DATE: 30th December 2020

SCHOOLOFCOMPUTERSCIENCE

July – December 2020

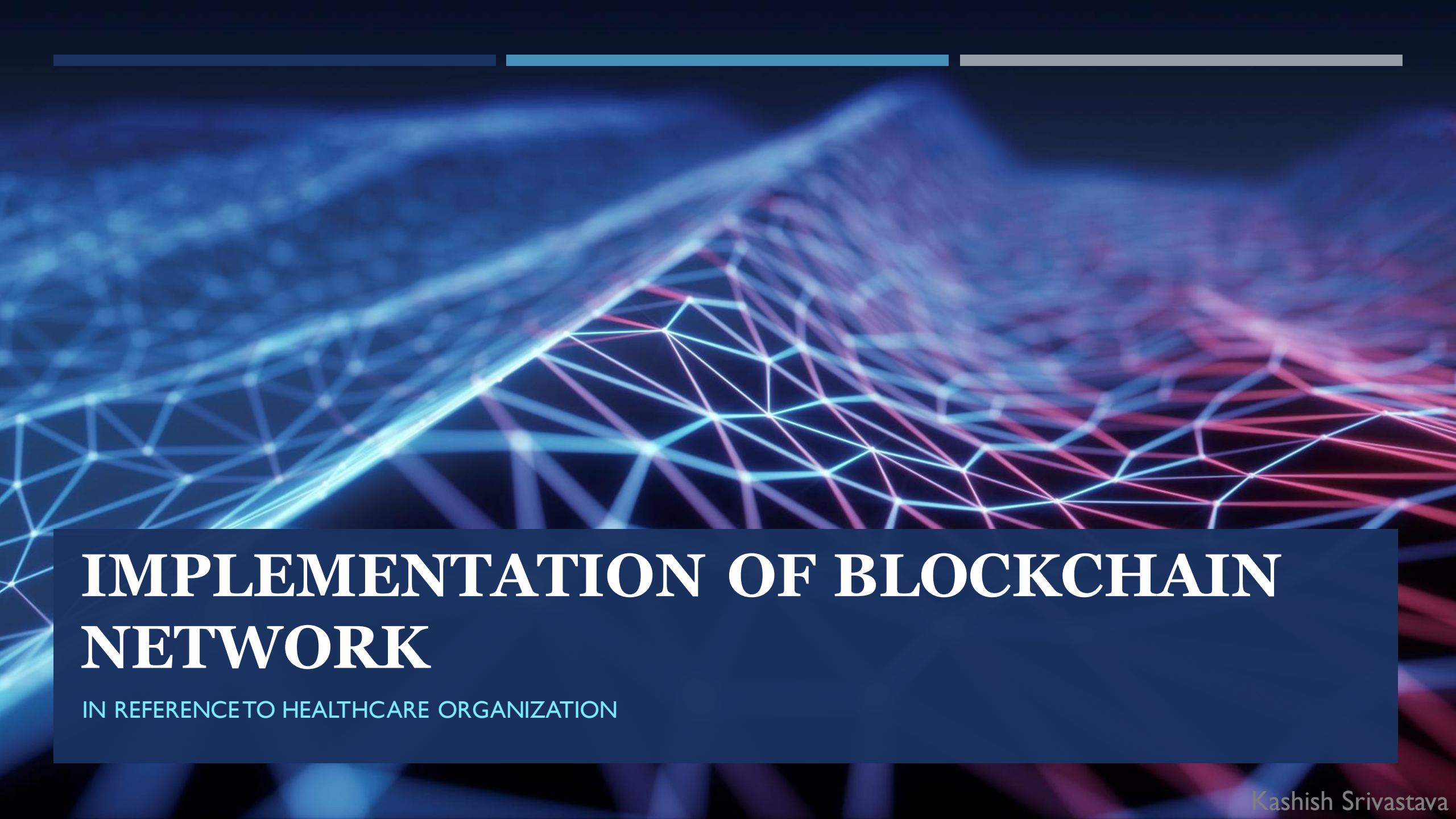
END-SEM REPORT
On
Implementation of Blockchain Network

Under the guidance of
Mr. Saurabh Jain
(Department of Systemics)

Kashish Srivastava

Kashish Srivastava
B.tech CSE-CSF (B2) 3rd year
(Enroll No. R134218079 & Sap id 500067405)

TEAM MEMBER



IMPLEMENTATION OF BLOCKCHAIN NETWORK

IN REFERENCE TO HEALTHCARE ORGANIZATION

Kashish Srivastava

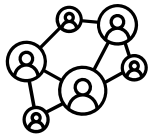
LIST OF CONTENTS

Blockchain is a decentralized distributed ledger that stores data, holds immutable property and verified transactions. It is faster than the centralized network.

The ledger can be shared and verified by anyone who has access eliminating the need for costly third-party verification.

Similarly talking about a concept known as hashing algorithm, it majorly focuses on generating a fixed length result for an input value.

