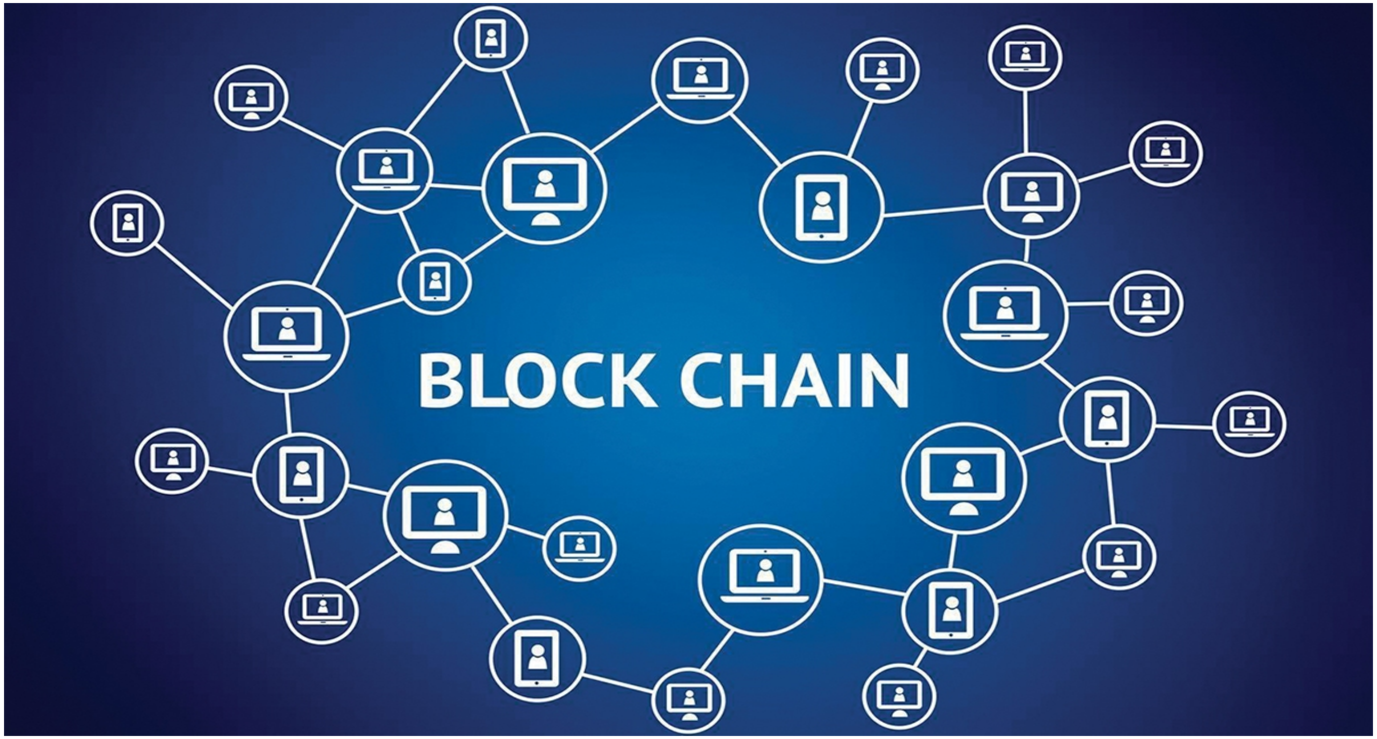


Blockchain Architechture

By – Udayveer Singh

Components of Block

- Block Number
- Block Hash
- Merkle Root
- Timestamp
- Previous Block hash
- Nonce

Verification of Block/Transactions

- After a transaction is made by some user, that unverified transaction is sent to the collection of unverified tranactions called the Mem pool.
- There are special nodes called the miners that verifies the transaction.
- All the miners compete against each other in a race to verify the block first because the miner who get the correct block hash gets the reward.

