Blockchain

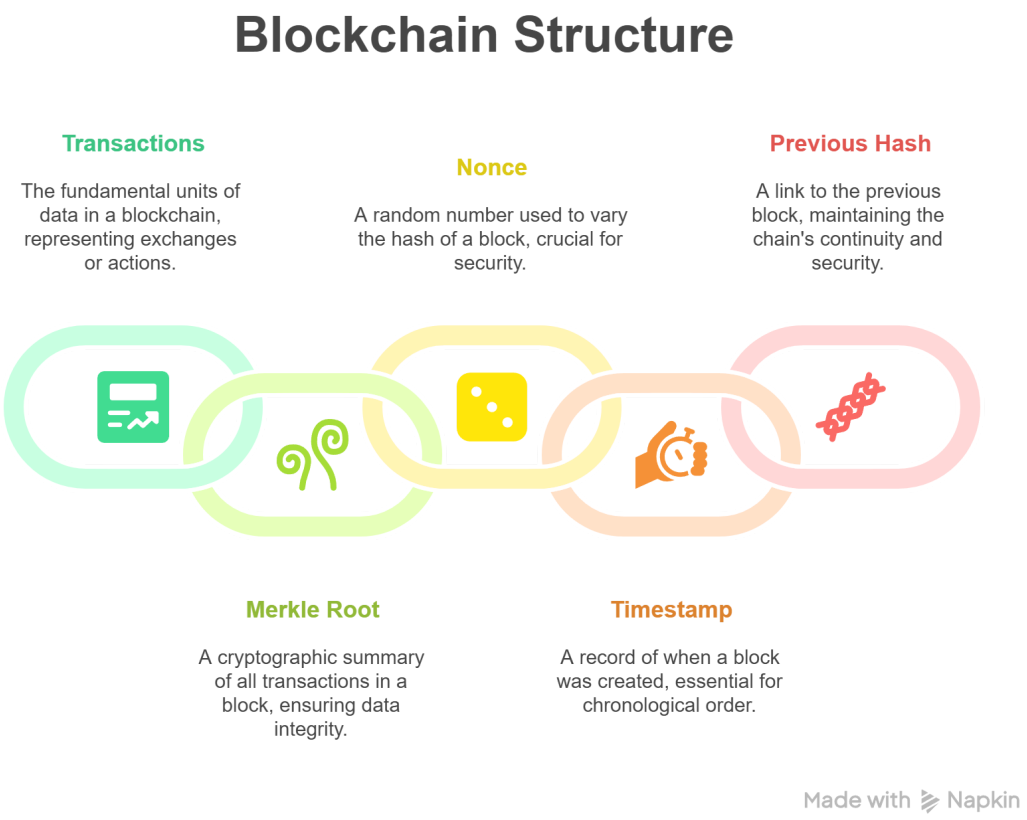
A blockchain is a decentralized and distributed digital ledger that records information in a secure, transparent, and tamper-proof way. It consists of a chain of blocks, where each block contains a set of data such as transactions, a timestamp, a unique hash, and the hash of the previous block. This linking of blocks creates a secure chain that makes it nearly impossible to alter previous records without changing every block that follows. Blockchain operates without a central authority, using consensus algorithms like Proof of Work or Proof of Stake to validate new entries. It ensures transparency, reduces the risk of fraud, and allows participants to trust the data without needing to trust each other.

Real-life Use Cases:

1. **Supply Chain Management:**
   Blockchain can track the movement of goods across different stages of production and delivery, making it easy to verify authenticity and reduce fraud or counterfeiting.

2. **Digital Identity:**
   Individuals can store their identity credentials (e.g., Aadhaar, passports, licenses) on a blockchain in a secure and verifiable way, allowing easy sharing of trusted identity proofs.

Structure of Blockchain



Merkle Root

The Merkle root is a single hash value that represents all the transactions within a block. It is derived by recursively hashing pairs of transactions until only one hash remains, Merkle root. This structure is called a Merkle Tree, and it plays a crucial role in ensuring data integrity in blockchain systems.

Working

Let's say a block contains 4 transactions:

- T1: A sends ₹100 to B
- T2: C sends ₹200 to D
- T3: E sends ₹50 to F
- T4: G sends ₹300 to H

1. First, each transaction is hashed:
   H1 = hash(T1), H2 = hash(T2), H3 = hash(T3), H4 = hash(T4)
2. Then, hash pairs are combined and hashed again:
   H12 = hash(H1 + H2), H34 = hash(H3 + H4)
3. Finally, these two are hashed to form the Merkle root:
   Root = hash(H12 + H34)

Verification

- Suppose someone tries to modify T2, changing the amount or recipient. This will change H2, which then changes H12, and finally changes the Merkle root.
- Since the Merkle root is stored in the block header, any such change will be immediately detectable because the newly calculated root won't match the stored one.
- Even if just one transaction is tampered with, the entire root hash changes, ensuring that no unauthorized edits go unnoticed.

Consensus Mechanism

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

Proof of Work (PoW) is a consensus algorithm used to validate new blocks by solving complex mathematical puzzles. Miners compete to find a solution (by adjusting the nonce) that results in a block hash below a certain target value. This process involves massive computations and trial-and-error, which consumes a lot of electricity and processing power. The high energy cost helps secure the network by making it expensive for attackers to manipulate the blockchain.

2. What is Proof of Stake and how does it differ?

Proof of Stake (PoS) is an energy-efficient alternative to PoW where validators are chosen to create new blocks based on the amount of cryptocurrency they “stake” or lock in the system. There’s no need for solving puzzles. The more coins a user stakes, the higher their chance of being selected. Unlike PoW, PoS saves energy, offers faster transaction speeds, and discourages attacks by putting validators’ own funds at risk.

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

In Delegated Proof of Stake (DPoS), token holders vote to elect a limited number of delegates or validators who are responsible for validating blocks and maintaining the network. Voting power is often proportional to the amount of cryptocurrency staked. DPoS increases speed and efficiency while allowing the community to hold validators accountable—if a delegate misbehaves or becomes inactive, they can be replaced through a voting process.