The main features of blockchain are:



Decentralization
Immutability
Scalability
Limited privacy
Transparency and Trust

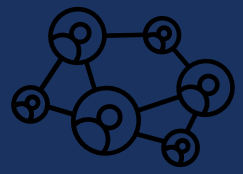
INTRODUCTION

Why reference of a healthcare area or industry?

To identify the use cases or the examples of blockchain-based applications in healthcare, but also to understand the limitations and challenges for the blockchain-based healthcare applications as well as the current trends in terms of the technical approaches, methodologies and concepts.
A firm which operates a blockchain-based healthcare platform for the validation of patients' identities for the citizens and the MedRec project, which is created to facilitate the management of permissions, authorization and data sharing between healthcare entities.

- Blockchain can become that decentralized health data management backbone from where all the stakeholders can have controlled access to the same health records, without any one playing the role of a central authority over the global health data.
- The immutability property of blockchain greatly improves the security of the health data stored on it, since the data, once saved to the blockchain cannot be corrupted, altered or retrieved.
- Even without accessing the plaintext of the records stored on blockchain, the integrity and validity of those records can be verified.

INTRODUCTION



PROBLEM STATEMENT

WHAT WE ARE TRYING TO DO?	WHAT VALUES WE ARE TRYING TO CAPTURE?	FOR WHOM?
RECORD	DATA AND KNOWLEDGE	EMPLOYEES
TRACK	ACCESS AND PERMISSION	CUSTOMERS
VERIFY	TRANSPARANCY AND TRUST	PRODUCERS AND SUPPLIERS
VALIDATE	TRANSACTIONS	CREDITORS
	DECENTRALIZED	CITIZENS

LITERATURE REVIEW

TITLES	REMARKS
Blockchain in healthcare and health sciences—A scoping review	The purpose of this study was to systematically review, assess and synthesize peer-reviewed publications utilizing/proposing to utilize blockchain to improve processes and services in healthcare, health sciences and health education.
Application of Blockchain Technology to Guarantee the Integrity and Transparency of Documents	This paper explains implementation of security in the blockchain network.
Performance Study of Enhanced SHA-256 Algorithm	It explains all the cryptographic hash functions and recalls merkle-damgard security properties of iterated hash functions.
Blockchain Technology in Healthcare: A Systematic Review	The review shows that a number of studies have proposed different use cases for the application of blockchain in healthcare
A Blockchain-based Authentication and Security Mechanism for IoT	This work explains about the IOT devices facing a challenge of data tampering which is recovered or solved by the blockchain technology and hashing algorithms.

C PROGRAMMING

The basic objective is to develop a blockchain model and apply various SHA256 hashing algorithms.The input data for the blocks will be entered through user , file handling concept is a good option for input due to which our file contents, irrespective of the quality and quantity of the content will be entered in the block making it more secure.

Sub Objectives

- First develop a blockchain model at any coding platform.
- Understand the theoretical concept of various hashing algorithms.
- Maintaining most of the features of the blockchain network in reference to linked list.
- **Develop the block structure of its parameters**

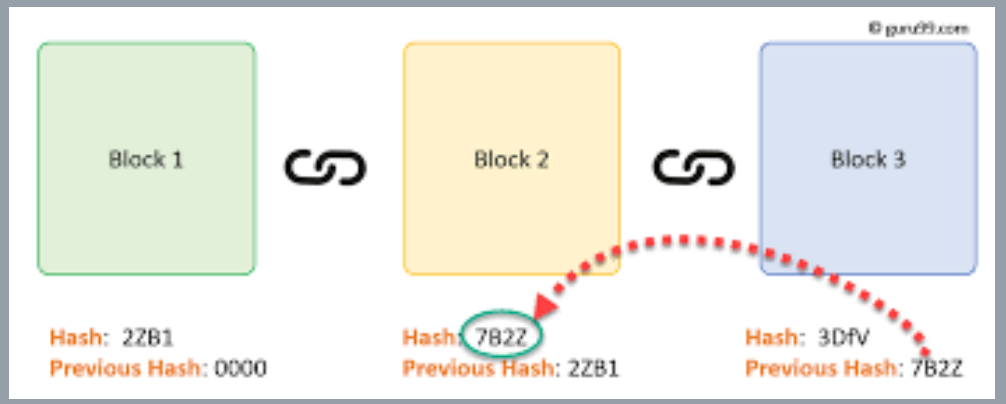
OBJECTIVES

C PROGRAMMING

For this project, major focus is going to be on the development of a blockchain structure based on its parameters in C programming. Use SHA-256 algorithm to calculate hash. SHA256 function is present in openssl/Crypto.h header file in C. We will use this library for the hashing mechanism of the blockchain.
The entire implementation of this project is explained in the following points:

