer to maintain these funds for all the layers on top of it. And Bitcoin is just that.

We should note, though, that a layered architecture was not envisioned by the inventor and early adopters of Bitcoin. They envisioned it more as a monolith: a single piece of software that handles all the possible use-cases and features in itself. At least, that is how I read the whitepaper: no-where was there a mention of “Application layers” or even “layers”.

Second layers can choose different models, use-cases, or different parameters. Lightning Network is complex but also (very) secure. It is decentralised, albeit maybe (time will tell) less so than Bitcoin itself. Other networks might opt for less security. Or even more centralisation. Or tweak other parameters.

If, for example, all you need to register is “I still owe you a beer”, there could very well be a layer that maintains “all the beers owed by everyone” in a central database (or it’s own blockchain) and which registers a daily “state of the beer” on the Bitcoin layer. The possibilities are endless.

A lot of altcoins (or their advocates) did not design a layered system either. So many of these altcoins offer some “feature”, like “speed”, or “programmability”, or “the ability to track bananas" in their core. They often present those built-in features as "the Bitcoin killer", but frankly, most of them have implemented these feature in the wrong place: as core part of their entire system, rather than as additional layers on top of standard value-transport-layers.

When you start looking at Bitcoin as "merely" *a the transport-layer for value*, you might start to see the opportunities for other layers on top. And you might see a missing feature as good design, rather than as a missed opportunity, or as a sign that Bitcoin is doomed.

You don't need "instant transactions, zero-fee" in your transport-layer, you need that in your application layer. So saying that "Ripple is better because it can scale up to Visa-Scale" is nonsense, because you should also mention the trade-off: Ripple has chosen to give away a lot of security maybe even all of it, in order to gain speed. And yes, I'm picking out Ripple because I consider that the biggest scam of the 21st century (closely followed by the Roger Ver Coin, by the way). Also, I'm not saying that it is a zero-sum game: that you can choose either speed or security. But making trade-offs is part of the game. Bitcoin does not make trade-offs if that hurts the decentralisation-property, or if it hurts security.

TCP/IP is not a very efficient system. A lot of resources are spent to ensure your "swipe for Leo" ends up at Leo's phone and not at Marks' phone, or even your current boyfriends phone. In some cases this overhead can be "ridiculous": sometimes far more data is sent around ensuring that your swipe arrives at the right place, than the actual content of, say, the swipe itself. I mean: TCP/IP is brilliant, but it needs a lot of trade-offs to be fault-tolerant, decentralised, secure and stable. Sometimes systems choose different protocols because TCP/IP is just not fast enough: you don't connect your computer-screen over the network to your computer, you use HDMI, or VGA: some other protocol that is much better at delivering pixels to your screen.

Bitcoin's function is similar: it needs to be solid and secure. It must be slow and clunky, if that is what is needed to be solid and secure. It's sole function is to guarantee that your funds are secure, that transactions are valid and that there is no single party that can take over the network or your funds.

As such, Bitcoin does not include a "programming language", like Ethereum does (Note: I actually *do* like Ethereum but for different reasons), because Bitcoin chooses security over "fancy" new features like programming languages. It leaves things like "smart contracts" or "programmability" to another layer. Instead of including it in the base layer. Note, though that such a smart-contract-layer does not (really) exist yet, but nothing fundamental stops it from being rolled out.

Nor does Bitcoin offer very good privacy (compared to e.g. Monero or Dash). But there could very well be an application layer, some alternative to Lightning Network that enhances privacy. So, rather than building it into the base layer, it leaves increased privacy to the application layer.

Bitcoin does not offer an exchange in it's base-layer either (Like e.g. Stellar does). Nor does it offer file-storage, computing power or tracking of Banana's in it's base layer.

By *not* implementing features, by choosing to be conservative, Bitcoin remains the most secure, most solid, and most predictable Transport Layer for transporting value. Ever. Exactly the features you want from such a basic layer.

As a closing note, I'd like to stress that there certainly are altcoin-projects that are completely layered by design. Quite some "cryptocurrency projects" are actually an application layer on top of another transport layer: a vast majority of altcoins are basically tokens on Ethereum: they *are the Application layer* on top of Ethereum! So: I'm not saying that all altcoins are wrong and only Bitcoin get's it right: I'm only offering an alternative way to view Bitcoin: not as a polished, finished, fancy project to be downloaded from the iTunes store, but as a single, technical layer. An important component in a vast and rapidly changing new field: managing value online.

