**Branch :- Computer Sci. & Engg. Class :- Final Year**

**Subject :-Block Chain Fundamentals Lab manual Sem :- VII**

**Student Manual**

**PRACTICAL NO 10**

**AIM**: Implement the consensus mechanisms of Proof of Work (PoW)

**S/W REQUIRED:** Python

**Proof of Work (PoW)** is the original consensus mechanism used in blockchain networks like **Bitcoin**. In PoW, participants (called miners) compete to solve a complex mathematical problem. The first one to solve it gets to add the next block to the blockchain and receives a reward.

The **goal** is to find a **nonce** (random number) that, when combined with the block data and passed through a **hash function**, produces a hash with a certain number of leading zeros — which represents the **difficulty** level.

**How Proof of Work Works**

First, the worker, which is called a miner, creates a temporary file (a block). If it wins the competition to solve for a winning hash, this file will be stored on the blockchain. The block has the four following fields:

* Block size
* Block header
* Transaction counter
* Transactions

The block header contains the following fields:

* Software version
* Previous block's hash
* Merkle root
* Timestamp
* Difficulty target
* Nonce

The mining program assembles this block and places the transactions it has prioritized in the transaction field. It continuously adjusts the nonce and the extra nonce (which is part of the coinbase transaction in the Merkle tree) and sends the information in the block through a hashing algorithm.

It repeats this process until it finds a solution, which is a value less than or equal to the difficulty target. The difficulty target is set so that a certain number of hashes per second must be attempted before a solution is found

**CONCLUSION:** This simple implementation of **Proof of Work(POW)** ensures consensus by making it **hard to add blocks** but **easy to verify**