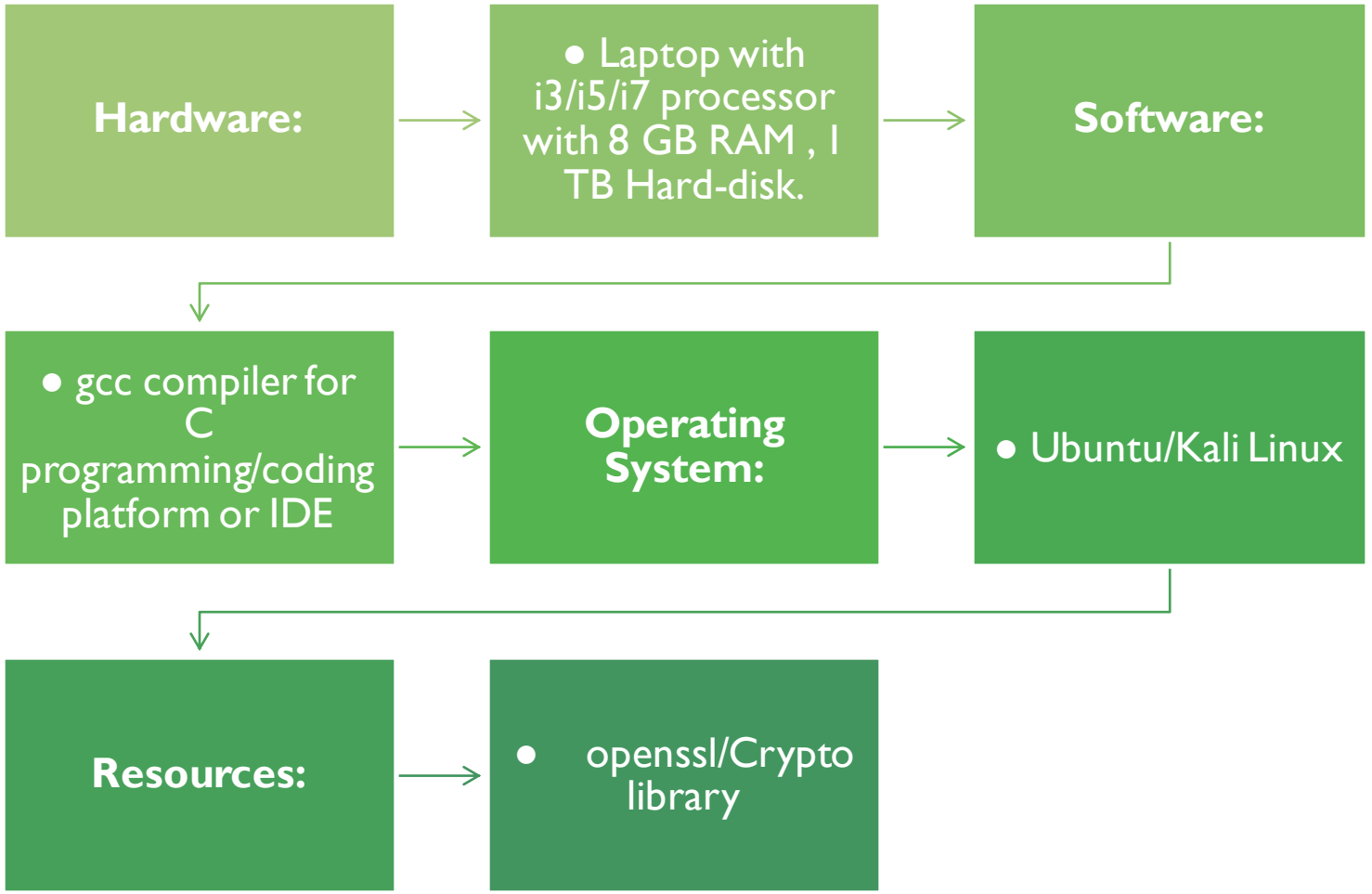
- The development of the basic blockchain structure will be proceeded on any coding platform.
- Number of blocks in blockchain will be entered via user.
- In our model, block's data will be introduced using file handling in future but for now it can be either asked manually by the user or entered randomly by random function in C. Therefore data of file will be stored in the block.
- Applying SHA256 hashing algorithms (via openssl/crypto.h) to generate hash values.
- These hash values will help in verifying about our blockchain structure hashes that are generated.
- The block is mined and is added with the other blocks in the existing structure of the block.
- If the hash of the previous block and this block is similar it will be verified.
- Therefore the blockchain structure gets validated.

