Mohammad H. Tabatabaei

Scaling Blockchain

There are many debates and efforts about changing the block size in order to achieve a better scalability in blockchain, however, this is not the ultimate solution for this challenge. Some other solutions are presented and can be considered which do not have the block size problem at all. There are some main challenges for scaling Bitcoin. The linear structure of blockchain is the first limitation in scaling Bitcoin. Other data structures such as tree or Directed Acyclic Graph can be helpful for mining two blocks at the same time and placing them into the data structure at the same height without conflicting. Another integral challenge in scaling is that the load on the system grows according to the grow in the number of nodes and transactions. Thus, it is needed to shard the blockchain in a way that each node just requires a subset of the blockchain and still be able to verify transactions.

One of the challenges in scaling Bitcoin is the creation of a block which needs to update the state of the UTXO set which requires bandwidth equal to all the transaction volume to keep up with the changes to what set. If a solution could turn the linear blockchain into a tree and split up the UTXO set such that individual miners only had to deal with subsets of this tree, the bandwidth that each miner would need to process could be reduced significantly.

Another solution for scaling Bitcoin is introducing sidechains but the main problem in this solution is that Bitcoin script simply is not powerful enough to verify an entire separate blockchain. However, it can be enabled with a practical soft-fork modification to Bitcoin. Bitcoin nodes can use lightweight SPV verification of events in the sidechain. To do even simplified verification, Bitcoin nodes would still have to connect to the sidechain's peer-to-peer network and track all of the sidechain block headers so that they can determine the longest sidechain branch. When a transaction tries to convert a coin in a sidechain back into a Bitcoin, it contains all the information that Bitcoin nodes need in order to verify its legitimacy, thus, instead of the previous costly action, it is more rational to verify that a particular sidechain transaction happened by its contained information. It is remarkable that problems on sidechains cannot damage Bitcoin and there is no way to redeem the same coin twice from a sidechain regardless of how faulty it may be.