Sam Wouters Follow
#Bitcoin & #Blockchain Speaker • Consultant @DuvalUnionC • INFJ • Learning more about #AI
Jul 4 · 6 min read

Why Schnorr signatures will help solve 2 of Bitcoin's biggest problems today

If you ask anyone in the Bitcoin space what the biggest challenge for Bitcoin is, you will likely hear the answer "scalability".

To explain you what Schnorr signatures are and how they can help solve scalability, I'll first give you a brief recap of why scalability needs to be solved at all and what is being done about it right now.

. . .

The recap

There has been much debate over the past few years on how the Bitcoin network should scale, so that millions (and eventually billions) of people can use it at once, in a frictionless way.

Today, Bitcoin can't handle this many users yet. There is limited space for transactions in the blocks that get added to the blockchain every ~10 minutes. This limitation is by design, to ensure that we can maintain the characteristics that make Bitcoin a mind-blowing innovation (censorship-resistance, decentralisation, immutability and open access).

All Bitcoiners want the network to scale, but we have **different priorities** when it comes to doing so:

- Some people primarily want to **empower** as many users as possible, to keep the characteristics of Bitcoin intact. They want to minimise the trust we need to put in others and ensure that if we do scale, we do so conservatively.
- Others primarily want to **onboard** as many users as possible, with the lowest possible fees and, in their eyes, acceptable security.

Since there is nobody in charge of Bitcoin, all stakeholders (Developers, Users, Miners and Businesses) need to agree on how to move forward,

which is difficult as you can imagine. Most of these stakeholders agree on all the steps that are necessary to make Bitcoin scale. **The debate is mostly about the timing and order of these steps**, as that critically impacts the health of the network.

Out of all of the debates, a technical solution called **Segregated Witness** was brought forward. It was not primarily developed as a scaling solution (though it **does add more space** for transactions), but as **a stepping stone towards a lot of scalability innovation**. SegWit solves a long standing bug in Bitcoin, which stands in the way of these innovations.

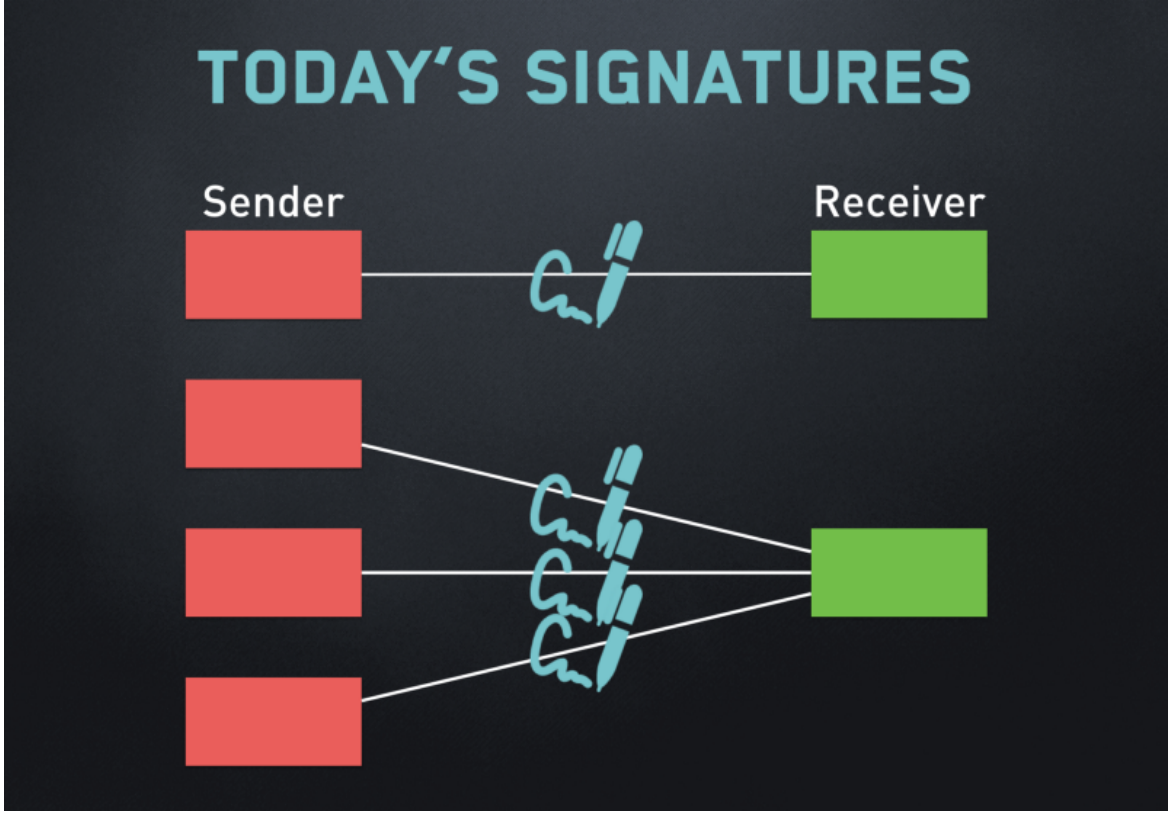
After over a year of testing, **SegWit now has widespread support across all stakeholder groups** (Developers, Users, Miners and Businesses) and will soon be implemented. This opens the door for one of the next innovations: Schnorr Signatures, which can further help to improve scalability.

