Cryptocurrency System using Blockchain

A Report of Minor Project (BCA 592) Submitted in

Partial Fulfillment of the Requirements

for the Degree of

Bachelor of Computer Application

(Abhishek Bhattacharya)

(MAKAUT ROLL NO-10401217119 AND REGISTRATION NO-171041010002)

(Debolina Saha)

(MAKAUT ROLL NO-10401217094 AND REGISTRATION NO-171041010027)

(Mayukh Ghosh)

(MAKAUT ROLL NO-10401217078 AND REGISTRATION NO-171041010043)

(Misa Halder)

(MAKAUT ROLL NO-10401217077 AND REGISTRATION NO-171041010044)

(Pratishruti Sarkar)

(MAKAUT ROLL NO-10401217065 AND REGISTRATION NO-171041010056)

DEPARTMENT OF COMPUTER APPLICATION

INSTITUTE OF ENGINEERING & MANAGEMENT

2019

DECLARATION CERTIFICATE

This is to certify that the work presented in the project entitled **"Cryptocurrency System using Blockchain"** in partial fulfillment of the requirement for the award of degree of **Bachelor of Computer Application** of **INSTITUTE OF ENGINEERING & MANAGEMENT** is an authentic work carried out under my supervision and guidance.

To the best of my knowledge the content of this project does not form a basis for the award of any previous Degree to anyone else.

Date:

_____

Prof Amitava Chatterjee

Dept. of Computer Application

Institute of Engineering & Management

_____

Prof. Abhishek Bhattacharya

Head of the Department

Dept. of Computer Application

Institute of Engineering & Management

CERTIFICATE OF APPROVAL

The foregoing project entitled **"Cryptocurrency System using Blockchain"** is hereby approved as Minor Project and has been presented in satisfactory manner to warrant its acceptance as prerequisite to the degree for which it has been submitted.

It is understood that by this approval, the undersigned do not necessarily endorse any conclusion drawn or opinion expressed therein, but approve the project for the purpose for which it is submitted.

(Internal Examiner) **(External Examiner)**

Acknowledgements

We would like to express our special thanks of gratitude to our Mentor (Prof Amitava Chatterjee) who helped us a lot in this project, his valuable suggestions helped us to solve tough challenges and without his help this project could not have been completed in time. A special thanks to our Head of Department (Prof Abhishek Bhattacharya) who gave us the golden opportunity to do this wonderful project on the topic (**Cryptocurrency System using Blockchain**), which also helped us in doing a lot of research and we came to know about so many new things we are really thankful to them. Secondly we would like to thank our friends who helped us a lot in finalizing this project within the limited time frame

Contents

Chapter 1

1.1 Introduction

Blockchain technology is an ever-growing, secure, shared record keeping system in which each user of the data holds a copy of the records, which can only be updated if all parties involved in a transaction agree to update. Blockchain was introduced with the invention of a digital currency called Bitcoin in 2008.

The concept of electronic cash or digital currency is not new. Since the 1980s, e-cash protocols have existed that are based on a model proposed by David Chaum. Two fundamental e-cash system issues needed to be addressed: accountability and anonymity.

Accountability is required to ensure that cash is spendable only once (double-spend problem) and that it can only be spent by its rightful owner. Double spend problem arises when same money can be spent twice. As it is quite easy to make copies of digital data, this becomes a big issue in digital currencies as you can make many copies of same digital cash.
Anonymity is required to protect users' privacy. As with physical cash, it is almost impossible to trace back spending to the individual who actually paid the money.

In 2009, this problem was solved when an electronic cash (e-cash) system named Bitcoin appeared. The term cryptocurrency emerged later. For the very first time, it solved the problem of distributed consensus in a trustless network. It used public key cryptography with a Proof of Work (PoW) mechanism to provide a secure, controlled, and decentralized method of minting digital currency. The key innovation

was the idea of an ordered list of blocks composed of transactions and cryptographically secured by the PoW mechanism

Consensus is a distributed computing concept that has been used in blockchain in order to provide a means of agreeing to a single version of the truth by all peers on the blockchain network.

What is Proof of Work?

