Task-1 Theoretical Part

Blockchain Basics:

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

   Ans: A blockchain is a decentralized, distributed digital ledger that securely records data across many computers so that the recorded transactions cannot be altered retroactively. Each piece of data (called a block) is linked to the previous one using cryptographic hashes, forming a secure and tamper-proof chain. Blockchains eliminate the need for central authority, allowing peer-to-peer transactions with transparency and trust. Once a block is validated through a consensus mechanism, it is added to the chain, and all participants have access to the same copy of the ledger, ensuring consistency and security across the network.

2. Real-life Use Cases

   Ans:

   - **Supply Chain Management –** Track the journey of goods in real-time and ensure product authenticity (e.g., food or medicine tracing).
   - **Digital Identity** – Individuals control their identity credentials securely without relying on centralized databases (e.g., decentralized KYC).

Block Anatomy:

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

```
+----------------------------------+
|         Block Header             |
+----------------------------------+
| Timestamp      | 2025-06-08      |
| Previous Hash  | 4e3f...a9d2     |
| Nonce          | 2945732         |
| Merkle Root    | 3bc1...ff09     |
+----------------------------------+
|          Block Data                |
| - Transaction 1                    |
| - Transaction 2                    |
| - ...                              |
+----------------------------------+
```

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

   Ans: A Merkle root is a hash that represents all the transactions in a block. Transactions are paired and hashed together repeatedly until a single root hash is generated. For example, if a block has four transactions, their hashes are combined like so:

   - Hash1 + Hash2 → HashA
   - Hash3 + Hash4 → HashB
   - HashA + HashB → Merkle Root

   If one transaction changes, the hash chain changes, altering the Merkle root. This helps quickly verify data integrity without re-checking every transaction.

Consensus Conceptualization

1. 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 mechanism where miners compete to solve complex mathematical puzzles to validate transactions and add new blocks. The first to solve it gets rewarded. This process requires significant computational power, hence high energy usage. The difficulty ensures the system remains secure against attacks, but it’s resource-intensive and environmentally costly.

Proof of Stake (PoS):

In Proof of Stake, validators are chosen to create new blocks based on the number of coins they hold and are willing to "stake" as collateral. It removes the need for energy-intensive computations, making it more eco-friendly. PoS relies on economic incentives—if a validator cheats, they lose their staked assets—ensuring network integrity.

Delegated Proof of Stake (DPoS):

Delegated Proof of Stake is a variation of PoS where token holders vote for a fixed number of trusted delegates (validators) to create blocks and secure the network. These delegates rotate in turns to validate transactions. The selection is democratic, and poor-performing or dishonest validators can be voted out, ensuring accountability and efficiency.