. . .

Problem #1: Scalability

To do successful bitcoin transactions, signatures are required. Unfortunately these signatures necessarily take up space in the blocks of the blockchain.

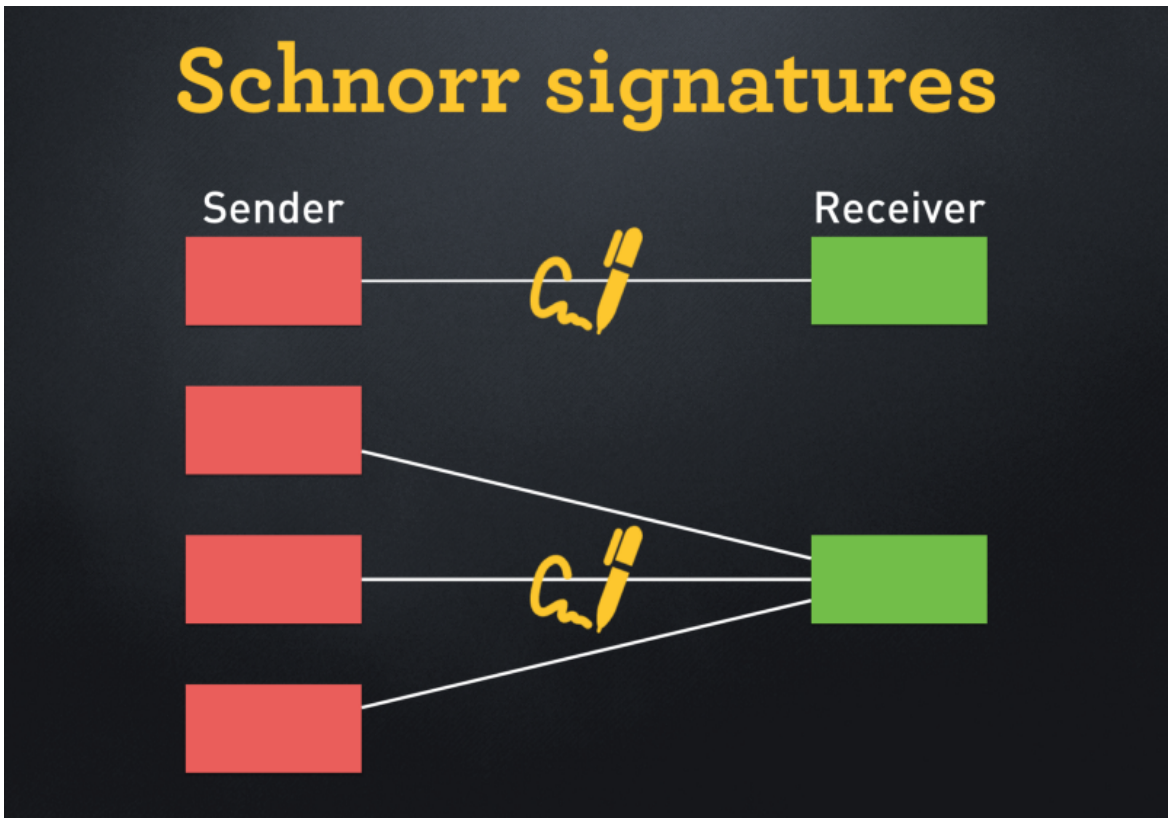
This becomes a problem when you want to send transactions from multiple addresses to one, as each of these transactions require their own signature.



