**Submitted by : Mani Verma**

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

#### Theoretical Part:

1. Blockchain Basics

A blockchain is a decentralized, immutable digital ledger that records transactions across a network of computers in such a way that the data is secure, transparent, and tamper-proof. It consists of a chain of blocks, where each block contains transaction data, a timestamp, and a cryptographic hash of the previous block. This linking of blocks ensures data integrity and chronological order. Blockchain operates without a central authority, relying instead on consensus algorithms like Proof of Work (PoW) or Proof of Stake (PoS) to validate transactions. This technology underpins cryptocurrencies like Bitcoin but has broader applications in areas requiring trust and transparency.

1. Two real life use case

**Supply Chain Management**: Companies use blockchain to track goods from origin to consumer, ensuring transparency and authenticity (e.g., Walmart's food traceability).  
**Digital Identity**: Blockchain allows secure storage and verification of personal credentials (e.g., Estonia’s e-residency program)  
+----------------------+

| Block |

+----------------------+

| Data: "Tx Data" |

| Previous Hash: abcd |

| Timestamp: 2025-06-08|

| Nonce: 1001 |

| Merkle Root: xxyz123 |

+----------------------+

**Merkle Root Explanation**:  
A Merkle root is a single hash derived from hashing all transactions in a block recursively in pairs. It summarizes and verifies the integrity of all the data in the block.  
**Example**:  
If one transaction in the block is altered, the Merkle root changes. This alerts the system that tampering occurred, as the hash no longer matches.

1. Consensus conceptulization

* **Proof of Work (PoW)**:  
  PoW requires validators (miners) to solve complex mathematical puzzles by brute force. This demands high computational power and energy. Once solved, the block is added to the chain. The energy cost ensures that cheating is expensive.
* **Proof of Stake (PoS)**:  
  Validators are chosen based on the amount of cryptocurrency they “stake.” The higher the stake, the higher the chance of being selected to validate the next block. This method consumes less energy and discourages bad actors due to the risk of losing their stake.
* **Delegated Proof of Stake (DPoS)**:  
  Stakeholders vote to elect a fixed number of delegates who validate transactions and create blocks. This is faster and more scalable than PoW or PoS, but can be more centralized due to limited validator numbers.