Blockchain

Paolo Bettelini

Contents

1 Block

Each user owns a pair of private and public key.

All the transactions broadcasted to the network are grouped into blocks, which contain

- Markle tree root hash
- Timestamp
- nBits
- Nonce
- Previous block hash
- Number of transactions

2 Proof of Work

Proof-of-Work (PoW) is a cryptographic proof that a party has spent a certian amount of computational effort.

When a miner solves the puzzle the current block is archived, a new block is generated and all the transactions in the previous block are confirmed. The miner is then rewarded by the system.