

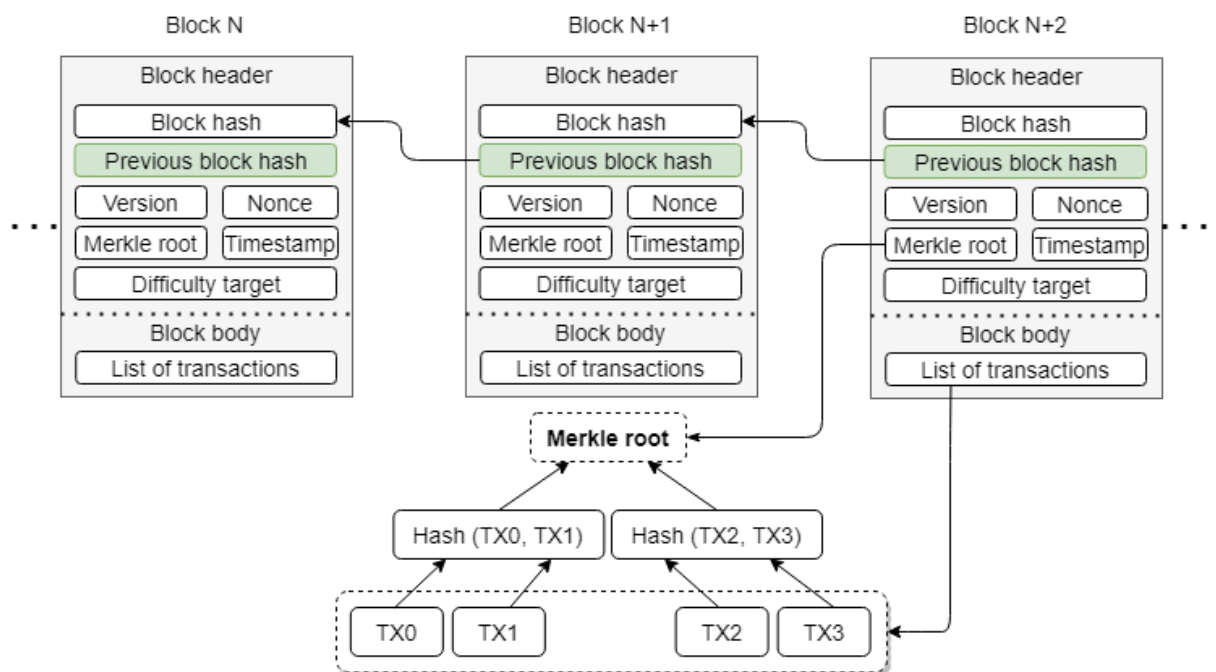
Theoretical Answer

1. **Blockchain Definition:** A blockchain is a digital ledger made up of linked blocks of data, where each block contains records of transactions. These blocks are connected using cryptographic hashes, making it nearly impossible to alter past records.

Real-life Use Cases:

- **Supply Chain Tracking:** Companies like Walmart use blockchain to trace the origin of food products (e.g., mangoes) to improve safety and transparency.
- **Digital Identity:** Projects like uPort or Aadhaar-on-Blockchain aim to give users control over their personal identity and documents without needing centralized servers.

2. Block Anatomy:



Merkle Root & Data Integrity:

The **Merkle root** is a hash that represents all transactions in a block. It is formed by hashing pairs of transaction hashes until one final root hash remains.

Example:

If a block has 4 transactions (T1, T2, T3, T4), their hashes (H1, H2, H3, H4) are combined as:

- $H12 = \text{hash}(H1 + H2)$
- $H34 = \text{hash}(H3 + H4)$

- Merkle Root = $\text{hash}(H_{12} + H_{34})$

If a hacker changes T1, H1 changes, altering the Merkle Root. This lets nodes instantly detect tampering, ensuring **data integrity**.

3. Consensus Conceptualization:

- **Proof of Work (PoW):**

PoW is a consensus method where miners compete to solve a complex mathematical puzzle (hashing with nonce) to add a new block. Solving it takes computational power and electricity, making attacks costly.

Example: Bitcoin uses PoW; miners solve hashes to earn BTC as reward.

- **Proof of Stake (PoS):**

In PoS, validators are chosen to create new blocks based on how many coins they “stake” (lock up). It’s energy-efficient since it doesn’t require solving puzzles.

Example: Ethereum 2.0 uses PoS where staking ETH increases chances of validating blocks and earning rewards.

- **Delegated Proof of Stake (DPoS):**

DPoS relies on token holders voting for a limited number of trusted validators (delegates) who produce blocks. It’s faster and more democratic.

Example: In EOS blockchain, users vote for 21 block producers to maintain the network.