Understanding Segwit and the Bitcoin Scaling Debate

Brendan McManus
Sep 1, 2017 · 8 min read

I've heard that the best way to learn on the internet is to post something and have people correct you, so please respond below with any improvements or suggestions!

It's been clear for a while now that Bitcoin has a scaling problem. The original network designed by Satoshi with a 1MB block size was simply not meant to handle the amount of traffic that is currently on the Bitcoin network. As more users send and receive Bitcoin, transactions can take hours or even days before finally being confirmed, a process that should normally take around 10 minutes. We've never been further from the original vision of a P2P electronic cash system.

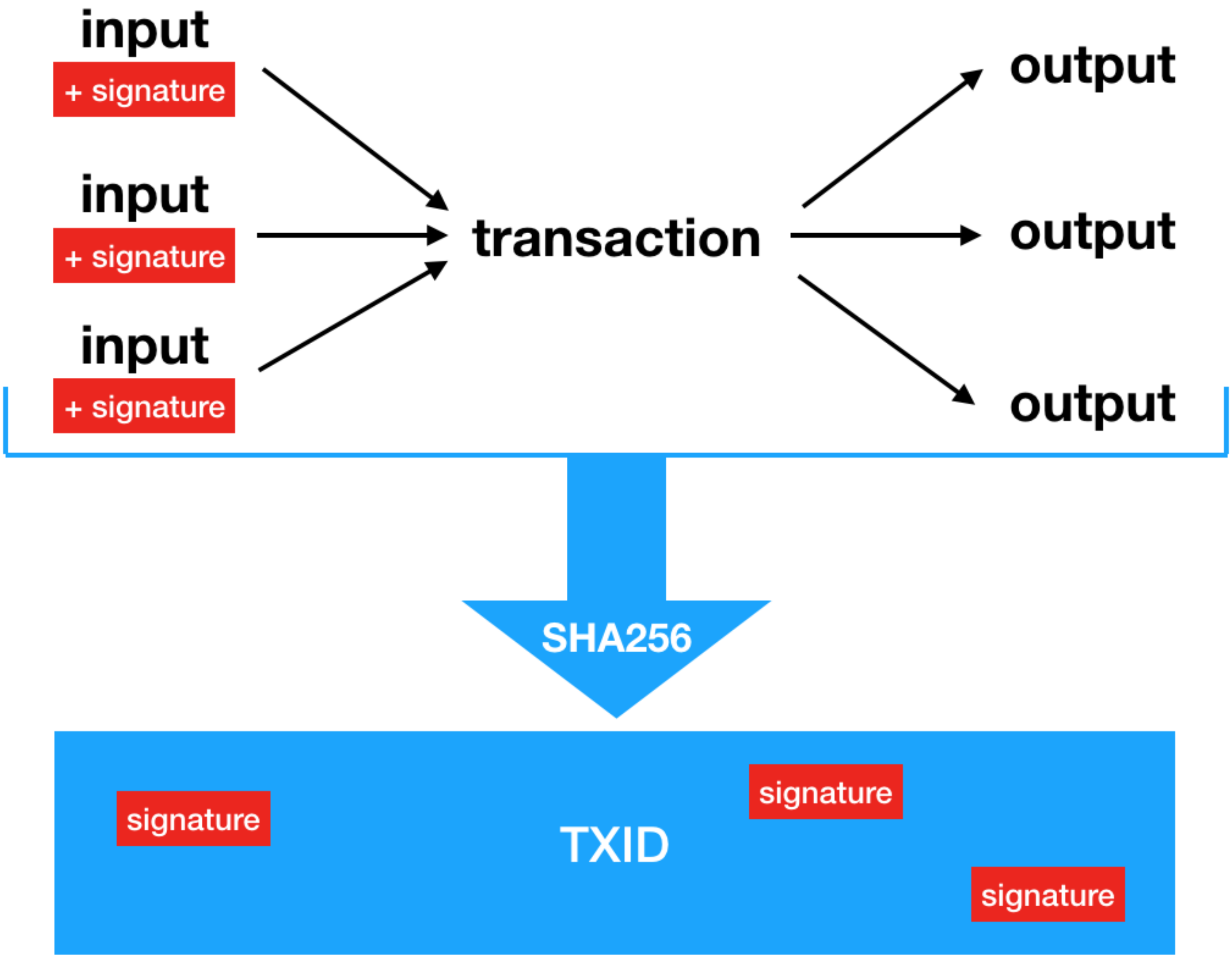
There has been a lot of talk happening recently over how to fix this scaling problem with most of the debate surrounding two proposed short-term solutions: **Segwit** and **Segwit2x.** Through this piece, I will discuss these solutions at a high level and where we are with the Bitcoin scaling problem today.

