Mini Task 1: Build & Explain a Simple Blockchain

Blockchain Basics

1 Define blockchain in your own words (100–150 words):

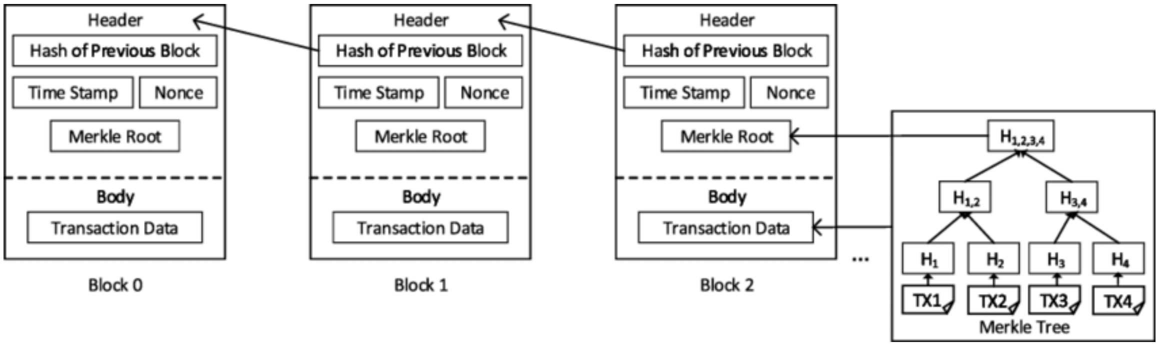
A blockchain is a decentralized and distributed digital ledger that records transactions across many computers so that the record cannot be altered retroactively without the consensus of the network. Each transaction is grouped into a 'block' and linked to the previous block using cryptographic hashes, forming a secure 'chain' of blocks. This structure ensures transparency, security, and immutability. Blockchain eliminates the need for a central authority, making systems more secure and trustworthy. It is most commonly associated with cryptocurrencies like Bitcoin, but its potential extends far beyond, providing solutions for various industries that require secure and tamper-proof data sharing.

2 real-life use cases:

1. Supply Chain Management – Blockchain helps track the origin and movement of goods through every stage of the supply chain, improving transparency and reducing fraud.
2. Digital Identity – Individuals can own and control their identity credentials securely without relying on centralized authorities, preventing identity theft and improving verification processes.

Block Anatomy

Block Structure Diagram



Explain how the Merkle root helps verify data integrity:

The Merkle root is a single hash that represents all transactions in a block. It is derived by repeatedly hashing pairs of transaction hashes until a single root hash is obtained. For example, if there are four transactions (Tx1, Tx2, Tx3, Tx4), they are hashed and combined: hash(Tx1+Tx2), hash(Tx3+Tx4), and then hashed again to get the Merkle root. If any single transaction is altered, its hash changes, causing the Merkle root to change as well. This allows quick verification of data integrity and ensures that no data within the block has been tampered with.

Consensus Conceptualization

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

Proof of Work (PoW) is a consensus algorithm that requires network participants (miners) to solve complex mathematical puzzles to validate transactions and add new blocks to the blockchain. This process requires significant computational power and energy, as it involves repeated hashing to find a nonce that meets the network’s difficulty target. The energy is essentially the cost of securing the network, making it expensive and difficult for bad actors to alter the blockchain.

What is Proof of Stake and how does it differ?

Proof of Stake (PoS) replaces the energy-intensive mining process with a system where validators are chosen to create new blocks based on the number of coins they hold and are willing to 'stake' as collateral. This means that validators with more stake have a higher chance of being selected to validate transactions. Unlike PoW, PoS is more energy-efficient and encourages honest behavior, as validators stand to lose their stake if they act maliciously.

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

Delegated Proof of Stake (DPoS) is a variation of PoS where token holders vote to elect a limited number of trusted delegates or validators who are responsible for validating transactions and maintaining the blockchain. This system is faster and more democratic, as it allows stakeholders to influence the governance of the network. Validators are selected based on community votes, and they can be replaced if they fail to act in the network's best interest.