1 . Blockchain Basics

- **Define blockchain in your own words (100–150 words).**
- **List 2 real-life use cases (e.g., supply chain, digital identity).**

Blockchain is a digital, distributed ledger where transactions are stored in a tamper-proof, open, and secure manner. Information is saved within each block, and the hash of the preceding block is referenced, forming a chain. Blockchain has no controlling authority, which positions it well for trustless systems. The information stored is immutable after it has been written, allowing for integrity and accountability. Blockchain supports cryptocurrencies, but it's implemented extensively across other industries.

Real-Life Use Cases:

- Healthcare Records
- Blockchain enables the secure, interoperable transfer of patient data across hospitals, enhancing care and minimizing medical mistakes.
- Voting Systems
- It provides transparent, secure online voting, rendering elections more trustworthy and safe.

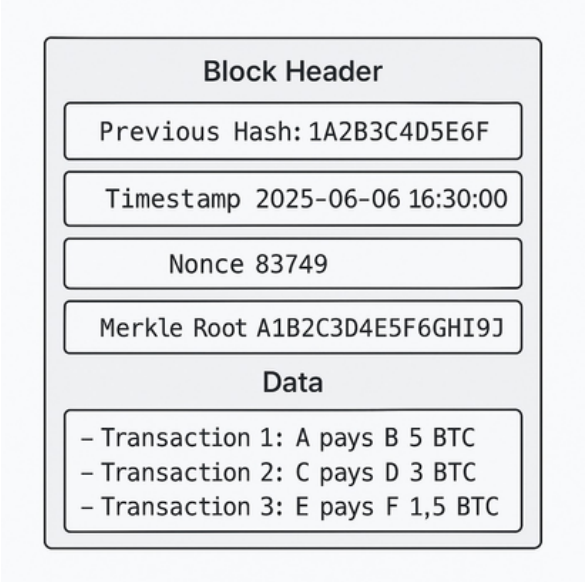
2.Block Anatomy

- **Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.**
- **Briefly explain with an example how the Merkle root helps verify data integrity.**

A Merkle root is the single hash value at the top of a Merkle Tree, built from the hashes of individual transactions. For example:

- Hash(Tx1), Hash(Tx2) → Hash1
- Hash(Tx3), Hash(Tx4) → Hash2
- Hash1 + Hash2 → Merkle Root

If any transaction is tampered with, its hash changes, which cascades upward and changes the Merkle Root. This makes it easy to verify if data has been modified without checking every transaction, ensuring integrity with minimal computation.



3. Consensus Conceptualization

- **Explain in brief (4–5 sentences each):**
  - **What is Proof of Work and why does it require energy?**
  -
  - **What is Proof of Stake and how does it differ?**
  -
  - **What is Delegated Proof of Stake and how are validators selected?**

Proof of Work (PoW)

Proof of Work is a consensus system in which members of the network (miners) race to solve difficult math puzzles to verify transactions and build new blocks. The winner solves the puzzle and gets to include the block and is rewarded. It uses a lot of computing power and electricity and is hence energy-guzzling. PoW is secure but ecologically wasteful, as with Bitcoin.

Proof of Stake (PoS)

Proof of Stake chooses validators depending on how many coins they "stake" or lock up as collateral. Validators are picked at random to make blocks and verify transactions, and the process is considerably more energy-friendly compared to PoW. It disallows malicious behavior by jeopardizing the validator's staked assets. Ethereum shifted to PoS in 2022 for improved scalability and sustainability.

Delegated Proof of Stake (DPoS)

In Delegated Proof of Stake, the coin holders vote to choose a small set of trusted validators (delegates) who get to generate the blocks. The voting power is directly proportional to the stake held to encourage democratic participation. DPoS enables faster processing of transactions and less energy consumption. It's employed in blockchains such as EOS and Tron to optimize for performance.