Positive feedback, as well as images of cats, calling me *literally hitler* for hating on your beloved altcoins, or other comments are very welcome at my twitter or on reddit.

The Anatomy of Proof-of-Work

By Hugo Nguyen

February 10, 2018

This is Part 1 of a 5 part series

- **Part 1 - The Anatomy of Proof-of-Work**
- Part 2 - Bitcoin, Chance and Randomness
- Part 3 - How Cryptography Redefines Private Property
- Part 4 - Bitcoin's Incentive Scheme and the Rational Individual
- Part 5 - Bitcoin: Two Parts Math, One Part Biology

Proof-of-Work (PoW) was originally invented as a measure against email spams. Only later it was adapted to be used in digital cash [1].

What PoW mining actually does under the hood, is that it converts kinetic energy (electricity) into a ledger block. A mining machine repeatedly performs hash operations until it solves a cryptographic puzzle. All hash operations are thrown away except for the one hash that solves it.

This one tiny hash, which itself takes very little energy to compute, is a direct representation of the huge ball of energy that was required to produce it. The "proof" that the block was minted. In order to rewrite the block, an attacker later will have to spend a roughly equivalent number of hash operations that was originally required.

Let's say that again: reverting takes an equivalent number of hash operations, not an equivalent amount of energy. That is because the hash is only a representation of the energy used, not the energy itself.

Over time, this representation of energy becomes less & less accurate—as improved hardware becomes more efficient. Energy itself doesn't change, but its old representations "leak".

Another way to visualize this process, is to think of PoW mining as attaching physical weights to virtual blocks. Over time the older blocks get damaged and get lighter & lighter. This also reduces the total weight of the chain, all else being equal.

Bitcoin combats this attrition process by constantly creating new blocks with fresh weights. This ensures that the tip of the chain is always heavy in the present, protecting the integrity of the entire chain. Heavy chain == secure chain.

(Some have suggested that "heaviest chain" is a better terminology than Satoshi's "longest chain." Longest chain can be very misleading when we don't really mean length in the literal sense.)

SHA256 is the hash function that backs Bitcoin PoW mining. SHA256 protects the ledger from being rewritten. One hash in (to mine), one hash out (to revert). This is what gives Bitcoin its immutability property [2].

It's amazing when you think about it. Hash operations dedicate their entire existence to the purpose of securing the ledger! Rarely anything in the real world has 100% dedication & efficiency. (e.g.: contrast that with gasoline & the combustion engine).

In reality, it is probably not 100% but something close to it. Because irreversibility relies on the hashed results being uniformly random (just like when you roll a fair dice), and algorithms can't truly simulate real-world randomness.

Luckily for us, hash functions such as SHA256 have shown to be sufficiently random, aka "pseudorandom". SHA256 has been reviewed & stress-tested for years, and has a rich research literature behind it. So it's not something we have to be too concerned about (yet).

Fundamentally, I believe the idea of "attaching energy" to blocks is the right one & probably the only way to simulate immutability virtually.

Using energy burnt to back a block allows us to view immutability objectively. Whereas any non-energy-based method ultimately requires someone's subjective interpretation of immutability . [3]

By attaching energy to a block, we give it "form", allowing it to have real weight & consequences in the physical world. We can also think of PoW as the magic that brings a bunch of 0s & 1s into life.

In other words, **PoW is the bridge between the digital & the physical**.

Compare that to some cryptokitties that someone creates, modifies & removes as they see fit. Their uniqueness & existence are neither guaranteed nor reliable.

Even if the current variant of PoW fails, I'm confident that there will be other ways of attaching energy to a block.

In conclusion, PoW's application in blockchains might prove to be far more significant & wide reaching than what it was originally invented for. PoW gives us immutability, which gives us uncensorable money, which could potentially change how society organizes itself. (Read Nick Szabo's wonderful essay on **social scalability** for more on that.)

(Original tweetstorm.)

**This is part 1 of the Bitcoin Fundamentals series. Check out the full series here: part 1 , part 2 , part 3 , part 4 , and part 5 .*

[1]: The idea of using PoW in digital cash might have originated from Wei Dai's b-money & Nick Szabo's bitgold proposals in the late 90's. Hal Finney created the first implementation of PoW in digital cash (RPOW) in 2004.