So what is Segwit?

Segwit, or “segregated witness”, is one proposal that can possibly help with the scaling problem on Bitcoin. In order to explain what Segwit does, we need to back up a bit to explain how the transactions work. In a transaction on the Bitcoin blockchain, there is a single or multiple inputs (or existing batches of Bitcoins), the signatures (needed to unlock the batches of Bitcoins), and the outputs, or where the Bitcoins will ultimately end up going.

Non-Segwit Transactions

With **non-Segwit transactions**, the signatures needed to unlock the inputs are included along with the rest of the transaction data in the hash to get the transaction id (TXID).

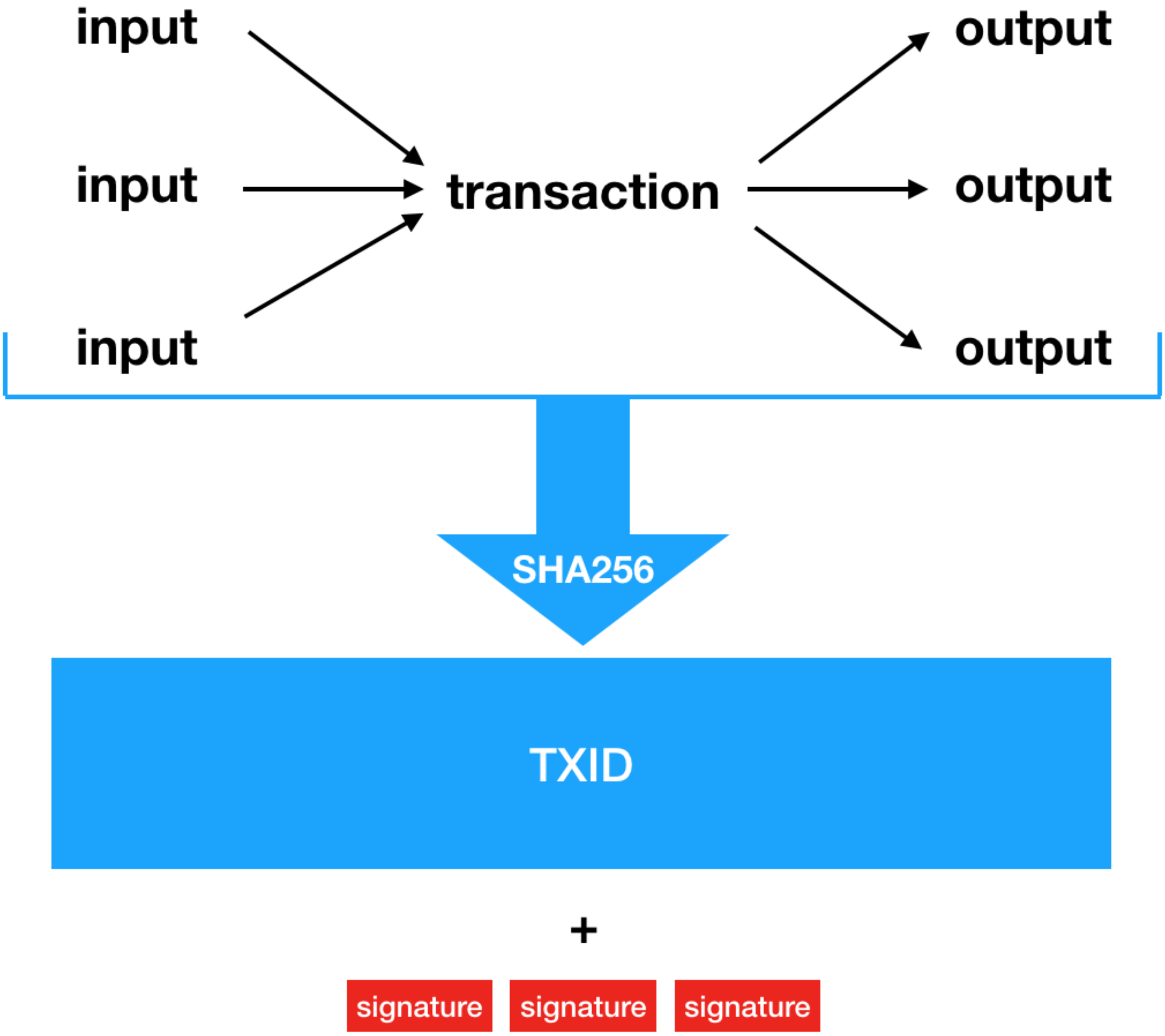


Non Segwit transactions include the signatures in the hash to get the TXID.

These transactions are then included in each block up to the 1MB limit in structures called Merkle Trees.

Segwit Transactions

With **Segwit transactions**, we have two fundamental changes.



Segwit transactions do not hash the signature data. Signature data is stored as "witness" data in the block.

1. The signature data is not included in the hash to form the TXID. Signatures are still stored in the block with the transactions as part of "witness" data, but they are longer included in the TXID hash.

2. The block size limit is changed from 1MB (1,000,000 bytes) to a 4,000,000 "weight" limit, an arbitrary new metric. A **normal byte** in a transaction has a weight of 4 while a **witness byte** has a weight of 1.

So what's the significance of Segwit? Well, there are two main benefits:

1. Transaction Malleability

With Bitcoin transactions before Segwit, there was a bug in the software called "transaction malleability". As we know by now, the TXID pre-Segwit is the result of hashing the transaction data including the signatures. Although there were checks and balances to ensure that the inputs and