BLOCKCHAIN

Unit3: Class 2

2. Consensus Algorithm – Proof of Work(PoW)

- The objective of consensus algorithm is to which block do we add next. There are multiple miners in the blockchain network. Each of them proposes a new block based on the transactions it heard about. It is not necessary that every miner proposes a same block. Whatever transactions they received till now, based on that, they create block. But there is a threshold to include number of transactions in a block.

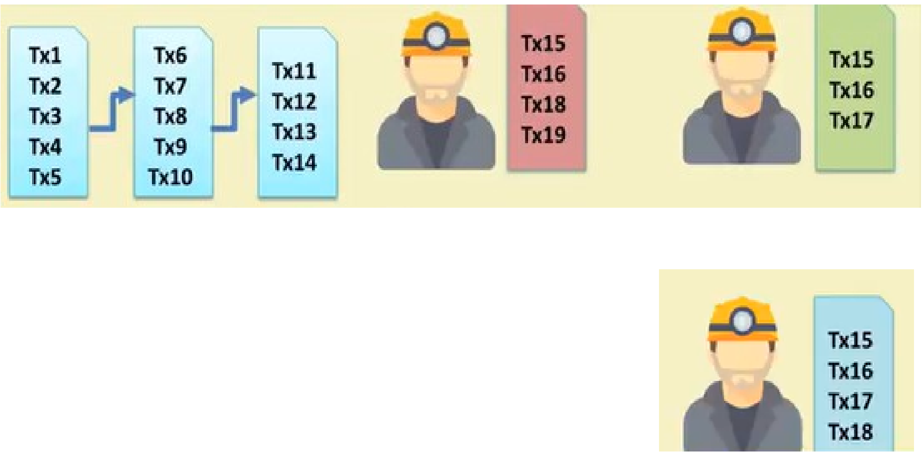

Fig. 1

- In Fig.1, there are there miners, each of them proposes a new block. Which block do we add next, out of three proposed block.
- The challenge is, miners do not know each other, Because it is open network, it is permission less network. Anyone can participate in the network as a miner and they can propose a block.
- Any valid block can be accepted. Valid block means block with all valid transactions. In Fig.1, transactions 11,12,13,14 has already been committed. So we do not need to include those transactions again in a new block. So miners can propose a new block my excluding the transaction which has already committed in the blockchain.
- Once valid block is accepted, broadcast accepted blocks to peers.

- The idea for Proof of Work(PoW) was first published in 1993 by Cynthia Dwork and Moni Naor and was later applied by Satoshi Nakamoto in the Bitcoin paper in 2008. It is Competitive consensus algorithms where each mining node on the blockchain is competing to secure blocks.. Every node who is competing to add block to blockchain has to do some computing work.
- It was originally developed to prevent denial of service attacks and other services like spam on network.
- The Proof of Work consensus algorithm involves solving a computational challenging puzzle in order to create new blocks in the Bitcoin blockchain. The process is known as 'mining', and the nodes in the network that engage in mining are known as 'miners'.
- When a miner finally finds the right solution, the node broadcasts it to the whole network at the same time,
- Energy consuming part is solving the 'hard mathematical problem' to link the new block to the last block in the valid blockchain.

2.1 Idea

Find or generate a value which is

- Difficult to generate (in terms of CPU power)
- And yet easily verifiable

2.2 Mathematical Puzzle-HashCash :Example:

- Block hash should have n leading zeros
- If n=4, block hash should have 4 leading zeros
- 0000AC23EF32DD3422…

Generate Nonce (may be by Brute force) Such that:

- Combination of nonce and block data generates the leading zeros.
- More the value of n more the difficulty

Each node(miners) needs to solve math puzzle to propose transaction. Lot of computation, power and time. Finding hash value based on the input message + hash value of the previous block. Math puzzle should be less than the difficulty level of the systems. Once puzzle is solved, all other nodes should agree to solution. The node that is first solve, rewarded for his work

