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 :

* Coding Phase: Pseudo Code / Flow Chart / Algorithm

ALGORITHM:

Start

Input the message or data.

Padding:

Add a single ‘1’ bit to the message.

Add enough ‘0’ bits so that the total length ≡ 448 (mod 512).

Append the original message length (64 bits) to make the total a multiple of 512 bits.

Initialize hash values (specific constant values defined by SHA standard).

Divide the message into 512-bit blocks.

For each block:

a. Prepare a message schedule (break into 32-bit words).

b. Perform **logical operations** (AND, OR, XOR, ROTATE, SHIFT) over multiple rounds.

c. Update the hash values.

Combine all updated values to produce the final hash (e.g., 256-bit output).

Stop

When data is given to the SHA algorithm, it creates a unique fixed-length hash.

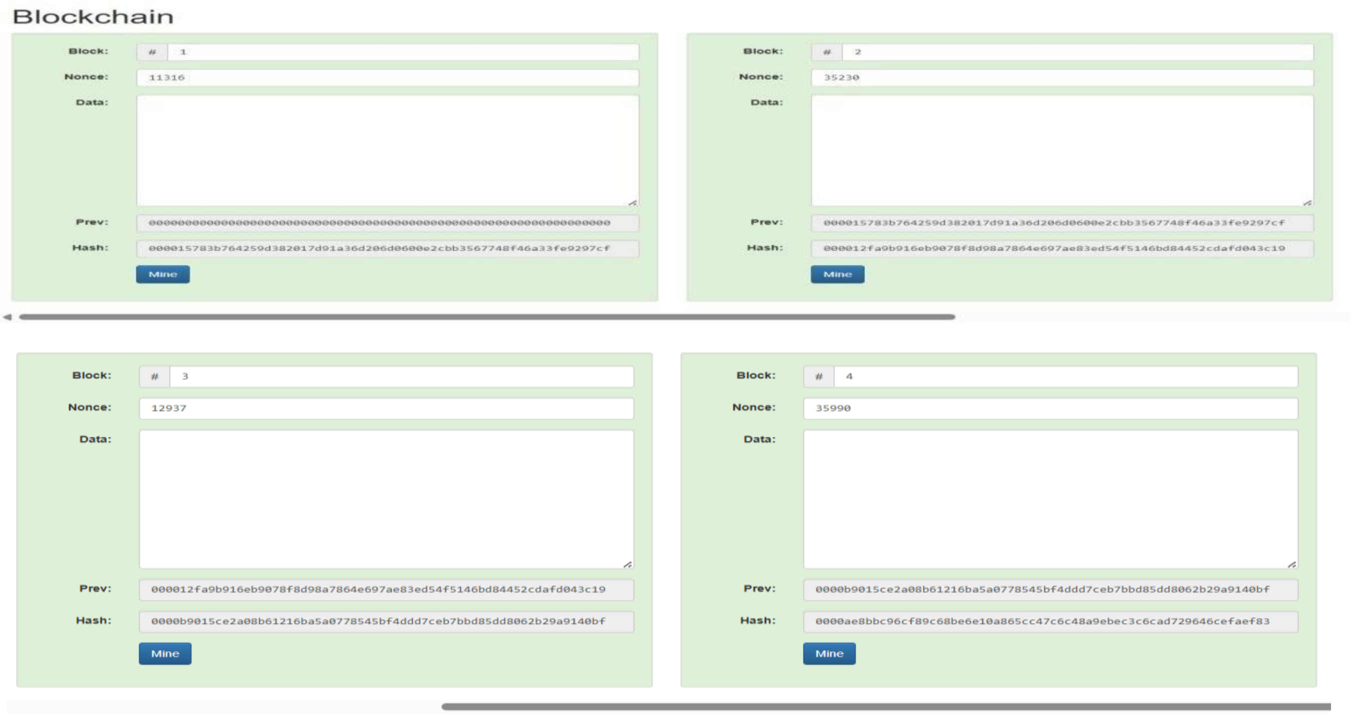
If any data changes, the hash changes completely.

In a blockchain, this change affects the next block’s previous hash,

causing a **chain reaction** — ensuring **data integrity and security**.

