**Mini Task 1**

**Blockchain:**

A blockchain is a distributed ledger(notebook) that records transactions across multiple computers. It is designed to be secure, transparent, and doesn’t need middleman like a bank. Each block in the blockchain contains a list of transactions, a timestamp, as well as its own unique alphanumeric code, called a hash. These cryptographically generated codes can be thought of as a digital fingerprint. They play a crucial role in linking blocks together.

**Why Blockchain?**

Blockchain is a revolutionary technology because it helps reduce security risks, Fraud Preventionand bring transparency in a scalable way.

Due to its Enhanced Blockchain security, every transaction is encrypted and recorded in a block.

**How blockchain and distributed ledger technology work**

* Blockchain uses a multistep process that includes the following five steps:
* An authorized participant inputs a transaction, which must be authenticated by the technology.
* That action creates a block that represents the specific transaction or data.
* The block is sent to every computer node in the network.
* Authorized nodes validate transactions and add the block to the existing blockchain.
* The update is distributed across the network, which finalizes the transaction.

These steps take place in near real time and involve a range of elements. Nodes in public blockchain networks are referred to as miners; they're typically paid for this task -- often in processes called proof of work (PoW) or proof of stake (PoS) -- usually in the form of cryptocurrency.

A blockchain ledger consists of two types of records: individual transactions and blocks. The first block has a header and data that pertain to transactions taking place within a set time period. The block's timestamp is used to help create an alphanumeric string called a hash. After the first block has been created, each subsequent block in the ledger uses the previous block's hash to calculate its own hash.

Before a new block can be added to the chain, its authenticity must be verified by a computational process called **validation or consensus**. At this point in the blockchain process, a majority of nodes in the network must agree the new block's hash has been calculated correctly. Consensus ensures that all copies of the blockchain distributed ledger share the same state.

Once a block has been added, it can be referenced in subsequent blocks, but it can't be changed. If someone attempts to swap out a block, the hashes for previous and subsequent blocks will also change and disrupt the ledger's shared state.

When consensus is no longer possible, other computers in the network are aware that a problem has occurred, and no new blocks are added to the chain until the problem is solved. Typically, the block causing the error will be discarded and the consensus process will be repeated. This eliminates a single point of failure.

**Blockchain Technology Across Various Industries:**

1. Finance and Banking
2. Cyber Security
3. Supply Chain Management
4. Healthcare
5. Government

**Finance and Banking:**

Financial services use blockchain to accelerate transactions and speed up close times. Some banks also use blockchain for contract management and traceability purposes. For example, PayPal, the online payment platform, launched a blockchain-based service in 2020 that lets users buy, hold and sell cryptocurrency.

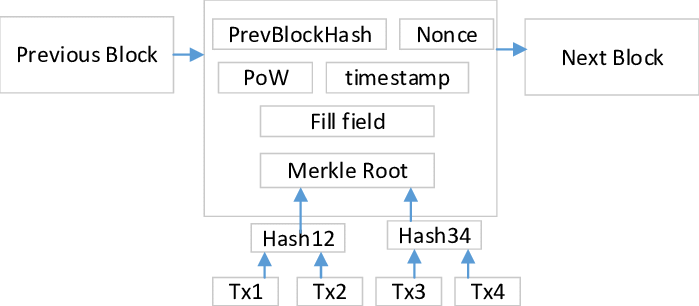
**Supply chain management**:

Tracking of a product can be done with blockchain technology, by facilitating traceability across the entire Supply chain. Blockchain gives the facility to verify and audit transactions by multiple supply chain partners involved in the supply chain management system.

Blockchain records transaction (history, timestamp, date, etc.) of a product in a decentralized distributed ledger

With blockchain, anyone can verify the authenticity or status of a product being delivered

**Block Anatomy**

Blockchain Structure shows data, previous hash, timestamp, nonce, and Merkle root.

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

Blockchain is a peer-to-peer network consisting of blocks linked together. A hash tree, or Merkle tree helps blockchain to encode data efficiently and securely. It enables quick verification and data movement. When a transaction happens on the blockchain it creates a hash, which is stored in a tree-like structure, linked to its parent.

The parent is a Merkle root which is the last transaction hash. It connects all transaction hashes in a block, creating an upside-down binary tree. The hashing starts at the lowest level nodes and continues at higher levels until reaching the single top root hash, the Merkle root.

This root hash contains all information about every transaction hash on the block, offering a single-point hash value that enables validating everything present on that block. The Merkle tree and Merkle root mechanism significantly reduce the levels of hashing required, enabling faster verification and transactions. How Merkle Tree Works?

Cryptographic hash functions are efficient and irreversible one-way functions used in cryptography. They are commonly used in Message Direct (MD), Secure Hash Function (SHF), and RIPE Message Direct (RIPEMD) families.

Now, take an example, if you use the SHA256 hash algorithm, you will get the following output

fbffd63a60374a31aa9811cbc80b577e23925a5874e86a17f712bab874f33ac9

In Merkle trees all transactions comes in a block and generate a digital fingerprint of operations, are built from the bottom using Transaction IDs. Each non-leaf node is a hash of its previous hash, while every leaf node is a hash of transactional data.

**Example:**

* Transactions: T1, T2, T3, T4
* Hash T1 and T2 → H1
* Hash T3 and T4 → H2
* Hash H1 and H2 → **Merkle Root**

If even one transaction (e.g., T3) is tampered with, the Merkle Root changes. This allows anyone to verify the **integrity of all transactions** without checking every single one — saving time and ensuring trust.

**Consensus Conceptualization:**

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

Proof of work (PoW) is a decentralized consensus mechanism that requires network members to expend effort in solving an encryption puzzle.

It is a secure peer-to-peer transaction processing without needing a trusted third party.

The extensive energy requirement of solving the calculation using nonce values from miners (to meet the difficulty criteria like specific hash beginnings, e.g.'0000.') requires vast computing power. An individual who successfully finds the requested hash can add the block and enjoys the reward. It maintains security but needs a substantial amount of power resources.

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

Proof of Stake selects validators based on the amount of cryptocurrency they "stake" or lock up. The more you stake, the higher your chance of being chosen to validate the next block. Unlike PoW, PoS doesn't require solving puzzles or using massive computing resources, making it more energy-efficient. It encourages honesty, because if validators cheat, they lose their stake.

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

DPoS is a variation of proof-of-stake. Instead of all stakers validating blocks, token holders vote to elect a small number of delegates. These delegates take turns adding new blocks. The system is fast and efficient, allowing high throughput.

The top-voted delegates get to validate blocks. If a delegate acts badly, voters can remove them. DPoS balances speed, efficiency, and decentralization.