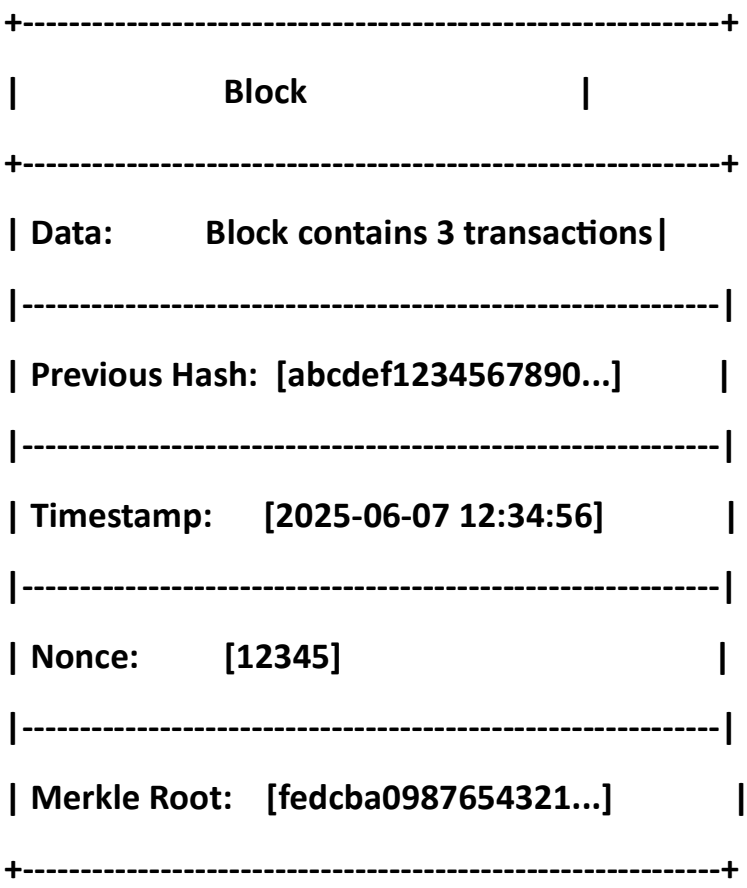
1.Blockchain Basics

- **Define blockchain in your own words (100–150 words).**
  -Blockchain is a decentralized, distributed digital ledger that records transactions across many computers in a secure and tamper-proof way. Each entry in the blockchain is stored in a "block," which contains data, a timestamp, and a cryptographic hash of the previous block — forming a chain. This structure ensures that once data is recorded, it cannot be altered without changing all subsequent blocks, which would require consensus from the majority of the network. Unlike traditional centralized systems, blockchain relies on peer-to-peer validation (consensus mechanisms) to verify transactions, making it more transparent, secure, and resistant to fraud. It is the underlying technology behind cryptocurrencies like Bitcoin, but its applications go far beyond digital money.
- **List 2 real-life use cases(e.g.,supplychain, digitalidentity).**
  - Supply Chain Management
  Blockchain can track the origin, movement, and status of goods across a supply chain. This ensures transparency, prevents fraud, and improves traceability — especially in industries like food, medicine, and luxury goods.
  -Digital Identity Verification
  Individuals can use blockchain to store and share their identity securely. It reduces the need for multiple identity verifications across platforms and gives users control over their own personal data.

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.**
  -The Merkle root is a single hash that summarizes all the transactions (or data) in a block. It is created by repeatedly hashing pairs of data until only one hash remains—the Merkle root.
  How it helps verify data integrity:
- If any transaction/data in the block changes, the Merkle root will also change.
- To verify a specific transaction, you only need a few hashes (not the whole block), making verification efficient.
  Example: Suppose a block contains 4 transactions: A, B, C, D.

1. Hash each transaction:

- hA = hash(A)
- hB = hash(B)
- hC = hash(C)
- hD = hash(D)

2. Hash pairs:
   - hAB = hash(hA + hB)
   - hCD = hash(hC + hD)
3. Merkle root:
   - root = hash(hAB + hCD)

   If transaction B is changed, hB changes, which changes hAB, and finally the Merkle root.
   This means any tampering is easily detected by checking the Merkle root.

3.Consensus Conceptualization

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): is a consensus mechanism where network participants (miners) compete to solve complex mathematical puzzles using computational power. The first miner to solve the puzzle gets to add the next block to the blockchain and receives a reward. This process requires significant energy because it involves running many calculations per second, often on specialized hardware. The high energy requirement makes it costly to attack the network, providing security through resource expenditure.

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 does not require solving energy-intensive puzzles; instead, the probability of being selected as a validator increases with the amount of stake held. This makes PoS much more energy-efficient and environmentally friendly. Security is maintained because validators risk losing their staked coins if they act maliciously.

Delegated Proof of Stake (DPoS): is a variation of PoS where token holders vote to elect a small group of delegates (validators) who are responsible for validating transactions and producing blocks. The voting power is proportional to the number of tokens held, and only the top-voted delegates participate in block production. This system allows for faster consensus and greater scalability, as fewer validators are involved in each round. Validators can be replaced through voting, ensuring accountability to the community.