METHODOLOGY



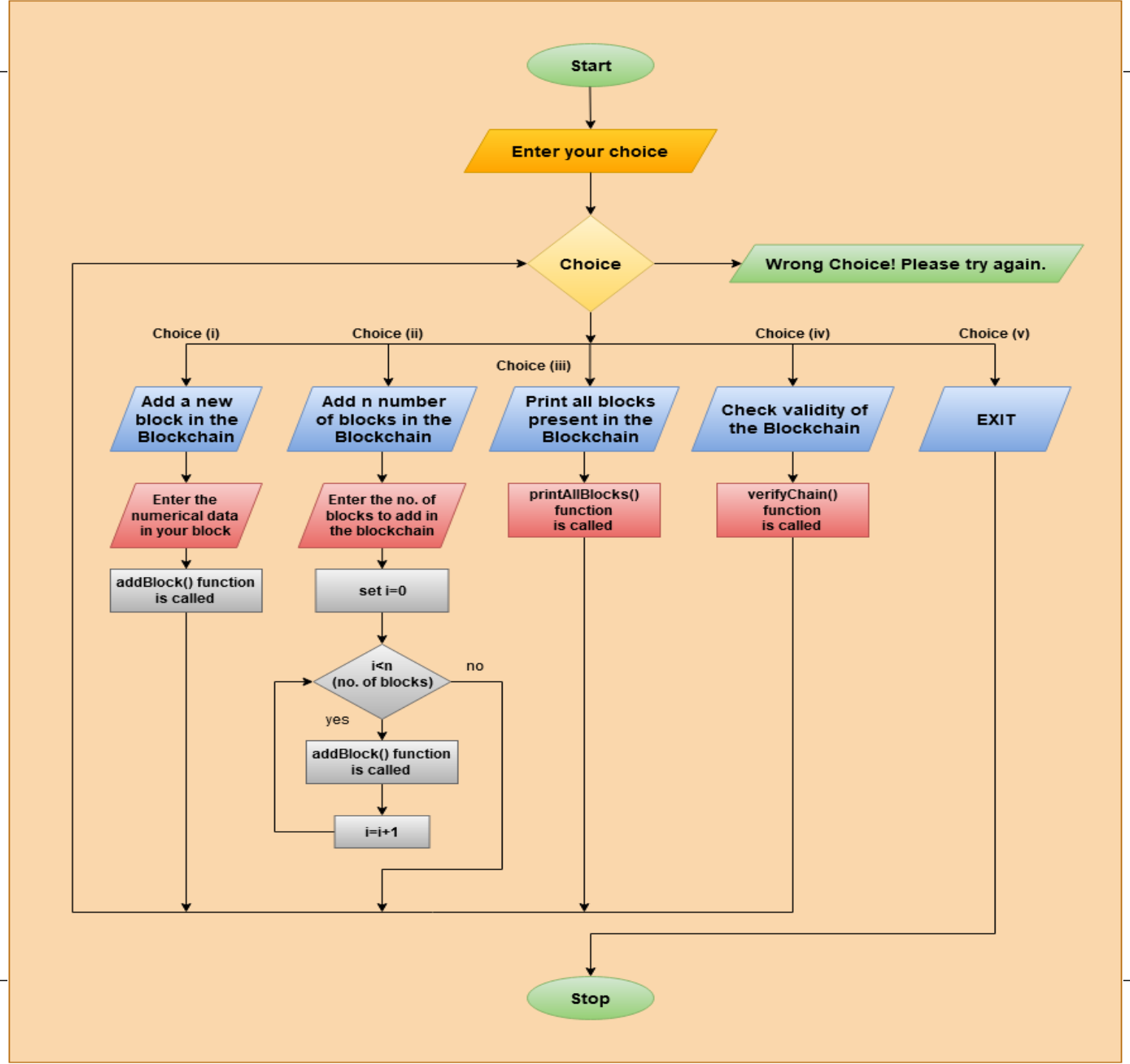
Kashish Srivastava

SYSTEM REQUIREMENTS



Kashish Srivastava

FLOWCHART



Kashish Srivastava

ALGORITHM

#Main_Program_for_implementation

Step 1: Start

Step 2 : Input the choice to perform operation in blockchain

We have following choices:

i- Add a new block in Blockchain

ii- Add n numbers of blocks in Blockchain

iii- Print all the blocks present in the Blockchain

iv- Check Validity of the Blockchain

v- Exit (Terminate the code)

Step 3: If (i) has been entered as the choice then

a- Input data to store in block

b- call addBlock() user define function than goto (Step 2)

Step 4: If (ii) has been entered as the choice then

a- Input the number of blocks that you want to add in Blockchain

b- Iterate a for loop (number of blocks that you want to add) times

c- In every iteration call addBlock() user define function

d- After for loop iterations goto (Step 2)

Step 5: If (iii) has been entered as the choice then

a- call printAllBlocks() user define function than goto (Step 2)

