Mini Task 1:- Build and explain simple Blockchain Theoretical part.

a (i) Blockchain Basics

1). Define blockchain in your own words
2). List 2 real-life use cases (e.g. supply chain, digital identity)

→ 1)

- Blockchain :-
  - Blockchain is the underlying technology a decentralized and distributed ledger that record data in a secure, immutable and transparent way

- purpose :-
  - Blockchain can be used for a wide variety of application, not just cryptocurrency.
  - it is designed to securly store and transmit any kind of data

- scope :-
  - Blockchain can be applied in numerous industries, such as supply chain management healthcare, finance, and voting system

example :-
Hyperledger :- is a blockchain framworks for enterprise solution that dosen't involve cryptocurrency.

2) List 2 real life use cases

1) Digital Identity

→

- challenges :- Traditional identity system are fragmented, insecure and often involve bureaucratic delays. - Managing citizens' identities, such as issuing ID or verifying personal details, is time-consuming and prone to fraud

- Blockchain solution :-
  - Blockchain enables the creation of secure, tamper-resistant digital identities that citizens can use for various services.
  - Governments can issue blockchain-based ID that are verifiable and accessible across multiple services (e.g healthcare, banking, society, security)
  - Estonia, for example, has implemented a blockchain-based e-Residency program allowing people to securely establish their identity online.

2) Supply chain Transparency

- Challenges :-
  - Governments procure various good and services and ensuring transparency in the supply chain is difficult leading

corruption and inefficiencies.

Blockchain solution :-
- Blockchain provides real-time, tamper-resistant visibility into the supply chain.
- Governments can track the origin, quality and movement of goods, from medical supplies to infrastructure materials.
- For instance, blockchain can help ensure that public funds are used appropriately by providing an auditable trail of all transaction and product movements.

Q.2 Block Anatomy
- Draw a block showing data, previous hash, timestamp, nonce, and merkle root

→

1) Previous Block Hash :-
- The hash of the previous block in the chain, which link the current block the previous one.

2) merkle Root :-
- The hash of all the transaction in the block, organized in the tree structure called the merkle tree

3) Timestamp :-

- The time when the block was created

4) Nonce :-
- A random number used in PoW system like Bitcoin to find a hash that meet certain criteria.

Block Header	
previous block Hash	: [Hash of previous block]
merkle Root	: [Hash of all transaction]
timestamp	: [creation time of the block]
Nonce	: [random number of pow]
version	: [blockchain version]
Difficulty Target	: [difficulty level]

Block Body	
Transaction 1 :	[details of transaction 1]
Transaction 2 :	[details of transaction 2]
...	
Transaction N :	[details of transaction N]

22. ~~list~~ Briefly explain with an example how the merkle root helps verify data integrity

