**Task 1: Build & Explain a Simple Blockchain**

**What is Blockchain?**

A blockchain is like a digital notebook that records information in a very safe and organized way. Once something is written in this notebook (a block), it cannot be changed. Each block is connected to the one before it, forming a long chain — that’s why it’s called blockchain. It is shared with many people (computers) around the world, so no one person controls it. Everyone checks and agrees before adding anything new. This makes it secure, honest, and transparent.

* **Two Real-Life Use Cases:**

**1. Supply Chain Tracking**

* **Tracks where goods (like food or medicines) come from.**
* **Helps verify authenticity and ensures safe delivery.**
* **Used by companies like IBM Food Trust.**

**2. Digital Identity Verification**

* **Creates a secure online ID using blockchain.**
* **Reduces fraud and protects privacy.**
* **Useful for voting, banking, and KYC (Know Your Customer) processes.**
* **What’s Inside a Block?**

Imagine a block like a small data box. It contains:

* **Timestamp** – When it was created
* **Data** – A message or transaction (e.g., “Person A sent 10 coins to Person B”)
* **Nonce** – A number used to solve a puzzle
* **Previous Hash** – The digital fingerprint of the last block
* **Merkle Root** – A special summary of all the data inside
* **Hash** – The block’s own fingerprint

**Simple Diagram of a Block:**

┌─────────────────────────────┐

│ BLOCK │

├─────────────────────────────┤

│ Timestamp : 2025-06-08 │

│ Data : "Tx A→B" │

│ Nonce : 54891 │

│ Previous Hash : a1b2c3... │

│ Merkle Root : f4e3d2... │

│ Hash : 9f8e7d... │

└─────────────────────────────┘

* **What is a Merkle Root?**

The Merkle root is like a summary of all transactions inside a block. Here's how it works:

* If there are 4 transactions: Tx1, Tx2, Tx3, Tx4
* Hash them: H1, H2, H3, H4
* Combine in pairs:
  + H12 = hash(H1 + H2)
  + H34 = hash(H3 + H4)
* Then combine those:
  + Merkle Root = hash(H12 + H34)

**NOTE** : If **any** transaction is changed, the Merkle root changes. This helps quickly check if anything was tampered with.

* **Consensus Mechanisms**

**1. Proof of Work (PoW)**

* Computers (miners) race to solve a math puzzle.
* It takes a lot of energy and time (like a brain workout).
* The first to solve it adds the block and gets a reward.
* It’s very secure but uses a lot of electricity.

**2. Proof of Stake (PoS)**

* People “lock” some coins as a promise to behave.
* More coins locked = higher chance to add the block.
* It’s faster and uses much less energy than PoW.

**3. Delegated Proof of Stake (DPoS)**

* Everyone votes for trusted people (delegates) to add blocks.
* Only elected delegates add blocks.
* It’s like picking class leaders — faster but needs good voting.

**Questions:**

**1.What is Proof of Work (PoW) and why does it require energy?**

* **Proof of Work** is like a race between computers to solve a complex math puzzle.
* The **first computer** (called a **miner**) to solve it gets to **add the next block** to the blockchain.
* To win, miners try different numbers (called **nonces**) until the answer (hash) starts with a specific pattern (like 0000...).
* This process takes a **lot of computer power** and **electricity**, which is why PoW is **energy-intensive**.
* The high energy use makes it **very secure** — because attacking the system would cost a huge amount of energy.

**2.What is Proof of Stake (PoS) and how does it differ?**

* **Proof of Stake** is a **more eco-friendly** alternative to PoW.
* Instead of solving puzzles, people who **own coins** (called **stakers**) can **lock up** some of their coins as a **stake**.
* The system then **randomly picks one of them** to add the next block — but those with **more stake** have **higher chances**.
* It doesn’t use high energy because there’s **no mining race** — just a fair selection.
* It encourages honesty: if someone cheats, they lose their **staked coins**.

**3. What is Delegated Proof of Stake (DPoS) and how are validators selected?**

* In **Delegated Proof of Stake**, everyone gets to **vote** for a small group of **trusted delegates**.
* These **delegates** are responsible for **validating blocks** and maintaining the network.
* The more coins you have, the **more voting power** you hold.
* Only the **top-voted** delegates (like class leaders) get to create new blocks.
* DPoS is **faster and more scalable** than PoW and PoS, but it depends on the **trustworthiness** of elected delegates.