Step 6: If (iv) has been entered as the choice then

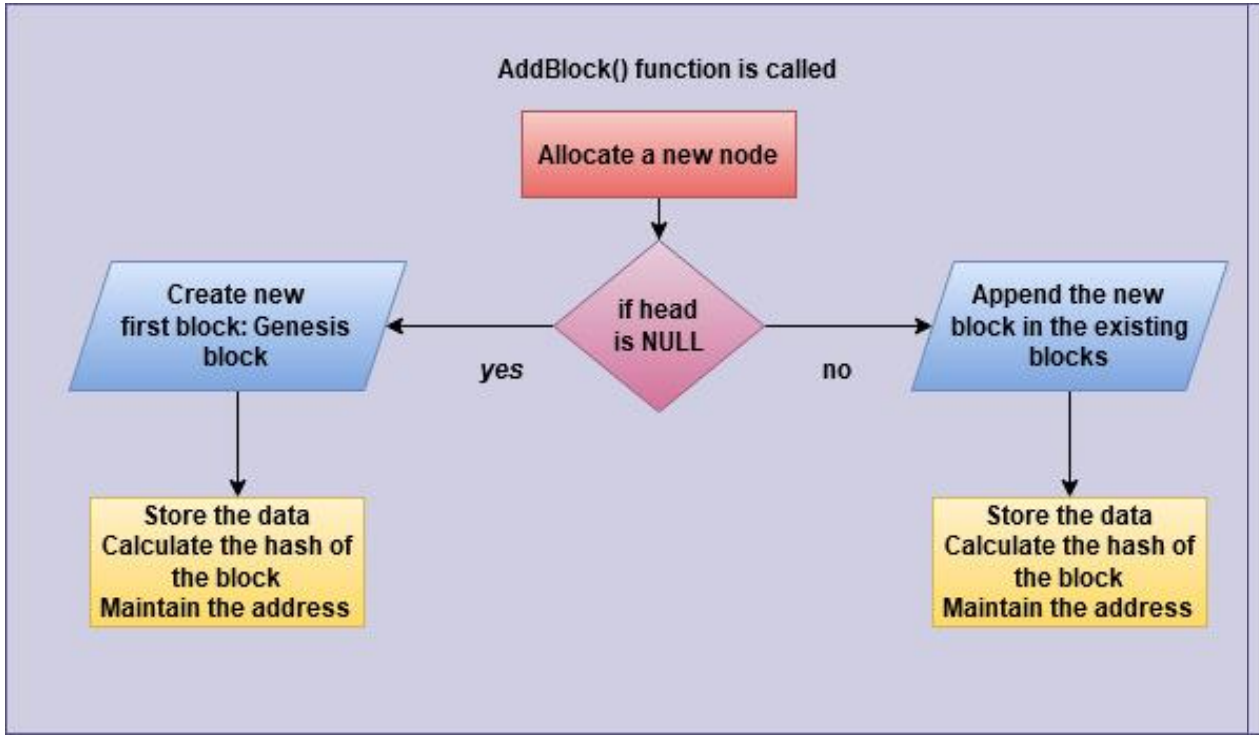
a- call verifyChain() user define function than goto (Step 2)

