UNIT IV DISTRIBUTED CONSENSUS

Types of Consensus Algorithms: Proof of Stake, Proof of Work, Delegated Proof of Stake, Proof Elapsed Time, Deposite-Based Consensus, Proof of Importance, Federated Consensus or Federated Byzantine Consensus, Practical Byzantine Fault Tolerance. Block chain Use Case: Supply Chain Management.

What is the Consensus Mechanism?

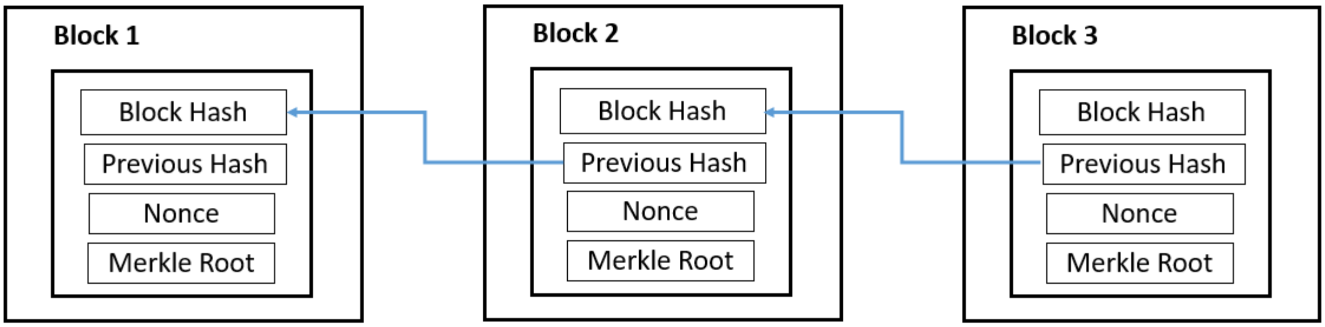
In simple terms, **Consensus** means achieving a decision state with which all network participants agree. For instance, a group of friends agrees to play football without conflicts. Here, deciding to play football together is a state of consensus or mutual agreement.

What is Proof-of-Work (PoW)?

Proof-of-Work (PoW) consensus mechanism is the oldest yet most popular. The idea first popped in 1993 when **Moni Naor and Cynthia Dowrk** published an article exploring the potential of algorithms to prevent fraud. Later, **Satoshi Nakamoto** coined the algorithm (an anonymous figure behind the discovery of Bitcoin) in his whitepaper on "Bitcoin: A peer-to-peer E-Cash system" in 2008.

PoW plays a significant role in the evolution of Blockchain Technology. **The idea is to create a verification system that is hard to crack**.

The **decentralized network** works on the principle of **not trusting but staying cooperative**. **Blockchain** (a decentralized network) **chain of linearly connected information-contained blocks** secured using cryptography. Here, each block contains the hash of its previous block to keep connected.



Moreover, every block contains several other pieces of information like timestamp, block height, transaction records, Merkle Root Hash, block hash, previous block hash, difficulty level, and many more in the block header. The other section contains a set of financial transactions whose hashes will eventually convert into the Merkle root. Hence, a blockchain is a chain of blocks of transactions.

Mining a Block

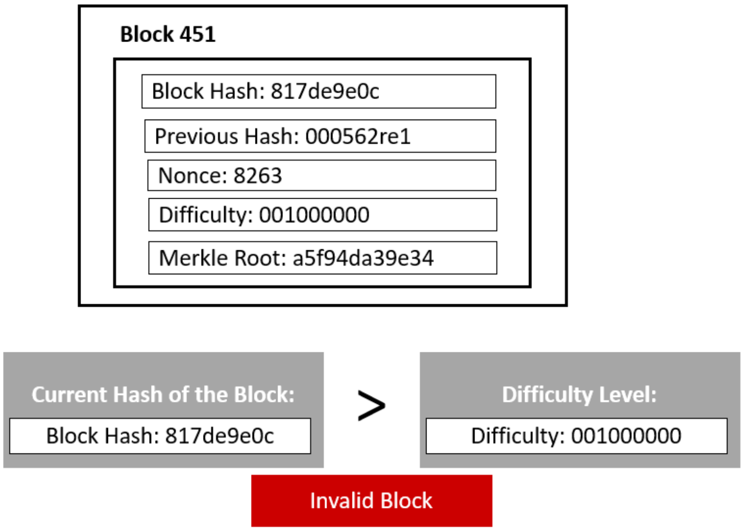
When it comes to **adding a new block to the chain**, it’s seen as a new update to the current system. Therefore, it requires network participants’ permission. To decide to add a new block or not, **Proof-of-Work (PoW)**, a consensus mechanism, is used. Only verified transactions get added to the network.
In contrast, not all blocks are valid. Most proposed blocks are considered invalid by the network. The Blockchain protocol defines the Block validity. A Blockchain network has an arbitrary “**Difficulty**” setting managed by the protocol, which changes how hard it is to mine a block. Here, **mining** means adding a new block.
Miners propose the new blocks in the chain. They are externals who wish to add their block to the network. The **work required to create a valid block** is where the value comes from. Miners receive rewards in proportion to their share of the computation power they spend to mine a new block. **By mining a valid block, the miner proves the work done**.
In Blockchains like the Bitcoin network or Ethereum, the difficulty level can change to ensure that blocks are created regularly.

