1. **Blockchain Basics**
   1. Define blockchain in your own words.

Blockchain is a decentralized, distributed network and public digital ledger where everyone in the network holds a copy of the data. The records are immutable and secure. This data is stored in units called blocks, which are linked together to form a chain, hence the name blockchain. The blocks are arranged in chronological order, reflecting the sequence of events. Each block contains a list of transactions, a timestamp, and a cryptographic hash of the previous block, ensuring integrity and continuity. Transactions can include operations like the transfer of cryptocurrency or digital assets. Before a block is added to the chain, the network reaches consensus using mechanisms such as Proof of Work or Proof of Stake. This eliminates the need for a central authority and builds trust among participants. The cryptographic and consensus-based structure of blockchain makes it highly secure and resistant to tampering or fraud.

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

Health Care, Voting

1. **Block Anatomy**
   1. Draw a block showing: data, previous hash, timestamp, nonce, and Merkle root.

**Single Block**

| Header |
| --- |
| Previous Block Hash |
| Timestamp |
| Nonce |
| Merkle Root |

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

Merkle Root is the topmost hash in a Merkle Tree. Merkle Tree is a binary tree structure in blockchain that is used to store data efficiently. This helps us to securely verify the integrity of large sets of data. Every transaction is hashed. Hashing pairs are created from the leaf node up to the root in a repeated process until a single hash value is obtained. So, if a single transaction is altered its hash value gets changed.This will trigger the change in hashes up till the root creating a new Merkle root. By comparing the current root value against the new one we can verify whether the data is tampered or not.

For example, if a block contains four transactions (T1, T2, T3, T4), their hashes are combined in pairs to form higher-level hashes, and finally a single Merkle Root. If T2 is changed, the Merkle Root also changes, helping us detect tampering.

1. **Consensus Conceptualization  
   a.** What is Proof of Work and why does it require energy?

Bitcoin is a large public blockchain network which consists of thousands of nodes from different parts of the world. Reaching consensus here is a huge challenge. So this network uses a mechanism that works on large networks even in the presence of bad or malicious nodes. Proof of Work (PoW) is the consensus mechanism used in Bitcoin to validate transactions and add new blocks to the chain. As the participants in the network are anonymous to each other there exists no trust. So, in order to reach an agreement and select a block, it issues a cryptographic puzzle to the participating nodes. Whoever solves the puzzle using computational power is the leader and can suggest the block. If valid, the block is accepted by the rest of the network. The miner is rewarded with a fixed amount of Bitcoin. Before adding the newly selected block to the chain, every node will validate it. The solution to the puzzle gets included in the selected block and other nodes can verify it. If the validation passes the new block is added to the chain.

PoW requires a large amount of energy because solving the puzzle demands powerful hardware running continuously, consuming electricity. The difficulty of the puzzle is intentionally high to prevent spam or attacks on the network. As more miners join, the competition increases, leading to higher energy consumption. This energy-intensive process is what secures the network but also raises environmental concerns.

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

Proof of Stake (PoS) is a consensus mechanism used in blockchain networks like Ethereum to validate transactions and add new blocks to the chain. Unlike Proof of Work (PoW), which relies on solving complex puzzles using powerful computers, PoS selects validators based on the amount of cryptocurrency they are willing to lock up as a stake.

Validators are usually chosen through a combination of stake size and random selection. The more a user stakes, the higher their chances of being selected, but randomness is included to avoid centralization and give smaller stakeholders a fair opportunity.

This method significantly reduces energy consumption, as it doesn’t involve computational mining. Once a validator is selected, they propose a block, and if other nodes verify and accept it, the block is added to the chain and the validator receives a reward.

Compared to PoW, PoS is more energy-efficient, cost-effective, and scalable. While PoW favors those with more computational power, PoS favors those with more staked assets, making it more suitable for modern blockchain networks aiming for sustainability and decentralization.

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

Delegated Proof of Stake (DPoS) is a variation of the Proof of Stake (PoS) consensus mechanism, designed to be faster and more democratic. Blockchains like EOS, Tron, and Steem use this consensus mechanism.

In DPoS, network participants vote for a small group of trusted validators, called delegates, who are responsible for validating transactions and adding new blocks. Each participant's voting power is usually based on the amount of cryptocurrency they hold (stake).

Out of all the candidates, only a limited number—usually the top N with the most votes (e.g., top 21 in EOS)—are selected to actively validate transactions and create new blocks.These chosen delegates take turns producing blocks in a round-robin fashion, and they are rewarded for their service. If a delegate fails to perform well or act honestly, users can vote them out and replace them with another. Because there are fewer validators and block production is more organized (delegates take turns), DPoS systems can process transactions much faster than PoW or PoS. It promotes community governance but can be more centralized due to the limited number of validators. If the same delegates keep getting elected, they might gain too much power, possibly leading to collusion or unfair practices.