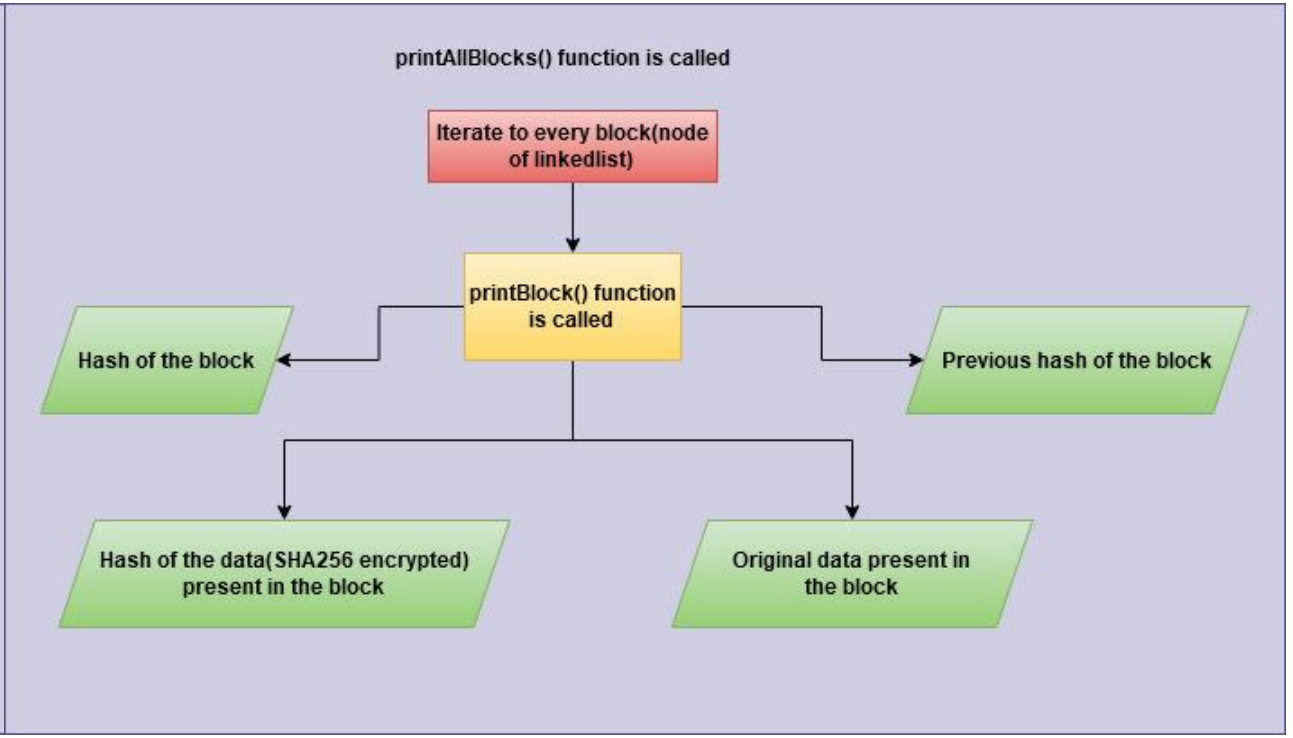
Step 7: If Choose (v) choice than

a- exit() function call and terminate the program

Step 8: Stop

FLOWCHART- **FUNCTION'S SEPARATE ALGORITHM**



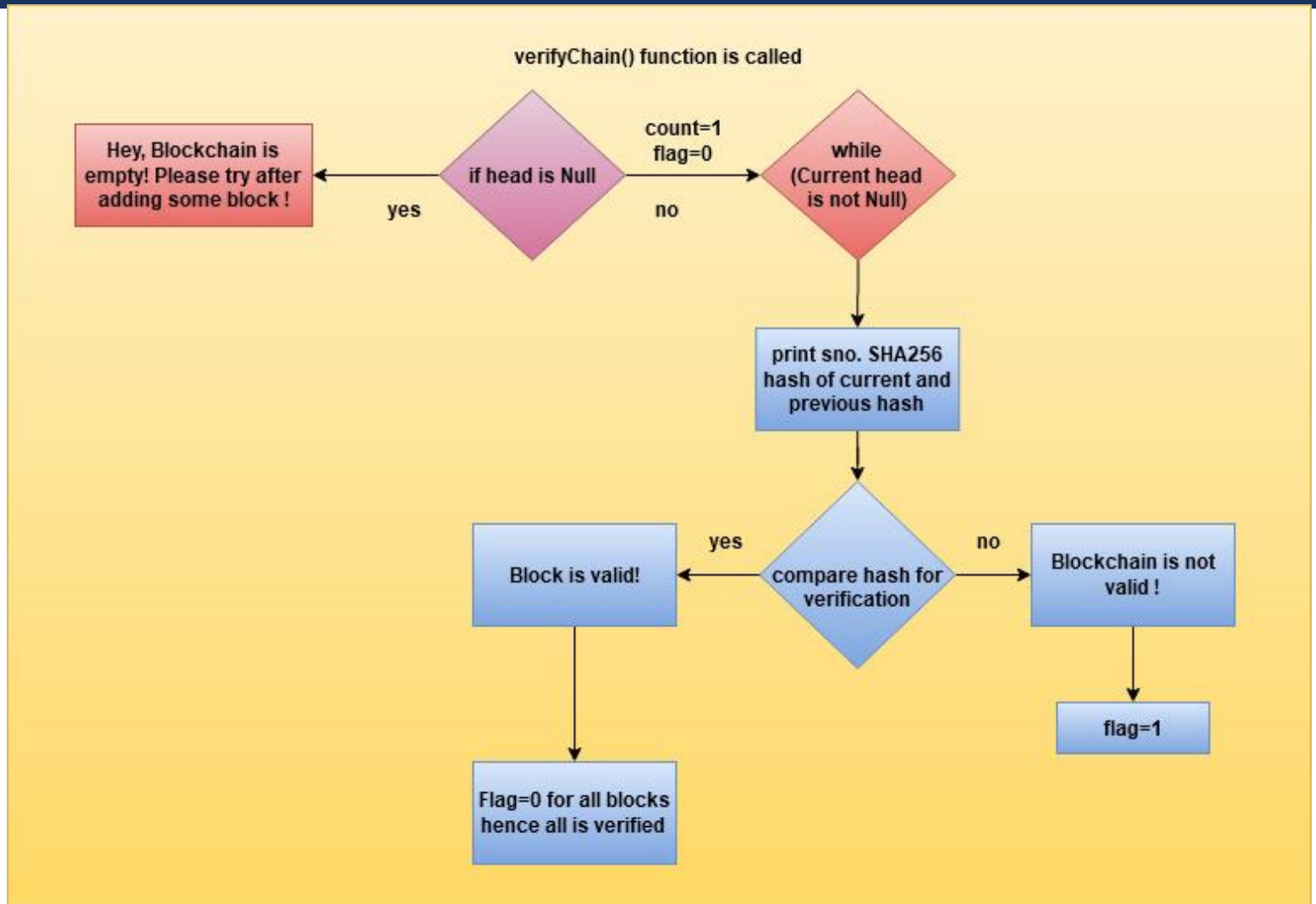


ALGORITHM - FUNCTION'S SEPARATE ALGORITHM

 # Algo of addBlock() function with block data parameter :
Step 1: Start
Step 2: Receive block data by user
Step 3: Check, a- if Blockchain is empty that create first block i.e. Genesis Block
else Add a new block in existing Blockchain
b- Calculate the hash value for this particular block
c- Store the block data in particular block
d- Manage addresses of blocks(nodes) according to concept of linked list
Step 4: Stop