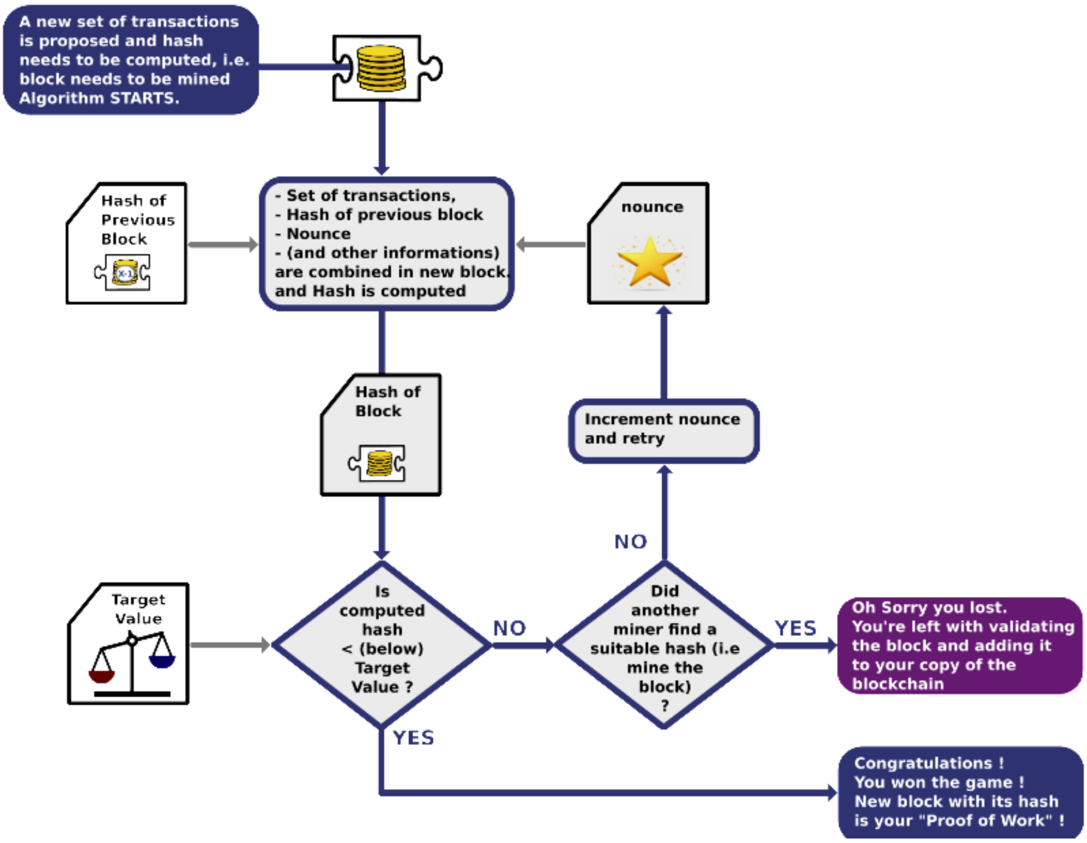
A new set of transactions is proposed and hash needs to be computed, i.e. block needs to be mined Algorithm STARTS.
Hash of Previous Block
- Set of transactions,
- Hash of previous block
- Nounce
- (and other informations) are combined in new block. and Hash is computed
nounce
Hash of Block
Increment nounce and retry
NO
Target Value
Is computed hash < (below) Target Value ?
NO
Did another miner find a suitable hash (i.e mine the block) ?
YES
Oh Sorry you lost. You're left with validating the block and adding it to your copy of the blockchain
YES
Congratulations ! You won the game ! New block with its hash is your "Proof of Work" !

Fig. 2

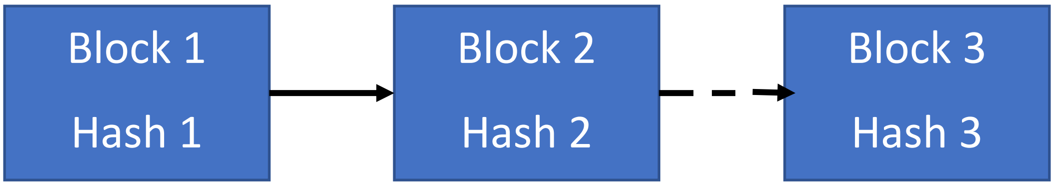

Fig. 3

Example:

- New Block, block 3 needs to be added to the existing chain as in Fig. 3. Every miners in the network will take this challenge.

