SNS COLLEGE OF ENGINEERING

Kurumbapalayam (Po), Coimbatore – 641 107 An Autonomous Institution Accredited by NBA – AICTE and Accredited by NAAC UGC wit'A' Grade Approved by AICTE, New Delhi & Affiliated to Anna University, Chennai

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING IOT Including CS&BCT

COURSE NAME : DISTRIBUTED LEDGER TECHNOLOGY

TOPIC: Block Mining

Introduction to Block Mining

Block mining is a critical process in the Bitcoin network where miners compete to add new blocks to the blockchain by solving complex mathematical puzzles. Mining ensures the security, integrity, and consensus of the network. It involves two main components: Proof of Work (PoW) and the creation of new Bitcoin through the block reward. Miners validate and confirm transactions, package them into blocks, and add them to the blockchain, securing the entire network from potential attacks or fraud.

The Mining Process

The process of mining in the Bitcoin network can be broken down into several stages:

1. Transaction Verification:
   - Before a new block is mined, miners verify all the transactions within the block to ensure their validity. This includes checking the digital signatures and ensuring that no double-spending occurs.
2. Constructing the Block:
   - Miners group valid transactions into a block. This block contains a block header (metadata about the block) and a block body (the list of transactions).
3. Solving the Cryptographic Puzzle:
   - To mine a new block, miners must solve a cryptographic puzzle based on the block header. The puzzle involves finding a hash value that meets the network's difficulty target.
   - Miners use computational power to try different values until they find the correct one, a process known as Proof of Work (PoW).
4. Block Addition and Propagation:
   - Once the correct hash is found, the miner broadcasts the new block to the network. Other nodes verify the solution, and if it's valid, the block is added to the blockchain, and the miner receives the block reward.

Bitcoin Mining Incentives

: Miners are incentivized to participate in the mining process in two main ways:

1. Block Reward:
   - The miner who successfully mines a block is rewarded with a set number of newly minted bitcoins (block reward). The current block reward as of 2020 is 6.25 BTC. This reward is halved approximately every four years, an event known as Bitcoin Halving.
2. Transaction Fees:
   - In addition to the block reward, miners also receive the transaction fees from the transactions included in the block. These fees are paid by users who wish to prioritize their transactions in the next block.
3. Increased Network Security:
   - Mining ensures that Bitcoin's decentralized network remains secure and resilient to attacks. By contributing computational power, miners also help maintain the integrity and immutability of the blockchain.

Mining Difficulty and Block Time

Difficulty Adjustment:

- The Bitcoin network adjusts the difficulty of mining every 2,016 blocks (roughly every two weeks). This adjustment ensures that the average time between blocks remains around 10 minutes, regardless of how many miners are participating in the network.
- When more miners join the network, the difficulty increases, and when miners leave, the difficulty decreases. This ensures the stability of the network's block creation rate.

Block Time:

- The block time is the time it takes for a miner to successfully mine a block. Bitcoin aims for an average block time of 10 minutes. If miners are finding blocks too quickly, the difficulty will increase to slow them down, and if it’s too slow, the difficulty will decrease.

Mining Pools:

- To improve their chances of mining a block and earning rewards, miners often join mining pools. These pools combine the computational power of many miners, allowing them to share the rewards based on each participant's contribution to solving the cryptographic puzzle.