BLOCKCHAIN ASSIGNMENT TASK 1

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

Blockchain is a decentralized digital ledger that records transactions across a network of computers in a secure and tamper-proof way. Each transaction is grouped into a block, and each block is connected to the previous one using cryptographic hashes, forming a chain. This makes it nearly impossible to alter any data without changing all subsequent blocks. Blockchain operates without a central authority and uses consensus mechanisms like Proof of Work or Proof of Stake to validate transactions. It ensures transparency, security, and trust between participants in a distributed system. Because all participants have a copy of the ledger, blockchain provides high data integrity and is resistant to fraud or hacking. It is widely used in sectors requiring trust, like finance, healthcare, and logistics.

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

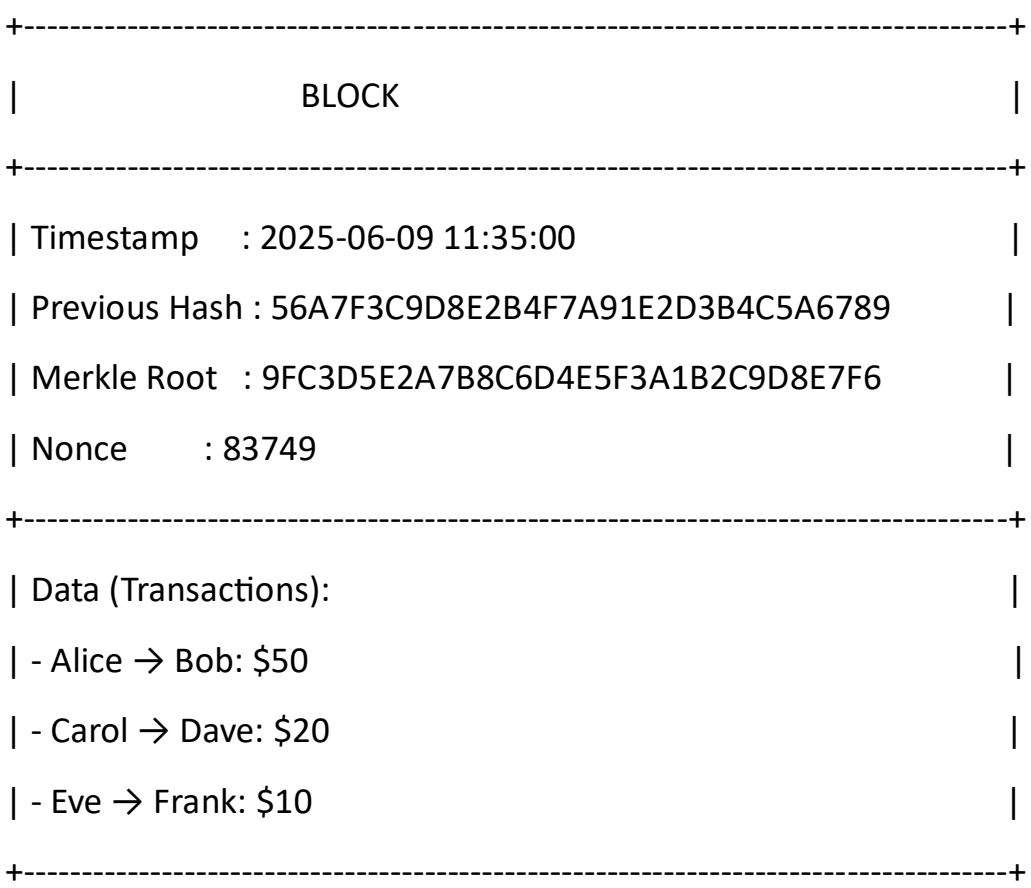
1. **Supply Chain Tracking** – Verifies product origin and prevents counterfeit goods.

- Blockchain allows all parties to track each step of the product journey in real time.
- This improves trust, reduces fraud, and ensures regulatory compliance.

2. **Digital Identity –** Provides secure, verifiable IDs without centralized databases.

- Users control their identity and share only necessary information with others.
- It helps prevent identity theft and simplifies online verification processes.

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



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

The Merkle root is a single hash that represents all transactions in a block. For example, if there are four transactions (Tx1, Tx2, Tx3, Tx4), their hashes are first paired: H1 = hash(Tx1 + Tx2), H2 = hash(Tx3 + Tx4). Then, the Merkle root = hash(H1 + H2). If even one transaction, say Tx2, is modified, H1 changes and the Merkle root becomes different.
This change indicates that the data in the block is no longer the same. The Merkle root allows verification of any specific transaction with minimal computation, ensuring data integrity without checking every transaction in the block.

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.