📘 Blockchain Basics

Q: Define blockchain in your own words (100–150 words):

A blockchain is essentially a decentralized digital ledger of information kept in a series of blocks that are cryptographically linked with one another. Each block contains a set of transactions or data, the unique hash of that block, and the hash of the previous block. This linkage ensures the integrity of information and makes the blockchain tamper-proof. It is distributed across many nodes (computers), so no single entity has control over the chain. Rather, its modification has to be agreed upon through consensus algorithms like Proof of Work or Proof of Stake. Blockchain technology does away with intermediaries to ensure transparency, security, and trust within peer-to-peer systems. This is most described as enabling cryptocurrencies like Bitcoin it's application beyond Finance.

Q: List 2 real-life use cases of blockchain:

1. **Supply Chain Management:**
   Blockchain helps track products from origin to delivery, ensuring transparency and authenticity (e.g., verifying if food is organic or ethically sourced).
2. **Digital Identity Verification:**
   Individuals can store and manage their personal credentials (IDs, certificates) securely on blockchain, reducing fraud and identity theft.

🧱 Block Anatomy

Q: Draw a block showing key components:

Here's a text representation of a block structure:

```
+------------------------------+
|       Block Structure        |
+------------------------------+
| Index: 2                     |
| Timestamp: 2025-06-09 21:00  |
| Data: {"amount": 100}        |
| Nonce: 54321                 |
| Previous Hash: a1b2c3...     |
| Merkle Root: f9d8e7...       |
| Hash: 0000abc1...            |
+------------------------------+
```

Q: How does the Merkle root help verify data integrity?

The Merkle root is the single hash of all transactions in a block. It is created by hashing pairs of transactions up a binary tree (Merkle Tree) until one final root hash remains: for example, if a block has 4 transactions (A, B, C, D), hashes are generated like this H1=hash(A), H2=hash(B), H3=hash(C), H4=hash(D) H12 = hash(H1 + H2), H34 = hash(H3 + H4) Merkle Root = hash(H12 + H34) If any transaction is tampered with, the Merkle root changes. It helps detect and prevent fraud without checking every transaction manually.

⚖️ **Consensus Conceptualization**

Proof of Work (PoW) is a consensus mechanism in which miners compete to solve a complex mathematical puzzle discovering a hash that starts with certain number of zeroes the first to solve it gets to add the next block to the chain and earn a reward it requires energy because the miners must perform trillions of hash calculations then therefore high computational power has to be consumed this system ensures security and fairness it's energy-intensive

---

Q: What is Proof of Stake and how does it differ?

Proof of Stake (PoS) selects validators based on the amount of cryptocurrency they "stake" or lock up as collateral. Instead of competing through energy use, validators are chosen pseudo-randomly, often weighted by the amount staked. It is more energy-efficient than PoW and discourages malicious behavior by risking the validator's staked funds.

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

Delegated Proof of Stake (DPoS) improves on PoS by introducing a democratic layer. Token holders vote for a small number of delegates or validators who are responsible for validating transactions and maintaining the blockchain. These delegates are rotated or re-elected based on performance and reputation. It offers faster block times and scalability but relies more on trust in elected delegates.