Scaling Blockchain

IN5420 Distributed Blockchain Technologies

Michael Eikeland

April 2018

Sidechains. The idea of sidechains is that Bitcoin has become so large that it is impossible to remain technologically innovative. Sidechains are other blockchains, that may have different or more functionality, where Bitcoin nodes can provide transaction inclusion proof (similar to SPV proofs) from this other blockchain in the main Bitcoin blockchain. This would only require minor changes to Bitcoin's scripting language.

Scalability challenges. Bob McElrath points at three challenges for scaling Bitcoin: "(1) Move from a chain to a more sophisticated data structure, (2) Move mining to the edges of the network (PoW for the p2p relay layer), (3) Shard the Blockchain" where (1) aims to steer the conversation from increasing the Bitcoin block size into "how to we remove the block size issue". (2) addresses the mining centralization and suggests that end-users of Bitcoin also need to mine. (3) addresses the issue of miners (and preferably users) being required to keep a local copy of the ever increasing Bitcoin ledger.

Braiding. Braiding is a term used for the idea of using competing blocks that do not conflict with each other in terms of transaction inclusion (i.e. double spending attempts), in order to increase block rate and reduce loss of work. The idea is that if two competing, non-conflicting blocks are discovered, they can be merged in a new block, that cites both of these blocks as its parents. Such a structure is often called a Directed Acyclic Graph.

Treechains. Treechains is an improvement suggestion to Bitcoin in order to solve some of its scalability issues. The idea is to have all blockchains as nodes on a single tree and having miners only work on the branches they are interested in. This structure will make it easier for miners to keep an overview over unspent transaction outputs and reduce the storage space needed for mining. Having a single tree for all chains will make it more resilient to attacks.