VCOINS

Submitted in partial fulfillment of the requirements

of the degree of

Bachelor of Engineering in Computer Engineering

By

Saransh Kotha (Roll No. 17102A0017)

Pearl Patel (Roll No. 17102A0071)

Under the Guidance of

Prof. Dilip Motwani

Department of Computer Engineering

Vidyalankar Institute of Technology

Wadala(E), Mumbai 400 037

University of Mumbai

2020-21

CERTIFICATE OF APPROVAL

This is to certify that the project entitled

“VCOINS”

is a bonafide work of

Saransh Kotha (Roll No. 17102A0017)

Pearl Patel (Roll No. 17102A0071)

submitted to the University of Mumbai in partial fulfilment of the requirement for the award of the degree of

Undergraduate in “Computer Engineering”.

Guide Head of Department Principal

Project Report Approval for B. E.

This project report entitled ***VCOINS*** by

1. ***Saransh Kotha (17102A0017)***
2. ***Pearl Patel (17102A0017)***

is approved for the degree of ***Bachelor of Engineering in Computer Engineering .***

Examiners

1.----------

2.----------

Date:

Place:

Declaration

I declare that this written submission represents my ideas in my own words and where others' ideas or words have been included, I have adequately cited and referenced the original sources. I also declare that I have adhered to all principles of academic honesty and integrity and have not misrepresented or fabricated or falsified any idea/data/fact/source in my submission. I understand that any violation of the above will be cause for disciplinary action by the Institute and can also evoke penal action from the sources which have thus not been properly cited or from whom proper permission has not been taken when needed.

Sr. No.	Name of Student	Roll No.	Signature
1.	Saransh Kotha	17102A0017	
2.	Pearl Patel	17102A0071	

Date:

Acknowledgements

Show, motivation, and inspiration consistently assumed a vital part in the accomplishment of any endeavour.

We wish to put on record our significant appreciation for Prof. Dr. Dilip Motwani who gave us wholehearted help and significant direction, ideas, and consolation all through this task. He generally spurred us and roused us to work more diligently. We are additionally grateful for the direction and oversight given by Prof. Swapnil Sonawane and any remaining employees from the Department of Computer Engineering of Vidyalankar Institute of Technology.

We also want to thank the Head of our Department, Prof. Sachin Bojewar, for permitting us to proceed with this task and furnishing us with his important direction and kind help. We additionally like the other instructing and non-training staff of Vidyalankar Institute of Technology without whose assist this project with having been finished.

In conclusion, we broaden our appreciation towards our loved ones who have fundamentally added to our task by establishing a particularly stable climate to work in and giving us all their help differently. Moreover, we might likewise want to thank our peruses who have given us productive criticism.

Abstract

Blockchain is characterized collection of chained blocks over a P2P organization. It is likewise considered as a decentralized record which holds the records of any online occasion. It offers a protected stage for information and worth exchange even in a conniving network. In advanced exchanges on blockchain, every exchange is confirmed by every one of the nodes inside the network utilizing agreement convention. It gives a believed channel to data and worth exchange, even in untrusted networks.

One of the significant utilizations of Blockchain is Cryptocurrency. Basically expressed, a digital money is another type of computerized cash. We present VCOINS – another Cryptocurrency which is an incorporation of Blockchain Technology and Artificial Intelligence over a P2P network dependent on an interesting consensus agreement named AI-POS.

The primary thought is to carry out a framework which can conquer the downsides of some usually utilized applications in order to improve. VCOIN can be a stage into distinguishing the genuine capability of this innovation. The presented type of consensus algorithm is essential objective to plan a dependable calculation to make the framework considerably more trust-commendable and artful to miners and users.

Table of Contents

List of Figures

List of Tables

Introduction

Introduction

- **What is BLOCKCHAIN?**

A blockchain is essentially a distributes database of transaction that have been executed and shared among participating parties. In Blockchain all the participants are anonymous such that the identity of the participant during transaction will be hidden by their public key which is also used for performing transaction. One can't identify as to who has done the transactions until one has known the mapping of the public key to person.