[2]: Immutability is a relative concept. When we say 'immutability' we usually mean it's practically immutable, not absolutely immutable. Even Gold can be synthesized given enough energy.

[3]: One such method is Proof-of-Stake. Read my article on Proof-of-Stake to understand its pitfalls & why it might be inferior to Proof-of-Work.

Crypto Innovation Spotlight: Schnorr Signatures

By Spencer Bogart

Posted February 22, 2018

Amid the commotion and flurry of excitement as crypto surged into mainstream, the significant implications of many real fundamental innovations being developed have been drowned out by the din of hand-wavy, hyperbolic claims. In this_ **_“Crypto Innovation Spotlight”_ *_series, I hope to shine a light on fundamental innovations that are driving our industry forward.***

Schnorr — What is it?

Schnorr is a digital signature algorithm. A digital signature algorithm, among other things, determines the relationship between public keys and private keys (“address” and “password”) — which means the choice has significant implications for security.

In addition, because digital signatures are a significant portion of all the data that comprises a transaction, the choice of digital signature algorithm has significant implications for privacy and efficiency.

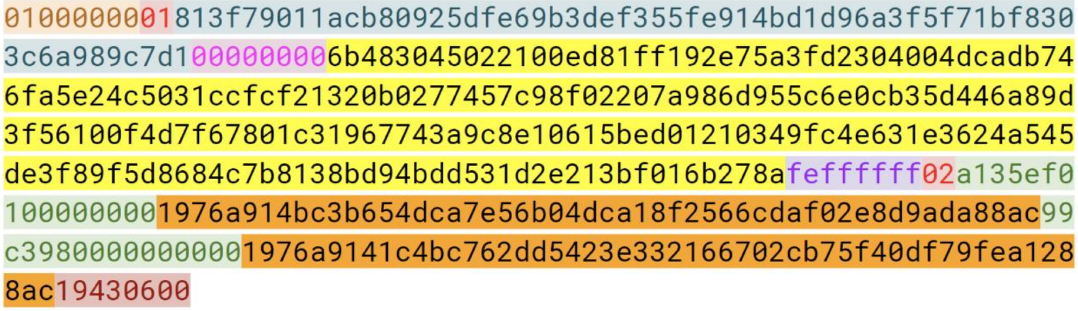
If adopted, Schnorr would be an alternative to Bitcoin’s current ECDSA (Elliptic Curve Digital Signature Algorithm).

What does it do?

To start, Schnorr signatures are appealing because they’re easy to compute and considered highly secure. However, the main benefits of Schnorr signatures actually derive from their aggregation capabilities.

What does “aggregation capabilities” actually mean? What are we aggregating?

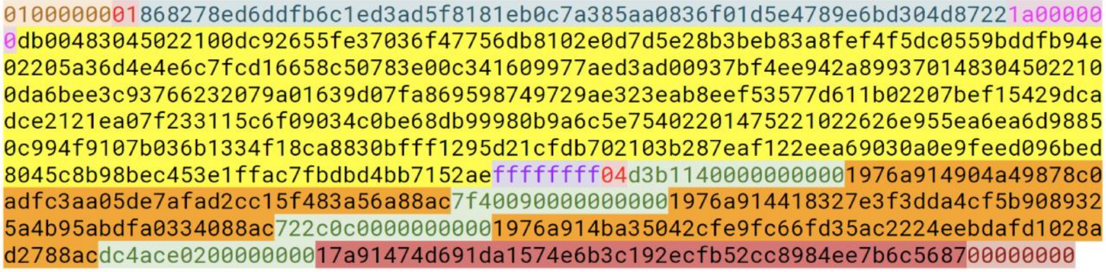
To put it simply, Schnorr signatures can aggregate multiple distinct signature into a single signature. This signature aggregation capability is particularly valuable in light of the amount of space that is consumed by signature data in a Bitcoin transaction — this is depicted visually in Figures 1 & 2, below:



```
0100000001813f79011acb80925dfe69b3def355fe914bd1d96a3f5f71bf830
3c6a989c7d1000000006b483045022100ed81ff192e75a3fd2304004dcadb74
6fa5e24c5031ccfcf21320b0277457c98f02207a986d955c6e0cb35d446a89d
3f56100f4d7f67801c31967743a9c8e10615bed01210349fc4e631e3624a545
de3f89f5d8684c7b8138bd94bdd531d2e213bf016b278afeffffff02a135ef0
1000000001976a914bc3b654dca7e56b04dca18f2566cdaf02e8d9ada88ac99
c39800000000001976a9141c4bc762dd5423e332166702cb75f40df79fea128
8ac19430600
```