→

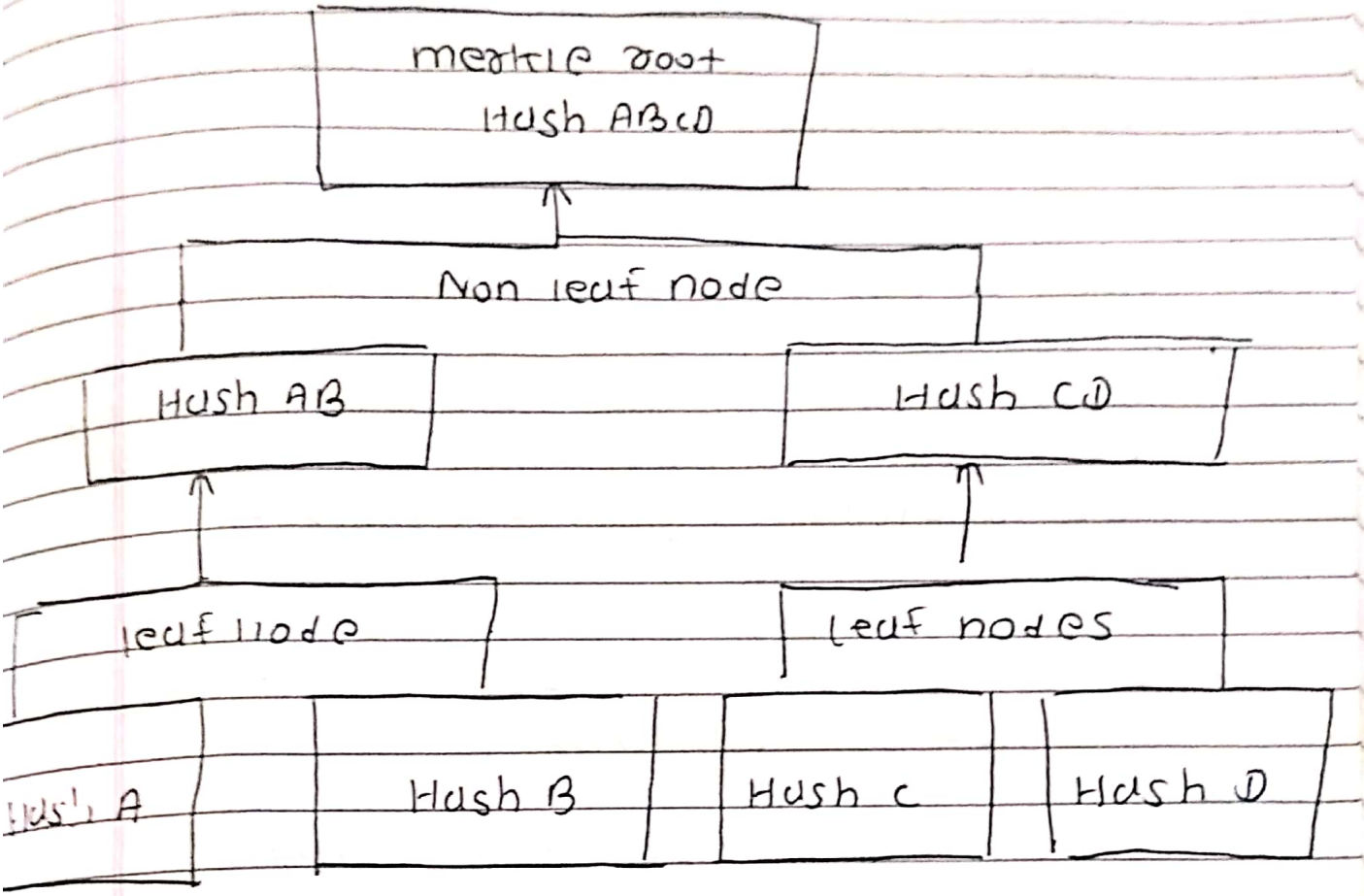
- validate the data's integrity :-
  - it can be used to validate the data's integrity effectively

- efficient verification :-
  - The data format is efficient and verifying the data's integrity takes only a few moment

- merkle tree work :-
  - A merkle tree adds up all of the transaction in a block and creates a unique digital fingerprint of the full set of instruction, allowing the user to check whether the block contain a transaction
  - They are designed from the ground up, with transaction ID as the foundation every non-leaf node hashes it ~~root~~ prior hash and every leaf nod in the merkle tree transaction data.
  - Hash A, Hash B, Hash C, and Hash D :-
    - when these hashes are combined they form a new hash
  - Hash AB and Hash CD :-
    - As a result the merkle root is made up of combining two hash

Hash

ABCD



Transaction ID:- A

Transaction ID B and C

Transaction ID :- D

Merkle tree

23) consensus conceptualization :-

- Explain in brief (4-5 sentences each) :-
- what is proof of work and why does it require energy?

→ miner compete to solve complex

complex mathematical puzzle to add a new block to the blockchain e.g., Bitcoin

2) what is PoS and How does it differ?

→ Validator are chosen to create new block based on the number of token they hold and are willing to stake are collateral e.g ethereum 2.0)

3) what is delegated PoS of stake and how are validator

→ Token holder vote for a small number of delegates who are responsible for validating transaction and creating new block (e.g EOS)