A Proof of Work algorithm (PoW) is how new Blocks are created or *mined* on the blockchain. This type of consensus mechanism relies on proof that adequate computational resources have been spent before proposing a value for acceptance by the network. This scheme is used in Bitcoin, Litecoin, and other cryptocurrency blockchains. Currently, it is the only algorithm that has proven to be astonishingly successful against any collusion attacks on a blockchain network. The goal of PoW is to discover a number which solves a problem. The number must be **difficult to find but easy to verify**—computationally speaking—by anyone on the network. This is the core idea behind Proof of Work.

What is Bitcoin?

Bitcoin has started a revolution with the introduction of the very first fully decentralized digital currency, and the one that has proven to be extremely secure and stable from a network and protocol point of view. As a currency bitcoin is quite unstable and highly volatile, albeit valuable.

Since its introduction in 2008 by Satoshi Nakamoto, Bitcoin has gained massive popularity, and it is currently the most successful digital currency in the world with billions of dollars invested in it. Its popularity is also evident from the high number of users and investors, increasing bitcoin price, everyday news related to Bitcoin, and the number of start-ups and companies that are offering bitcoin-based online exchanges, and it's now also traded as Bitcoin Futures on Chicago Mercantile Exchange (CME).

Steps of working :

- A node starts a transaction by first creating and then digitally signing it with its private key. A transaction can represent various actions in a blockchain. Most commonly this is a data structure that represents transfer of value between users on the blockchain network.
- A transaction is propagated (flooded) by using a flooding protocol, called Gossip2. protocol, to peers that validate the transaction based on preset criteria. Usually, more than one node are required to verify the transaction.
- Once the transaction is validated, it is included in a block, which is then propagated onto the network. At this point, the transaction is considered confirmed.
- The newly-created block now becomes part of the ledger, and the next block links itself cryptographically back to this block. This link is a hash pointer. At this stage, the transaction gets its second confirmation and the block gets its first confirmation.
- Transactions are then reconfirmed every time a new block is created. Usually, six5. confirmations in the Bitcoin network are required to consider the transaction final.

Chapter 2

2.1 Scope of the project

The objective of the project is to demonstrate the working of a blockchain ledger by implementing our very own cryptocurrency called **Lightcoin.** The project demonstrates the process of mining cryptocurrency by implementing a proof of work algorithm and allows user to make transactions by using Lightcoin as tokens. This lays the groundwork for developing a fully fledged cryptocurrency system based on blockchain.

2.2 User wise Functionalities

Mining: This is the process by which new blocks are added into the blockchain. Each block contains a list of all pending transactions that are hence verified with the new block. The volunteer node lends some of its computational resources to solve a complex computational problem. Usually it gains some currency as compensation.

