Mini Task 1: Build & Explain a Simple Blockchain

Theoretical Part:

1. **Blockchain Basics**

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

   Blockchain is a decentralized and distributed digital ledger that records transactions in a secure, transparent, and tamper-proof way. Instead of being controlled by a single authority, the blockchain is maintained by a network of computers (called nodes), where each participant has access to the same copy of the data. Information is stored in blocks that are linked together chronologically, forming a chain. Each block contains data, a timestamp, the hash of the previous block, and its own hash, which ensures the integrity of the chain. Once a block is added, the data cannot be altered without changing all the following blocks, making it highly secure against fraud or manipulation. Blockchain is the core technology behind cryptocurrencies like Bitcoin, but its use extends far beyond, including supply chains, digital identity, and secure voting systems. It promotes transparency, trust, and decentralization in digital systems.

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

   1. **Supply Chain Management:**
      Blockchain helps track the movement of goods from origin to destination. For example, in the food industry, it can record every step—from farm to supermarket—ensuring transparency, reducing fraud, and verifying the authenticity of products. Companies like Walmart and IBM use blockchain to track food safety and recall issues quickly.
   2. **Digital Identity Verification:**
      Blockchain allows individuals to create secure, tamper-proof digital identities. It gives users control over their personal information while making identity verification faster and safer. For example, governments and banks can use blockchain to verify documents like passports, licenses, or KYC information without the risk of data leaks.

2. Block Anatomy

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

Index: Position of the block in the chain.

Timestamp: When the block was created.

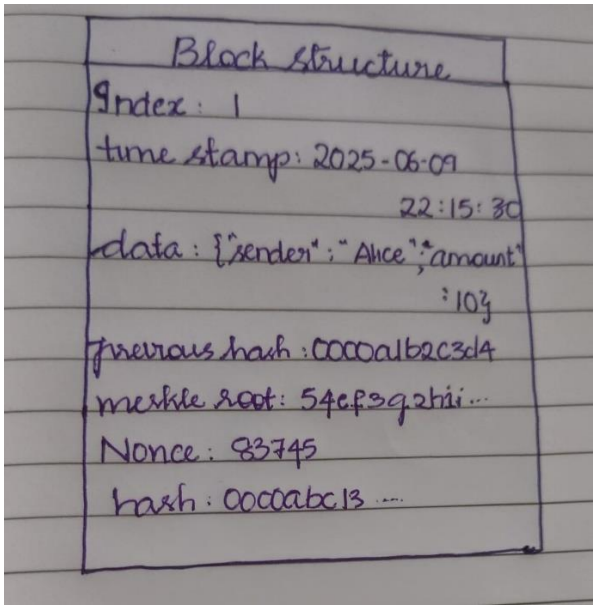
Data: Transaction or payload stored in the block.

Previous Hash: Hash of the previous block ensures chaining.

Merkle Root: A single hash summarizing all transactions inside.

Nonce: A random number changed during mining to find a valid hash.

Hash: Final SHA-256 hash that uniquely identifies the block.



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

The Merkle root is a single hash value that represents all transactions in a block. It is generated by repeatedly hashing pairs of transaction hashes until only one final hash remains. This final hash is the Merkle root. Even if a single transaction is altered, the corresponding hash changes, which affects the hashes above it and ultimately changes the Merkle root. This allows to detect any tampering without checking the entire dataset.

Example:

Suppose a block contains 4 transactions:

- Tx1: "Alice → Bob"
- Tx2: "Bob → Charlie"
- Tx3: "Charlie → Dave"
- Tx4: "Dave → Eve"
    - Hash each transaction → H1, H2, H3, H4
    - Hash pairs:
    - H12 = Hash(H1 + H2)
    - H34 = Hash(H3 + H4)

- Merkle root = Hash(H12 + H34)

If Tx2 is changed, H2 changes → H12 changes → Merkle root changes → integrity is broken.

3. **Consensus Conceptualization**
   Explain in brief (4–5 sentences each):

- **What is Proof of Work and why does it require energy?**

Proof of Work (PoW) is a consensus mechanism used in blockchain systems like Bitcoin to validate transactions and add new blocks. In PoW, miners compete to solve complex mathematical puzzles by repeatedly hashing data with different nonces until they find a hash that meets a required difficulty . This process is intentionally resource-intensive to make it difficult for attackers to take over the network. It requires significant computational power and electricity, as thousands or millions of calculations may be needed before a valid solution is found. The energy cost acts as a security layer, making tampering with the blockchain economically unfeasible.

- **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 "stake" or lock up as collateral. Unlike Proof of Work, which relies on solving energy-intensive puzzles, PoS selects validators in a more energy-efficient manner usually giving higher chances to those with larger stakes. This reduces the need for powerful hardware and high electricity usage. The main difference is that PoS secures the network through economic commitment **(s**take) rather than computational effort. If a validator tries to act maliciously, they risk losing their staked assets, making it a self-enforcing system.

- **What is Delegate Proof of Stake and how are validators selected?**

Delegated Proof of Stake (DPoS) is a variation of Proof of Stake where token holders vote to elect a small group of trusted delegates (also called witnesses or validators) to validate transactions and produce blocks on their behalf. Instead of every staker participating in validation, the voting system chooses a fixed number of delegates based on community trust and reputation. The more tokens a user holds, the more weight their vote carries. This method improves scalability and speed, as fewer validators are involved in consensus. Validators can be replaced through voting, ensuring accountability and decentralization through democratic selection.