outputs couldn't be changed (i.e. the parties in a transaction and the amounts of Bitcoin being sent), the signature used to unlock the inputs could be modified slightly (such that it was still a valid signature), but would completely change the TXID when hashed. With the signature no longer a part of the TXID in Segwit, transaction malleability is no longer a problem!

2. Increased Block Capacity

By changing the block size limit from a bytes limit to a new 4,000,000 weight limit, the number of transactions allowed in each block can be increased while maintaining backwards compatibility with the existing cap of 1MB per block. How? Simple math. Our equation for Segwit nodes is as follows:

$$4 \text{ x normal bytes} + 1 \text{ x witness byte} = 4{,}000{,}000$$

Non-Segwit nodes in the network will not be able to see the witness data, making their equation:

$$\begin{aligned} 4 \text{ x normal bytes} &= 4{,}000{,}000 \\ \text{normal bytes} &= 1{,}000{,}000 \end{aligned}$$

So with Segwit, we'll never go over the 1MB block size limit on older nodes, making this backwards compatible! Only Segwit nodes will be able to see the signature data, but existing nodes will still have access to all of the transactions.

Segwit won't bring about nodes with a block size of 4MB though as blocks aren't comprised 100% of witness bytes. The actual size of the blocks will depend on the adoption rate of Segwit, although the expected average block size will be around 1.7–2MB based on tests showing around 60% of a transaction to be witness data.

Segwit Proposal Background

Segwit (or segregated witness) is a part of BIP141 ("Bitcoin Improvement Proposal") supported by Bitcoin Core, originally introduced in November 2016. This proposal didn't originally get activated for two reasons:

1. It required a super majority (95%) of miners to activate.
2. Some miners were potentially waiting for a block size increase.

