Theoretical Part:

1. Blockchain Basics

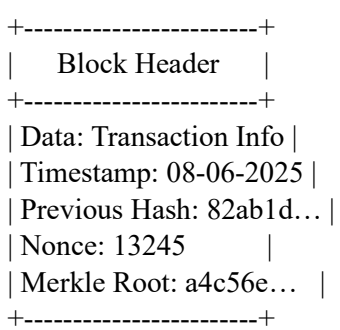
- **Define blockchain in your own words (100–150 words).**

  Blockchain is a type of digital record system. It stores data in small blocks, and each block is connected to the previous one. Every block has some data, a timestamp, a hash, and the previous block's hash. A hash is a special code that is created using the block's data. If someone tries to change the data, the hash will also change, and the chain will break. This helps in keeping the data safe and secure. Blockchain does not need any central control and all people in the network can see the data. It is mostly used in Bitcoin and other cryptocurrencies, but now it is also used in banks, hospitals, and supply chains. The best part is that once data is added, it cannot be easily changed**.**

- **List 2 real-life use cases (e.g., supply chain, digital identity).**
  - Digital Identity: People can use blockchain to safely store and control their personal identity details, like ID cards or certificates.
  - Supply Chain Management: Companies use blockchain to track goods from the factory to the customer. This helps make sure nothing is lost or changed during delivery.

2. Block Anatomy

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



- **Briefly explain with an example how the Merkle root helps verify data integrity.**
  - A Merkle Root is like a summary of all the data in a block. It helps to quickly check if any transaction has been changed.
  - Example: Suppose there are 4 transactions. Each transaction is turned into a hash. Then, the hashes are paired and hashed again until only one root hash remains and that is the Merkle Root.
    If someone changes even one transaction, the Merkle Root will also change. This helps detect any change in data immediately**.**

3. Consensus Conceptualization

- **Explain in brief (4–5 sentences each):**

1. **What is Proof of Work and why does it require energy?**
   Proof of Work is a system where computers compete to solve a difficult puzzle. The first one to solve it gets to add the new block to the blockchain. This process needs a lot of computing power and electricity. It makes the network safe because attackers would need huge energy to cheat. Bitcoin uses Proof of Work.

2. **What is Proof of Stake and how does it differ?**
   In Proof of Stake, there are no puzzles to solve. Instead, people who own more coins get a better chance to add new blocks. It saves energy because it does not need powerful computers. It also encourages users to act honestly, since bad behavior could make them lose their staked coins**.**

3. **What is Delegated Proof of Stake and how are validators selected?**
   Delegated Proof of Stake is a system where users vote for trusted people (called validators) to confirm transactions and create blocks. These validators are selected based on votes, not on how much coins they own. This method is faster and more democratic, as users choose who represents them in the blockchain network.