# Mini Task 1

## Theoretical Part:-

① (a) Define Blockchain in your own words.

Ans:- Blockchain is like a book that store information in linked blocks in chain but digitally. Each block has data or transaction, time when it is created and a unique hash to identify. It is like once data is added, it can't be ~~eat~~ changed without notifying all other blocks, that makes it secure.

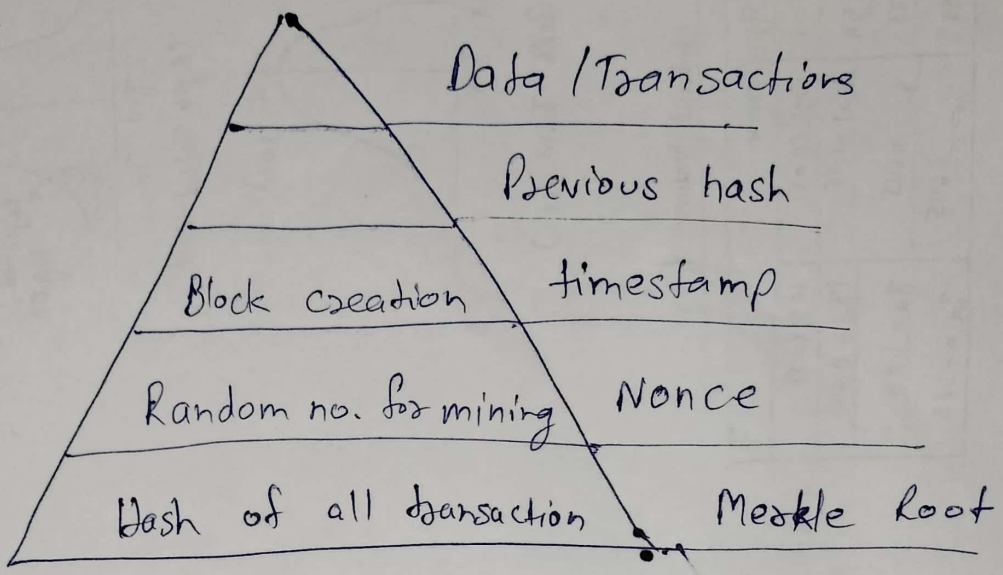
(b) List 2 real-life use cases.

Ans:- Cross-Border Payments: It enables low-cost, middleman free, easy and bypass to a traditional long process system for cross-border payments.

Voting System :- Replacing traditional EVMs with blockchain based tamper proof system, prevents fraud and with verifiable results.

(2) (a) Draw a block showing: data, previous hash, timestamp, nonce and merkle root.

Ans:-




(b) Briefly explain with an example how the merkle root helps verify data.

Ans:- Let we have a block which as 5 transactions. The merkle root is like a compressed fingerprint of all transactions. If someone changes any transaction, the merkle root changes telling everyone that the data is tempered.

(3) Explain in brief:-

(a) Proof of work & why does it require energy?

Ans:- Miner solve complex math problems to add new blocks. The first miner to solve gets rewards like in bitcoin.

It needs energy because solving these puzzles require powerful computers running non-stop.

(b) Proof of Stake and how it differs?

Ans:- Instead of mining, validators are chosen based on how much cryptocurrency they stake like as collateral. More stake means more chance to validate blocks.

It is different from POW because of no energy wasting puzzle, cheaper & faster.

(c) Delegated Proof of Stake & how validators selected?

Ans:- Users vote for few trusted delegates or validators. These delegates take turns creating blocks. Faster than POW & POS, fewer people need to agree.

Validators are selected by users vote or token holder vote, top validators are chosen, if they act malicious or go offline they can be voted out & replaced.