In March 2017, BIP148 was released. This proposal intended to circumvent BIP141 and activate Segwit through UASF ("user activated soft fork" — where users, merchants, exchanges, wallet providers reject blocks without the changes, theoretically forcing the miners to change software) which would potentially cause a network split (and a competing currency) if the full economic majority doesn't support the new rules.

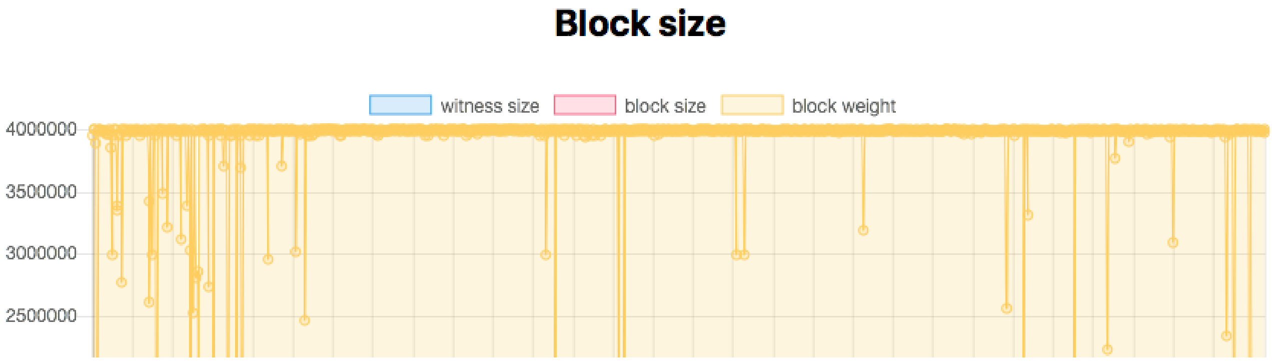
Enter BIP91, a proposal to help move along the original Segwit proposal, BIP141. Specifically, BIP91 was created to orphan off any blocks not signaling for BIP141 (Segwit). BIP91 was seen by many as an attempt to head off BIP148 to prevent the UASF. The key reason it would pass:

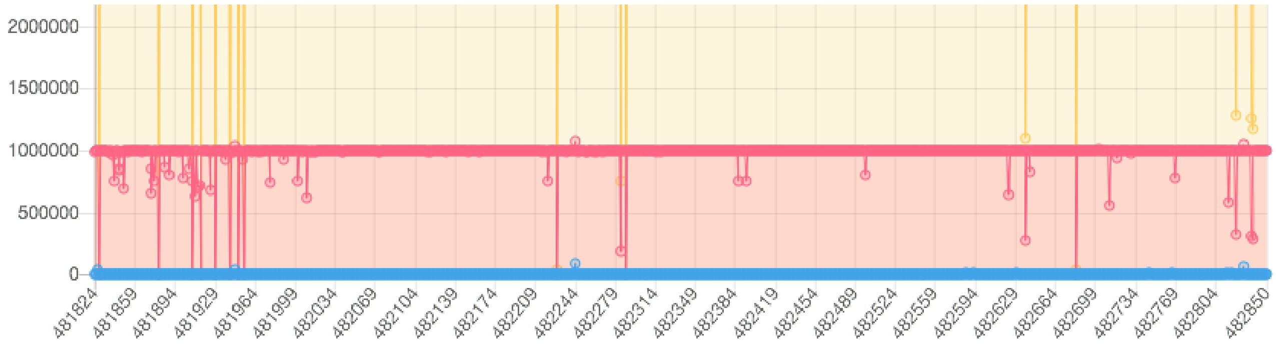
1. BIP91 requires 80% of miner support vs. the 95% required with BIP141
2. The activation window (amount of time signaling must be in place) was reduced from 2,016 blocks (BIP141) to 336 blocks (BIP91).

Long story short, BIP91 activated around July 20, thus superseding BIP148. Miners could have still chosen to not support BIP141 and mine blocks without the signaling bits at this point, but this didn't happen and BIP141 ended up activating on August 24.

