Theoretical Part

- Define Blockchain in your own words (100-150 words)

Blockchain is a decentralized digital ledger that records transactions across multiple computer in a secure, transparent, and tamper-proof way. Each record, called a "block", contain a list of transactions and is linked to the previous block, forming a chain — hence the name "blockchain". This system ensures that once data is added, it cannot be altered without changing all the following blocks, making it highly secure and trustworthy. Unlike traditional system managed by a central authority, blockchain operates on a peer-to-peer network where all participants share equal control. It uses cryptographic techniques to validate and secure data, ensuring trust without the need for intermediaries. Blockchain is widely known for powering cryptocurrencies like Bitcoin, but its potential extends to various field like supply chain management, voting system, healthcare, and finance where transparency and security are essential.....

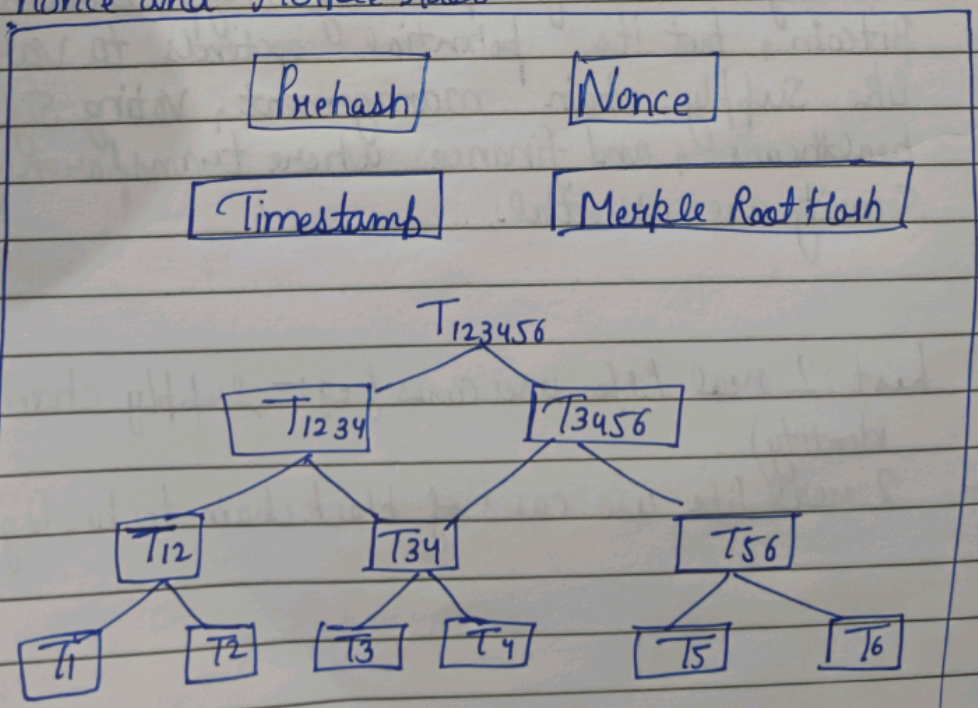
- List 2 real life use cases (eg:- supply chain, digital identity)

Ans — 2 real life use cases of blockchain technology

1. Supply Chain Management :-
Blockchain helps tracks the movement of goods from the origin to the destination with full transparency.
For ex:- IBM Food Trust uses blockchain to trace food products through the supply chain, improving food safety and reducing waste by identifying contamination sources quickly.

2. Digital Identity Verification :-
Blockchain allows individuals to control and verify their identities securely. For instance ID2020 and Microsoft's ION projects use blockchain to create tamper proof digital IDs helping people prove their identity without relying on centralized authorities - espically useful for refuges or those without traditional ID documents.

- 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.

Ans- The Merkle root helps verify data integrity by summarizing all transactions in a block using a tree structure (called Merkle Tree), where each leaf node is a hash of a transaction and parent nodes are hashes of their child nodes. The final single hash at the top is the Merkle Root.

Ex:- Suppose we have 4 transactions:-

T_1, T_2, T_3, T_4

1. First, hash each transactions:-

$H_1 = hash(T_1)$

$H_2 = hash(T_2)$

$H_3 = hash(T_3)$

$H_4 = hash(T_4)$

2. Combine and hash them in pairs:-

H_{12} :- $Hash(H_1 + H_2)$

H_{34} :- $hash(H_3 + H_4)$

3. Then hash the two results:-

$Root = hash(H_{12} + H_{34})$

That Root is called Merkle Root.

- Explain in brief:-

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

Ans→ Proof of Work (PoW) is a consensus mechanism used in blockchain networks like Bitcoin to validate transactions and add new blocks. It require participants (miners) to solve complex mathematical puzzles using computational power. The first to solve the puzzle get to add the new block and earn a reward. This process require powerful hardware running continously, consuming large amount of electricity. The energy ensures network security, as altering data would require redoing the expensive computation.

Q⇒ What is Proof of Stake and how does

Ans:- Proof of Stake (PoS) is a Consensus method where Validators are chosen based on the amount of crypto-currency they "stake" or lock up as collateral. Unlike PoW, PoS doesnot require solving puzzles or heavy energy use—Validators are selected to create blocks in proportion to their stake. This makes it more energy-efficient and scalable. If validators act dishonestly, they risk losing their staked funds

Q⇒ What is Delegated Proof of Stake and how are Validation Selected?

Ans:- Delegated Proof of Stake (DPoS) is a Variation of PoS where token holders vote to elect a small number of trusted delegates (validators) to validate transaction

and produce blocks. Voting power is proportional to the number of tokens held. The elected validators rotates duties and are rewarded for honest behaviour. If a validator misbehes, voters can replace them.