Current digital economy is based on the reliance on a certain trusted authority. Our all online transactions rely on trusting someone to tell us the truth; it can be an email service provider telling us that our email has been delivered; it can be a certification authority telling us that a certain digital certificate is trustworthy; or it can be a social network such as Facebook telling us that posts regarding our life events have been shared only with our friends, or it can be a bank telling us that our money has been delivered reliably to our dear ones in a remote country. The blockchain consists of series of blocks which are made up of many transactions. Every block is linked to one another like a linked list, in order of being created and added to the chain. The authenticity of every transaction is verified by digital signatures based on Elliptic Curve Cryptography (ECC). This process of verification is carried out by some members of the network called miners. The miners use specialized and easily available software along with the processing power of their computers to verify the transactions. This sounds simple enough, but the processing power required to do so is quite herculean. And since the miners

are using their bandwidth and electricity to do the verification process, they need tobe compensated. This is where the Block Chain begin to take shape. The key characteristics of a blockchain includes, Decentralization which helps one in removing third-party involvement in validation, Persistency which ensures system integrity and non-repudiation, Anonymity which preserves the real identity of users and Auditability which enables tracking and verification of transactions.

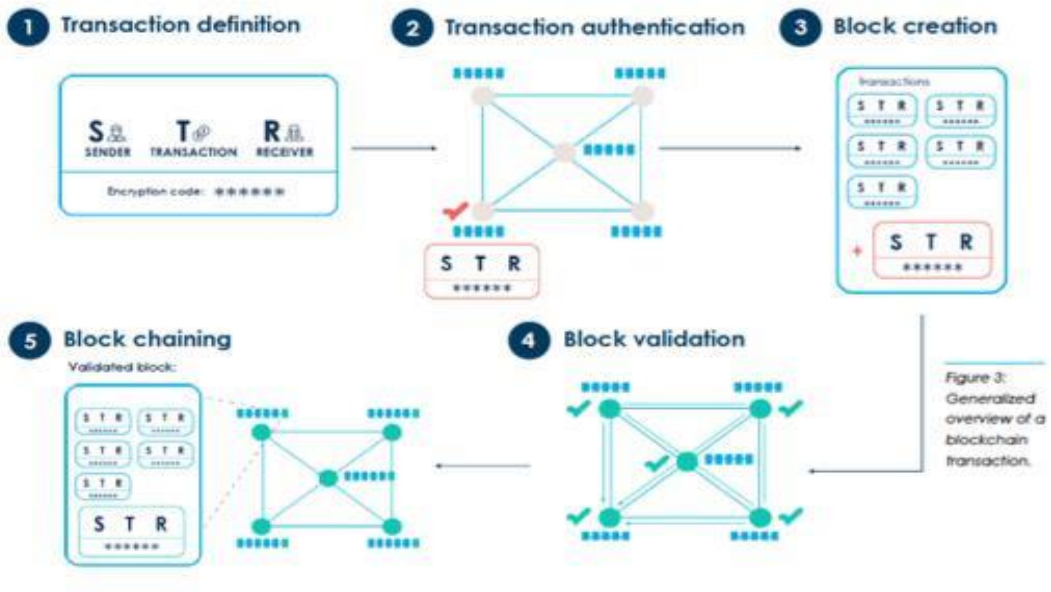

Fig.1 Cryptocurrency working model

- **Blockchain technical architecture:**

They are layers of Infrastructure, Utility, Ledger, Consensus, Consensus, System Management, Interface, Application and Operation, and Maintenance.