Condition for correct block

- After the unverified transactions are collected from the Mem pool by the miner, they create the merkle root and all other components expect the NONCE and the block hash.
- Get the the condition of getting the correct block hash is that the Block hash must contain some leading zeros
- Ex-0x000000001234567891234567891234567891234567890123456789012345678901234567890123456789

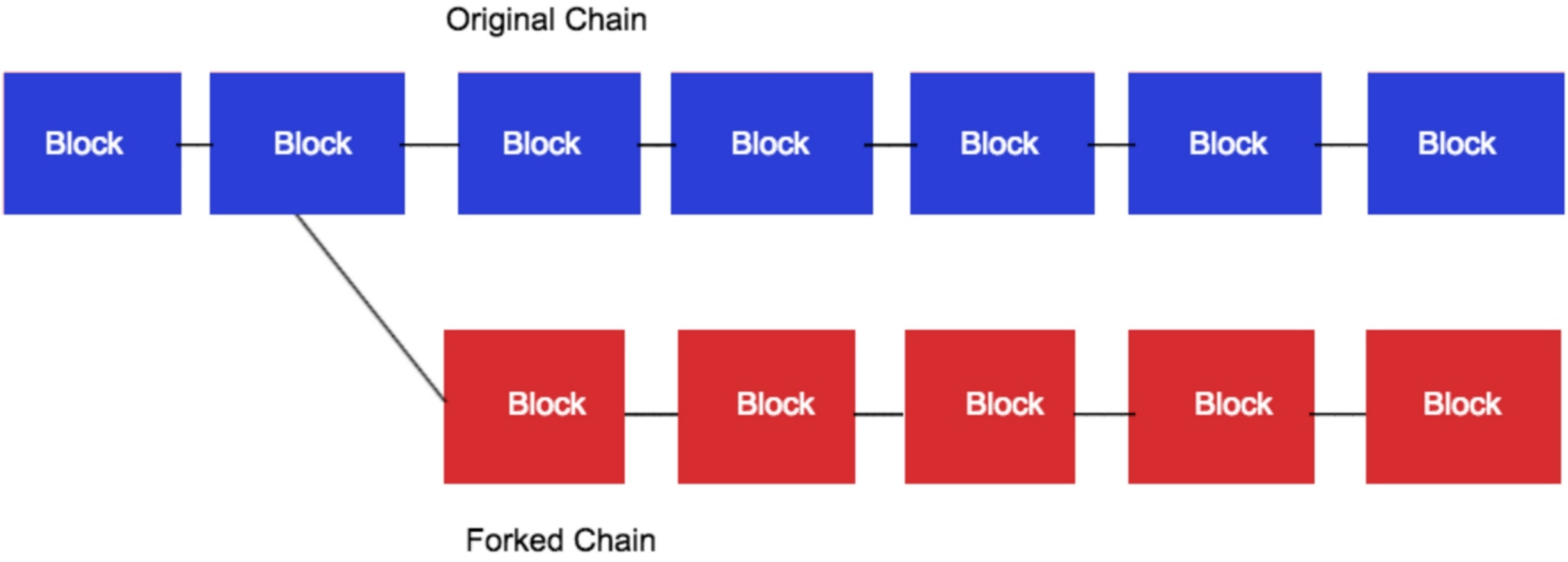
Role Of NONCE

- All the other components of block except the NONCE is fixed. The only component that the miner can change is the nonce.
- Miners change this nonce again and again till the time they get a hash that the required number of leading zeros.
- They iterate this nonce starting from 1 till the correct nonce.

Role of NONCE

- This iteration require a lot of computational power and all the miners are actually working to verify the same block.
- So the miner with highest computational speed will win the race.
- After he forms a correct block he/she broadcast this block in the network for other node to confirm and add this block in their local copy of chain.

Longest Chain Rule



UTXO Model

- Bitcoin works on the concept of UTXO model
- UTXO stands for the Unspent Transaction Output. It behaves like Cash.
- Example – User 1 has 3 UTXO’s of 0.4 BTC, 0.7BTC and 0.3 BTC
- User2 has 0.1 BTC and 0.4BTC
- If user1 want to send 0.9BTC to user2 he will send 0.7 and 0.3 BTC to user 2 and user to will return back 0.1BTC.