IOTA

Lars Erik Wik

April 5, 2022

Summary

Instead of the blockchain data structure used to represent the ledger in other popular crypto currencies, IOTA uses a Directed Acyclic Graph called the tangle. In this data structure the vertices represent transactions, whilst edges represent transaction approvals. Unapproved transactions are called tips.

There are no rewards for participating in the network, instead participation is required in order to use the network. Whenever a user submits a transaction, the user has to approve two other transactions, resulting in the user contributing to the network security.

Nodes in the network are incentivised to gossip transactions, based on the fact that other nodes in the network are incentivized to get rid of connections to lazy nodes. Thus a node that does not gossip transactions will get a weaker connection to the network.

To avoid the network from overflooding with tips approving old sites, honest nodes use a tip selection algorithm in the form of a weighted random walk. This way, fresh tips with a larger cumulative weight, have a higher probability of being approved.

Honest nodes are assumed to check the validity of a transaction during approval. This includes checking that there is not a conflicting transaction. Transaction conflicts are resolved by the node running the tip selection algorithm multiple times in order to see which transaction or more likely to be included. The more likely transaction is included, whilst the less likely transaction is orphaned.