# #Theoretical Part:

## PART1: Blockchain Basics

Q1:Define blockchain in your own words (100–150 words).

Blockchain is a chain of blocks in which each block is cryptographically linked to the previous one. It is a decentralised digital ledger that operates on a secure peer-to-peer network, thereby preventing central control. Each block contains information like transaction records(data), timestamp marks, unique hash identifier(merkle root), previous hash information and nonce. The chain acts like a linked list, which is immutable. As each block depends on the hash of the previous block, tampering with the information in any of the blocks breaks the chain, making the system very secure. All the data is stored across many computers/nodes in a network, providing the same copy to everyone. This structure ensures transparency, security and trust so no single person can change the data without others knowing.

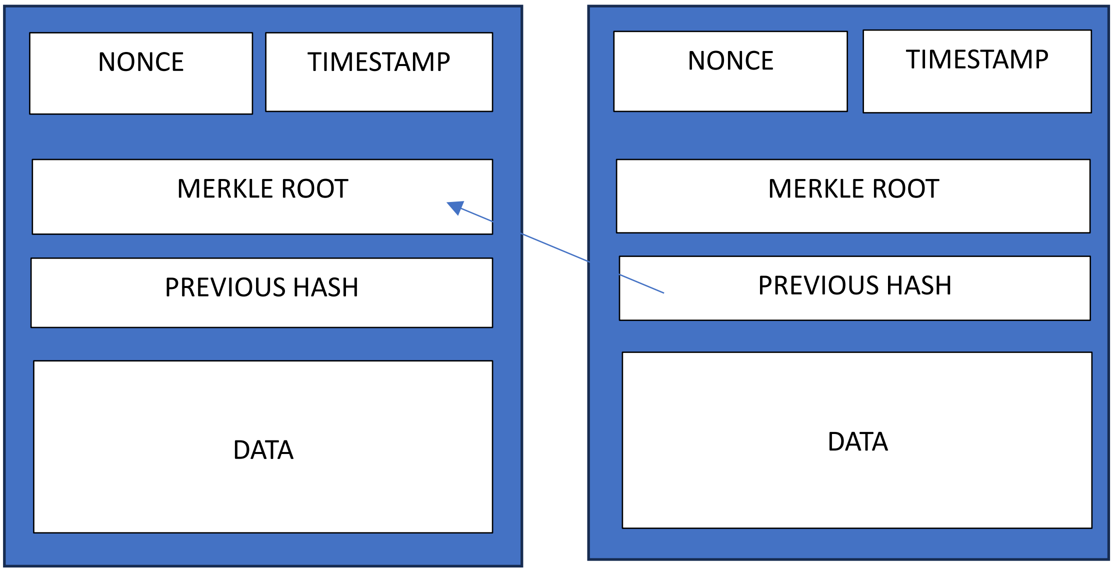
Q2: List 2 real-life use cases (e.g., supply chain, digital identity).

Two real-life use case of Blockchain are:-
1.Walmart – Food Supply Chain Tracking
Walmart, in partnership with IBM's Food Trust, uses blockchain to track the origin and journey of food products like mangoes and pork. Earlier, it used to take days to trace contaminated food, but with the help of blockchain, it takes just seconds to trace where a product came from, improving food safety and transparency.

2.Estonia – Digital Identity for Citizens
Estonia uses blockchain to manage its citizens' digital identities and public services. Through this, citizens can access healthcare, vote online, and manage bank accounts securely. Blockchain ensures data integrity, privacy, and tamper-proof records in government services.

**PART2: Block Anatomy**

Q1:Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.



#1 #2

Q2:Briefly explain with an example how the Merkle root helps verify data integrity.

A Merkle tree organises the transactions in all the blocks by repeatedly hashing pairs of hashes together until only a single hash remains. This final hash is called the Merkle root, which summarises all the transactions.

For example if we have five transactions T1,T2,T3,T4,T5.

1. Hash individual hashes:
   H1=hash(T1) , H2=hash(T2) , H3=hash(T3) , H4=hash(T4) , H5=hash(T5)
2. Pair and hash(duplicate the last hash to make pair)
   H12=hash(H1+H2), H34=hash(H3+H4) and H55=hash(H5+H5)
3. Pair the next level(again duplicate if needed)
   H1234=hash(H12+H34) and H5555=hash(H55+H55)

4. Final hash
   H12345555=hash(H1234+H5555)
   This H12345555 is known as the Merkle root.

**PART3: Consensus Conceptulization**

Q1:What is Proof of Work and why does it require energy?

Proof of Work(PoW) is a consensus mechanism used in Bitcoin to validate transactions, in which miners have to solve a complex cryptographic puzzle by trying different values or nonces to produce a valid hash. The miner who solves the problem is rewarded with cryptocurrency.PoW requires computational power to solve these puzzles, which consumes a lot of energy. This is because the problem is solved by trial and error, and millions of calculations may be needed before finding the correct answer.

Q2:What is Proof of Stake and how does it differ?

Proof of Stake(Pos) is a consensus mechanism used in Ethereum in which validators are chosen to validate a new block by the amount of cryptocurrency they stake or put up as collateral. Instead of solving complex puzzles, the validators are chosen in a way that favours those with a larger stake or a longer-held stake. When they validate a block correctly, they earn rewards; if they try to cheat, they risk losing their staked coins. PoS differ from PoW in how validators are selected and how energy is used. PoS consumes less energy as there is no need for massive mining hardware, and is considered more environmentally friendly as compared to PoW.

## Q3:What is Delegated Proof of Stake and how are validators selected?

Delegated Proof of Stake (DPoS) is a consensus mechanism used in TRON where token holders vote to elect a small number of trusted delegates (also called witnesses or validators) who are responsible for validating transactions and producing blocks. Instead of everyone competing to create blocks (as in PoW), only the selected delegates take turns doing so, making the process faster and more energy-efficient. Token holders can change their votes at any time, which keeps delegates accountable and promotes honest behaviour.
Validators are selected through a democratic voting system. Each token holder can vote for a set of delegates by using their tokens like votes—the more tokens they hold, the more influence they have. The top-voted delegates become the active validators, while others wait as backups. This system allows for high performance and decentralisation through community participation.