Task – 01

Name: Shrilakshmi Kakati

Group: B

1. Define blockchain in your own words

Ans: Blockchain is hashed linked list in other words it is a chain of blocks which contains details about transactions. It is also defined as digital ledger technology which is secure, tamperproof, decentralised, distributed technology, has peer to peer network giving every participant access to the same version of the data., follows consensus mechanisms like PoW, PoS, PoA, PBFT and many more, This makes blockchain is trustworthy. Blockchain was introduced in first introduced in 1991 when researchers Stuart Haber and W. Scott Stornetta developed a system to timestamp digital documents using cryptography, preventing them from being tampered with or misdated. It came into picture when Japanese researcher Satoshi Nakamoto published whitepaper on Bitcoin in 2008 using blockchain.

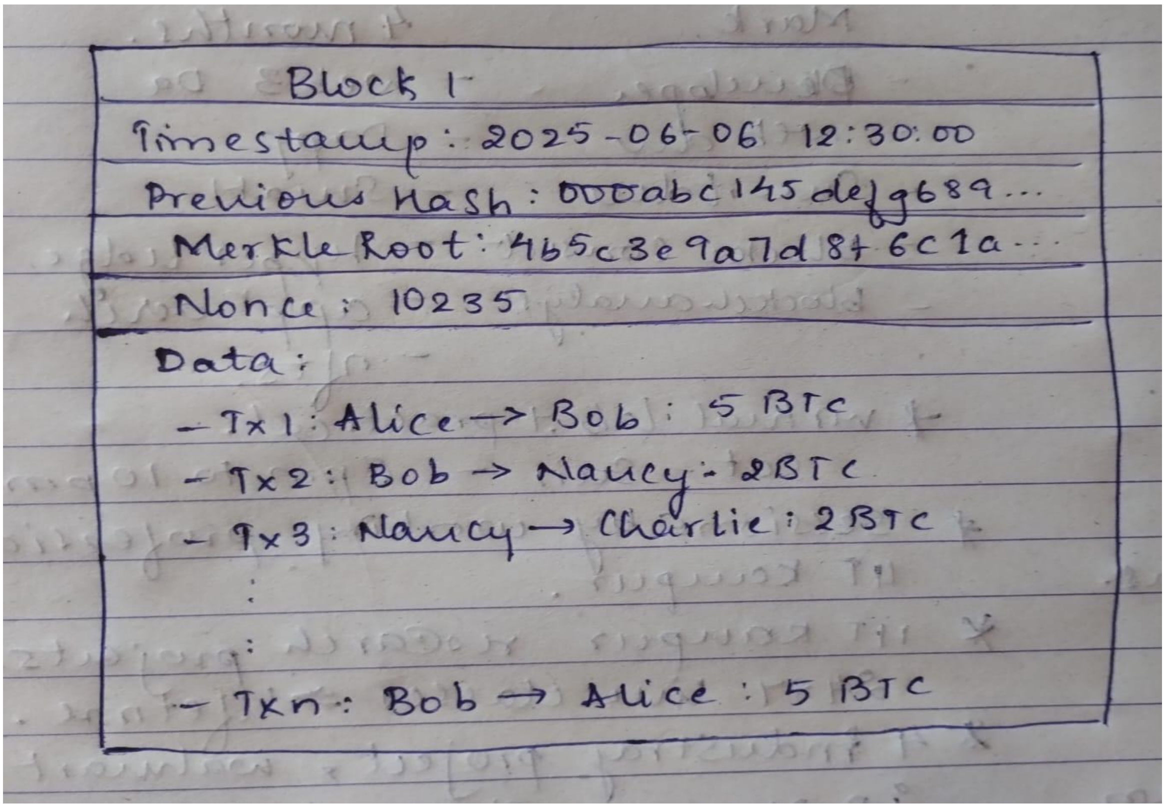
2. List 2 real-life use cases

Ans: Two real-life use cases are

Academic Credential Verification: Universities and institutions use blockchain to store and verify academic records like degrees and mark sheets. For example, MIT issues digital diplomas using blockchain, allowing employers to instantly verify a candidate's qualifications without relying on paper documents or third-party verification.

Supply Chain Management: Companies like IBM and Walmart use blockchain to track the movement of goods from origin to destination. For instance, Walmart uses blockchain to trace the journey of food products like mangoes or pork, helping quickly identify sources of contamination and ensuring food safety and transparency in the supply chain.

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



Block 1

Timestamp: 2025-06-06 12:30:00

Previous Hash: 000abc145defg689...

Merkle Root: 4b5c3e9a7d8f6c1a...

Nonce: 10235

Data:

- Tx1: Alice → Bob : 5 BTC
- Tx2: Bob → Nancy: 2BTC
- Tx3: Nancy → Charlie: 2BTC

:

:

- Txn: Bob → Alice : 5 BTC

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

Ans: Merkle tree is like binary tree which summarizes all transactions in a block. It's like a digital fingerprint of the entire block's data. Even if a tiny change is made to a single transaction, entire Merkle root will change, making it a reliable way to detect tampering.

How merkle tree works is, let’s assusme in a block there are four transactions, in first transaction Alice is sending 5BTC to Bob, In second transaction Bob is sending 2BTC to Nancy, in third transaction Nancy is send 2BTC to Charlie and in fourth transaction Bob sends 5BTC to Alice. Here, each transaction is hashed using cryptographic hash function ie SHA256 as H1, H2.H3 and H4. These are the leaf nodes is bottom level of the tree which is level 0, in level 1 these hases are paired like H12= hash(H1+H2) and similarly with H34 = hash(H3+H4). In level 2, the hashes H12 and H34 are combined and hashed again making it merkle root = hash(H12+H34). This merkle root is stored in block header and it represents all transactions in that block.

How it ensures Integrity is if suppose someone tries to change tx2 where Bob is sending 2BTC to Nancy instead bob sends 4BTC to Nancy then tx2 changes, hence H2 changes and H12 changes and later merkle root also changes. Now this is how merkle tree ensures intehrity of the block.

5. Explain in brief (4–5 sentences each):

a. What is Proof of Work and why does it require energy?

b. What is Proof of Stake and how does it differ?

c. What is Delegated Proof of Stake and how are validators selected?

Ans: a. Proof of Work (PoW) is a consensus mechanism used in blockchains like Bitcoin to validate transactions and add new blocks. It requires miners to solve complex mathematical puzzles using computing power. This process ensures security and decentralization but demands significant computational energy, as only one miner can win the right to add a block and earn rewards. The intense calculations make it difficult for bad actors to manipulate the network.

b. Proof of Stake (PoS) is an alternative to PoW where validators are selected to create new blocks based on the amount of cryptocurrency they "stake" or lock in the network. Unlike PoW, it does not require solving energy-intensive puzzles, making it much more energy-efficient. Validators are incentivized to act honestly, as they risk losing their staked coins if they behave maliciously. PoS significantly reduces the environmental impact and allows for faster transactions.

c. Delegated Proof of Stake (DPoS) is a variation of PoS where token holders vote to elect a limited number of delegates or validators who are responsible for validating transactions and creating blocks. These delegates are often chosen based on community trust and performance, with voting power proportional to the amount of stake held. DPoS offers faster transaction processing and scalability but can be more centralized due to the smaller number of validators. The elected delegates can be replaced at any time through ongoing voting.