What is Blockchain ?

Blockchain is a decentralized and distributed digital ledger that records transactions across a network of computers in a secure, transparent, and tamper-resistant manner. Each record, or "block," contains a list of transactions, a timestamp, a cryptographic hash of the previous block, and a nonce, forming a continuous chain.

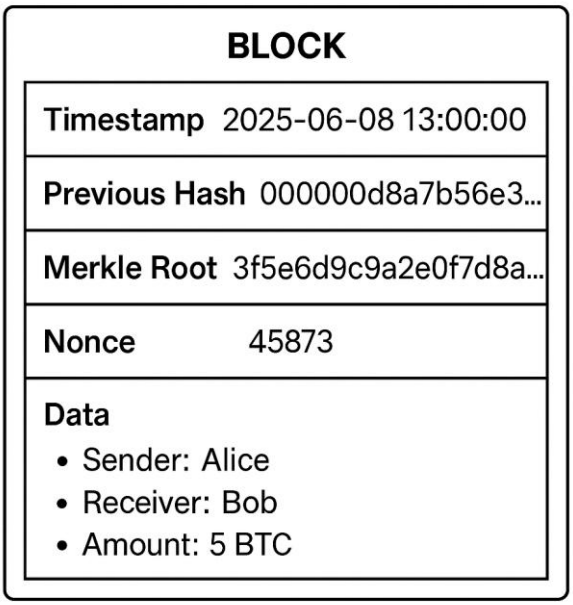
This structure ensures that once data is recorded, it cannot be altered without changing all subsequent blocks, which requires consensus from the network. Blockchain operates without a central authority, relying on consensus mechanisms like Proof of Work or Proof of Stake to validate transactions.

It enhances trust, reduces fraud, and increases efficiency in processes such as supply chain tracking, digital identity verification, and cryptocurrency systems like Bitcoin. Its core strengths lie in immutability, transparency, and decentralization, making it a transformative technology across industries.

Real life use cases of Blockchain

1. **Supply Chain Management**
   Blockchain provides end-to-end visibility in supply chains by recording each step a product takes, from origin to delivery. For example, in the food industry, companies like IBM and Walmart use blockchain to trace the journey of food items. If a contamination issue arises, blockchain allows companies to quickly identify the source and location of the affected batch, reducing waste and enhancing food safety.
2. **Digital Identity Verification**
   Blockchain can securely store and manage personal identification data. Instead of relying on centralized databases vulnerable to breaches, individuals can control their own identity information through a blockchain wallet. For example, governments and organizations use blockchain for secure ID systems that enable faster, tamper-proof access to services like banking, healthcare, and voting.

Block Anatomy



How the Merkle root helps verify data integrity ?

The **Merkle root** is a single hash that represents all the transactions in a block. It is derived by repeatedly hashing pairs of transaction hashes until one final hash (the root) remains. This root allows efficient and secure verification of any transaction within the block.

If even one transaction is altered, its hash changes, which then alters all parent hashes up to the Merkle root. Thus, any tampering is immediately detectable by comparing the current Merkle root with the original.

Example:

Imagine 4 transactions: T1, T2, T3, T4

1. Hash each:
   H1 = hash(T1), H2 = hash(T2), H3 = hash(T3), H4 = hash(T4)
2. Pair and hash again:
   H12 = hash(H1 + H2), H34 = hash(H3 + H4)
3. Merkle Root = hash(H12 + H34)

To verify T3, you only need H3, H4, and H12. If T3 is altered, the final Merkle root won't match, proving tampering.

This method ensures **data integrity** with minimal data and computation.

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

Proof of Work (PoW) is a consensus mechanism used in blockchains like Bitcoin to validate and add new blocks to the chain. It requires participants, known as miners, to solve complex mathematical puzzles by repeatedly hashing data until they find a hash that meets a specific condition (usually a number of leading zeros). This process is deliberately hard to ensure fairness and security, making it nearly impossible for any single entity to take control of the network.

It requires significant **computational power and energy** because miners must perform **trillions of hash calculations per second** to find a valid solution. This massive computation consumes electricity, which is why PoW-based blockchains are often criticized for their high energy usage. However, the energy cost also acts as a deterrent against attacks, since altering the blockchain would require redoing all that work.

What is Proof of Stake and how does it differ?

Proof of Stake (PoS) is a consensus mechanism where validators are chosen to create new blocks and verify transactions based on the amount of cryptocurrency they "stake" or lock up as collateral. The more coins a participant stakes, the higher their chances of being selected to validate the next block. Unlike Proof of Work, PoS does not involve solving complex mathematical problems, making it much more energy-efficient.

The key difference from **Proof of Work** is in how consensus is achieved: PoW relies on computational effort (and energy), while PoS relies on economic stake. PoS reduces energy consumption drastically and makes attacks more costly, as attackers would need to own and risk large amounts of the currency. Popular PoS-based blockchains include Ethereum (after its 2022 upgrade), Cardano, and Polkadot.

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

Delegated Proof of Stake (DPoS) is a variation of Proof of Stake designed to increase speed and scalability in blockchain networks. In DPoS, token holders don’t directly validate blocks—instead, they **vote for a small group of trusted delegates (also called witnesses or validators)** who are responsible for validating transactions and creating new blocks. Voting power is typically proportional to the amount of tokens a user holds.

Validators in DPoS are selected through a **continuous voting process**, where token holders elect a fixed number of delegates (e.g., 21 in EOS). These delegates take turns producing blocks, and if they act dishonestly or perform poorly, they can be voted out and replaced. This system ensures efficiency and democratic participation while maintaining decentralization and network integrity.