How does the PoW Algorithm work?
A **Proof-of-Work (PoW) consensus algorithm** works so that each miner needs to cross the difficulty level to prove the block valid. A block is only marked as “**valid**” if the hash value of the entire block is below the difficulty hash.
Block Hash < Difficulty Hash
A block contains crucial transaction information that can’t be changed. So, the Miners change the **nonce** to get the hash lower than the difficulty threshold. The nonce is a block component that can be altered to achieve difficulty-level restrictions.
Let’s take an example to understand how it works.
Harry is a Bitcoin miner who wishes to add his block of Bitcoin (a digital currency) transactions to the network. However, to make his block valid. First, he has to change the block nonce until the hash of his block gets lower than the difficulty threshold.

Let’s say,

Harry’s block Hash: 817de9e0c
Difficulty Hash: 001000000
Nonce: 8263
For, this, Block Hash > Difficulty Hash, which is considered invalid.

817de9e0c1 > 001000000



Block 451

Block Hash: 817de9e0c

Previous Hash: 000562re1

Nonce: 8263

Difficulty: 001000000

Merkle Root: a5f94da39e34

Current Hash of the Block:
Block Hash: 817de9e0c

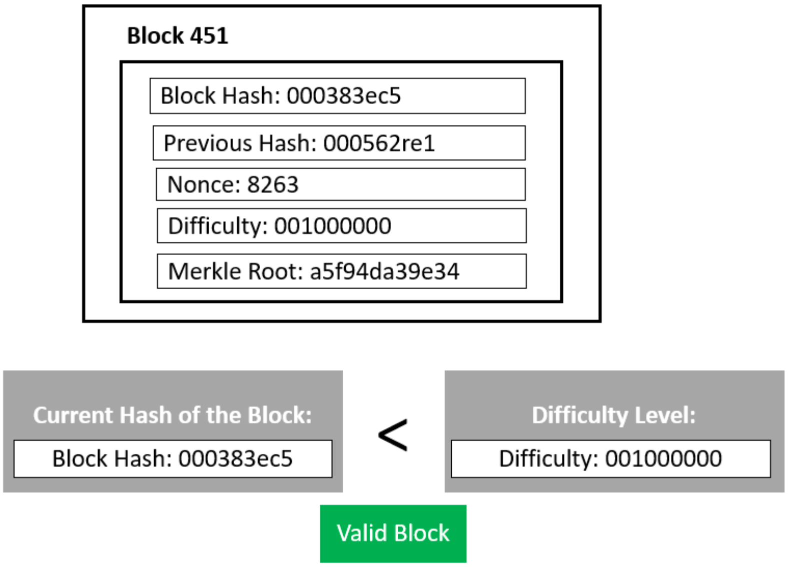
>

Difficulty Level:
Difficulty: 001000000

Invalid Block

Harry will change the nonce until he gets the first 3 digits as zeroes.
After continuously changing nonce for hours, he finally got the hash.

Harry's block Hash: 000383ec5
Difficulty Hash: 001000000
Nonce: 6778
Now, the difficulty threshold got achieved. **Block Hash < Difficulty Hash.**



Hence, Harry's block will be marked as valid and will get added to the blockchain. Harry gets a few bitcoins as block rewards for mining a block in the bitcoin blockchain for spending the computation power to find the valid hash.

This process is entirely based on chance. Hence, the miner's job is to change the nonce value until the overall block hash reaches lower than the difficulty hash. There are other responsibilities of miners, but that's a topic for another article.

Benefits of PoW

The following are the advantages of the Proof-of-Work (PoW) mechanism:

- **A hard-to-find solution. Yet, easy verification.**
- **Initial consensus mechanism**, PoW doesn't need the initial staking of coins before mining. One can start with 0 coins, and it will go only positive.
- **Easy to implement** in comparison with other blockchain consensus mechanisms.
- It is **fault-tolerant.** It means the failure of one component will not shut down the whole blockchain network.
- Give miners an **earning opportunity** for adding a block.
- PoW is the **oldest, most trusted, and most popular** consensus protocol.