- Calculate hash3
  - H(Block 3,hash 2, Nonce) < Difficulty level (0000000….234)
  - Incrementing nonce help in solving puzzle

Example:

- Iteration 1- H(Block 3, hash 2, 1) < Difficulty level (0000000….234) outcome –No
- Iteration 2- H(Block 3, hash 2, 2) < Difficulty level (0000000….234) outcome –No
- …
- Iteration 2000007- H(Block 3, hash 2, 2000007) < Difficulty level (0000000….234) outcome –yes
- Verification by other nodes using nonce=2000007

2.3 Cryptocurrencies using PoW:

- Litecoin
- Ethereum
- Monero coin
- Dogecoin

Miners receive 12.5 bitcoins for finishing first

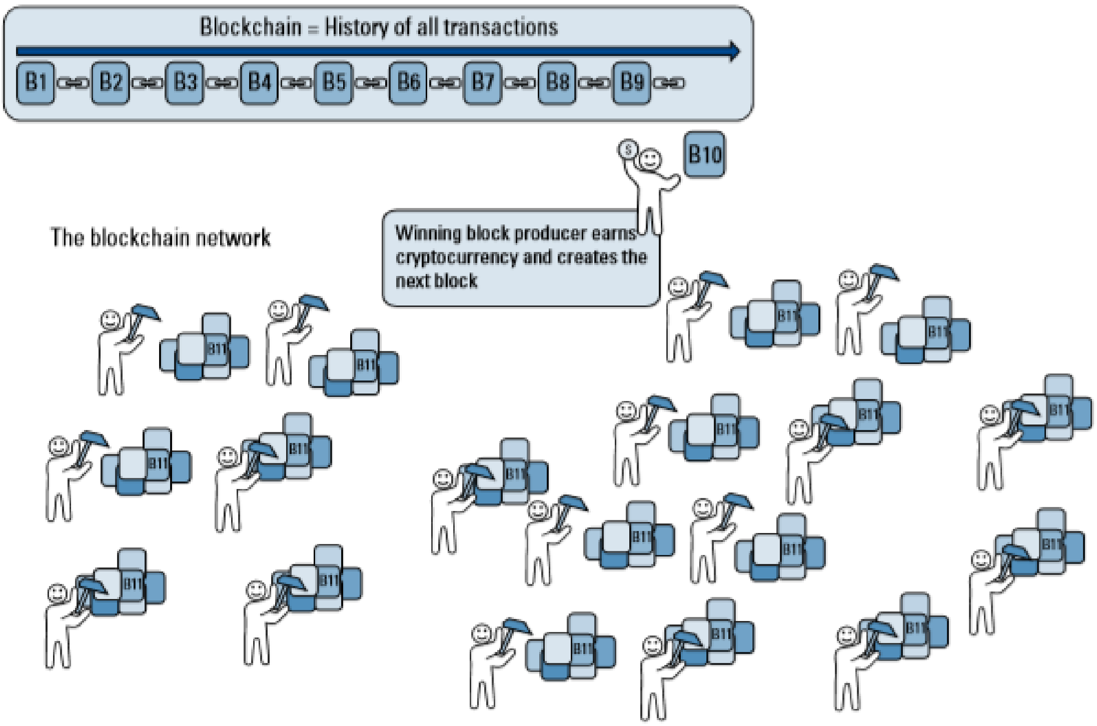
Blockchain = History of all transactions
B1
B2
B3
B4
B5
B6
B7
B8
B9
B10
The blockchain network
Winning block producer earns cryptocurrency and creates the next block
B11

Fig. 4

- Protected from corruptions as long as 51% or more of the block being created by miners are legitimate

2.4 Pros:

- It has been tested since 2009 and still works great
- It is slower and safer- you know your transaction will not be rolled back.
- It is trustless - no one can block your transaction from processing. If you want to send and/or receive money from someone you don't need to trust in third-party services.

2.5 Cons:

- It is slow- you have to wait for your transaction to be confirmed.
- It is costly- transaction costs can go up with the number of users.
- It is susceptible to centralization over time- those with the most resources can pool together their efforts in mining.