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

* Testing Phase: Compilation of Code (error detection)



Blockchain

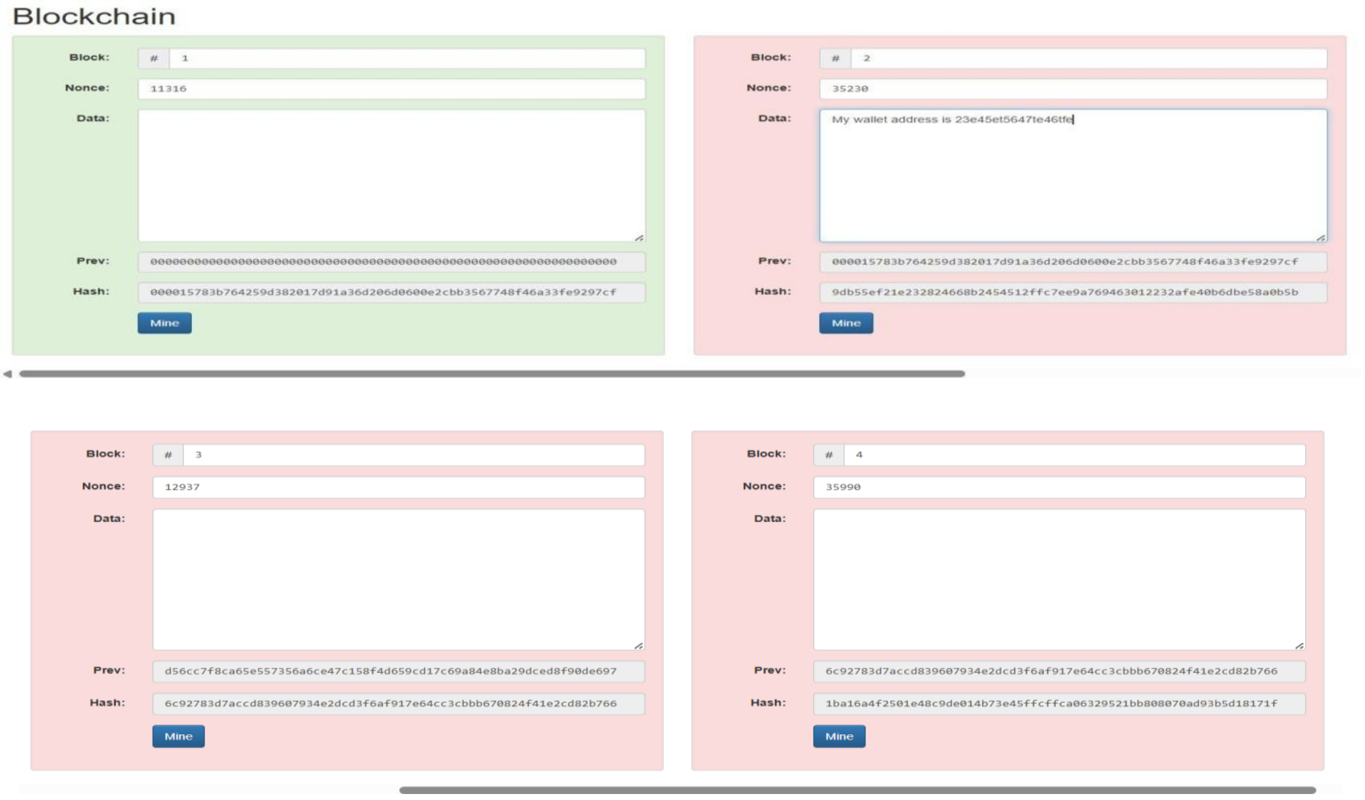
Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Block: # 2
Nonce: 35230
Data:
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf
Hash: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd043c19

Block: # 3
Nonce: 12937
Data:
Prev: 000012fa9b916eb9078f8d98a7864e697ae83ed54f5146bd84452cdafd043c19
Hash: 0000b9015ce2a08b61216ba5a0778545bf4ddd7ceb7bbd85dd8062b29a9140bf

Block: # 4
Nonce: 35990
Data:
Prev: 0000b9015ce2a08b61216ba5a0778545bf4ddd7ceb7bbd85dd8062b29a9140bf
Hash: 0000ae8bbc96cf89c68be6e10a865cc47c6c48a9ebec3c6cad729646cefaef83

In above there are normal blocks without data in next step we have to add data to a particular block to chek the chaining effects.



Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Block: # 2
Nonce: 35230
Data: My wallet address is 23e45et5647te46tfe
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf
Hash: 9db55ef21e232824668b2454512ffc7ee9a769463012232afe40b6dbe58a0b5b

Block: # 3
Nonce: 12937
Data:
Prev: d56cc7f8ca65e557356a6ce47c158f4d659cd17c69a84e8ba29dced8f90de697
Hash: 6c92783d7accd839607934e2dcd3f6af917e64cc3cbbb670824f41e2cd82b766

