Mining and Consensus

raed**RASHEED**

Mining

- The purpose of mining is not the creation of new bitcoin. That’s the incentive system.
- Mining is the mechanism by which bitcoin’s security is decentralized.
- Miners validate new transactions and record them on the global ledger.
- A new block, containing transactions that occurred since the last block, is “mined” every 10 minutes on average, thereby adding those transactions to the blockchain.

Mining

- Miners receive two types of rewards in return for the security provided by mining:
  - new coins created with each new block, and
  - transaction fees from all the transactions included in the block.
- The solution to the problem, called the Proof-of-Work, is included in the new block and acts as proof that the miner expended significant computing effort.

Consensus Models

- Proof of Work Consensus Model.
- Proof of Stake Consensus Model.
- Round Robin Consensus Model.
- Proof of Authority/Proof of Identity Consensus Model.
- Proof of Elapsed Time Consensus Model.

Proof of Work Consensus Model

- In the proof of work (PoW) model, a user publishes the next block by being the first to solve a computationally intensive puzzle.
- The puzzle is designed such that solving the puzzle is difficult but checking that a solution is valid is easy.
- This enables all other full nodes to easily validate any proposed next blocks, and any proposed block that did not satisfy the puzzle would be rejected.
- The target value may be modified over time to adjust the difficulty (up or down) to influence how often blocks are being published.

Proof of Work Consensus Model

- For example, Bitcoin, which uses the proof of work model, adjusts the puzzle difficulty every 2016 blocks to influence the block publication rate to be around once every ten minutes.
- The adjustment is made to the difficulty level of the puzzle, and essentially either increases or decreases the number of leading zeros required.
- Adjustments to the difficulty target aim to ensure that no entity can take over block production.

Proof of Stake Consensus Model

- The proof of stake (PoS) model is based on the idea that the more stake a user has invested into the system, the more likely they will want the system to succeed, and the less likely they will want to subvert it.
- Stake is often an amount of cryptocurrency that the blockchain network user has invested into the system.
- With this consensus model, there is no need to perform resource intensive computations (involving time, electricity, and processing power) as found in proof of work.

Round Robin Consensus Model

- Within this model of consensus, nodes take turns in creating blocks.
- To handle situations where a publishing node is not available to publish a block on its turn, these systems may include a time limit to enable available nodes to publish blocks so that unavailable nodes will not cause a halt in block publication.
- This model ensures no one node creates the majority of the blocks.

Proof of Authority/Proof of Identity Consensus Model

- The proof of authority (also referred to as proof of identity) consensus model relies on the partial trust of publishing nodes through their known link to real world identities.
- Publishing nodes must have their identities proven and verifiable within the blockchain network.

Proof of Elapsed Time Consensus Model

- Within the proof of elapsed time (PoET) consensus model, each publishing node requests a wait time from a secure hardware time source within their computer system.
- The secure hardware time source will generate a random wait time and return it to the publishing node software.
- Publishing nodes take the random time they are given and become idle for that duration.
- Once a publishing node wakes up from the idle state, it creates and publishes a block to the blockchain network, alerting the other nodes of the new block; any publishing node that is still idle will stop waiting, and the entire process starts over.

The difficulty of mining

- The difficulty of mining a bitcoin block is approximately 10 minutes of processing for the entire network, based on the time it took to mine the previous 2,016 blocks, adjusted every 2,016 blocks.
- This is achieved by lowering or raising the target.

New Target = Old Target * (Actual Time of Last 2016 Blocks / 20160 minutes)