Figure 1: A standard Bitcoin transaction. Note how much space is consumed by signature data (highlighted in yellow) ***Source:*** *Class materials from Jimmy Song's* Programming Blockchain Seminar

Even worse, this signature data grows in size linearly with the number of signers in a multi-signature transaction. For example, the yellow signature area in the figure above nearly doubles when we go from a standard transaction (1-of-1) to a 2-of-2 multi-signature transaction, as illustrated in Figure 2 below.

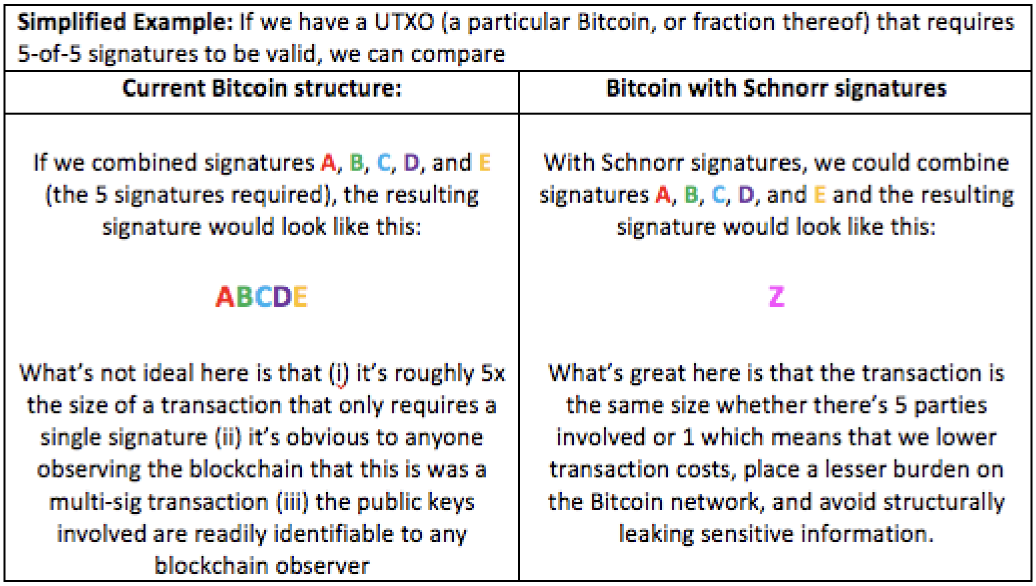


```
0100000001868278ed6ddfb6c1ed3ad5f8181eb0c7a385aa0836f01d5e4789e6bd304d87221a00000
0db00483045022100dc92655fe37036f47756db8102e0d7d5e28b3beb83a8fef4f5dc0559bddfb94e
02205a36d4e4e6c7fcd16658c50783e00c341609977aed3ad00937bf4ee942a89937014830450221
0da6bee3c93766232079a01639d07fa869598749729ae323eab8eef53577d611b02207bef15429dca
dce2121ea07f233115c6f09034c0be68db99980b9a6c5e754022014752210226 26e955ea6ea6d9885
0c994f9107b036b1334f18ca8830bfff1295d21cfdb702103b287eaf122eea69030a0e9feed096bed
8045c8b98bec453e1ffac7fbdbd4bb7152aeffffffff04d3b11400000000001976a914904a49878c0
adfc3aa05de7afad2cc15f483a56a88ac7f400900000000001976a914418327e3f3dda4cf5b908932
5a4b95abdfa0334088ac722c0c00000000001976a914ba35042cfe9fc66fd35ac2224eebdafd1028a
d2788acdc4ace020000000017a91474d691da1574e6b3c192ecfb52cc8984ee7b6c568700000000
```

Figure 2: A multi-signature Bitcoin transaction — signature data highlighted in yellow. ***Source:*** *Class materials from Jimmy Song's* Programming Blockchain Seminar

Schnorr signature aggregation is potentially helpful in a few different ways that each has derivative benefits for the Bitcoin network and its users.

First, the ability to aggregate multiple signatures into a single signature is particularly valuable for "multi-signature transactions" — that is, Bitcoin transactions that require multiple signatures in order to be considered valid by the network. In Bitcoin's current structure, these "multi-signature" transactions are much larger than standard single-signature transactions — which has negative implications for efficiency and privacy (more on that later).



