After the implementation of SegWit, the door is open for the next innovations: Schnorr Signatures, which can further help to improve 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.

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.

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.

Another major benefit of Schnorr signatures 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.

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.

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.

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.

Click on Schnorr Signatures for more details.