Blockchain Basics

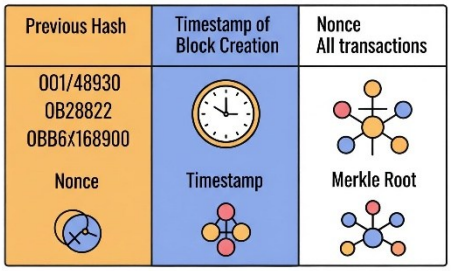
A blockchain is a decentralized digital ledger that records transactions across a network of computers in a secure, transparent, and immutable way. Each record, known as a block, contains transaction data, a timestamp, a cryptographic hash of its contents, and the hash of the previous block, forming a chain. Because blocks are linked and cryptographically secured, altering any block would require changing every subsequent block — a practically impossible task in a large network. Blockchain operates without a central authority, making it ideal for trustless systems like cryptocurrencies. It relies on consensus mechanisms like Proof of Work or Proof of Stake to validate new entries, ensuring all participants agree on the ledger's state.

Real-Life Use Cases:

Supply Chain Management: Track goods from source to destination, ensuring transparency and traceability (e.g., food safety).

Digital Identity: Store and verify identity documents securely without centralized databases (e.g., national ID systems).

Block Anatomy



Merkle Root Explanation (Example):

Merkle root is the top hash of a binary tree of all transaction hashes in a block.

Example: If a block has transactions A, B, C, D:

Hash A + B = H1, C + D = H2

Merkle root = hash(H1 + H2)

If any transaction changes, the root hash changes — enabling fast, secure verification of data integrity.

Consensus Conceptualization

Proof of Work (PoW):

PoW is a mechanism where validators (miners) solve complex mathematical puzzles to add a new block. This requires computational power and energy, ensuring that block creation is costly and deters tampering. It's used in Bitcoin and ensures security via difficulty.

Proof of Stake (PoS):

PoS selects validators based on how much cryptocurrency they stake. The more stake a user locks, the higher their chances to validate a block. It reduces energy consumption compared to PoW, as no puzzle-solving is required.

Delegated Proof of Stake (DPoS):

In DPoS, stakeholders vote to elect a few trusted validators (delegates) to create blocks. Voting power is based on stake. It’s faster and more scalable than PoW or PoS, used in platforms like EOS.