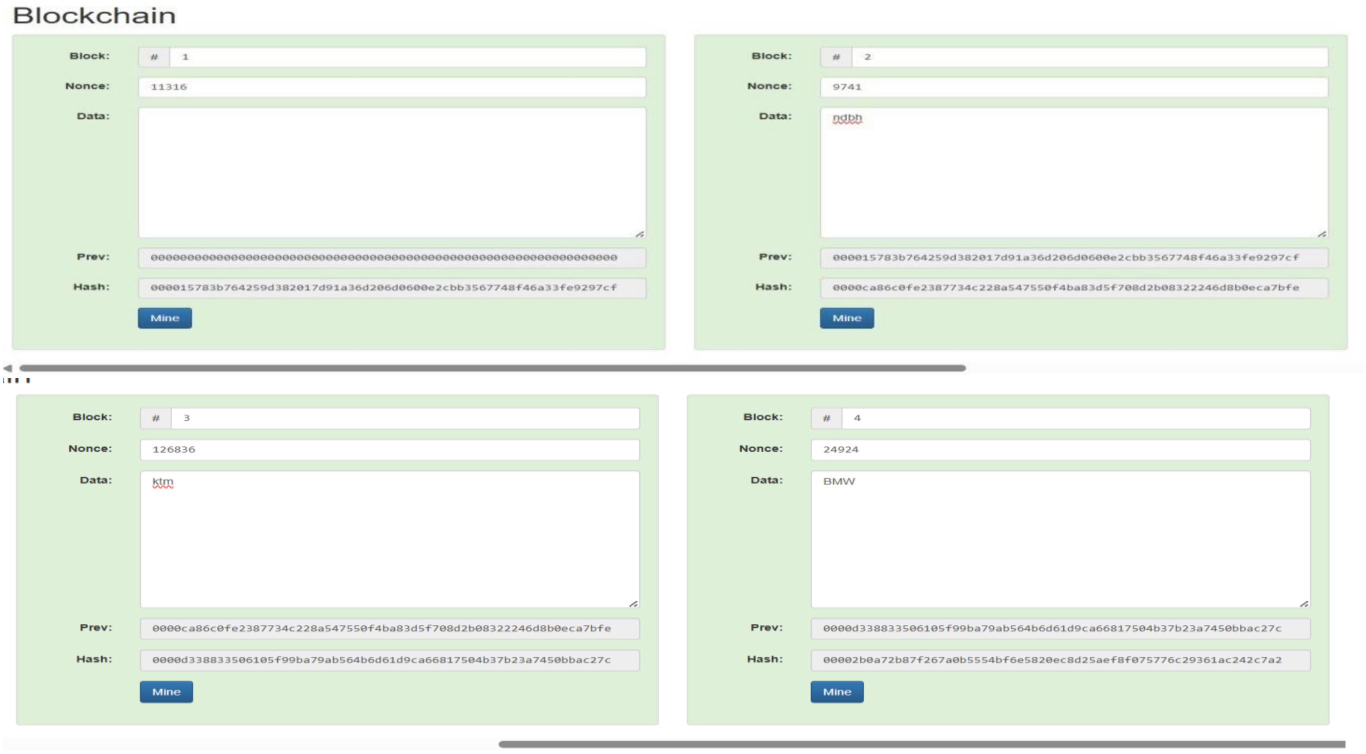
Block: # 4
Nonce: 35990
Data:
Prev: 6c92783d7accd839607934e2dcd3f6af917e64cc3cbbb670824f41e2cd82b766
Hash: 1ba16a4f2501e48c9de014b73e45ffcffca06329521bb808070ad93b5d18171f

In this i add a data to the block 2 then we see the colour and hash are changes for the next blocks

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

* Implementation Phase: Final Output (no error)

After add the data of block 2 the next blocks are wrong because of the wrong hash and once in block 2 ,to fix this we have start mine for each block ,and after mining there was a perfect has and nonce for each block



Blockchain

Block: # 1
Nonce: 11316
Data:
Prev: 0000000000000000000000000000000000000000000000000000000000000000
Hash: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf

Block: # 2
Nonce: 9741
Data: ndbh
Prev: 000015783b764259d382017d91a36d206d0600e2cbb3567748f46a33fe9297cf
Hash: 0000ca86c0fe2387734c228a547550f4ba83d5f708d2b08322246d8b0eca7bfe

Block: # 3
Nonce: 126836
Data: ktm
Prev: 0000ca86c0fe2387734c228a547550f4ba83d5f708d2b08322246d8b0eca7bfe
Hash: 0000d338833506105f99ba79ab564b6d61d9ca66817504b37b23a7450bbac27c

Block: # 4
Nonce: 24924
Data: BMW
Prev: 0000d338833506105f99ba79ab564b6d61d9ca66817504b37b23a7450bbac27c
Hash: 00002b0a72b87f267a0b5554bf6e5820ec8d25aef8f075776c29361ac242c7a2

Observation:

>SHA generates a **unique, fixed-length hash** for any input data.
>Small data changes cause a completely different hash.
>The process is **one-way** — you can’t get the original data from the hash.
>It ensures **data integrity and security**.
>In blockchains, a change in one block’s hash affects all the next blocks (chain reaction).

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 :

Signature of the Faculty:

Regn. No. :

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