

Scaling Blockchain

Xiaojie Zhu

April 10, 2018

1 Scaling blockchain

Currently, many alter chains are proposed and implemented. However, present alter chains have several weakness in following aspects. First, since each alter chain is implemented separately, effort are frequently duplicated. Second, each alter chain has its own currency and it is hard to transfer between different currencies. To avoid above embarrassing dilemma, sidechain is an approach. There are many innovative ideas about sidechains.

- Pegged sidechain. The main idea is to allow all the side chains can exchange assets. Specifically, *two-way peg* is proposed, which defines the protocol between parent chain and sidechain.
- Braiding. The main idea is to avoid the orphan block by applying directed acyclic graph. Each block is allowed to have multiple parents but no incest is allowed.
- Treechains. The main idea is to split the UTXO set such that individual miners/full nodes can deal with subsets of the universe UTXO.
- Move from a chain to a more sophisticated data structure. For example, the previously mentioned *block-braid* is a new data structure.
- Move mining to the edges of the network. Mining centralization has been a concern for the stability of network. One way to solve this issue is to reduce the size of block and another way is to move mining to the point of transaction submission.
- Shard the Blockchain. Bitcoin with its linear chain structure is *fragile*. The load on the system grows as the number of nodes grow. It is desirable to *shard* the blockchain so that a single node can hold only a subset of the blockchain, but still be able to verify transactions.