Centurion University
Shaping Lives... Empowering Communities...

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 : Mine It – Basic Proof-of-Work Simulation

Objective/Aim:

To study and simulate the Proof-of-Work (PoW) mining process by finding a nonce value such that the hash of a given input string and the nonce starts with a specific number of leading zeros (difficulty level).

Apparatus/Software Used:

- Laptop
- Word for documentation,
- Proof of work simulator
- Internet for research

Theory/Concept:

What is POW (proof of work)?

Proof-of-Work (PoW) is a blockchain consensus algorithm in which network participants, known as **miners**, compete to solve a computationally intensive puzzle. This process secures the blockchain by ensuring that adding a new block requires significant computational work.

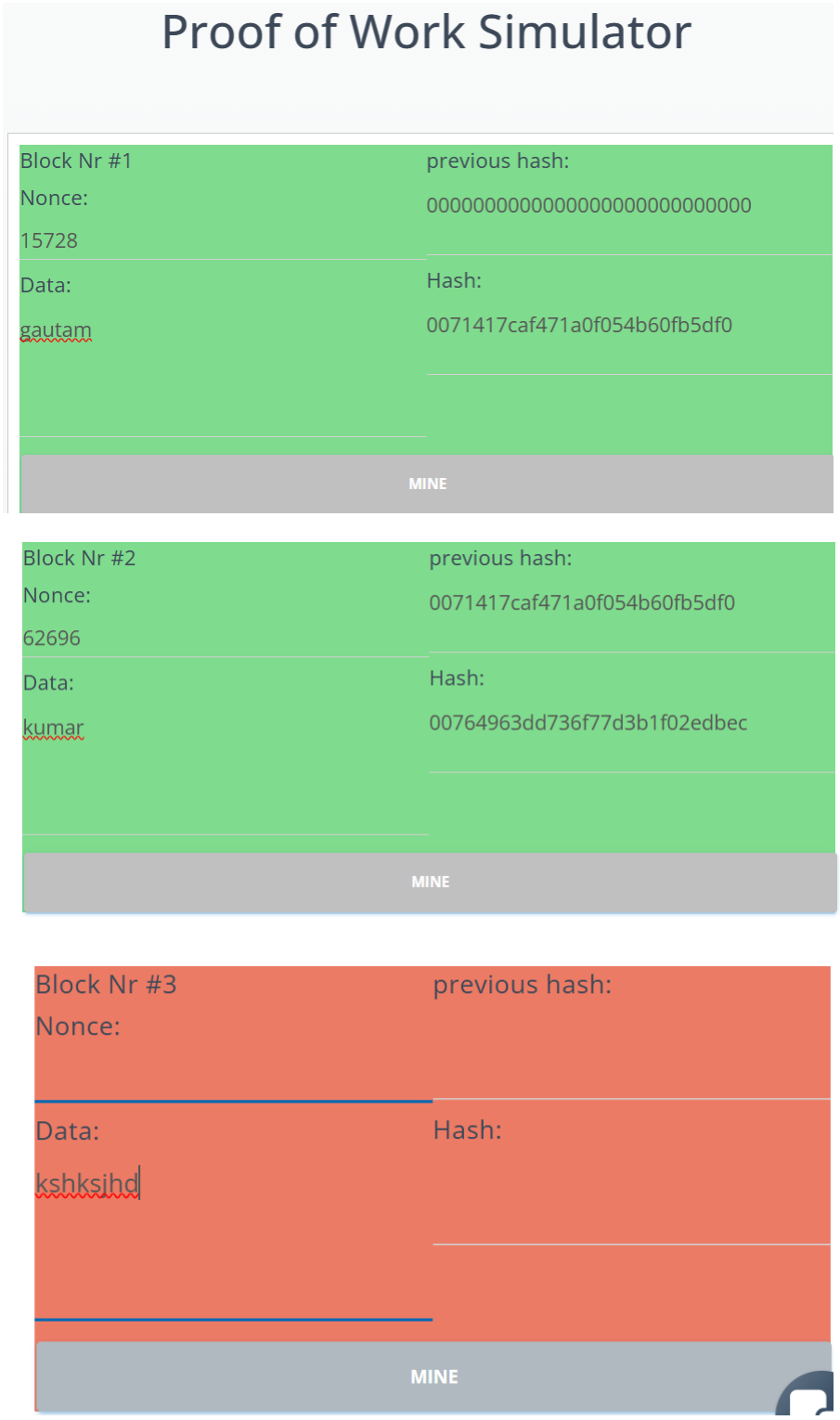
In PoW mining, the block header is repeatedly hashed using a cryptographic hash function (e.g., **SHA-256**) while changing a numeric value called the **nonce**. The goal is to find a hash output that meets a predefined **difficulty target**, which is typically defined as the number of leading zeros in the hexadecimal representation of the hash.

Key Points:

- **Nonce**: An arbitrary number added to the block header and changed on each attempt to generate a different hash.
- **Difficulty**: A measure of how hard it is to find a valid hash. Each additional required leading zero increases the difficulty exponentially.
- **Hash Function (SHA-256)**: Produces a fixed-size 256-bit output that is deterministic, irreversible, and highly sensitive to input changes.

Procedure:

Step 1: - Open the browser
Step 2: - There is a proof of work simulator where in realtime you can enter the data and mine a block
at: **https://blockchain-academy.hs-mittweida.de/2021/05/proof-of-work-simulator/**
Step 4: There are blocks where you can give the input the data and mine it
Step 5: One by one give data and mine all the block.



Observation:

- For the same input it will generate the same hash but if single alphabet or Number or space changes then it changes the hash even if the change.
- The SHA-256 algorithm provides a one-way hash—it is not possible to retrieve the original input from the hash, ensuring data confidentiality.

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: