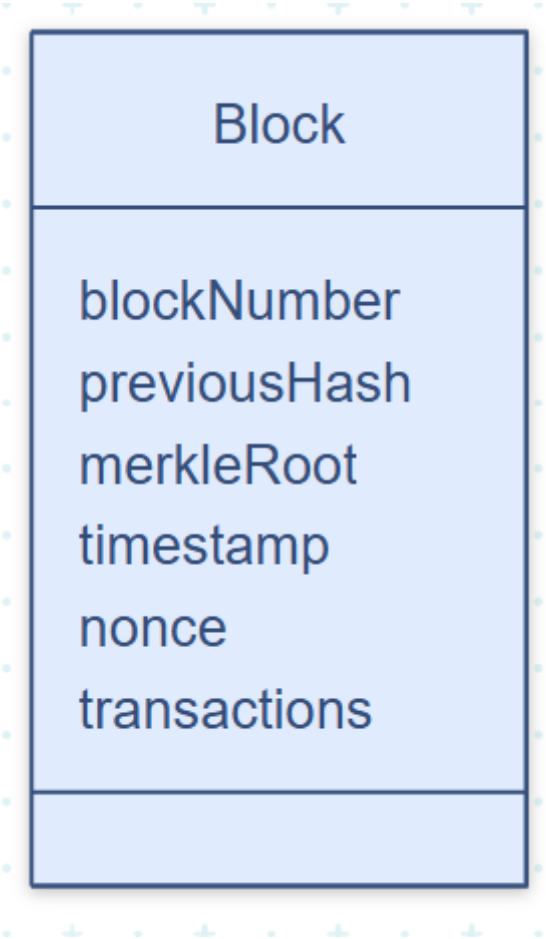
Blockchain Basics

A **blockchain** is a decentralized, distributed digital ledger that securely records transactions across a network of computers. Each block in the chain contains a set of transactions, a timestamp, and a cryptographic hash of the previous block, ensuring immutability and chronological integrity. Once data is recorded, altering it without altering all subsequent blocks and gaining majority consensus is nearly impossible, making the system tamper-resistant. Blockchain operates without a central authority, relying on consensus mechanisms like Proof of Work or Proof of Stake to validate transactions. It promotes transparency, traceability, and trust in multi-party systems.

Real-life Use Cases:

1. **Supply Chain Management** – Track goods from origin to delivery, ensuring authenticity and reducing fraud.
2. **Digital Identity** – Secure and control personal identity data for authentication and verification.

Block Anatomy



Merkle Root Explanation

The **Merkle root** is a single hash value that represents all transactions in a block by repeatedly hashing pairs of transaction hashes until one root hash remains. This allows efficient and secure verification of individual transactions without revealing the entire dataset.

Example: Suppose a block has 4 transactions: T1, T2, T3, and T4.

- Hashes: H1 = hash(T1), H2 = hash(T2), H3 = hash(T3), H4 = hash(T4)
- Pairwise: H12 = hash(H1 + H2), H34 = hash(H3 + H4)
- Merkle Root = hash(H12 + H34)

If someone wants to verify T1, they only need H2 and H34, not the whole block. This helps verify data integrity efficiently.

Consensus Conceptualization

What is Proof of Work and why does it require energy?

Proof of Work (PoW) is a consensus mechanism where miners compete to solve complex mathematical puzzles to add a block to the blockchain. Solving these puzzles requires significant computational power and energy. This ensures security, as altering data would require redoing the PoW for all subsequent blocks, making attacks highly costly. Bitcoin uses PoW to maintain its network integrity.

What is Proof of Stake and how does it differ?

Proof of Stake (PoS) replaces miners with validators who are chosen to create new blocks based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. It's energy-efficient compared to PoW since it doesn't require solving complex puzzles. PoS incentivizes honest behavior because malicious validators risk losing their staked assets.

What is Delegated Proof of Stake and how are validators selected?

Delegated Proof of Stake (DPoS) involves token holders voting for a small number of delegates (validators) who are responsible for validating transactions and producing blocks. The top-voted delegates become active validators, and they rotate in generating blocks. This model is faster and more democratic but can be more centralized, depending on the voting power distribution.