1. Blockchain Basics
○ **Define blockchain in your own words (100–150 words).**
○ **List 2 real-life use cases (e.g., supply chain, digital identity).**

A blockchain is a decentralized and distributed digital ledger that records transactions across numerous computers to enable security, transparency, and unchangeable transaction records.

All transactions are recorded in a block of digital information, and all blocks are cryptographically linked together chronologically.

Once information is recorded in a blockchain, it is usually impossible to change that information unless the whole network agrees to change the information since, otherwise, the original data cannot be amended.

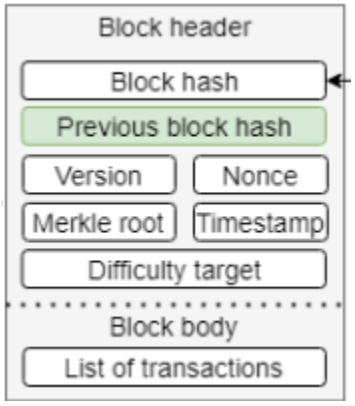
Instead of having a central authority validate the transactions, a blockchain uses a consensus mechanism such as Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions.

Blockchain increases trust between actors in a digital ecosystem by taking away the need for intermediaries which validate peer to peer.

<u>Examples of Real-World Use Cases:</u>
Supply Chain Management:

Tracking goods in a way that is consistently transparent from point of origin to end point.
Improves verification of product authenticity and increases visibility of logistics.
Digital Identity Verification
Giving individuals ownership and control of their own digital identities.
Reduces concerns of identity theft and allows for validating identity securely online.

2. 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.**



A Merkle Root is the first hash in a Merkle Tree. A Merkle Tree is a binary tree structure where:

Each leaf node is a hash of a single transaction.
Each parent node is a hash of its two child nodes.

This continues until only a single hash remains: the Merkle Root.

How this allows for data integrity validation:

To determine whether Tx1 is contained in the block, all you need is:
H1, H2, H34 (not every one of the transactions)
Then, you just recompute the Merkle Root using the 3 hashes.
If your Merkle Root matches the Merkle Root in the block header, you have validated Tx1.
This is an efficient method to verify data integrity without having to access the entire dataset.

3. Consensus Conceptualization
○ **Explain in brief (4–5 sentences each):**
■ **What is Proof of Work and why does it require energy?**
■ **What is Proof of Stake and how does it differ?**
■ **What is Delegated Proof of Stake and how are validators selected?**

What is proof of work and why does it consume energy?
Proof of Work is a consensus mechanism where miners compete against each other to solve complex mathematical puzzles, validate transactions and add another block to the chain.

The first miner to solve the puzzle gets to add the next block and is rewarded with cryptocurrency.

These puzzles are designed to require large amounts of computational power, which means expensive hardware and electricity.

This energy-demanding process is designed to secure the network and protect against attacks like double-spending.

What does Proof of Stake (PoS) mean and how is it different?
Proof of Stake uses validators that put up an amount of cryptocurrency they “stake” or lock up as collateral.
Validators are then randomly selected based not on computational power, but on how much cryptocurrency they have staked, and sometimes additional factors, like coin age.

The energy efficiency of PoS is significantly greater than PoW, as miners no longer have to constantly solve complex puzzles.

In short, PoS is economic commitment instead of computing resources to validate cryptocurrency transactions for network security.

What is Delegated Proof of Stake (DPoS) and how are Validators chosen?
Delegated Proof of Stake is a type of consensus mechanism in which coin holders vote to select a relatively small number of trusted delegates or validators.

These elected validators validate transactions and create new blocks.

Voting power is proportional to the amount of stake in hand by the voter.

DPoS has many benefits such as increased speed of transactions and scalability, but it can pose some potential centralization because of a limited pool of validators.