 # Algo for printAllBlocks()
Step 1: Start
Step 2: Iterate every block in Blockchain (nodes in linked list)
Step 3: Call printBlock() function.
Step 4: *Check if the head of the block is Null or not. If null the blockchain structure is empty else print parameter to every block*. <<optional>>
Step 5: Print all the blocks parameters (Block Hash Value, Previous block hash value, Block data, address of next block)
Step 6: Stop

FLOWCHART - FUNCTION'S SEPARATE ALGORITHM



Kashish Srivastava

ALGORITHM- FUNCTION'S SEPARATE ALGORITHM

 # Algo for verifyChain()

Step 1: Start

Step 2: Compare if head is equal to Null

- Yes, print "Hey, Blockchain is empty! Please try after adding some block"
- No, set two counter variable count=1 for iterating and flag=0 for verification

Step 3: Since the current node is not Null, the serial number is printed, along with previous hash and current has in SHA256 form, if both are verified then the block is valid.

Step 4: If the block is not valid flag turns 1 and verification is denied.

Step 5: If flag stays 0 for all the blocks validation then the verification is confirmed.

Step 6: stop

OUTPUTS

We run our code, we get various options for the user-input.

- Add a new block in Blockchain
- Add n numbers of blocks in Blockchain
- Print all blocks present in Blockchain
- Check validity of Blockchain
- Exit (Terminate the code)

```
root@kali:~/Minor_Project# gcc -o Kashish_minor Kashish_minor.c -lssl -lcrypto
root@kali:~/Minor_Project# ./Kashish_minor
```

```
        ********************************************************************************
        !!!                                                                          !!!
        !!!  Minor I Project : Implementation of Blockchain Network in C language   !!!
        !!!                                                                          !!!
        ********************************************************************************


 ENTER YOUR CHOICE
1: Add a new block in the Blockchain
2: Add n numbers of blocks in Blockchain
3: Print all blocks present in Blockchain
4: Check Validity of Blockchain
5: EXIT
```

OUTPUTS

```
Choice: 1
Enter the numerical data you want in your Block: 36
1 Block is added in Blockchain successfully

 ENTER YOUR CHOICE
1: Add a new block in the Blockchain
2: Add n numbers of blocks in Blockchain
3: Print all blocks present in Blockchain
4: Check Validity of Blockchain
5: EXIT
```

We enter 36 as the value/data for the first block of the blockchain. AddBlock() function is called.

Now we would see, if we could add n number of blocks in the blockchain and form a chain.

```
Choice: 2
How many Blocks you want to add in chain? : 6
Entering random numerical data (by rand()function) in this Block: 43
Entering random numerical data (by rand()function) in this Block: 46
Entering random numerical data (by rand()function) in this Block: 57
Entering random numerical data (by rand()function) in this Block: 55
Entering random numerical data (by rand()function) in this Block: 53
Entering random numerical data (by rand()function) in this Block: 55
6 Blocks are added in Blockchain Successfully

 ENTER YOUR CHOICE
1: Add a new block in the Blockchain
2: Add n numbers of blocks in Blockchain
3: Print all blocks present in Blockchain
4: Check Validity of Blockchain
5: EXIT
```

We have added 6 blocks in the blockchain, therefore our blockchain has total 8 number of blocks.

OUTPUTS

```
Choice: 3

These are the Parameters in a Block of our Blockchain :
0×1312980       6e340b9cffb37a989ca544e6bb780a2c78901d3fb33738768511a30617afa01d        [36]    0×13129d0
0×13129d0       ec2b0a1f50aa8f0fd3d9983f99a38108be52b95861ec18e309499b8f9fcee36f        [43]    0×1312a20
0×1312a20       ca3e2fd692c1cb9fdec85711b7a4ddc7ebf19256007f41ad7d6ceb70475703ff        [46]    0×1312a70
0×1312a70       3631b80da5f69c0cad8092b8c6feb38b6c35272e757da7422be7fe3558511429        [57]    0×1312ac0
0×1312ac0       4b41076e5aef7f04e50ce5b70c110559a12dd94c0eff42360855f332bcb59278        [55]    0×1312b10
0×1312b10       f7eaa36ac106930703904542511f9efa33eed6117678490148bbf76d4c9475fd        [53]    0×1312b60
0×1312b60       0ac57bb3039df201f51ac0e8ac4f102f8eaf3971750507ec4788aeb4a153f02e        [55]    (nil)


 ENTER YOUR CHOICE
1: Add a new block in the Blockchain
2: Add n numbers of blocks in Blockchain
3: Print all blocks present in Blockchain
4: Check Validity of Blockchain
5: EXIT
```

We may print all the data present in the blockchain along with the attributes or the parameters present for a block.