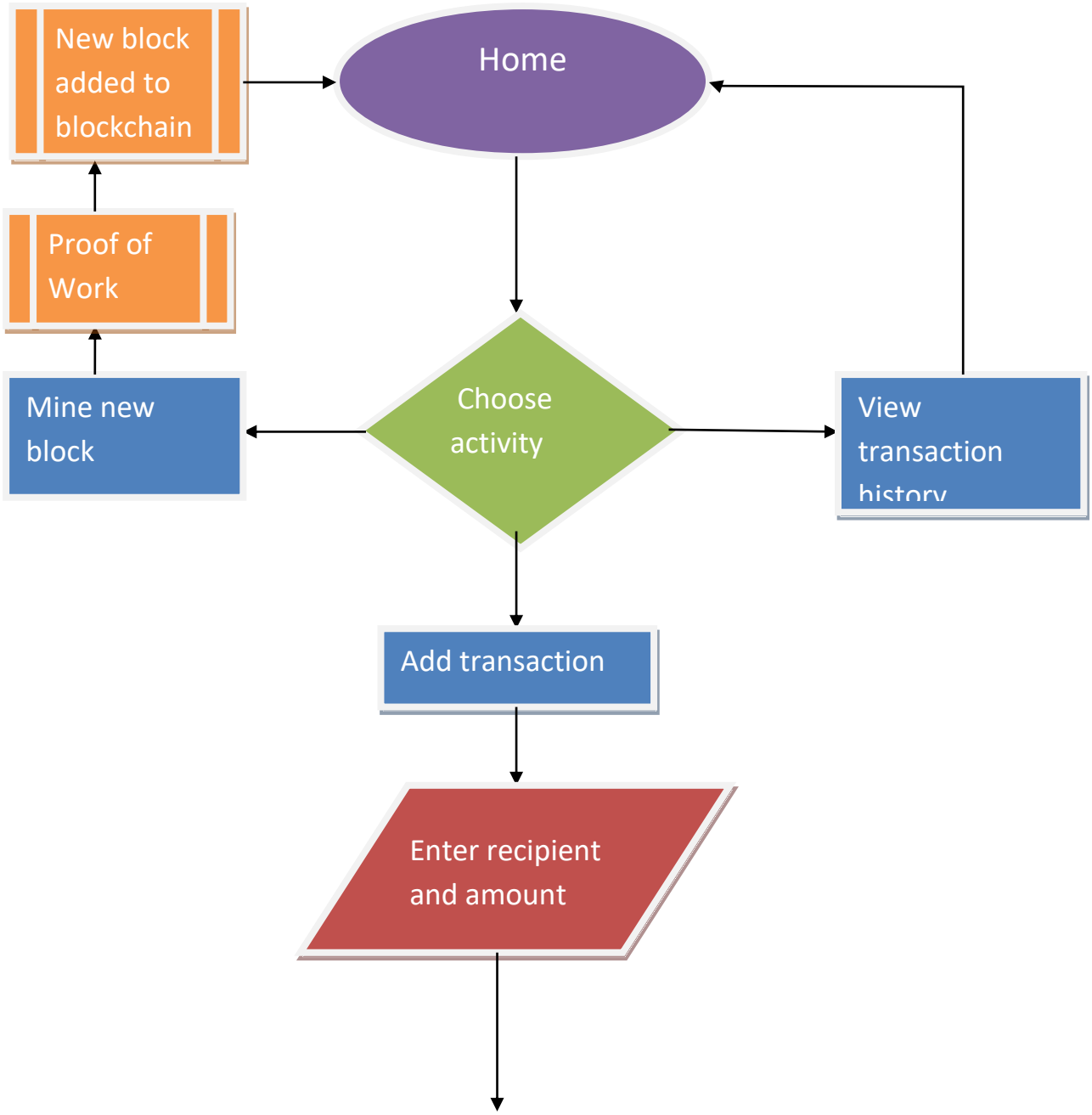
Transaction: This is the process by which user adds a new transaction to be verified by the blockchain. User specifies the recipient and the amount and the transaction is validated by the next block that is mined. The amount must be less than the balance of the user.

