1. Blockchain Basics :-

A blockchain is a distributed digital ledger that records transactions in a secure, transparent, and immutable way. Each block in the chain contains a list of transactions, and once added, it cannot be altered without changing every subsequent block, which ensures data integrity. The blockchain is maintained by a network of nodes (computers) that validate and store copies of the ledger. Its decentralized nature removes the need for a central authority, making it ideal for trustless environments. Blockchain uses cryptographic techniques like hashing and consensus algorithms to ensure security and agreement among participants.

Real-life use cases:

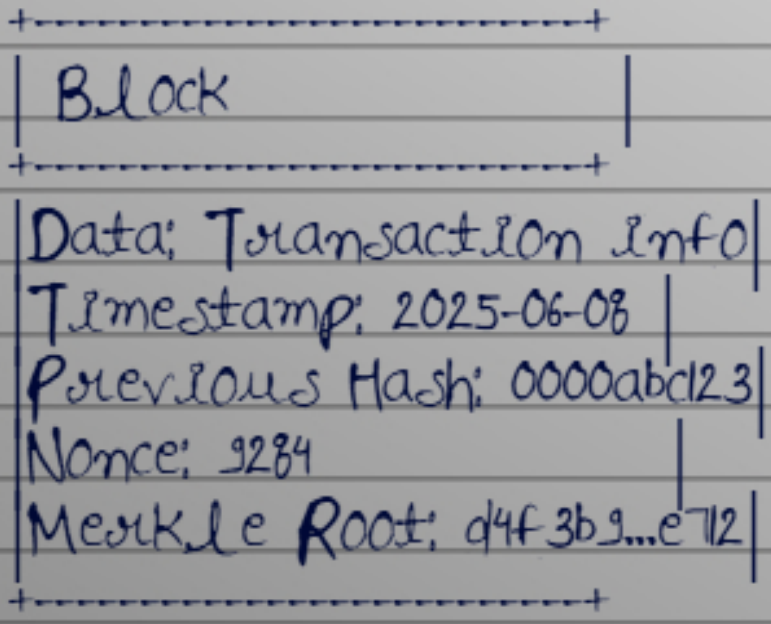
Supply Chain Management: Companies use blockchain to track products from

origin to delivery, ensuring transparency and reducing fraud.

Digital Identity: Blockchain helps individuals securely manage and verify their identities without relying on centralized entities.

2. Block Anatomy

Simple Block Diagram :-




Merkle Root Explanation (Example):
The Merkle root is a single hash that summarizes all transactions in a block. It is calculated by repeatedly hashing pairs of transactions until

one final hash remains. For example, if a block contains transactions A, B, C, and D, their hashes are combined as:

hashAB = hash(hash(A) + hash(B))

hashCD = hash(hash(C) + hash(D))

Merkle Root = hash(hashAB + hashCD)

If someone tampers with any transaction, the Merkle root changes, making it easy to detect data integrity breaches without checking each transaction.

3. Consensus Conceptualization :-

Proof of Work (PoW):

PoW is a consensus mechanism where miners compete to solve complex mathematical puzzles to add a new block to the blockchain. The first miner to find the correct solution broadcasts it to the network, and once verified, the block is added. This process requires significant computational power and energy, as it involves millions of calculations per second. PoW secures the blockchain

but is criticized for high energy consumption, like in Bitcoin mining.

Proof of Stake (PoS):
PoS selects validators to create new blocks based on the amount of cryptocurrency they "stake" or lock up as collateral. Unlike PoW, it doesn't require massive energy use or hardware. The higher the stake, the more likely a validator is chosen. PoS is more energy-efficient and scalable compared to PoW, making it popular in newer blockchains like Ethereum 2.0 and Cardano.

Delegated Proof of Stake (DPoS):
DPoS is a variation of PoS where coin holders vote to elect a small number of delegates (validators) to produce blocks and secure the network. Each vote's power depends on the amount staked by the voter. DPoS allows for faster transactions and more scalability by reducing the number of

validating nodes. Blockchains like EOS and TRON use this method, emphasizing governance and community participation.