Blockchain Assignment - Theoretical Part

1. Blockchain Basics

Definition

A blockchain is a decentralized, distributed digital ledger that records transactions across multiple computers in a way that makes them extremely difficult to alter or hack. Each "block" contains a collection of transactions, a timestamp, and a cryptographic hash of the previous block, creating an immutable chain. This structure ensures that once data is recorded, it cannot be changed without altering all subsequent blocks, which would require consensus from the majority of the network. The decentralized nature means no single entity controls the blockchain, making it transparent and resistant to censorship. Blockchain eliminates the need for trusted intermediaries by using cryptographic proof and consensus mechanisms to validate transactions, creating a trust-less system where participants can transact directly with confidence.

Real-Life Use Cases

1. Healthcare Records Management

Use Case: Secure and interoperable medical records
Example:
MedRec, a blockchain-based project by MIT, allows patients and healthcare providers to access and share medical data securely.
It ensures:

- Tamper-proof patient history
- Data privacy and control by the patient
- Interoperability across hospitals and systems without a central database

2. Voting Systems

Use Case: Transparent and tamper-resistant digital voting
Example:
In 2019, **West Virginia** (USA) piloted blockchain voting for overseas military personnel using the **Voatz** app.
This enabled:

- Secure identity verification
- End-to-end verifiable voting
- Elimination of ballot tampering or manipulation

2. Block Anatomy

BLOCK #2

Index: 1

Timestamp: 2025-06-07 10:30:00

Data: "Nitin Sent 1 BTC"

Previous Hash:
c01e35d4523d5d75062ae450c48f5ca5b7a54169f7655eb52cef0af3ce63a7da

Merkle Root: 45xyz890...abc123

Nonce: 147852

Hash:
01a1f615f49d8cf7780b5e3b246873456c8bb1b9e60394beb19bdba960f76714

Merkle Root Explanation

The **Merkle root** is a cryptographic summary of all transactions in a block. It is generated by hashing pairs of transactions repeatedly until a single root hash is obtained. The Merkle root is a single hash that represents all transactions in a block through a binary tree structure. For example, if a block contains 4 transactions [T1, T2, T3, T4]:

- Level 1: Hash(T1), Hash(T2), Hash(T3), Hash(T4)
- Level 2: Hash(Hash(T1)+Hash(T2)), Hash(Hash(T3)+Hash(T4))
- Level 3 (Root): Hash(Level2_Left + Level2_Right)

This helps verify data integrity because any change to a single transaction would cascade up the tree, completely changing the Merkle root. If any transaction (e.g., T2) is altered, the Merkle root changes, signaling tampering. This helps in efficiently verifying data integrity without checking every transaction. You can verify specific transactions exist without downloading the entire block by providing a "Merkle path" - just the hashes needed to reconstruct the root.

3. Consensus Conceptualization

Proof of Work (PoW)

Proof of Work is a consensus mechanism where miners compete to solve computationally intensive puzzles to validate blocks and add them to the blockchain. Miners repeatedly hash block data with different nonce values until they find a hash meeting specific difficulty criteria (e.g., starting with multiple zeros). This process requires significant computational power and electricity because miners must perform millions of hash calculations. The energy requirement is intentional - it makes the network secure by making attacks economically unfeasible, as an attacker would need to control more computational power than the rest of the network combined.

Proof of Stake (PoS)

Proof of Stake selects validators to create new blocks based on their stake (ownership) in the network rather than computational power. Validators are chosen probabilistically, with higher stakes increasing selection chances. Instead of mining, validators "forge" blocks and earn transaction fees as rewards. PoS differs from PoW by consuming 99% less energy since there's no computational competition. Validators risk losing their staked tokens if they act maliciously, creating economic incentives for honest behavior without requiring massive energy consumption.

Delegated Proof of Stake (DPoS)

Delegated Proof of Stake is a more democratic version where token holders vote to elect a limited number of delegates (typically 21-101) who take turns producing blocks. Validators are selected through continuous voting, and delegates with the most votes become active block producers. This system is faster than PoW and PoS because fewer validators need to reach consensus. Delegates can be voted out if they misbehave, and they share rewards with voters who supported them. DPoS trades some decentralization for improved scalability and transaction speed.