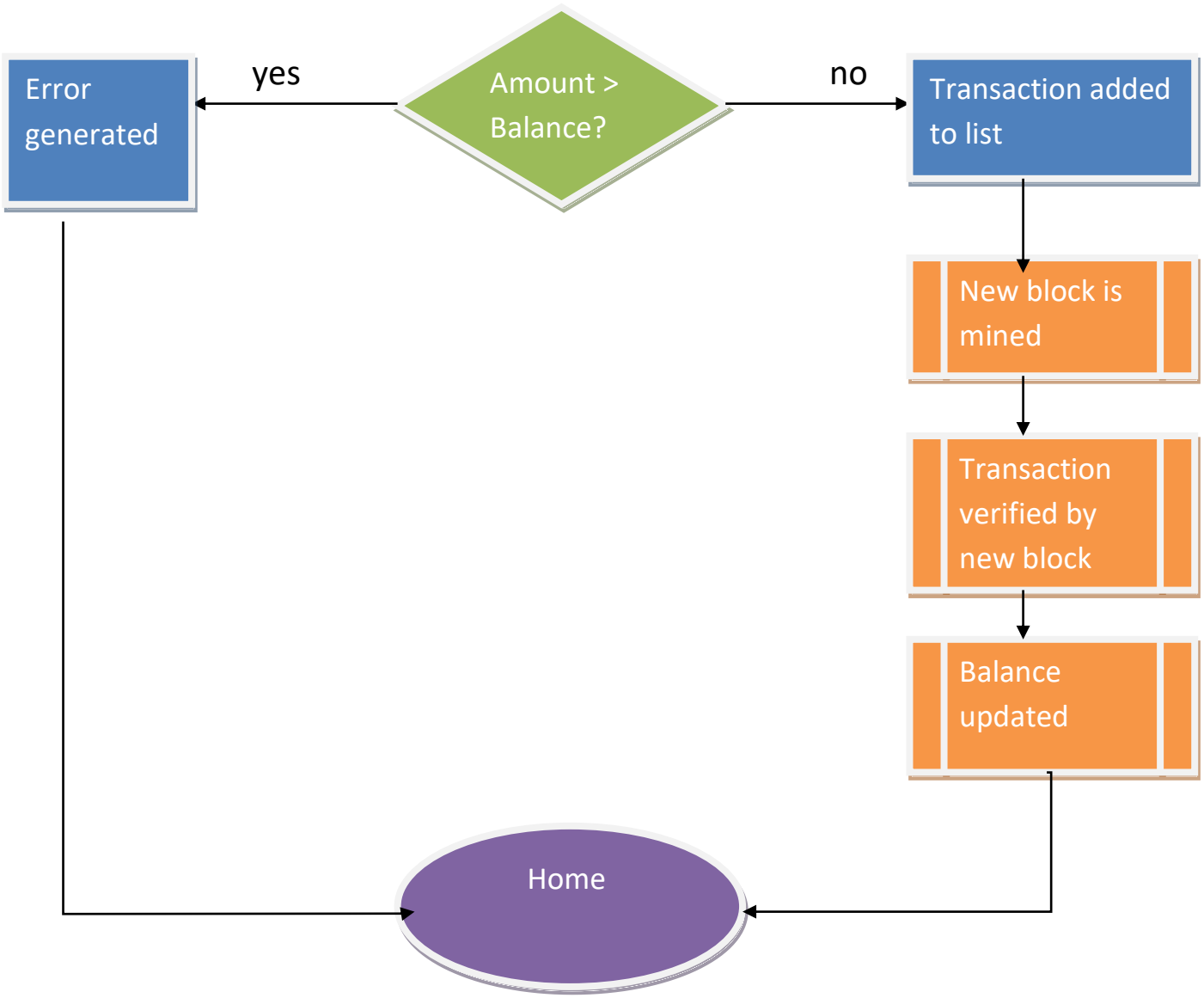
View Transaction History: User may view the list of all transactions committed as verified by its node. It shows the complete blockchain with each block containing a list of transactions.

Chapter 3

3.1 Design diagrams

Flowchart




Amount > Balance?
yes
Error generated
no
Transaction added to list
New block is mined
Transaction verified by new block
Balance updated
Home