<table>
<tr><td colspan="2"><b>Simplified Example:</b> If we have a UTXO (a particular Bitcoin, or fraction thereof) that requires 5-of-5 signatures to be valid, we can compare</td></tr>
<tr><th>Current Bitcoin structure:</th><th>Bitcoin with Schnorr signatures</th></tr>
<tr><td>If we combined signatures A, B, C, D, and E (the 5 signatures required), the resulting signature would look like this:
ABCDE
What's not ideal here is that (i) it's roughly 5x the size of a transaction that only requires a single signature (ii) it's obvious to anyone observing the blockchain that this is was a multi-sig transaction (iii) the public keys involved are readily identifiable to any blockchain observer</td><td>With Schnorr signatures, we could combine signatures A, B, C, D, and E and the resulting signature would look like this:
Z
What's great here is that the transaction is the same size whether there's 5 parties involved or 1 which means that we lower transaction costs, place a lesser burden on the Bitcoin network, and avoid structurally leaking sensitive information.</td></tr>
</table>

Second, it appears it's also possible to extend to concept of Schnorr signature aggregation — with a scheme known as MuSig — to aggregate the signatures pertaining to multiple UTXOs into a single signature. Conceptually, it's the same process as the example above but instead of just aggregating multiple-signatures that are required to spend a *single* UTXO, we extend the concept to also consolidate signatures across *multiple* UTXOs.

The end result is that while the former example enables us to achieve 1 signature *per UTXO* (even if the UTXO is technically constrained by multiple signatures), the latter example helps us to achieve 1 signature *per transaction* (which in itself could consume multiple UTXOs as inputs). This would mean a drastic reduction in the amount of data that needs to be processed and stored across the Bitcoin network (the benefits of which are discussed in more detail below).

Why do we care? What are the advantages and economic implications?

In short, these aggregation capabilities improve Bitcoin's efficiency and privacy.

In terms of ***efficiency***, the big benefit is smaller transactions — which means lower storage and computation costs. Indeed, Schnorr multi-signature transactions are even more compact and efficient than single-signature transactions in Bitcoin today. That's important because it lowers transaction fees for users and minimizes resource requirements for network participants (e.g. full nodes, mining).

Also, because Schnorr multi-signature transactions are the same size and cost as non-multi-signature transactions, the adoption of Schnorr signatures should encourage an increasing variety — and perhaps complexity — of multi-signature transactions on the network. It's a win-win: Users can create more complex transaction arrangements without burdening the network or incurring additional costs.

In terms of ***privacy***, the advantages of a Schnorr signatures (or a Schnorr-based scheme like MuSig) are two-fold. The first is that multi-signature transactions are indistinguishable from single-signature transactions. Second, an aggregated Schnorr multi-sig does not reveal the individual public key inputs (participants of the multi-sig contract).

Said differently, Schnorr signatures help us avoid leaking info about the public-key identities that are party to a multi-sig contract and even help us avoid revealing whether or not a transaction is multi-sig or not.

Lastly, Schnorr-based MuSig could also offer an indirect privacy advantage by improving the economics of multi-sig contracts: if we can aggregate signatures across multiple UTXOs, MuSig could incentivize the usage of privacy-enhancing functions such as “coinjoin”. That is, with MuSig, users could realize lower transaction costs by aggregating their transactions with others (effectively sharing the cost of your transactions space with others) — which would improve network privacy as a whole.

Ultimately, I’m excited about the potential for Schnorr signatures in Bitcoin because they reduce the size of transactions (lower cost, less network overhead), minimize network resource demands (easier for people to verify transactions), and improve privacy.

Key People & Resources

· **Research paper** “Simple Schnorr Multi-Signatures with Applications to Bitcoin” authored by Gregory Maxwell, Andrew Poelstra, Yannick Seurin, Pieter Wuille, Jan 1018

· Bitcoin.org **blog post** summarizing the benefits of Schnorr signatures.

Acknowledgements

Thank you to Andrew Poelstra and Jimmy Song for generously reviewing earlier drafts and offering corrections.

Disclaimer:

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

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

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

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

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

DYOR | BTFD | HODL

Thanks for your attention and support. I appreciate your feedback and hope you enjoy this publication.

- @_joerodgers