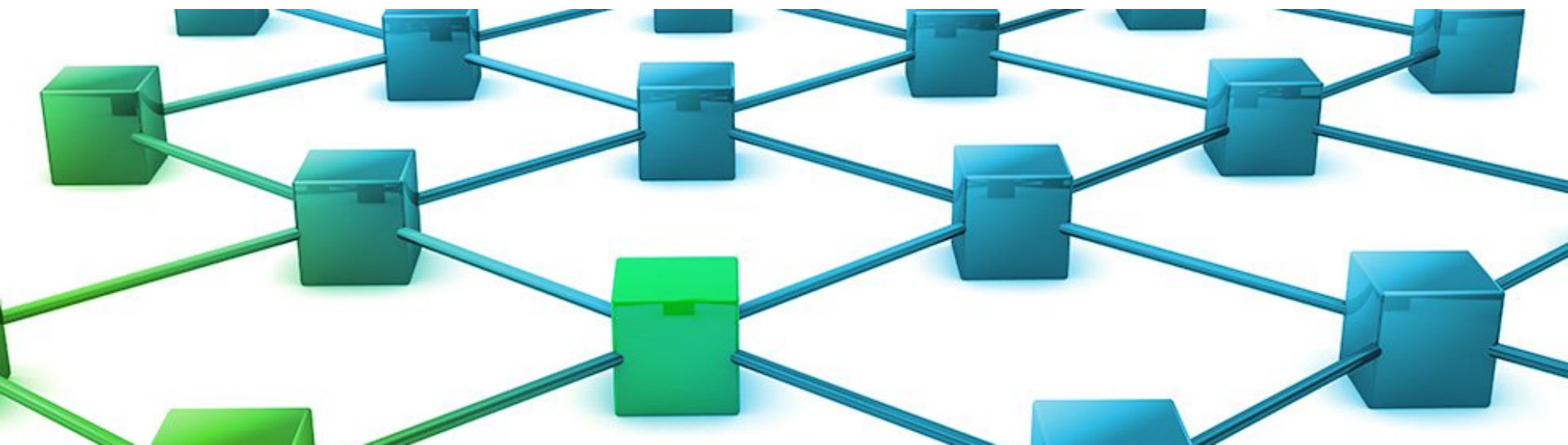
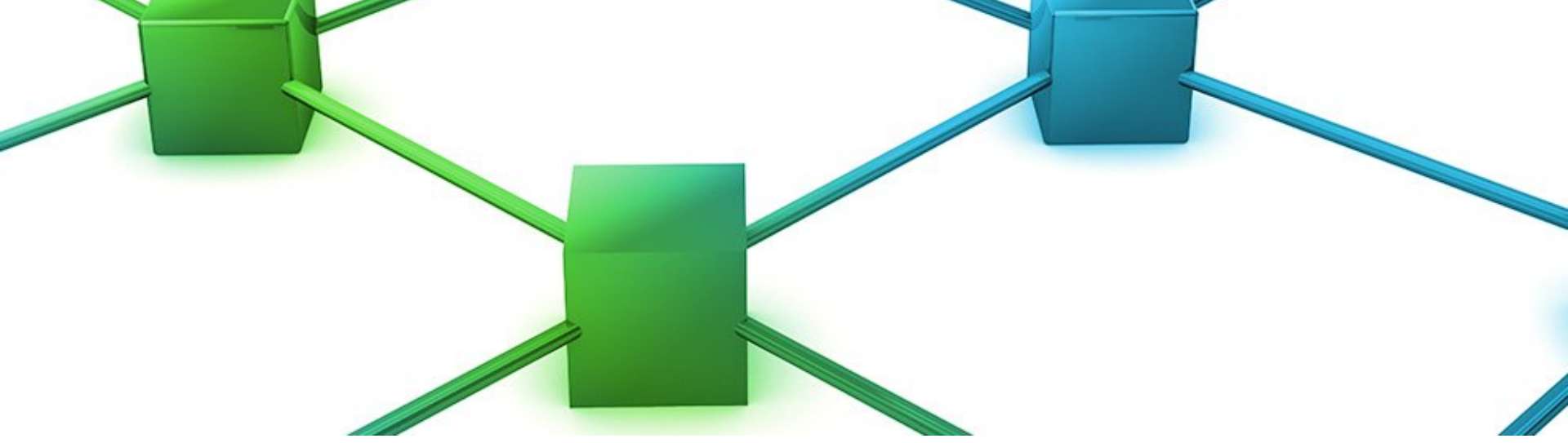
Amid Bitcoin Scaling Debate, Segregated Witness Testnet Enters Public Stage

by Aaron van Wirdum

10:39 AM CST
January 21st, 2016

- Aa +





In the midst of a heated debate over block size and Bitcoin's future, Bitcoin Core developers Dr. Pieter Wuille, Eric Lombrozo and Johnson Lau have launched a third iteration of the Segregated Witness "testnet." Dubbed SegNet, the latest version of the Bitcoin test network includes several improvements over its predecessors, and is available to anyone who wants to try it or experiment.

