Mini Task 1: Build & Explain a Simple Blockchain Task Instructions:

Theoretical Part:

1. *Blockchain Basics*

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

Blockchain is distribute, Immutable digital Ledger system that records transaction across network of computers (also called Nods). This structure ensures that once data is recorded, it becomes immutable—meaning it cannot be altered or deleted. Essentially, blockchain acts as a shared, public record where anyone can view transactions, but no single entity controls it.

Blockchain operates without a central authority, relying on consensus mechanisms like Proof of Work or Proof of Stake to validate transactions. Its applications extend beyond cryptocurrencies, impacting sectors like finance, healthcare, supply chain management, and voting systems by providing transparent, secure, and efficient ways to record and verify information.

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

1. **Healthcare Data Management – Estonia's eHealth System**

Estonia has implemented a blockchain-based eHealth system to secure patient health records. Over 95% of the country's health information is digitized and underpinned by blockchain, allowing authorized healthcare providers to access real-time, accurate patient data. This system enhances patient privacy, reduces administrative burdens, and improves overall healthcare delivery.

1. **Digital Identity – Microsoft's ION**

Microsoft's ION is a decentralized identity system built on the Bitcoin blockchain. It enables users to create and manage their digital identities without relying on third-party providers. Users have full control over their personal data, enhancing privacy and security while simplifying access to various online services

1. *Block Anatomy*

+-------------------------------------------------------------------------------------------------+

| Block Header |

+-------------------------------------------------------------------------------------------------+

| Previous Hash: 0000000000000000000a1b2c3d4e5f6789abcdef123456 |

| Timestamp: 2025-06-07 09:31:50 UTC |

| Nonce: 2083236893 |

| Merkle Root: 4d5e6f7a8b9c0d1e2f3a4b5c6d7e8f9a0b1c2d3e4f5a6b7 |

+--------------------------------------------------------------------------------------------------+

| Block Body |

+--------------------------------------------------------------------------------------------------+

| Transactions: |

| - TXID1: a1b2c3d4e5f6... |

| - TXID2: b2c3d4e5f6g7... |

| - TXID3: c3d4e5f6g7h8... |

| ... |

+--------------------------------------------------------------------------------------------------+

**Explanation of Components:**

* **Previous Hash**: This is the cryptographic hash of the preceding block's header, linking the blocks together and ensuring the immutability of the blockchain.
* **Timestamp**: Indicates the exact time when the block was created or mined. This helps in maintaining the chronological order of blocks.
* **Nonce**: A random number that miners adjust to find a hash that meets the network's difficulty target. It's a crucial part of the Proof-of-Work consensus mechanism.
* **Merkle Root**: A single hash value representing all transactions in the block. It's derived from a Merkle Tree, which efficiently summarizes and verifies the integrity of the transactions.
* **Transactions**: The actual data or records included in the block, such as cryptocurrency transfers or smart contract executions. Each transaction has a unique identifier (TXID).

This structure ensures data integrity, transparency, and security within the blockchain network.

1. *Consensus Conceptualization*

Explain in brief (4–5 sentences each):

■ *What is Proof of Work and why does it require energy?*

**Proof of Work (PoW)** is a consensus mechanism used in blockchain networks like Bitcoin to validate transactions and maintain network security. In this system, miners compete to solve complex mathematical puzzles, and the first to solve one earns the right to add a new block to the blockchain and receive a reward.

**Why Does PoW Require Significant Energy?**

The energy-intensive nature of PoW arises from several factors:

1. **High Computational Demand**: Solving PoW puzzles requires substantial computing power. Miners use specialized hardware to perform countless calculations per second, consuming significant electricity.
2. **Continuous Operation**: To maximize chances of solving puzzles, mining rigs operate 24/7, leading to constant energy consumption.
3. **Cooling Requirements**: Mining equipment generates considerable heat, necessitating cooling systems that further increase energy usage.
4. **Redundant Effort**: Only one miner wins the right to add a new block, rendering the efforts of all other miners in that round as energy expended without direct reward.

These factors contribute to the high energy consumption associated with PoW, prompting discussions about its environmental impact and the exploration of alternative consensus mechanisms like Proof of Stake (PoS), which require significantly less energy.

■ *What is Proof of Stake and how does it differ?*

**Proof of Stake (PoS)** is a consensus mechanism used in blockchain networks to validate transactions and maintain security. Unlike Proof of Work (PoW), which relies on miners solving complex mathematical puzzles, PoS selects validators based on the amount of cryptocurrency they "stake" or lock up as collateral.

 **Energy Efficiency**: PoS is more environmentally friendly due to its lower energy requirements compared to PoW.

 **Security**: While PoS reduces energy consumption, it introduces concerns about centralization, as those with more significant stakes have more influence.

■ *What is Delegated Proof of Stake and how are validators selected?*

**Delegated Proof of Stake (DPoS)** is a consensus mechanism that enhances the efficiency and scalability of blockchain networks by allowing token holders to elect delegates responsible for validating transactions and producing new blocks. This system aims to address the limitations of traditional Proof of Stake (PoS) by introducing a more democratic and performance-oriented approach.

**How Are Validators (Delegates) Selected?**

In DPoS, token holders participate in a voting process to elect a limited number of delegates, also known as witnesses or block producers, who are entrusted with the responsibility of validating transactions and adding new blocks to the blockchain. The selection process typically involves the following steps:

1. **Voting Power**: Each token holder's voting power is proportional to the number of tokens they hold. This means that users with more tokens have a greater influence in the election of delegates.
2. **Delegate Election**: Token holders vote for their preferred delegates. The delegates with the highest number of votes are selected to validate transactions and produce blocks.
3. **Delegate Rotation**: The number of elected delegates is fixed and can range from 20 to 100, depending on the network's protocol. These delegates work in a round-robin fashion, taking turns to produce blocks.
4. **Continuous Voting**: Voting is an ongoing process, allowing token holders to replace underperforming or malicious delegates at any time, ensuring accountability and responsiveness within the network.