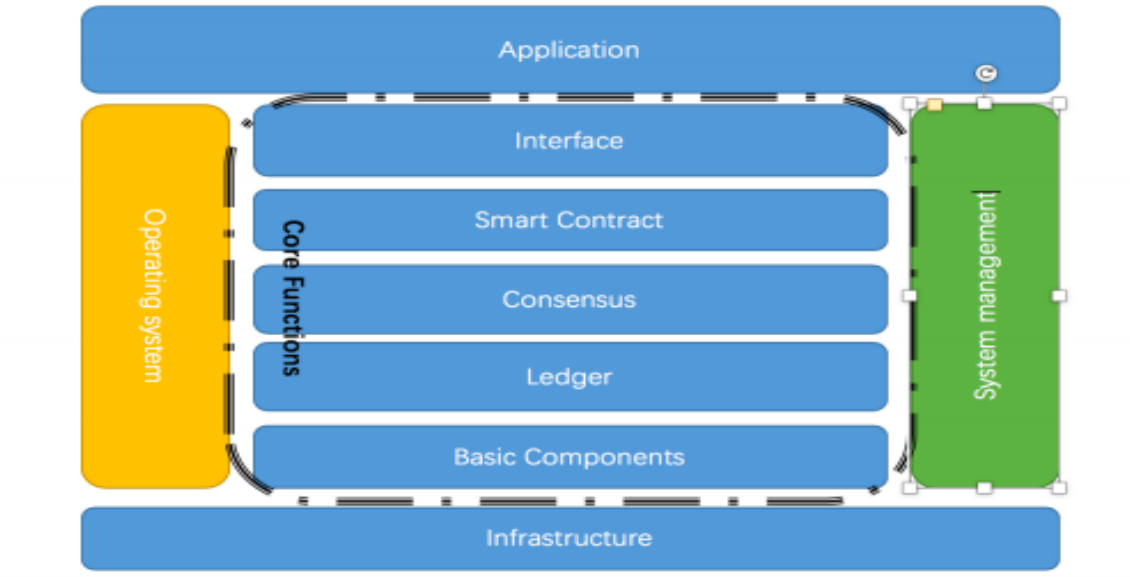

Fig. 2 Layered block diagram of Blockchain

Some technical architecture are as follows:

1.Infrastructure

The infrastructure layer provides physical resources and drivers for the upper layers and is the base support for the blockchain system.

2.Utility

The utility layer enables the recording, verification and dissemination of information in the network of blockchain systems.

3.Ledger

The ledger layer is responsible for the information storage of the blockchain system, including collecting transaction data and generating data blocks for validity of the local data and passing the checked block to the blockchain.

4.Consensus

Consensus algorithms are required to agree on one consistent state of blockchain, as it has many copies residing on each node of network. Consensus algorithm should separate one state from the rest of the states so that one state gets accepted by entire network. Various schemes are employed to achieve this. Some of them are:

1. Proof of Work
2. Proof of Stake

- **PoW v/s PoS:**

Characteristic	PoW	PoS
Node Management	No permission required	No permission required
Transaction Latency	High (in minutes)	Low (in seconds)
Throughput	Low	High
Energy-saving	No	Yes

Fig. 3.1 POW v/s POS

Security Boundary	Malicious computing power is no more than 1/2.	Malicious equity is no more than 1/2.
Representative application	Bitcoin, Ethereum	Peercoin
Scalability	Well	Well

Fig. 3.2 POW v/s POS

- **Timestamp Server:**

A timestamp server works by taking a hash of a block of items to be timestamped and widely publishing the hash. The timestamp proves that the data must have existed at the time, obviously, in order to get into the hash. Each timestamp includes the previous timestamp in its hash, forming a chain, with each additional timestamp reinforcing the ones before it.

- **Hashing Function:**

Cryptography hash function is a hash function that is designed to provide special properties, including collision resistance and preimage resistance that are important for many application in information security. For example, a cryptography hash function increases the security and efficiency of a digital signature scheme when the digest is digitally signed instead of the message itself. Various hash function used in symmetric key cryptography are typically either SHA-256 or SHA-01.

- **The Innovation of Blockchain Technology Is Becoming More and More Dynamic:**

More and more foreign companies have been involved in the development and contribution of Blockchain source code. According to the data on GitHub, the proportion of Blockchain projects in 2010 was less than

1%, but it ran up to 11% in 2017. And there were lots of open source platforms or individual collaboration ecosystem coming into being, such as Bitcoin, Ethereum, Hyperledger and Ripple.