Chapter 4

4.1 Software requirement

Platform used: Windows 10

Language used: Python 3.7

Modules used: hashlib, flask

IDE used: Pycharm

Designing tools used: yWorks

4.2 Hardware Requirement

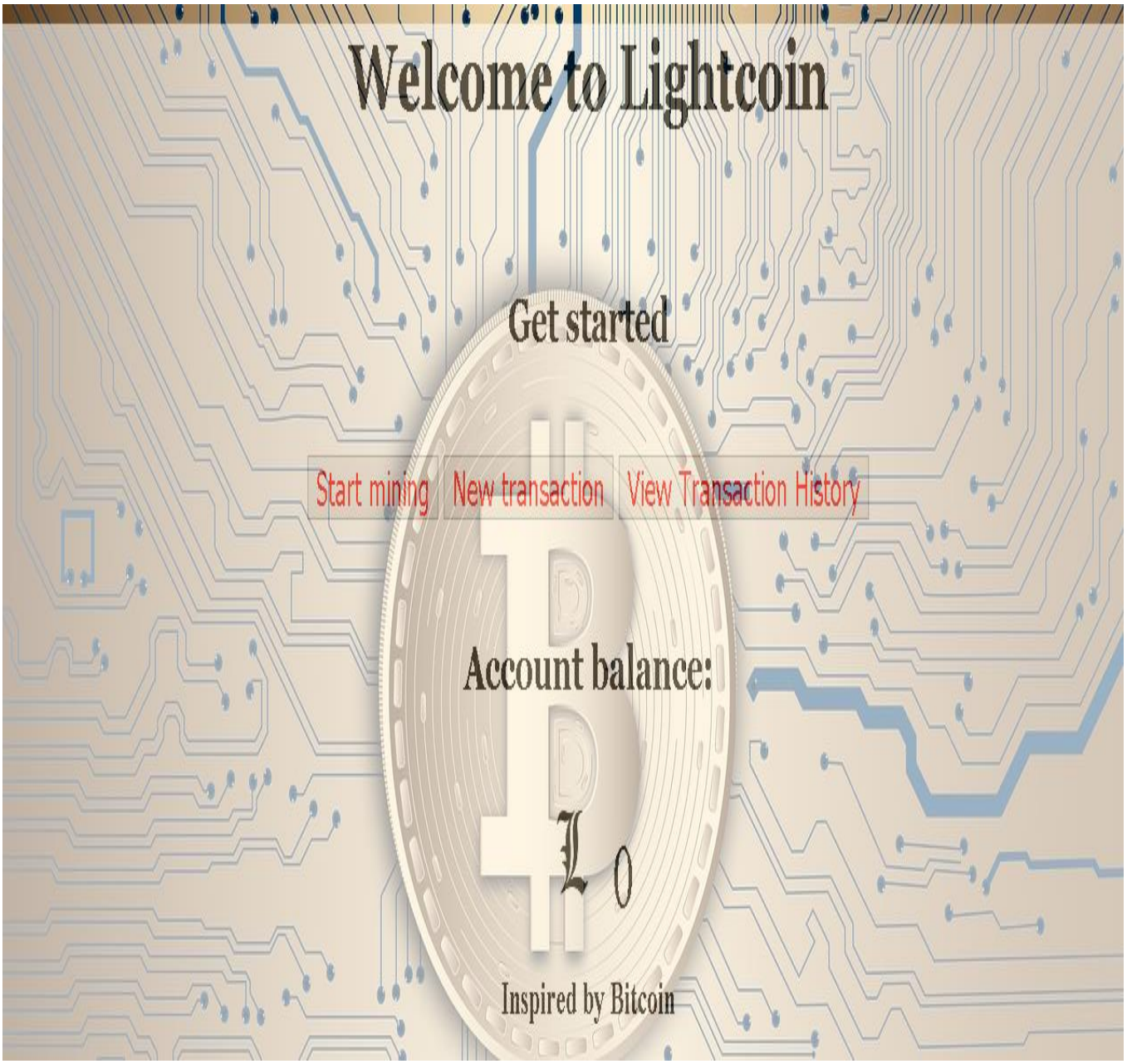
4GB RAM

10GB Hard Disk

Chapter 5

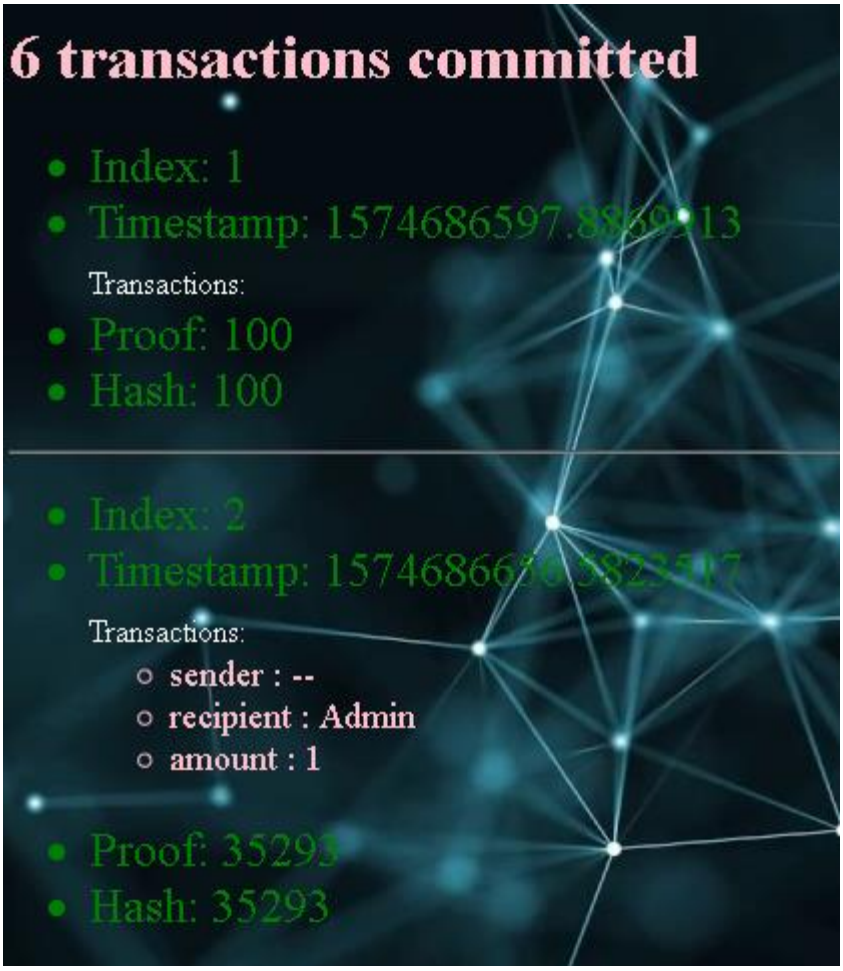
5.1 Results and discussion

This is the home page that the user will first see



After user successfully mines a block

User may view the transaction history thus far



User may create their own transaction that will be validated in the next block

In case transaction fails

In case transaction succeeds

The transaction visible in the next block that is mined.

Proof of Work code:

```
def proof_of_work(self, last_proof):
    proof = 0
    while self.valid_proof(last_proof, proof) is False:
        proof += 1
    return proof

@staticmethod
def valid_proof(last_proof, proof):
        guess = f'{last_proof}{proof}'.encode()
        guess_hash = hashlib.sha256(guess).hexdigest()
        return guess_hash[:4] == "0000"
```

This algorithm concatenates the previous proof and current trial number and tests whether the resultant hash will give 4 leading zeroes. The number is incremented until the test is successful

Frontend:

mine.html

```
<!DOCTYPE html>
<html>
<head>
    <title>Lightcoin</title>
    <link rel="stylesheet" type="text/css"
href="{{url_for('static',
filename='css/style.css')}}">
</head>
<body>
    <a href="/" style="float: right;">Home</a>
