Definition of Blockchain

- Blockchain is a **digital ledger** used to record transactions in a secure and decentralized manner.
- It stores data in units called **blocks**, which are linked using cryptographic hashes, forming a **chain**.
- Each block contains:
    - Transaction data
    - Timestamp
    - Its own hash
    - Hash of the previous block
- Once a block is added, it is **nearly impossible to alter** without changing all following blocks.
- It operates without a central authority, relying on **consensus mechanisms** like Proof of Work or Proof of Stake.
- Blockchain ensures:
    - **Transparency**
    - **Data integrity**
    - **Security**
- Popularly used in **cryptocurrencies** like Bitcoin, but also useful in many other industries.

2 Real-Life Use Cases of Blockchain

1. Supply Chain Management

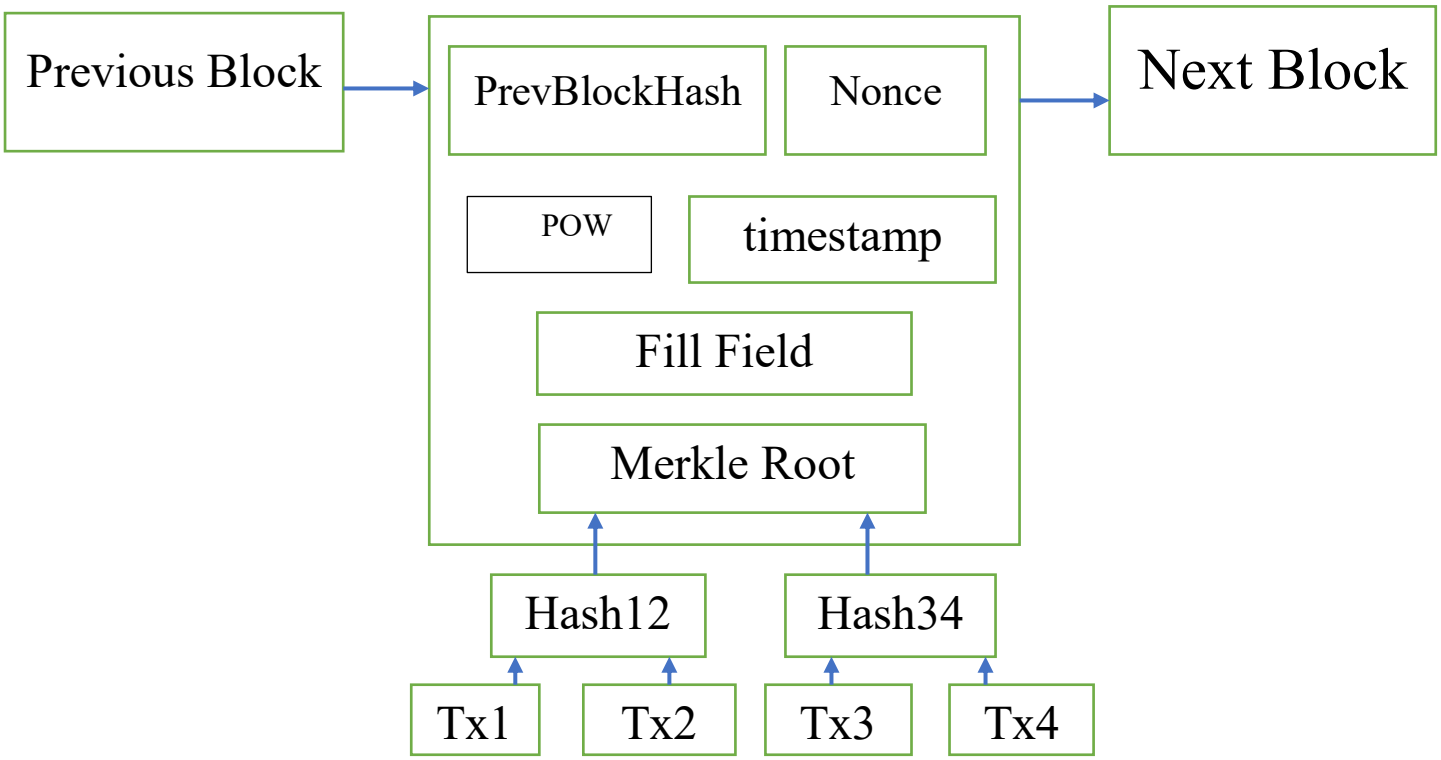
- Example: Walmart uses blockchain to track the origin of food items (like mangoes or pork).
- How it works: Each step in the supply chain (farm, processor, distributor, store) adds data to the blockchain.
- Benefits:
    - Improves transparency
    - Quickly identifies sources of contamination
    - Reduces food fraud and delays

2. Digital Identity

- Example: Estonia uses blockchain to manage citizen digital IDs.
- How it works: Citizens control their personal data and authorize who can access it (e.g., banks, hospitals).
- Benefits:
    - Data privacy and ownership
    - Prevents identity theft

- Speeds up verification processes

Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.



Explanation of Merkle Root and Data Integrity

- **What is Merkle Root?**
  The Merkle root is a single hash value that represents all the transactions (data) in a block. It is created by repeatedly hashing pairs of transaction hashes until only one hash remains—the Merkle root.
- **How it helps verify data integrity:**
  Instead of checking every transaction individually, you can check just the Merkle root to confirm if the data in the block has been tampered with.

Suppose a block contains four transactions:

Tx1, Tx2, Tx3, Tx4

Hash each transaction:

H1 = hash(Tx1)

H2 = hash(Tx2)

H3 = hash(Tx3)

H4 = hash(Tx4)

Pairwise hash:

H12 = hash(H1 + H2)

H34 = hash(H3 + H4)

Finally, hash the pair:

Merkle Root = hash(H12 + H34)

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

Proof of Work is a consensus algorithm where participants (called miners) compete to solve complex mathematical puzzles to validate transactions and add blocks to the blockchain. This process is called mining. Solving the puzzle requires significant computational power, which consumes a large amount of electricity and energy. The first miner to find a valid solution gets to add the block and earn a reward. PoW ensures network security but is energy-intensive and slower compared to other methods.

What is Proof of Stake (PoS) and how does it differ?

Proof of Stake selects validators based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. Unlike PoW, PoS does not involve solving puzzles, so it is energy-efficient. Validators are randomly chosen to propose and validate new blocks, depending on their stake size and sometimes other factors like coin age. This reduces the need for powerful hardware and electricity. PoS promotes eco-friendliness and allows faster transaction processing.

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

Delegated Proof of Stake improves PoS by introducing a voting system. Token holders vote to elect a small group of trusted validators (also called delegates or witnesses) who are responsible for verifying transactions and adding blocks. The more tokens a user holds, the more voting power they have. This makes the system faster and more scalable, but slightly more centralized. Validators can be voted out if they act dishonestly or become inactive.