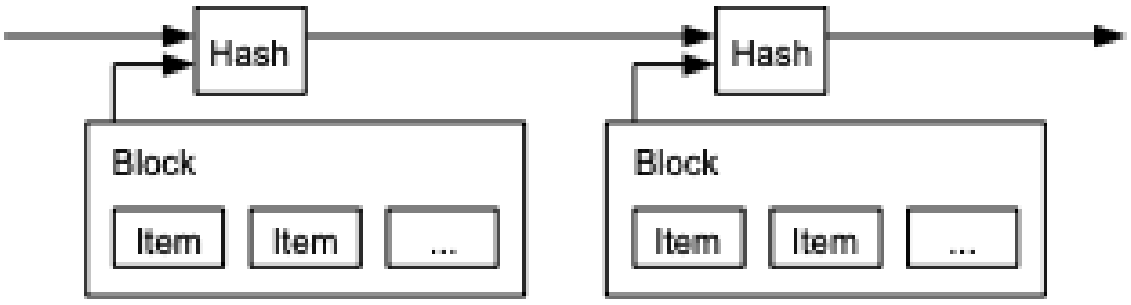

Fig.4 Blockchain connectivity

At the same time, a number of international Blockchain industry alliances have emerged, such as the R3 Blockchain Alliance (Corda), Hyperledger Blockchain Alliance which supported by the Linux Foundation, the Enterprise-level Ethernet Alliance (EEA) and so on.

- **Hidden dangers at the mature level of Blockchain technology:**

At present, the Blockchain technology is not mature in terms of system stability, application security, business model and so on. There are five main problems: the performance cannot meet the three requirements of "high efficiency with low energy", "decentralization" and "security" simultaneously. The transaction throughput that can be performed on the Blockchain is not high, and it’s difficult to meet the needs of the high frequency service; From the perspective of energy consumption, the consensus algorithm such as Proof of work have high energy consumption and high cost, which makes the Blockchain waste a lot of network computing power and resources; From ecological point of view, the current Blockchain products are immature, it lacks of relevant development, integration, operation and maintenance system, and it’s short of standards as well. China

doesn’t have too much right and influence on Blockchain open source platform; Asfor the security , Blockchain is facing a grim situation of platform security and application security which including privacy protection, harmful information, smart contract vulnerabilities, consensus mechanism and private key protection, 51% computational attack, cryptographic algorithm security and so on; From the perspective of the supervision, encryption technology has posed great challenges to legal monitoring, customer identification, anti-money laundering and other regulatory means. At the same time, multi-party collaborative governance of Blockchain also puts higher requirements on supervision.

PROBLEM DEFINITION

Problem Definition

Artificial Intelligence and Blockchain Technology are playing a major role in the development of tech industries. From designing robots to making regular transaction, both of these technologies have given users and developer much advance and secured resources. Both these technologies were playing the supreme role in their respective domains over decades.

Purely based on research and development, in order to move one step forward towards revolutionization, integration of two of the most advance technologies was overdue. Designing a cryptocurrency by integration the principles of Blockchain Technology with the ever so advanced AI models could be one small attempt to unfold the hidden applications of these two technologies.

AIM AND OBJECTIVE

AIM AND OBJECTIVE

The main aim and objective of the project is to understand, research and develop a cryptocurrency by integrating Blockchain Technology with Artificial Intelligence. In order to get a step closer to such a revolutionary application, we closely monitored various cryptocurrencies, researched about various algorithms for implementing our consensus model and read multiple thesis and research papers based on theoretical relations of AI and Blockchain. This project can be first of many future application based on both these technologies and a step towards decentralization.

