What is Segregated Witness?

By **Bisola Asolo** - November 1, 2018

What is Segregated Witness?

Last Updated: 1st November 2018

Segregated Witness, or SegWit, is a soft fork method that can be used to increase the capacity of the blockchain by removing signature data from transactions. A soft fork is simply a backwards compatible method of upgrading the blockchain. Check out this article here if you are uncertain about what a soft fork is.

To first understand how Segregated Witness is used to increase the capacity of the blockchain, It is important to first understand how a transaction works.

How a transaction works

A transaction simply consists of inputs and outputs. An input is the culmination of previous transactions which gives the present account balance that can be used to start a new transaction. If we consider the transaction, "Alice sends 10 Bitcoins to Bob", for this transaction to occur, Alice needs to have received Bitcoins from previous transactions. The 10 Bitcoins she is sending to Bob is considered as the input for the transaction. The output on the other hand, is simply the number of Bitcoins Bob would have once the transaction has been completed.

The problem is, transactions are mostly made up of what is known as signature data. Signature data is used by senders, in this case Alice, to prove that they are the rightful owners of the account with which they are using to send funds from in the first place. About 65% of a Bitcoin transaction is made up of signature data.

Bitcoin's scaling issue

As more people use Bitcoin on a regular basis, a greater number of transactions therefore need to be processed in-order to be added to the blockchain. This is known as the mining process. If you're unsure about what the mining process is, then check out this article here.

Transactions are added to the blockchain in blocks, and each block has a maximum size limit of 1 MB. However, has more people use Bitcoin and the number of transactions increase, the size limit of 1 MB has shown to be ineffective in handling the increased transaction volume. The result being, some users having to wait hours or even days to have their transaction validated, and therefore added to the blockchain.

This is precisely the scaling issue. The issue that the Bitcoin network is unable to scale with the increasing number of users. However, Segregated Witness is the proposed solution to this scaling problem.

Segregated Witness

Remembering that signature data accounts for 65% of a transaction, and a block is simply a bundle of transactions, by moving this signature data into what is called an extended block, we can free up space in the original block. An extended block is simply a side block that would run parallel to the original block. So by transferring this signature data to the extended block, space is able to be freed up in the original block, therefore allowing for more transactions to be added. Consequently, this results in a real block size increase from 1 MB to 4 MB.