Note that these are digital signatures, you don't need to sign anything!

All this signature data increases the transaction size, and thus the transaction fee that is paid to the miners with it. You are claiming space that could be used for other transactions, which means you must pay to take their place.

At the end of the day, if it is just one person sending that transaction from multiple sources, there should be some way to do so with just one signature, right? This is what Schnorr signatures allow us to do.



One transaction has one signature

Estimates are that **this upgrade would reduce the use of storage and bandwidth by at least 25%**. To point out the obvious: that is a huge efficiency gain.

There is more though.

Another major benefit of Schnorr signatures (not problem #2 of the article), is **increased privacy as to how you are securing your bitcoins**.

Some users intentionally use multiple signatures to send transactions, as this is a way to increase security. You can require multiple people or devices to send a transaction for example, which is commonly known as MultiSig. This is just one of the great benefits of having programmable money.

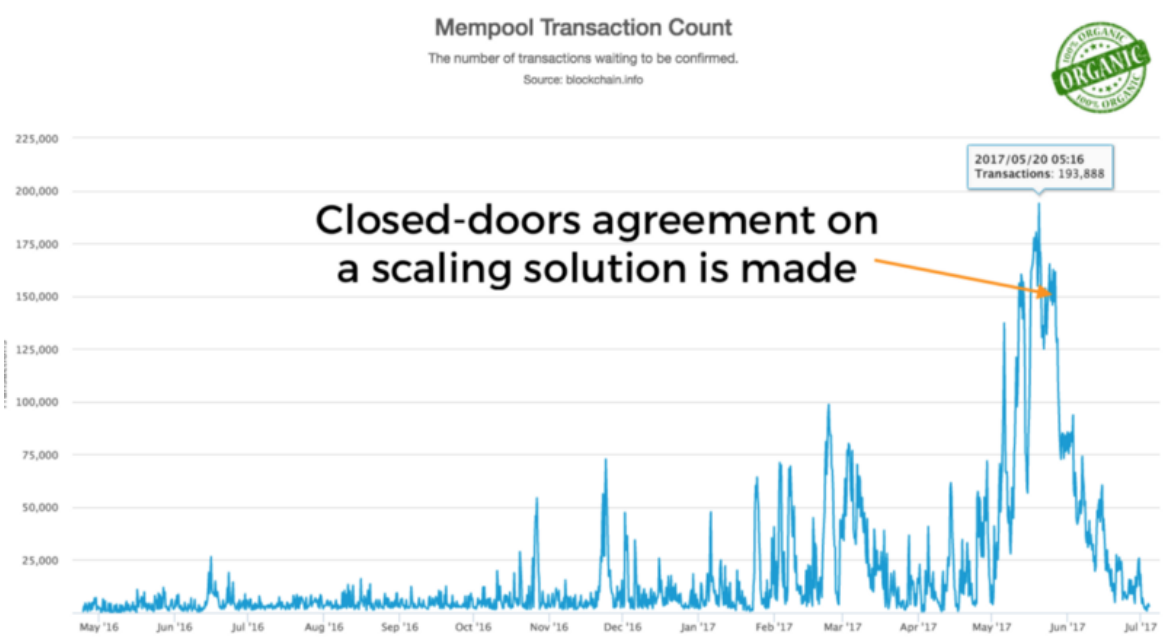
Of course you don't want outsiders to see that you are doing this, and Schnorr signatures would make your signatures look like any other.

Problem #2: Spam attacks

Over the past 6 months, the bitcoin network has suffered from countless spam attacks.

The reason why I call it a spam attack is because **it was done to push a political agenda**. A group of people desperately wanted to push their ideas to increase scalability. The moment a scaling solution was agreed upon behind closed doors towards the end of May, the attacks suddenly ended.