HARDWARE AND SOFTWARE USED

HARDWARE AND SOFTWARE USED

Hardware requirements :

- PC/Laptop with minimum 4GB RAM

Software Requirements:

- Python 3
- JavaScript
- Following Python Libraries and APIs were used for the implementation of this project:
- Requests and Flask
- TensorFlow 2.0
- Crypto
- Dataset used: bigquery-public-data.crypto_ethereum

METHODOLOGY OF PROPOSED SYSTEM

Methodology of Proposed System

The complete methodology is been divided in following modules:

- Designing the blockchain
    - Blockchain is designed using Python
- Designing the UI for the Blockchain
    - UI for the Blockchain is designed using HTML and JavaScript
- AI model for miners
    - To design the AI model we used Neural Network
- Defining the credit score system
    - In order to develop a credit score system we Trained the AI model against a customised Dataset from Ethereum
- Integrating Blockchain and Artificial Intelligence model
    - We developed suitable environment in order to integrate the AI code with blockchain code using python and various libraries

The user interface is divided into two parts:

(1) Wallet (Client) and (2) Fullnode (Miner)

At the client side, a user can generate their public and private keys using the Wallet Generator. This is done using existing Python Libraries. These keys are saved on

the device and can be used to sign off the Transactions. The Client side fetches data from the Blockchain that is stored on a fullnode. This data is used to display the transaction history and the total balance for the particular wallet address.

For creating a new transaction, user can enter the public key of the receiver. Once the transaction is confirmed, it is sent across all fullnodes on the network for verification and adding it to the blockchain.

On the fullnode, once the transactions arrives from the clients, a miner can start the mining process. The AI model is invoked which selects the suitable miner based on the data available from the Blockchain that is stored on the Node. If the current miner is selected as the miner, a new block (consisting of all the transactions and a new transaction which contains the block reward for the selected miner) is added to the blockchain, and the updated chain is broadcasted across the network so that all the other fullnodes can update their chains.

