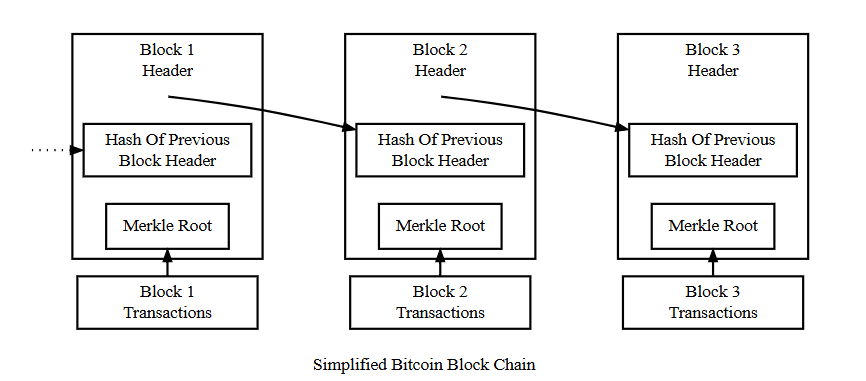
**Blockchain Basics**

A **blockchain** is a decentralized and distributed digital ledger that records transactions in a secure, transparent, and tamper-proof manner. Each record, known as a block, is linked to the previous one using cryptographic hashes, forming a chain. Instead of relying on a central authority, blockchain networks are maintained by multiple nodes that validate and agree on transactions through consensus mechanisms. This ensures transparency, immutability, and security of data. Blockchains are widely used in cryptocurrencies, but their utility spans many industries, making them a foundational technology for trustless systems.

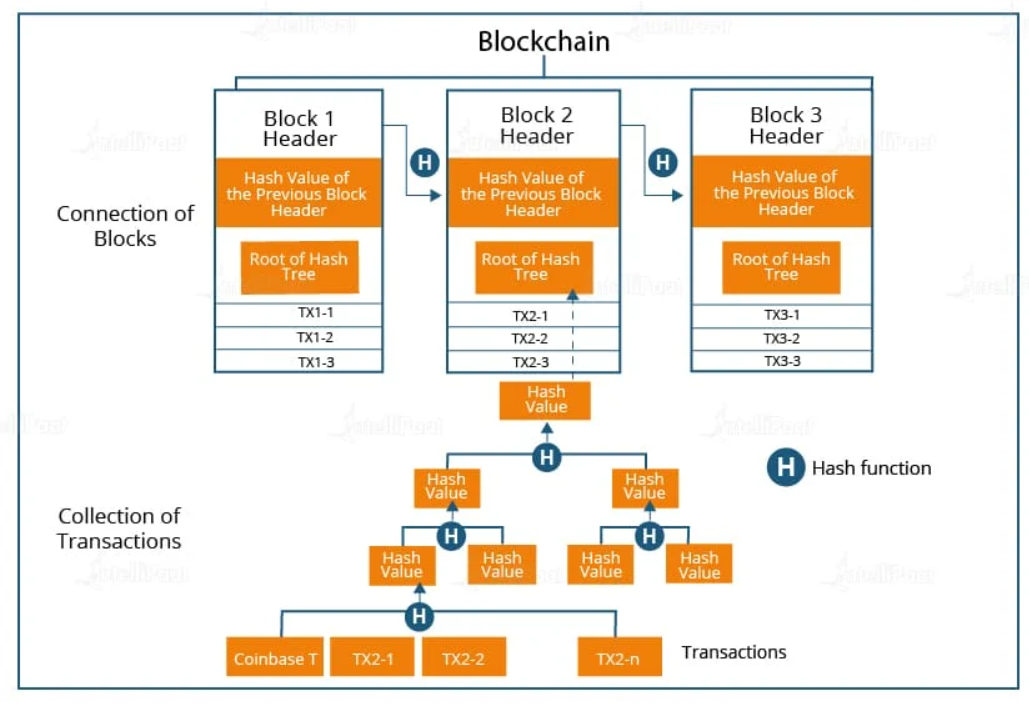
**Real-life use cases:**

1. **Supply Chain Management** – Blockchain provides end-to-end visibility and traceability for goods, reducing fraud and increasing efficiency.
2. **Digital Identity Verification** – Users can control and share their identity securely, reducing identity theft and fraud.

**Block Anatomy**

**Merkle Root & Data Integrity:**

The **Merkle root** is a hash that represents all transactions in the block. Transactions are paired and hashed repeatedly until a single hash remains – this is the Merkle root.  
*Example:* If one transaction (say, Tx2) is altered, its hash changes, which changes the hashes above it and eventually the Merkle root. This alerts the network that data has been tampered with, ensuring data integrity efficiently without checking every single transaction.



**Consensus Conceptualization**

**Proof of Work (PoW):**  
PoW is a consensus mechanism where participants (miners) solve complex mathematical problems to validate transactions and create new blocks. This requires significant computational power and energy, making it difficult for any single entity to control the network. The energy cost is what makes the network secure, as altering the blockchain would require immense resources.

**Proof of Stake (PoS):**  
In PoS, validators are chosen based on the number of coins they "stake" or lock up in the network. Instead of solving puzzles, validators are randomly selected to propose blocks. It is energy-efficient compared to PoW and provides economic incentives for validators to act honestly, as malicious behavior can lead to loss of staked assets.

**Delegated Proof of Stake (DPoS):**  
DPoS involves stakeholders voting to elect a small number of delegates (validators) who are responsible for validating transactions and producing blocks. These delegates are rotated periodically. DPoS improves transaction speed and scalability but relies more on community governance and trust in elected delegates.