

1- Define blockchain in your own words

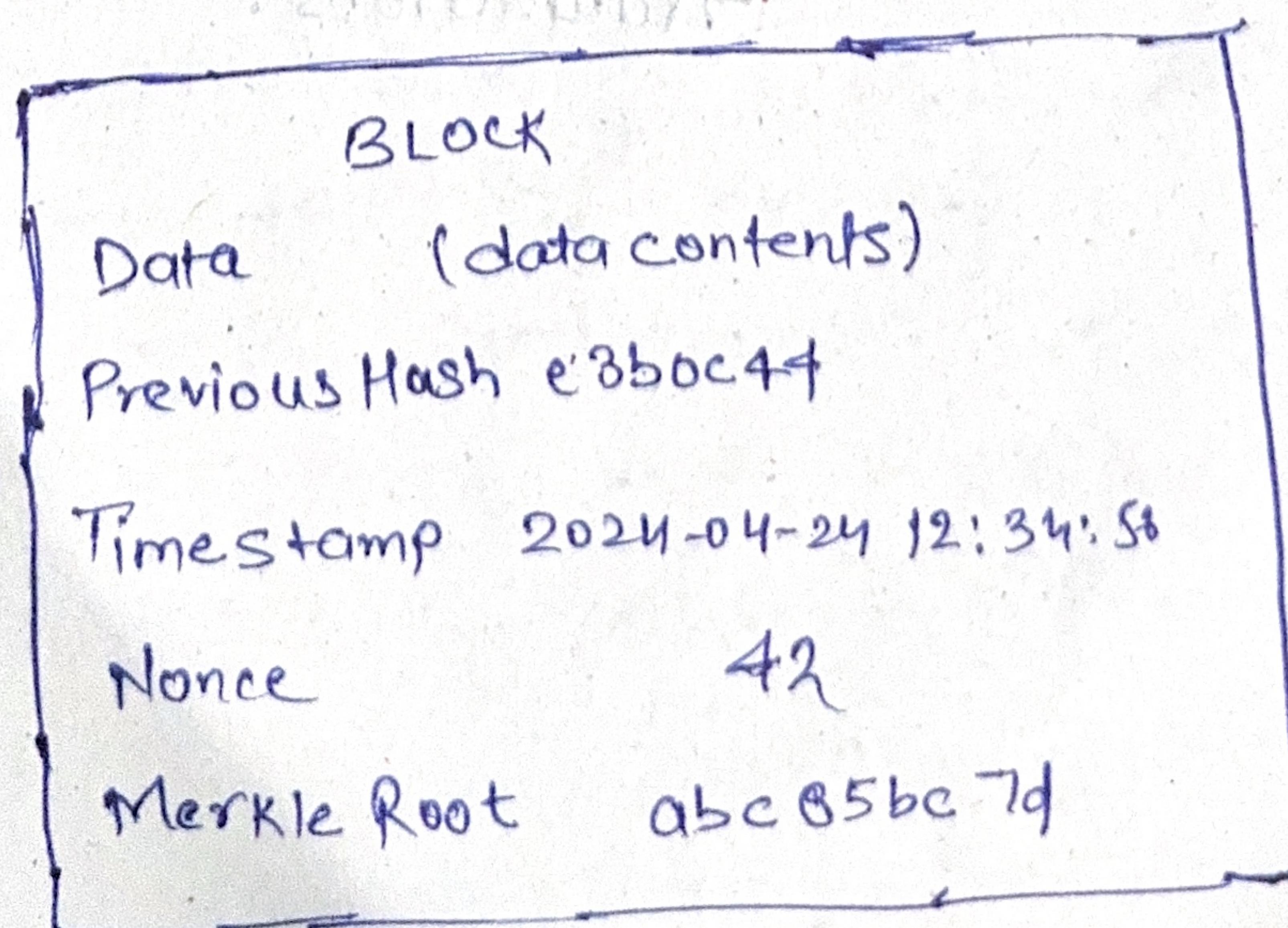
Ans:- A digital database or ledger that is distributed among the nodes of a peer-to-peer network.

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

Ans: (i) Supply chain management :- Blockchain can track products from origin to consumer, ensuring authenticity and quality control. Companies like Walmart use blockchain to monitor food products from farms to shelves, improving transparency and traceability.

(ii) Voting :- Blockchain can be used to create secure and transparent voting system ensuring accurate and verifiable election results.

3- Draw a block showing : data , Previous hash , timestamp , nonce , and Merkle root .



4- The Merkle root ensures data integrity by creating a single hash (root) that represents all transactions in a block. If any transaction changes, the Merkle root will also change.

ex:- Imagine a block with 4 transactions

- TX1 = Hash1
- TX2 = Hash2
- TX3 = Hash3
- TX4 = Hash4

1. Pair & Hash:

$$H1 = \text{hash}(\text{hash1} + \text{hash2})$$

$$H2 = \text{hash}(\text{hash3} + \text{hash4})$$

2. Combine and hash again

$$\text{Merkle Root} = \text{hash}(H1 + H2)$$

Now, Merkle Root = a single hash summarizing all transactions.

5- Proof

meta
comp

add
comf

must

hash

mak

and

Pow

em

dik

n

6- F

r

c

c

do

out

b

5- Proof of work :- Proof of work is a consensus method used in blockchains where miners solve complex puzzles to validate transactions and add new blocks. This process requires high computational power and energy, as miners must try many combinations to find a valid hash. The energy used is intentional, making it costly to manipulate the system and thus securing the network. However, Pow's high electricity consumption raised environmental concerns. As a result, alternatives like proof of stake are being explored for more energy-efficient solutions.

6- Proof of stake (POS) :- is a blockchain consensus mechanism where validators are chosen to create new POS blocks based on the amount of cryptocurrency they "stake" or lock up as collateral. Unlike Proof of work, Pos does not require solving complex puzzles, so it uses far less energy. Validators are selected in a semi random process, often favoring those with more stake, but without requiring intense computation. This makes Pos more environmentally friendly and scalable compared to the

energy-heavy Proof of Work System.

Delegated Proof of Stake (DPOS) is a consensus mechanism where token holders vote to elect a small group of trusted validators (also called delegates) to create and verify new blocks. Unlike regular Proof of Stake, where anyone with enough stake can validate, DPOS separates voting and block production. Validators are selected based on the number of votes they received from the community, which reflects the amount of stake each voter holds. This system increases efficiency and speed but relies more on reputation and community trust to prevent centralization.