PRACTICAL 1

AIM: Hands-on session explaining the structure of a blockchain.

1. Blocks

A blockchain is made up of a series of blocks, which are linked together in a chain (hence the name "blockchain"). Each block contains three main components:

- **Header**: Contains metadata about the block, like the timestamp, version, and a hash of the previous block (this forms the chain).
- **Body**: Contains the actual data. This can vary depending on the type of blockchain. In Bitcoin, for example, it contains transaction information (sender, receiver, and amount).
- **Hash of the block**: A unique identifier for that specific block, generated using a cryptographic hash function. This hash ensures that no data within the block can be changed without altering the hash (making it tamper-resistant).

2. Chain

- Every block in the blockchain is linked to the block before it through its **previous hash**. This creates a chronological chain of blocks.
- The **first block** in the blockchain is called the **Genesis Block**, and it doesn't have a previous block, so its previous hash is set to a default value (often 0).

3. Transactions

Transactions are the core of any blockchain. In a typical blockchain, like Bitcoin, transactions contain:

- **Sender's Address**: The public key of the user sending the assets.
- **Receiver's Address**: The public key of the user receiving the assets.
- **Amount/Assets Transferred**: The value of the transaction (e.g., number of Bitcoin or Ether).
- **Digital Signature**: The sender signs the transaction with their private key to verify their identity and consent.

4. Consensus Mechanism

Blockchain relies on a consensus mechanism to validate transactions and add blocks to the chain. There are various mechanisms:

- **Proof of Work (PoW)**: Used by Bitcoin, miners must solve complex mathematical problems to validate transactions. The first to solve it adds the block and is rewarded.
- **Proof of Stake (PoS)**: Validators are chosen based on the amount of cryptocurrency they hold and are willing to "stake" as collateral. They validate the transaction and add the block to the chain.

5. Decentralization and Distributed Ledger

One of the main features of blockchain is decentralization. Instead of being controlled by a central authority, the blockchain is distributed across a network of nodes (computers).

- Each node has a copy of the entire blockchain.
- When a new block is added, all nodes update their copy of the blockchain.
- This ensures transparency and security, as altering one copy would require changing every single copy across the network.

6. Immutability

Once a block is added to the blockchain, it’s extremely difficult to alter. This is due to the cryptographic hash function.

- Any change in a block (e.g., changing a transaction) would alter its hash.
- Since each block references the hash of the previous block, altering any block would change the entire chain, making tampering easily detectable.