Mini Task 1: Build & Explain a Simple Blockchain

Theoretical Part:

1. **Blockchain Basics**

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

     A distributed and decentralized digital ledger that safely logs transactions over a network of computers is called a blockchain. Blockchain works via a peer-to-peer network in which every participant (node) has a copy of the complete ledger, negating the need for a central authority. A secure and immutable chain of data is ensured by grouping transactions into blocks, each of which contains a cryptographic hash of the one before it. The system is extremely tamper-resistant since once a block is added, it cannot be changed without changing all subsequent blocks and obtaining consensus from most of the network. Blockchain guarantees trust, transparency, and immutability in situations where participants might not have complete faith in one another. It serves as the foundational technology for cryptocurrencies like Bitcoin and Ethereum and has uses in supply chains, healthcare, and identity management.

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

     1.Healthcare Data Management

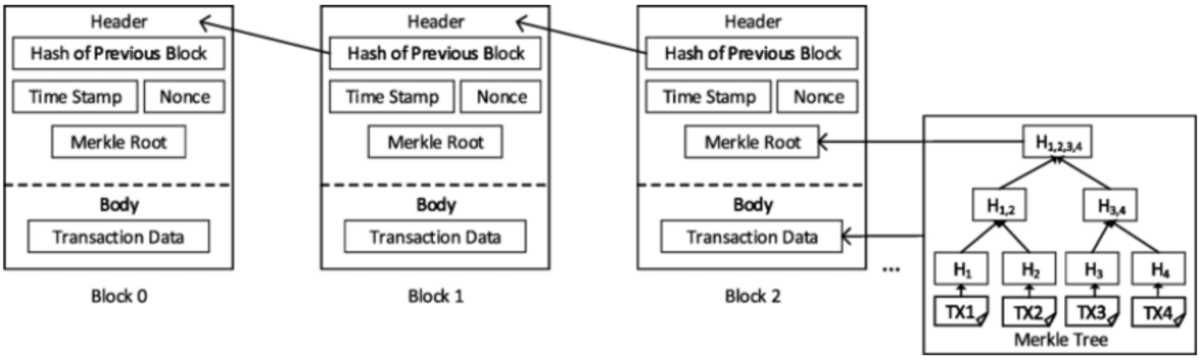
     Blockchain can securely store and share patient medical records across hospitals and healthcare providers. It ensures data integrity, privacy, and interoperability. Patients can control access to their records, while providers can avoid duplicate tests and reduce errors. This leads to improved treatment coordination and patient outcomes.\

     2. Voting Systems (E-Voting)

     Blockchain-based voting systems can offer a **transparent, secure, and tamper-proof** platform for elections. Each vote is recorded as a transaction that cannot be altered once added to the blockchain. It ensures voter anonymity while allowing verifiable results, helping to eliminate fraud and increase trust in democratic processes.

1. **Block Anatomy**

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



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

Merkle Root: Verifying Data Integrity

A Merkle Root is the top hash of a binary hash tree called a Merkle Tree. It is used to efficiently and securely verify the integrity of a large set of data, such as transactions in a blockchain.

Example:

Suppose there are four transactions: Tx1, Tx2, Tx3, and Tx4.

1. First, each transaction is hashed individually:

- H1 = hash(Tx1)
- H2 = hash(Tx2)
- H3 = hash(Tx3)
- H4 = hash(Tx4)

2. Then, these hashes are paired and hashed again:

- H12 = hash(H1 + H2)
- H34 = hash(H3 + H4)

3. Finally, the two paired hashes are combined and hashed to get the Merkle Root:

- Root = hash(H12 + H34)

The Merkle Root represents the entire set of transactions.

Verifying Integrity:

To verify if Tx2 is included in the data without checking all transactions, only a small subset of hashes is needed: Tx2, its sibling hash H1, and the hash H34.

By computing hash(H1 + hash(Tx2)) to get H12, then hash(H12 + H34) to get the Root, we can compare this with the stored Merkle Root. If they match, Tx2 is confirmed as part of the original data and has not been tampered with.

Advantages:

- Verification is efficient, requiring only a few hashes instead of all data.
- It is scalable, as the number of hashes needed grows logarithmically with the number of transactions.
- It ensures security, since any change in any transaction changes the Merkle Root.

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)

          Proof of Work is a consensus mechanism where miners compete to solve complex mathematical puzzles to validate transactions and create new blocks. It requires significant computational power and energy because solving these puzzles demands high-performance hardware working intensively. This energy consumption acts as a security feature, making attacks expensive and difficult. The first miner to solve the puzzle gets to add the block to the blockchain and receive a reward.

        - What is Proof of Stake and how does it differ?

          Proof of Stake is a consensus method where validators are chosen to create new blocks based on the amount of cryptocurrency they hold and “stake” as collateral. Unlike PoW, PoS does not require energy-intensive computations, making it more energy-efficient. Validators are incentivized to act honestly since they can lose their stake if they validate fraudulent transactions. This mechanism replaces mining puzzles with economic stake as the security source.

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

  Delegated Proof of Stake is a variation of PoS where cryptocurrency holders vote to elect a limited number of trusted delegates or validators. These elected validators are responsible for validating transactions and maintaining the blockchain. Because only a small number of validators participate, DPoS can achieve faster transaction speeds and greater scalability. The voting process ensures that validators are accountable to the community that elects them.