So how is Segwit affecting the network right now?

Well, Segwit has shown limited adoption by users and companies so far, with many of them completing internal testing and / or waiting to add support for security reasons.





There are only a few blips where the block size increased above 1MB since activation. Source: segwit.party

This brings us to the next chapter and a large point of debate in the Bitcoin community right now, Segwit2x.

. . .

What is Segwit2x?

Segwit2x Proposal Background

It started with Consensus 2017 in May with a group of 58 companies representing a critical mass of the bitcoin ecosystem agreeing to activate Segwit at a 80% threshold (*check! this part is finished*) and activate a 2MB hard fork within six months (*this remains to be seen*) in what is now known by many as the New York Agreement. This ultimately led to the development of **Segwit2x** (*this is different from Segwit!)*, which is currently being developed as a fork of Bitcoin Core in the repository BTC1 with Jeff Garzik (CEO of Bloq and a former contributor to Bitcoin Core) as lead.

So what’s different in Segwit2x from Segwit?

Segwit2x is a combination of BIP141 (Segwit) and BIP102, a proposal put forth by Garzik suggesting increase the blocksize from 1MB to 2MB that was never integrated into Bitcoin Core. Segwit2x includes the improvements from segregated witness and additionally enacts a 2MB (8,000,000 block weight limit) hard fork that will activate three months after Segwit. This means that Segwit2x will cause a hard split in the Bitcoin network leading to a new chain and a new currency (this part is a bit confusing, which I’ll explain in a bit).

Why is Segwit2x contentious?

Opposition to the fork

Segwit2x is out of the hands of Bitcoin Core, who have been overseeing the development of Bitcoin since Satoshi created it, and they certainly do not support it. They argue that scaling Bitcoin by increasing the block size is not right at this time, stating that more research and testing is absolutely necessary; many developers opposed to the hard fork state that executing a 2MB hard fork with all of the proper testing in three months is extremely challenging and could result in users losing Bitcoin if not properly done.

Additionally, many believe that another fork of Bitcoin so soon after the fork into Bitcoin Cash is not desirable and believe that the overall effect on publicity for Bitcoin would be negative. If we do see a hard fork, the majority of users may be using a version of Bitcoin not developed by Bitcoin Core (and thus sending transactions and mining blocks on a different chain from the original Bitcoin), leading to potential confusion. Some may recognize the Bitcoin Core version of Bitcoin, the potential minority chain, as the legitimate Bitcoin while others may not.

Some on the side against the fork would prefer that a mortatorium be placed on a hard fork while the community works together on the Lightning Network, a secondary layer scaling solution.

Proponents of the fork

Proponents of the fork will argue that Segwit and the Lightning Network do not provide an immediate enough solution, especially as development of the Lightning Network could take anywhere from 3–12 months, which is definitely not a short term solution. Some also would like to see a different path for Bitcoin, one that isn’t necessarily owned by the Bitcoin Core team (but then we get into the same confusion mentioned above — will the real Bitcoin please stand up?).

Will Segwit2x happen and lead to a hard fork?

As of writing this, around 90–95% of blocks are signalling support for the New York agreement, but signaling for Segwit2x is completely different from running the software. If the original ~83% of hashing power alleged in the New York Agreement remains committed, then we could very well see a hard fork, but many of these companies could renege (as some already are here are here) now that BIP141 has locked in. It makes sense that many miners may renege — after all, smaller block size = more network latency (slower transaction) = higher fees for them. Only time will tell.

. . .

I know that this was a lot, so I've made a brief timeline highlighting the key events:

. . .

I hope this has been somewhat informative about what Segwit actually is from a high-level technical overview, and I hope that the Segwit vs. Segwit2x debate is a bit more clear now than it was (if it wasn't, please let me know where I can improve / fix the explanation).

If you ever want to talk about anything Blockchain related, hit me up on Twitter @brendanmmcmanus.

Special thanks to Shiv Patel for helping me to proof and think through this.

Bitcoin Blockchain Segwit Cryptocurrency