

Lecture 10 – Scaling blockchain – Tien Dat Le

Bitcoin is the first blockchain that comes up with the idea of proof of work to solve Byzantine Fault Tolerance problem. It works in practical, however, there is still a challenge in scalability for throughput, since PoW is estimated to handle around 20 transactions per second and interoperability, i.e: interact between different blockchain.

There are a couple of solution is proposed to solve this challenge:

1. Sidechains (Or pegged chain): is the idea proposed to solve interoperability problem. The design of sidechains aim at moving the digital assets between the 2 chain in a trustless manner. The security is indeed equal to the security of the weaker blockchain. A Simple payment verification proof (SPV) will be used to verify and hence moving the digital assests back and forth.
2. Braiding: a technique is used to avoid orphan blocks, hence increase the efficiency of mining power. Each block is allowed to have many parents via directed acyclic graph.
3. Treechains: The idea is to divide the UTXO spaces into sub-space via tree structure, hence it is more efficiency for nodes, miners to deal with subset of UTXO.
4. Sharding: is a divide and conquer strategy. The main blockchain is splitted into a number of partial chain called a shard. During consensus phases, each shard will contribute to the commit of the mainchain via a fair algorithm.