    <h1>{{item['length']}} transactions
committed </h1>
    {% for block in item['chain'] %}
    <ul>
        <li>Index: {{block['index']}}</li>
        <li>Timestamp:
{{block['timestamp']}}</li>
        Transactions:
```

```
        {% for transaction in
block['transactions'] %}
            <ul>
            {% for key,value in
transaction.items() %}
                <li> {{key}} : {{value}}</li>
            {% endfor %}
            </ul>
            <br />
        {% endfor %}
        <li>Proof: {{block['proof']}}</li>
        <li>Hash: {{block['proof']}}</li>
    </ul>
    <hr/>
    {% endfor %}
</body>
</html>
```

5.2 Future Scope

This project lays the groundwork for a fully fledged cryptocurrency platform. Two modules are required for this.

- Addition of multiple users to the cryptocurrency network who can conduct transactions among themselves
- Addition of multiple nodes which will lend its resources for mining each maintaining a part of the ledger

Chapter 6

6.1 Conclusions

With this project we have successfully demonstrated the functionality of blockchain using our own small scale cryptocurrency called Lightcoin which implements its very own proof of work algorithm. Thus far the system is robust, free of bugs and works as intended.

6.2 Bibliography

Mastering Blockchain 2nd edition by Imran Bashir

https://blockgeeks.com/guides/what-is-blockchain-technology/

https://www.javatpoint.com/blockchain-tutorial

https://en.wikipedia.org/wiki/Blockchain