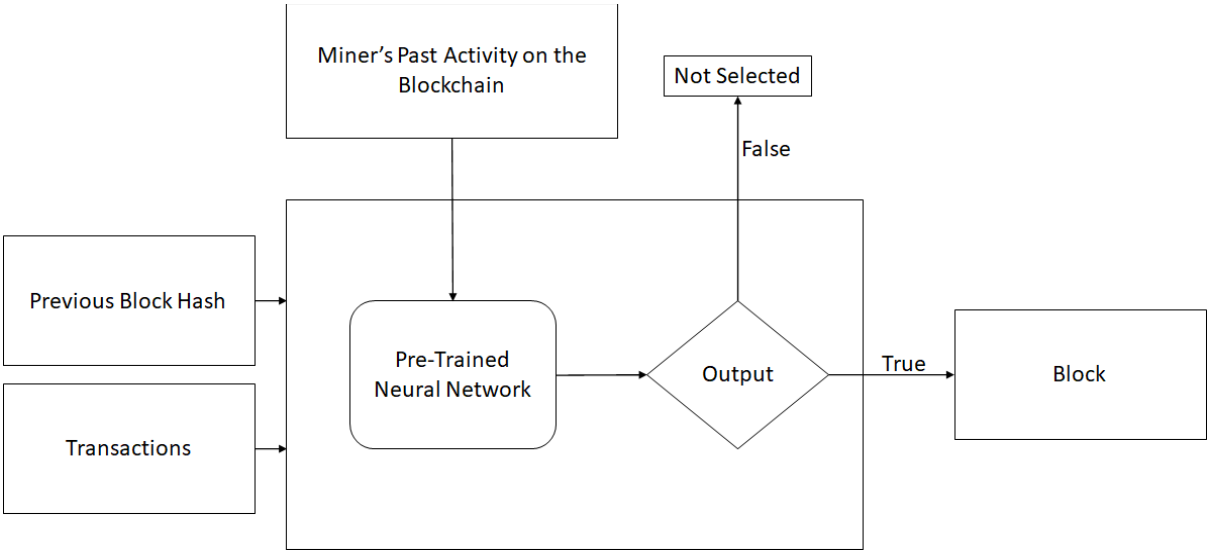

Fig 5.1 Node Side Block Diagram

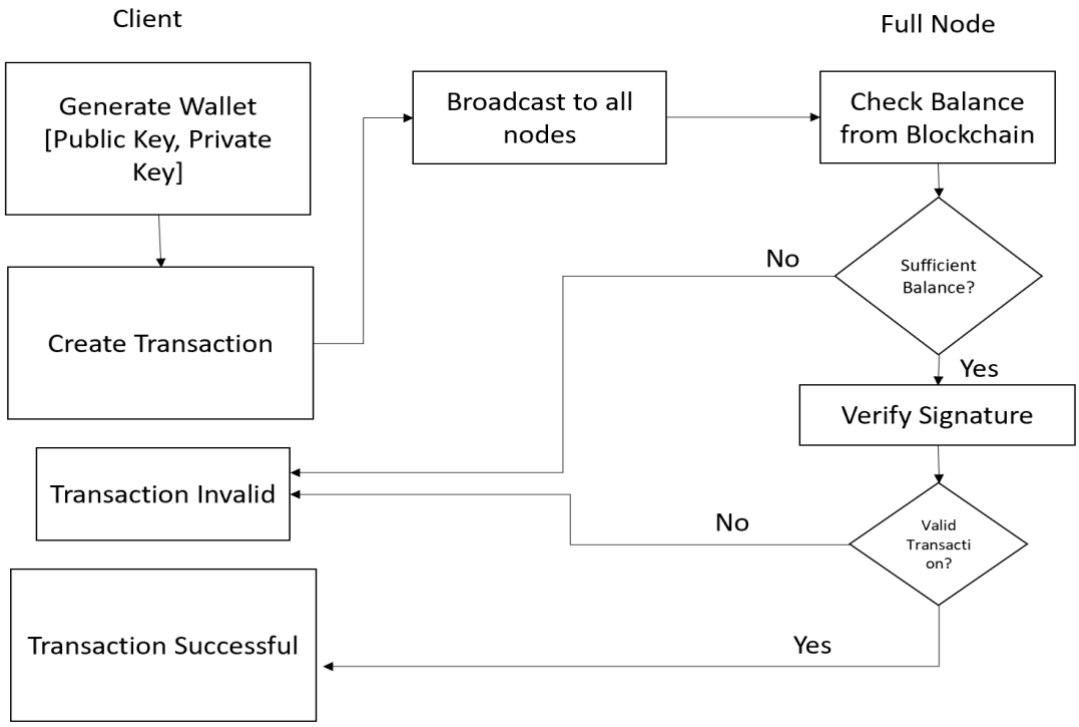

Fig 5.2 Client side Block Diagram

LITERATURE SURVEY

Literature Survey

- **What Is CRYPTOCURRENCY?**

Cryptocurrency is a collection of concepts and technologies that form the basis of a digital money ecosystem. Units of currency called cryptocurrency network. Cryptocurrency users communicate with each other using the cryptocurrency protocols primarily via internet , although other transport network can also be used. The cryptocurrency protocol stack, available as open source software, can be run on a wide range of computing devices, including laptops and smartphones, making the technology easily available.

Unlike traditional currencies cryptocurrency are entirely virtual. There are no physical coins or even digital coins per se. the coins are implied in transactions that transfer values from sender to recipient. Users of cryptocurrency own keys that allow them to prove ownership of cryptocurrency in the network. With these keys they can sign transactions to unlock the values and spend it by transferring it to s new owner. Keys are often stored in a digital wallet on each user's computer or smartphone. Possession of the keys that can sign a transaction is the only prerequisite to spending cryptocurrency. Cryptocurrency is a digital currency system which runs through consensus network. It uses decentralised peer-to- peer payment network that is powered by its users with no central authority or middlemen. While there are about 110 other digital currencies.

