Blockchain

Paolo Bettelini, Giacinto Di Santis, Gianni Grasso

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 (PoW)
- Nonce (PoW)
- Previous block hash
- Number of transactions

With each block being confirmed, the blockchain is created.

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.

3 Proof of Stake

4 Smart Contracts

Smart contracs are programs associated with an address and run on the blockchain. The nodes run code from the contract program at a relevant event, such as a received transation.

Users can interact with the contract via transactions. Contracts can often interact with other contracts and some of them are Turing-complete.

4.1 Deployment

A smart contract is deployed by sending a transaction to the blockchain which includes the compiled program as well as a special receiver address.

The program is added to the current block. When the block is added to the blockchain, the contract will execute one time to set its initial state, at which point the smart contract will now be valid and running.