Mohammad H. Tabatabaei

Bitcoin in Research

Bitcoin introduced some new concepts that made online transactions between the users without an intermediary possible. The importance of replacing the third party is that the intermediary can no longer refuse to carry out certain transfers, to change balances or to demand high fees in exchange for its services. Thus, Bitcoin described the notion of miners that can join at any time in the network and download the history of transactions to maintain the network by their contribution in the next processes of accepting transactions. In order to allow each node to act independently without trusting each other or third party, data is replicated and each participant repeats all verification work.

The main components of Bitcoin can be categorized in three concepts such as transactions, the consensus protocol and the communication network. Transactions are series of messages which are published to transfer money from one user to another. The transactions consist of an array of inputs and outputs. It is important for a valid transaction to have the sum of the values of the input greater than the sum of the values of output. Consensus protocol and mining are the other elements that are used for collecting the valid transactions into a block and doing some computational work on it to be able to append the block to the blockchain. If two valid blocks are found at the same time by separate miners, a temporary fork will be created. At the next steps, miners can select one of the forks to proceed the blockchain. It should be considered that at any given time, the longest chain is the version which is the consensus blockchain. Finally, the third component is the communication network, which uses flooding algorithm for propagating new blocks and pending transactions to the whole network.

Bitcoin architecture is also divided into five planes in terms of scalability. First is the network plane which is described above. However, it is noteworthy to say that the Bitcoin's network protocol does not fully utilize the underlying bandwidth that can make this plane a bottleneck for transaction processes. Second plane is consensus protocol that is necessary for globally accepting set of transactions and their order. One important matter in this layer is that the Bitcoin's blockchain protocol introduces a tradeoff among bandwidth, security and consensus speed. Storage plane is the third part which holds the ledger of the system as well as the states for smart contracts. One of the shortages of Bitcoin in this plane is its disability to delete transactions which may cause lack of enough storage for nodes to store all the history of the network after a period of time. The next plane is view plane that can help miners not to need downloading all the network for joining which can takes a lot of time. However, Bitcoin does not have this option in its implementation. Side plane is the last plane which is used for taking some actions and services outside of the main blockchain to increase the performance of the network. On the other hand, the matter of centralization will be appeared by creating this new plane.