Task-1

Theoretical Part:

1. Blockchain Basics

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

Blockchain is a type of distributed database that stores data in blocks that are linked together in a sequence and secure manner. Instead of being controlled by a single entity, it operates across a network of computers like a docker image, making it decentralized and resistant to manipulation. Every block holds a batch of transaction data and is connected to the previous one using cryptographic techniques like SHA-256, ensuring the chain's integrity. Once data is recorded, it is nearly impossible to change without altering every up comming block and reaching agreement from the majority of the network **(51% of blocks like u metioned in class**). This makes blockchain highly secure and trustworthy. Originally developed for digital currencies like Bitcoin, blockchain technology is now being applied in many fields, such as supply chain management, identity verification, and healthcare. Its core advantages include transparency, security, and decentralization.

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

- **Cross-Border Payment :**
  Blockchain enables fast, low-cost international money transfers. **Ripple (XRP)** and **St**are used by financial institutions to settle cross-border payments in seconds with minimal fees.
- **Voting Systems :**
  Blockchain can make elections more transparent and tamper-proof. Countries and organizations have piloted **blockchain-based voting systems** (e.g., in Estonia and West Virginia) to increase trust and reduce fraud.

---

2. Block Anatomy

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

A BLOCK

Data: (all transaction details)

Previous hash :
de790ac526a6db98eb4293e0352015cc9be2022f60da6d253f04a69278b6940e

Timestamp : 09-06-2025 , 12:00

Nonce : 0 (for initial block)

Merkel root :
3b93485159da19a2a784d2bd33896518bd1063bd92cd1cb592fe2bce9f453c5e

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

The **Merkle root** ensures data integrity in a block by summarizing all transactions in a cryptographic tree structure called a **Merkle tree**.

How it works:

1. Each transaction is hashed.
2. Pairs of transaction hashes are combined and hashed again.
3. This process continues until one final hash remains — the **Merkle root**.

Example:

Imagine a block with 4 transactions: T1, T2, T3, T4

1. Hash each:
   H1 = hash(T1), H2 = hash(T2), H3 = hash(T3), H4 = hash(T4)
2. Pair and hash again:
   H12 = hash(H1 + H2), H34 = hash(H3 + H4)
3. Final Merkle root:
   Root = hash(H12 + H34)

If someone changes T2, then H2, H12, and the root will all change — proving the data was altered.

---

3. **Consensus Conceptualization**

a. **What is Proof of Work and why does it require energy** :-> Proof of Work is a consensus mechanism where miners compete to solve complex mathematical puzzles using computational power. The first miner to solve the puzzle gets the right to add a new block to the blockchain and earn a reward. It requires significant energy because solving the puzzle involves intensive trial-and-error computations, demanding powerful hardware running continuously. PoW ensures network security by making attacks costly and resource-intensive.

b. **What is Proof of Stake and how does it differ** :-> Proof of Stake selects validators based on the amount of cryptocurrency they "stake" or lock in the network, rather than relying on computational power. The more coins a user stakes, the higher the chance they have to be selected to validate the next block. It consumes far less energy than PoW because it doesn't require solving complex problems. PoS promotes energy efficiency and encourages users to act honestly to avoid losing their staked assets.

c. **What is Delegated Proof of Stake and how are validators selected** :-> Delegated Proof of Stake is a variation of PoS where token holders vote to elect a fixed number of validators (also called delegates or witnesses). These elected validators are responsible for creating and confirming blocks on behalf of the network. Validators are selected based on reputation and vote count, not just staked coins. DPoS offers higher scalability and transaction speed but relies on a smaller set of trusted validators, making it more centralized than PoW or PoS.