SegNet, like the previous versions, is essentially a clone of Bitcoin, specifically intended as a demo version. But while the two earlier SegNets were open only to developers working on the project, now everyone can use it.

Speaking to *Bitcoin Magazine*, Ciphrex CEO and Segregated Witness developer Lombrozo said:

> "All wallet and other app developers are invited to test and experiment with the latest version of SegNet, and offer feedback. We've opened up an IRC channel on Freenode, #segnet-dev, and welcome all discussion pertaining to integrating and supporting Segregated Witness transactions in wallets. Many developers have already joined the effort. I'm happy to see the excitement and enthusiasm, and hope many others will join, too."

Segregated Witness, the talked-about centerpiece of the scalability "roadmap" proposed by Bitcoin Core, is set to introduce several significant improvements to the Bitcoin network. Most

important, it allows for an increased number of transactions by circumventing the original 1-megabyte block size limit, using an add-on to existing blocks called the "witness." This could increase the effective block size up to some 1.75 to 2 megabytes, depending on the types of transactions.

"Compared to earlier SegNet versions, this latest iteration includes four main improvements," said Lombrozo, whose mSIGNA wallet will implement Segregated Witness once it is rolled out. "First off, we moved the 'add-on anchor' - the Merkle root of the witness – to a different part of the coinbase transaction. We did some research, and as it turns out that works better for existing mining-hardware. Second, we changed the signature hashing algorithm such that verification requires fewer steps. This makes running a full node less burdensome, closes off a denial-of-service vector that is particularly nasty for bigger blocks, and decreases block relay time over the network. Third, transaction input values will be signed. This prevents some fringe attack vectors, where users can accidentally pay too high a fee. And fourth, we lowered the cost for typical, non-multisig transactions. Since these are still in the majority on the network, that should increase total throughput."

One of the interesting attributes of Segregated Witness, as first presented at the Scaling Bitcoin workshop in Hong Kong, is that it can be rolled out as a soft fork. This means that to use it, only miners need to change their software; all other users can "opt-in" if and when they choose to. For this and other reasons, the Bitcoin Core development team prefers soft forks over hard forks, which require a synchronized network-wide switch of all users.

Over the past week, however, the idea of implementing Segregated Witness as a soft fork came under increased scrutiny. The team behind the recently launched Bitcoin Classic implementation believes that a change in fee policy is undesirable, questions whether the increased transaction throughput will be sufficient, and points out that there is a security degradation for nodes that don't upgrade to the latest version of the software. Critics also maintain that the proposed soft fork method requires an "ugly" hack, which could complicate development of wallet and app software.

The Bitcoin Core development team, however, maintains that the security tradeoffs are highly theoretical and negligible, and far fewer than those associated with a hard fork. They point out that soft forks have been implemented several times before: when multisig was rolled out, or more recently with CheckLockTimeVerify. Core developers also contend that the increased throughput almost equals that of the 2-megabyte hard fork solution planned by Bitcoin Classic, and could in some cases amount to a bit more. They consider the changed fee policy a feature, not a bug, because it incentivizes users to utilize the added space in blocks.

"As for the 'ugliness' of the workaround… I'll lay it out bluntly here," Lombrozo said. "A simple block size increase via a hard fork puts all of the burden on the infrastructure rather than the app developers. What we're proposing with Segregated Witness places a little bit of burden on app developers - which we think is fair. As a bonus, it also means these apps will be ready to support much more sophisticated features in the future, such as smart contracts, the Lightning Network and other payment channel solutions. It's still not a very complicated thing to support, and many wallet developers seem eager and excited by all this."

Segregated Witness is scheduled to be rolled out in Bitcoin Core and the Bitcoin network by April of this year. BitGo, BitcoinJS, BlockTrail, Breadwallet, Coinkite, Coinomi, Digital Bitbox, EI8HT, Electrum, GreenAddress, Green Bits, Ledger, Libbitcoin, libbtc, mSIGNA, Mycelium, NBitcoin, Omnicore and Samourai Wallet have indicated support, so far.

For more information on Segregated Witness, see Bitcoin Magazine's *three-part series on the proposal*.

Read More: bitcoin developers core transactions more...

COMMENT SHARE TWEET UPVOTE SHARE

EMAIL