Below you can see a graph of the memory pool, which contains all of the unconfirmed transactions that are waiting to be added to the blockchain at any given time.

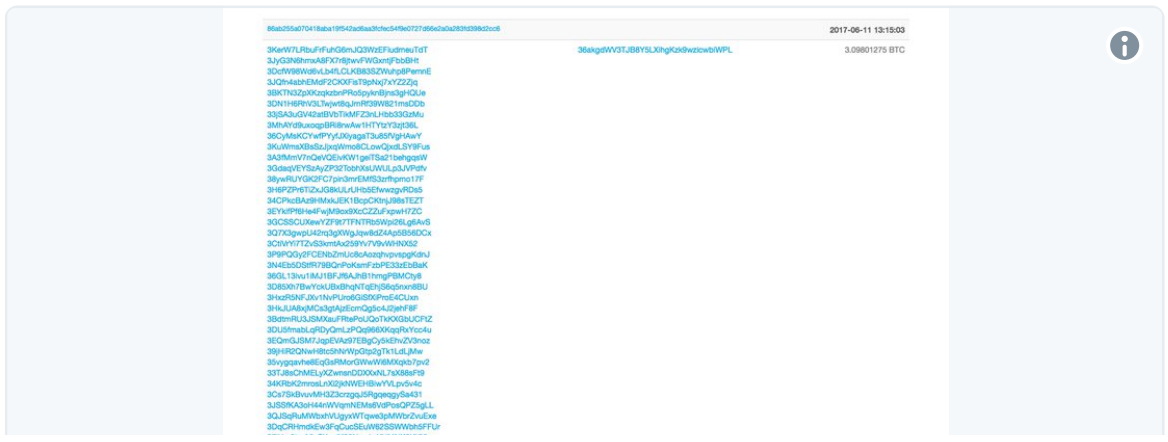


Graph on Blockchain.info

While some people were hopeful or deceptive about these spikes in unconfirmed transactions being organic growth, further analysis clearly shows it was spam.

To push people into increasing the blocksize, the attackers made it expensive to send bitcoin transactions for weeks in a row, by using up as much transaction space as possible through all kinds of constructions.

One of their methods was to include dozens of signatures in transactions by constantly sending transactions from many sources, as can be seen in the image below.



Upon further analysis, it is clear that each of the sources of this transaction was put there just days earlier. This was just one out of dozens of transactions I identified, all following the same patterns and methods. You can view block 470824 as one of many examples of these spam attacks.

Fortunately for us, **Schnorr signatures would help combat this kind of spam attack**. If we only have one signature per transaction, more transactions will fit into blocks and a spammer would need to send far more transactions in competition with more people, and thus likely spend more money to take up the same transaction space. **Signatures are often the largest individual part of a transaction**, so the attacker would be disadvantaged.

If the attacker chooses not to use Schnorr signatures and continues to use old signatures, then other users that do use Schnorr will still have smaller transactions to send and will thus have to pay less. This would still make an attack more expensive than before.

While the price for these spam attacks is estimated to be in the millions of dollars, this is a tiny investment for any wealthy individual(s), government(s) or large corporation(s), that wants to sabotage the network.

While some public actors clearly know more about the origins of these attacks, I'll leave speculation aside in this post as to who is responsible. At the end of the day, Bitcoin will need to be resistant to these attacks, regardless of whether they are done by an insider or an outsider.

What's interesting to me though is that in both cases, **an attack like this is counterproductive**:

- If it is an internal attack to push an agenda, it results in people not taking your agenda seriously, because the attack is very obvious (as seen in the images).
- If it is an external attack to attempt to sabotage Bitcoin, it only increases publicity and validates the fact that it is a threat to centrally controlled currencies.

There would definitely be discomfort for users in both cases, but ultimately solutions would be found or perhaps the attackers would run out of money.

. . .

I for one am super excited to see Schnorr signatures implemented in Bitcoin after SegWit is activated. Like SegWit, Schnorr signatures are

both useful as an upgrade by itself, as well as a stepping stone for future innovations such as **CoinJoin**, a massive potential privacy improvement for bitcoin transactions. That's perhaps for another post though…