Limitations of PoW

The following are the disadvantages of the Proof-of-Work (PoW) mechanism:

- **A lot of energy gets wasted as only one miner can eventually add its block.**

- **It requires heavy computation power** hence massive resource and energy consumption.
- A **51% attack** risk on the network. The controlling entity can acquire 51% to dominate the network.
- Spread **environmental hazards** using additional machinery.
- Pow is a **time and energy-consuming** process.
- It needed **heavy expenses** for hardware.
- Risk of **denial of service attacks** by intruders.

Which cryptocurrencies use PoW?

Following are the cryptocurrencies which are currently using Proof-of-Work (Pow):

- Bitcoin
- Ethereum
- Dogecoin
- Litecoin
- Monero
- Bitcoin Cash
- DigiByte
- Bitcoin Gold
- Ethereum Classic
- Zcash
- Kadena
- Bitcoin SV
- Ravencoin
- Siacoin
- Horizen

1. Introduction to Consensus Algorithms

- **Definition**: Consensus algorithms are protocols that consider a transaction valid and agree on the state of a distributed ledger.
- **Purpose**: They ensure all participants in a blockchain network agree on the same state of the blockchain, which is crucial for maintaining trust and security.

2. Overview of Proof of Work

- **Concept**: PoW is a consensus mechanism used to validate transactions and add new blocks to the blockchain.
- **First Implementation**: Introduced by Bitcoin in 2009 by Satoshi Nakamoto.
- **Goal**: To secure the network against attacks, especially Sybil attacks, and to determine which participant gets to add the next block.

3. How Proof of Work Works

- **Mining**: Participants (miners) compete to solve complex mathematical problems (hash puzzles).
- **Hash Function**: A cryptographic hash function (e.g., SHA-256 in Bitcoin) takes an input and produces a fixed-size output. The output must meet certain criteria (e.g., having a certain number of leading zeros).
- **Difficulty Adjustment**: The network adjusts the difficulty of the puzzles to ensure that blocks are added at a steady rate (approximately every 10 minutes for Bitcoin).

4. Process of Block Creation

1. **Transaction Collection**: Miners collect pending transactions from the memory pool.
2. **Block Formation**: Miners create a candidate block that includes:
   - A list of transactions
   - A reference to the previous block (hash)
   - A nonce (a random number)
3. **Hash Calculation**: Miners hash the block header, including the nonce. If the resulting hash meets the difficulty target, the block is considered valid.
4. **Block Broadcast**: Once a miner finds a valid hash, they broadcast the new block to the network.
5. **Block Verification**: Other nodes verify the block's validity and the included transactions before adding it to their own copy of the blockchain.

5. Advantages of Proof of Work

- **Security**: PoW is resistant to various types of attacks (e.g., double-spending) due to the computational effort required.
- **Decentralization**: No central authority is required; anyone can participate in mining.
- **Incentives**: Miners are rewarded with newly minted coins and transaction fees, promoting network participation.

6. Disadvantages of Proof of Work

- **Energy Consumption**: PoW is criticized for its high energy usage, as mining requires substantial computational power.
- **Centralization Risks**: Over time, mining can become centralized in large mining pools, which can undermine the decentralized ethos.
- **51% Attack**: If a single entity controls more than 50% of the mining power, they can manipulate the network (e.g., double spending).

7. Comparison with Other Consensus Algorithms

- **Proof of Stake (PoS)**: Unlike PoW, PoS selects validators based on the number of coins they hold and are willing to "stake" as collateral.
- **Delegated Proof of Stake (DPoS)**: A variation of PoS where stakeholders elect a small number of delegates to validate transactions.
- **Practical Byzantine Fault Tolerance (PBFT)**: A consensus mechanism designed for permissioned networks that requires a supermajority for agreement.

8. Future of Proof of Work

- **Hybrid Models**: Some projects are exploring hybrid consensus models combining PoW and PoS.
- **Environmental Concerns**: Increasing scrutiny over energy consumption is prompting discussions about more sustainable alternatives.
- **Regulatory Attention**: Governments are beginning to regulate mining activities due to their environmental impact.

9. Conclusion

- PoW remains a foundational technology in the blockchain space, particularly for Bitcoin.
- Understanding its mechanics, advantages, and challenges is crucial for anyone interested in blockchain technology and cryptocurrency.