OUTPUTS

```
Choice: 4

1.      [43]    f269057a23fd74bde41d436350f98358ce932a990f3bca8e0716245af275bdce - ec2b0a1f50aa8f0fd3d9983f99a38108be52b95861ec18e309499b8f9fcee36f
 Block is valid !

2.      [46]    0fe5075d6aeec1db1e47670099ee1551ad9d551df274976564bc4e969b9be6b3 - ca3e2fd692c1cb9fdec85711b7a4ddc7ebf19256007f41ad7d6ceb70475703ff
 Block is valid !

3.      [57]    00746f5a6ca0980a7407c85f63ce5a42376584f7190ac599c430add7cba4da3f - 3631b80da5f69c0cad8092b8c6feb38b6c35272e757da7422be7fe3558511429
 Block is valid !

4.      [55]    171183cb2443c283f525cac0c5b23bbf89ebf9c3fc55b602440a6d3e0f417dfe - 4b41076e5aef7f04e50ce5b70c110559a12dd94c0eff42360855f332bcb59278
 Block is valid !

5.      [53]    64ab5ce9d9ae3fe769ec80902645fdbc117b09b52b51b8fbede73f080d4e19de - f7eaa36ac106930703904542511f9efa33eed6117678490148bbf76d4c9475fd
 Block is valid !

6.      [55]    8fdca81c7af1141b96b84ecf094cb9c0f4a702c5cabd7515aa96f64cb822fc2f - 0ac57bb3039df201f51ac0e8ac4f102f8eaf3971750507ec4788aeb4a153f02e
 Block is valid !

 ***** Kashish's blockchain is validated and verified! *****

 ENTER YOUR CHOICE
1: Add a new block in the Blockchain
2: Add n numbers of blocks in Blockchain
3: Print all blocks present in Blockchain
4: Check Validity of Blockchain
5: EXIT
```

As all the blocks have been visible along with their parameters. We should check the validity for these blocks. The block needs to be hashed to keep the integrity of the data. A SHA-256 is taken over the content of the block. It should be noted that this hash has nothing to do with "mining", since there is no Proof Of Work problem to solve.

OUTPUTS

At any given time we must be able to validate if a block or a chain of blocks are valid in terms of integrity. This is true especially when we receive new blocks from other nodes and must decide whether to accept them or not.
The block parameters of the blockchain are verified and validated.
Hence, we terminate the program.

```
Choice: 5
FINALLY DONE!
 **All your choices were accepted. Thankyou for your patience**

 -KASHISH SRIVASTAVA
 R134218079
 500067405
 CSF-B2
root@kali:~/Minor_Project#
```

CONCLUSION AND FUTURE SCOPE

- In this project implementation of structures, pointers, linked lists, user define functions, control and jumping statements was initiated. For further project work file handling concept will be applied in our end term.
- The objective of the study behind this implementation was to identify the blockchain technology use cases in healthcare, the example applications that have been developed for these use cases, the challenges and limitations of the blockchain-based healthcare applications, the current approaches employed in developing these applications and areas for future research.
- Since in our model we can create a block, add into the block and check the validity of the block. This will improve in maintaining access control, scalability and the content or transactions information stays secure.
- Further research is also needed to supplement ongoing efforts to address the challenges of better scalability, latency, interoperability, security and privacy in relation to the use of blockchain technology in healthcare.

REFERENCES

[1] https://www.sciencedirect.com/science/article/pii/S138650561930526X [Blockchain in healthcare and health sciences—A scoping review]
[2] https://www.researchgate.net/publication/283517888_Performance_study_of_enhanced_SHA
-256_algorithm [Performance Study of Enhanced SHA-256 Algorithm]
[3] http://paper.ijcsns.org/07_book/201812/20181202.pdf [Application of Blockchain
Technology to Guarantee the Integrity and Transparency of Documents]
[4]https://www.researchgate.net/profile/Wei_Peng4/publication/328247073_A_BlockchainBased_Authentication_and_Security_Mechanism_for_IoT/links/5e03736c4585159aa4999c0e/A
Blockchain-Based-Authentication-and-Security-Mechanism-for-IoT.pdf [A Blockchain-basedAuthentication and Security Mechanism for IoT]
[5] http://ceur-ws.org/Vol-1979/paper-09.pdf [A Comprehensive Reference Model forBlockchain-based Distributed Ledger Technology]
[6] https://journals.sagepub.com/doi/abs/10.1177/1460458212442933 [Privacy and data security in E-health: requirements from the user's perspective]
[7]https://scholar.google.com/scholar_lookup?title=11%20blockchain%20technology%3A%20principles%20and%20applications%20Research%20Handbook%20on%20Digital%20Transformations&publication_year=2016&author=M.%20Pilkington [11 blockchain technology: principles and applications Research Handbook on Digital Transformations]
[8] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6627742/ [Blockchain Technology in Healthcare: A Systematic Review]
[9] https://www.theiet.org/media/4478/blockchain-in-healthcare-report-web.pdf [Blockchain in Healthcare]
[10] https://www.peerbits.com/blog/blockchain-technology-on-healthcare-industry.html [Impact of Blockchain technology on healthcare sector]
[11] https://www.hitachi.com/rev/archive/2017/r2017_01/103/index.html [Creating Blockchain-driven Financial Services and Business Models]

THANK YOU

HOPE YOU LIKED MY PROJECT!

Kashish Srivastava