**Mini Task 1: Build & Explain a Simple Blockchain**

**Goal:**

Understand blockchain fundamentals, block structure, and consensus mechanisms by simulating a mini blockchain and explaining how it works — both technically and conceptually.

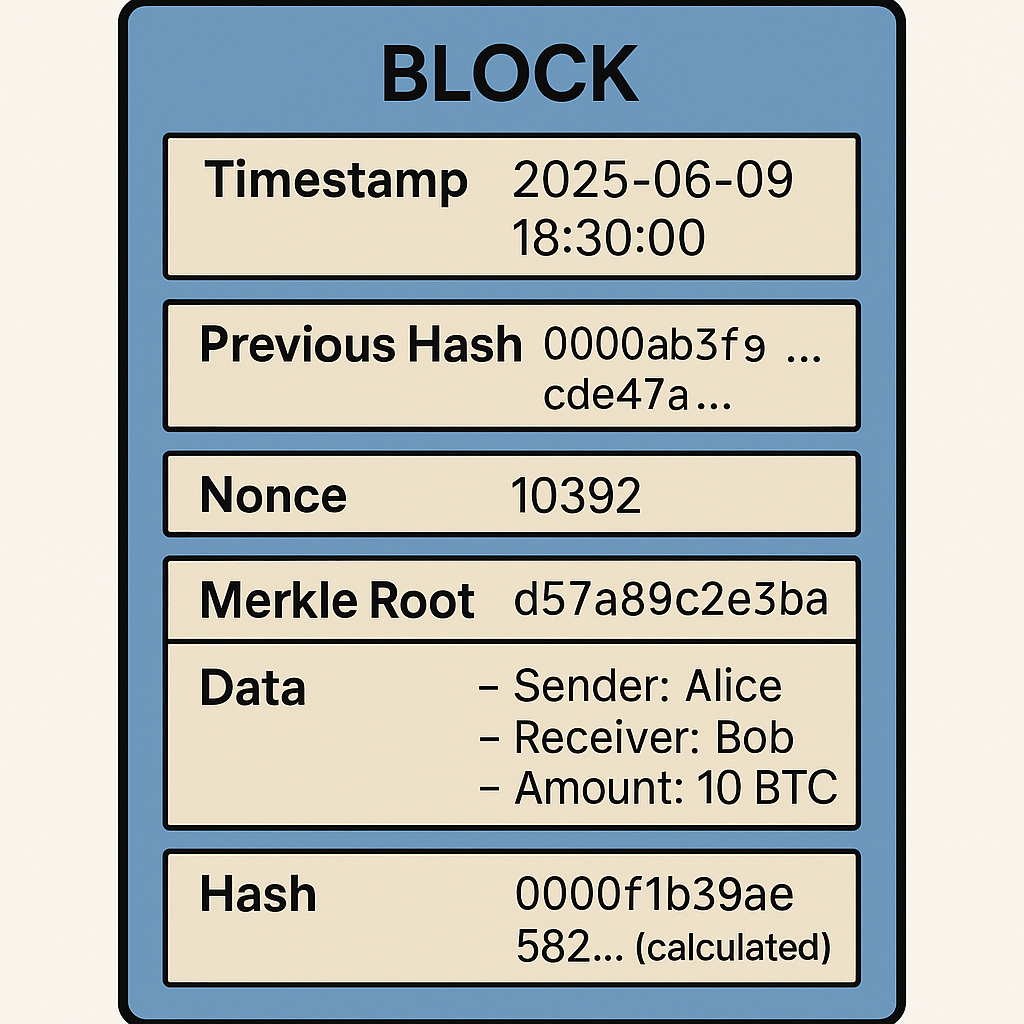
**Theoretical Part:**

* **Blockchain Basics:-**
* **blockchain in your own words (100–150 words).**
* A blockchain is a secure, decentralized digital ledger that records transactions in a series of connected blocks. Each block contains data, a timestamp, and a cryptographic hash of the previous block, creating a chain that is nearly impossible to alter. Unlike traditional databases managed by a central authority, blockchain is maintained by a network of computers (nodes) that work together to verify and record transactions through a consensus mechanism like Proof of Work or Proof of Stake. This makes the system transparent, tamper-resistant, and trustless—meaning users don't need to rely on a central authority to ensure data integrity. Blockchain technology is widely known for powering cryptocurrencies like Bitcoin, but its use extends to supply chain management, digital identity, smart contracts, and more. Its core value lies in providing a reliable, verifiable record of transactions without needing intermediaries.

* **List 2 real-life use cases (e.g., supply chain, digital identity).**
* Two different real-life use cases of blockchain technology are:-

1. Healthcare Records Management:  
   Blockchain is being used to securely store and share electronic health records. For example, Medical chain allows patients and doctors to access medical records securely without risking data breaches, ensuring privacy and faster diagnosis.
2. **Digital Identity Verification**:  
   Governments and tech companies are using blockchain to create secure, tamper-proof digital identities. For example, Estonia uses blockchain-based ID cards that allow citizens to access public services, vote online, and sign documents digitally.

* **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.**
* The **Merkle root** is a single hash that represents all the transactions in a block. It is generated by repeatedly hashing pairs of transaction hashes until only one hash remains — the Merkle root. This structure helps **quickly and securely verify** if a transaction exists in the block without checking every transaction.

**Example:**

Imagine a block with 4 transactions:

Tx1, Tx2, Tx3, Tx4

First, hash each transaction:

H1 = hash (Tx1), H2 = hash (Tx2), H3 = hash (Tx3), H4 = hash (Tx4)

Pair and hash them:

H12 = hash H1 + H2)

H34 = hash (H3 + H4)

Then:

Merkle Root = hash (H12 + H34)

Now, to verify if **Tx3** is valid, you only need H4 and H12 to recompute the Merkle root — **not all transactions**. If the computed root matches the block's Merkle root, the data is intact. This is **fast** and **efficient**, even for blocks with thousands of transactions.

* **Consensus Conceptualization :-**
* **Explain in brief (4–5 sentences each):** 
  1. **What is Proof of Work and why does it require energy?**
* Proof of Work (PoW) is a consensus mechanism where miners solve complex mathematical puzzles to add a new block to the blockchain. The first miner to solve the puzzle gets to add the block and is rewarded with cryptocurrency. This process requires massive computational power, which in turn consumes a lot of electricity. The energy is needed to make the mining process secure and resistant to attacks, as altering a block would require redoing the work for all subsequent blocks.

1. **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 PoW, PoS doesn't require energy-intensive computations, making it more eco-friendly. The chance of being selected as a validator increases with the size and age of the stake. PoS focuses on economic commitment rather than computational effort for security and consensus.

Q**. What is Delegated Proof of Stake and how are validators selected?**

* Delegated Proof of Stake (DPoS) is a variation of PoS where token holders vote to elect a limited number of delegates (also called witnesses or validators) to produce and validate blocks. These elected delegates are responsible for maintaining the network and are rewarded for their service. The voting process makes DPoS more democratic and scalable, as fewer nodes participate in consensus. Validators are selected based on the number of votes they receive from stakeholders.