BLOCKCHAIN ASSIGNMENT TASK 1

Q1: Define blockchain in your own words (100–150 words).

Blockchain is a distributed ledger technology that securely records transactions across multiple computers in a way that prevents tampering and ensures transparency. Instead of relying on a central authority, blockchain uses a peer-to-peer network where each participant maintains a copy of the ledger. Transactions are grouped into blocks, which are cryptographically linked to previous blocks, forming an immutable chain. This structure makes it extremely difficult to alter past records without detection. Blockchain employs consensus mechanisms such as Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions, ensuring trust among participants. Due to its decentralized nature, blockchain enhances security, reduces fraud, and eliminates the need for intermediaries. It is widely used in industries like finance, supply chain, and healthcare, where data integrity and transparency are crucial.

Q2: List 2 real-life use cases (e.g., supply chain, digital identity).

1. **Healthcare Records Management** – Securely stores and shares patient data across hospitals.
   - Patients control access to their medical history.
   - Reduces errors, prevents unauthorized changes, and improves interoperability.
2. **Voting Systems** – Ensures transparent and tamper-proof elections.
   - Each vote is recorded on the blockchain, preventing fraud.
   - Increases trust in electoral processes by providing verifiable results.

Q3: Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.

```
+--------------------------------------------------------------------------------+
|                              BLOCK                                              |
+--------------------------------------------------------------------------------+
| Timestamp     : 2025-06-09 11:35:00                                             |
| Previous Hash : 56A7F3C9D8E2B4F7A91E2D3B4C5A6789           |
| Merkle Root   : 9FC3D5E2A7B8C6D4E5F3A1B2C9D8E7F6           |
| Nonce         : 83749                                                           |
+--------------------------------------------------------------------------------+
| Data (Transactions):                                                            |
| - Alice → Bob: $50                                                               |
| - Carol → Dave: $20                                                             |
| - Eve → Frank: $10                                                              |
+--------------------------------------------------------------------------------+
```

Q4: Briefly explain with an example how the Merkle root helps verify data integrity.

The Merkle root is a cryptographic hash that summarizes all transactions in a block. For instance, if four transactions (Tx1, Tx2, Tx3, Tx4) exist, their hashes are paired and hashed again until a single root hash is generated. If someone alters Tx2, the hash of Tx2 changes, affecting the Merkle root. Since the Merkle root is stored in the block header, any modification in transactions becomes evident. This allows quick verification of data integrity without checking every transaction individually.

Q5: What is Proof of Work and why does it require energy?

Proof of Work (PoW) is a consensus mechanism used to validate transactions and add new blocks to a blockchain. It requires participants, called miners, to solve complex mathematical puzzles by repeatedly hashing data until they find a valid result. This process demands significant computational power.
As miners compete to solve the puzzle first, it leads to high energy consumption due to continuous use of processors and electricity. The energy cost adds security because altering the blockchain would require redoing all the work, making attacks extremely expensive.

Q6: What is Proof of Stake and how does it differ?

Proof of Stake (PoS) is a consensus mechanism where validators are chosen to create new blocks based on the amount of cryptocurrency they hold and lock up as a stake. Unlike Proof of Work, PoS does not require solving complex puzzles or high computational power, which significantly reduces energy consumption. Validators are randomly selected, often weighted by their stake, to propose and validate blocks. This method is more energy-efficient and faster compared to Proof of Work.

Q7: What is Delegated Proof of Stake and how are validators selected?

Delegated Proof of Stake (DPoS) is a consensus mechanism where token holders vote to elect a small group of trusted delegates or validators. These elected validators are responsible for validating transactions and creating new blocks on behalf of the entire network. Voting power depends on the number of tokens held, and delegates can be replaced through voting if they misbehave or underperform. This system is designed to be more efficient and democratic, enabling faster transaction processing while maintaining security.