School: ..... Campus: .....

Academic Year: ..... Subject Name: ..... Subject Code: .....

Semester: ..... Program: ..... Branch: ..... Specialization: .....

Date: .....

Applied and Action Learning

(Learning by Doing and Discovery)

Name of the Experiement : Hash Your First Block – Blockchain Basics and Setup

Objective/Aim :

To understand the basic structure of a block-chain by creating and hashing the first block using cryptographic hashing (SHA-256), and to demonstrate how data integrity is maintained in a block-chain system.

Apparatus/Software Used:

- Laptop/PC
- PowerPoint/Word for documentation
- Internet for research

Theory/Concept:

A **blockchain** is a decentralized, distributed digital ledger used to record transactions across multiple computers in a way that ensures the security and immutability of the data.

Each **block** in a blockchain contains:

- **Index**: Block number in the chain
- **Timestamp**: Time of block creation
- **Data**: Transaction or message data
- **Previous Hash**: Hash of the previous block
- **Current Hash**: Cryptographic hash of the current block's conten

✳ Key Concepts:

- **SHA-256**: A cryptographic hash function used to secure data.
- **Immutability**: Once a block is hashed and added, its data cannot be altered without changing the entire chain.
- **Integrity**: Hashing ensures that the data is tamper-proof and verifiable.
- **Chaining**: Each block is linked to the previous one through its hash, forming a secure chain of blocks.

Procedure:

1. **Nonce :** A number miners change to achieve a valid hash.
2. **Hash Difficulty :** Here, it's met when the hash starts with `0000`.
3. **Proof of Work :** The process of trial and error to find a valid nonce.
4. **Hash Uniqueness :** Any change in data = completely different hash.
5. **Block Integrity :** If even a letter changes, the hash and block identity break.

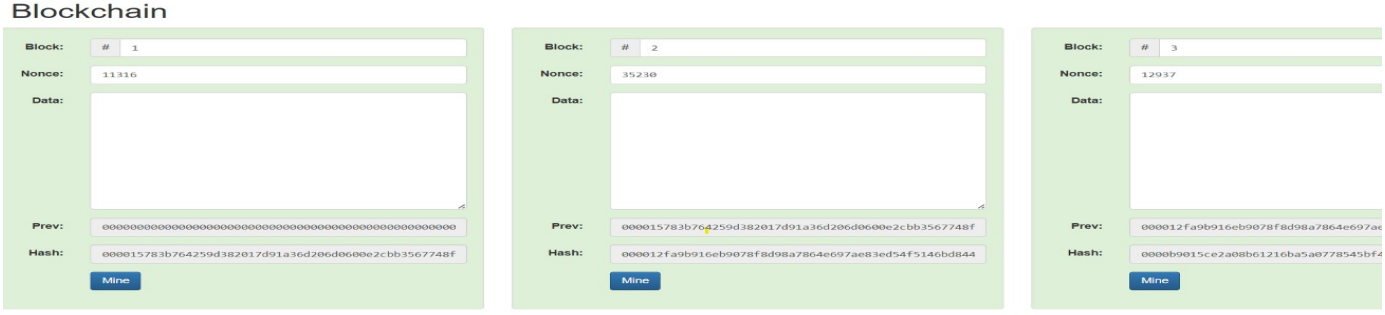
This is a **block simulator** used to demonstrate:

- How data, nonce, and block number affect the final hash
- The core concept of **mining and proof-of-work**

Let me know if you want:

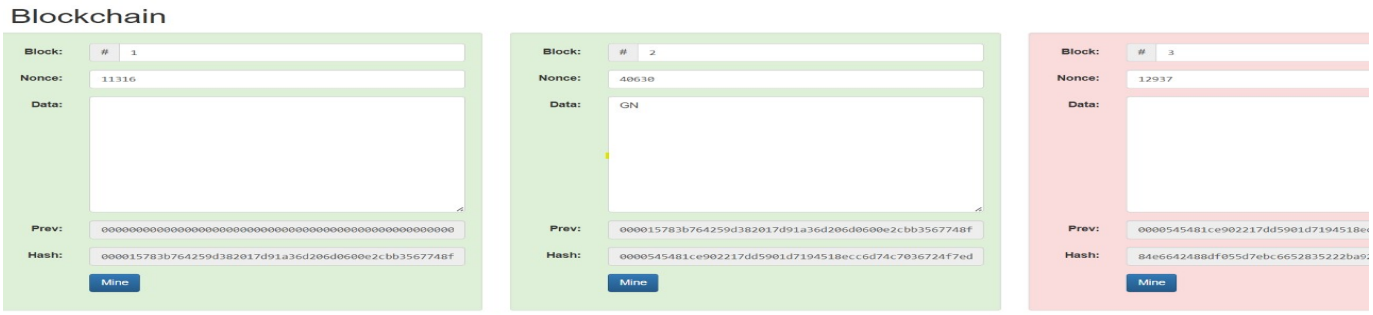
- The code behind this simulator (HTML + JS)
- How to run this on your system
- Viva questions based on this lab

Then create a blockchain consisting of three blocks (Block 1, Block 2, and Block 3), each mined with its own nonce, data, and hash, and all connected through their previous hashes.



Then, a blockchain was created with **three blocks (Block 1, Block 2, and Block 3)** — each mined with its own **nonce**, **data**, and **hash** — and all blocks were **linked together through their previous hashes**.

- **Block 1 (Genesis Block)** had no previous hash (set to all zeros), and was successfully mined with a valid hash starting with `"0000"`.
- **Block 2** was linked to Block 1 by storing Block 1's hash as its previous hash. It was also mined successfully with a valid hash.
- **Block 3** was connected to Block 2, but its hash did not start with `"0000"`, which means it was **not yet mined** and hence marked as **invalid** (red background).



Observation:

I observed the process of creating a blockchain and hashing a block. Each block was constructed with data, a nonce (number used once), and was hashed using SHA-256. The hash of the current block depends on both its contents and the hash of the previous block, forming a secure chain.

I also noticed:

- The importance of a **nonce** in mining a block.
- Hashing creates a **unique fingerprint** of the block's contents.
- The hash of the previous block is stored in the next block, making the chain **tamper-proof**

ASSESSMENT

Rubrics	Full Mark	Marks Obtained	Remarks
Concept	10		
Planning and Execution/ Practical Simulation/ Programming	10		
Result and Interpretation	10		
Record of Applied and Action Learning	10		
Viva	10		
Total	**50**		

Signature of the Student:

Name :

Regn. No. :

Signature of the Faculty:

** As applicable according to the experiment.*
Two sheets per experiment (10-20) to be used.