Blockseblock-task1

Mini Task-1

- Theoretical part

1) Blockchain Basics

- Define blockchain in your own words

→ A blockchain is a special type of database that stores info in blocks. This blocks are intern connected to each other through the previous hash. Each block contains data, time-stamp, a reference to the previous block, and a unique code called a hash. Once data is added to the blockchain it cannot be changed easily, which ~~means~~ makes it very secure. It is immutable. It is a decentralized, meaning it is ~~not~~ not controlled by a single person or computers. Blockchain is often used for ~~cryptography~~ cryptocurrencies like bitcoin.

The below are characteristics:

1. Decentralized - No single authority controls the network.
2. Immutable - Data is tamper-proof and cannot be altered
3. Transparent - All transactions are publicly visible
4. Consensus - Network nodes verify and agree on transactions.
5. Secure - protected by cryptographic algorithms
6. Distributed - Data is stored across a network of nodes.
7. Autonomous - self executing contracts can be created.

Types of Blockchain

1. public Blockchain

→ open to anyone decentralized and transparent (eg Bitcoin, ethereum).

2. Private Blockchain

→ Restricted access, central control and limited transparency

3. Consortium Blockchain

→ Hybrid of public and private blockchains, with restricted access and decentralized control

4. Hybrid Blockchain

→ combines elements of public and private blockchains, offering flexibility and customization

6) Federated Blockchain

→ A decentralized network with a group of trusted nodes validating transactions.

- List 2 real-life cases:

(1) <u>Supply chain management</u>

→ Blockchain helps to track product movement from manufacturers to the customers, ensuring transparency & reducing fraud.
eg: vechain is a Blockchain platform used for supply chain management

(2) Digital Identity

→ It can be used to securely stored & managed personal identity information, helping prevent identity theft and improving online verification.

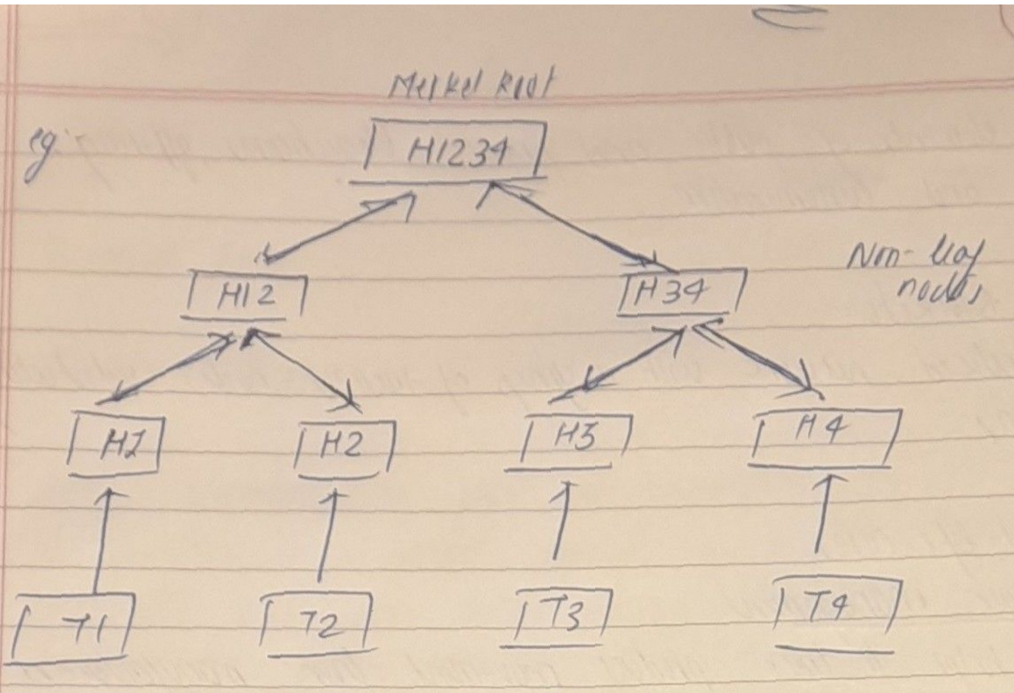
(2) Block Anatomy

(4) Draw a block showing:

Data: "ABC pays XYZ 2BTC"
previous Hash: 000a1b2c3...
Timestamp: 2025-06-06 10 30:00
Nonce: 39247
merkel Root: abcd1234efgh5678...

(5) merkel Root Explanation (with example)

→ In a blockchain, a merkel root is cryptographic hash representing the entire set of transactions with in a block. It's the royal node of merkel tree, a data structure that effectively verifies the integrity of data in a block by summarizing the transactions eg:-



Working:-

(1) Hashing: Each transactions within a block is hashed individually

(2) pairing and Hashing: These hashes are then paired up and hashed again, and this process continues until a single hash remains.

(3) Merkel Root - This final hash is the merkle root

(4) Verification - Anyone can verify the integrity of block by comparing the merkel root calculated locally with the one stored in the block header

(5) Security - If even a single transaction is altered, the merkel root changes, revealing the tampering

eg:- If someone tries to change "ABC" pays XYZ 2BTC" to "ABC pays XYZ 5BTC", the merkel root will no longer match, showing that the data has been altered

(3) Consensus Conceptualization

Q What is proof of work and why does it require energy?

→ Proof of work (PoW) is a system where computers compete to solve a complex math problem. The first one to solve it gets to add a new block to the blockchain. This process requires alot of computer power and energy because the problem is hard to solve but easy to check. It ensures that adding blocks is difficult, making it secures & protecting the network from spam or attacks.

(b) What is proof of stake and how does it differ?
→ PoS is an alternative to PoW. Instead of solving math problems, validators are chosen based on how many coins they are "staked" or lock up as a security deposit. The more coins you stake, the higher your chance to validate the next block. PoS uses much less energy than PoW because it doesn't need powerful computers solving puzzles.

(c) What is Delegated proof of stake and how are validators selected?
→ DPoS is a voting based version of PoS. Token holders vote to ~~each~~ elect a few trusted ~~[illegible]~~ validators who are ~~repo~~ responsible for validating transactions & creating new blocks. This method is faster & more scalable. The selected validators are rewarded. If they act badly can be voted out by the community.