- **What exactly is Blockchain mining?**

A peer-to-peer computer process, Blockchain mining is used to secure and verify bitcoin transactions. Mining involves Blockchain miners who add bitcoin transaction data to Bitcoin's global public ledger of past transactions.
In the ledgers, blocks are secured by Blockchain miners and are connected to each other forming a chain.
The process using which cryptocurrency mining works is as follows:

1. Cryptocurrency are mined from blocks. Each block is a part of the blockchain (a ledger of all the transaction made using Cryptocurrency).
2. Blocks are where the complex mathematical code is stored.
3. To mine, Cryptocurrency have to make a new block.
4. Blocks are linked together by hash code.
5. To make a new block, miners have to come up with a new hash which meets specific requirements, such as including the header of the block before and at above or below the target value. Using consensus protocol we get the desired level of difficulty for hash value which is denoted by number of zeros before hash function value.
6. This can be a process of trial and error until miners find a hash that works.
7. Users must then solver the mathematical problem, using their computer CPU's to run the problem solving software.
8. . Once the problem is solved, cryptocurrency are transferred to the miner's unique address.

- **What are Mining Pools?**

A mining pools are basically a group of cryptocurrency miners who combine their computational power and resources over a network. A particular individual contributes its computational powers with other miners in order to find a block and get rewards which the particular miner receives within the mining pool who successfully calculated the hash code for the block and contributed to the blockchain. In some cases, individual miners must show proof of work in order to receive their rewards.

All cryptocurrency mining pools does not function in the same way or have same protocols. But some of the most popular/common mining pools are:

1. Proportional mining pools
2. Pay-per-share pools
3. Peer-to-Peer mining pools

- **Advantages of Mining Pools:**

1. More predictable pay-outs - pools usually pay you on a more regular schedule - be it once you reach a certain threshold, daily or the like. Solo mining only pays you when you find a block, which can take a few days, years, or never.
2. Extra features - Pools usually let you quickly check the status of your miners from anywhere, notify you of extra setup time on your own.
3. Less space - If you are solo mining, you need to keep your own copy of the blockchain. Pools handle all that by themselves.
4. It is easier - There is a low less setup required to do pooled mining, especially when we are talking about merged mining and so forth.

- **Disadvantages of Mining Pools:**

1. Smaller expected earnings - pools usually charge a fee and sometimes use a reward system (like Pay Per Share) that can give you a lower pay-out.
2. Having to rely on third party system to earn your money - websites go down, and when they do, your miners can be idling.
3. Trust - you have to trust the pool owner not to swindle money from you, either by creating fake miners in the pool that do not work but still receive rewards or otherwise.
4. Giving power to the pool owner - some important decisions regarding Bitcoin future are made by people voting with their blocks. Some time ago the Bitcoin community had to choose between two BIPs that fulfilled the same role. The voting was done by the Coinbase transactions containing a vote for either one of the BIPs. By giving their computing powers to the pools, the miners essentially gave their votes to pool owners to vote as they chose.

EXECUTION OF PROPOSD SYSTEM

Execution of Proposed System

The proposed system is designed by integrating Artificial Intelligence with Blockchain Technology. The AI model would be able to detect the super miner from the proposed group of miner within the network based on specially designed credit score based system. The select miner will then mine the upcoming block and will add it into the blockchain. The network will reward the miner for mining the block.

The entire project is based on the principles of Blockchain Technology. Thus making the cryptocurrency more secured and decentralised. The proposed system uses AI-POS consensus algorithms instead of just POW or POS and monitors the selected miner such that no miner can be super miner consecutively two times in order to make the process of selecting a miner more advanced and fair.

AI-POS

We introduce a novel consensus mechanism called Artificial Intelligence Delegated Proof-of-Stake. It combines the prowess of existing Proof-of-Work and Proof-Of-Stake algorithms along with our own AI-based miner selection procedure to create a robust blockchain based Cryptocurrency. Instead of picking the miner according to either PoW or PoS mechanism, in AI-PoS, we have a pre trained neural network based model that scans the entire blockchain history and selects the miner who would make the best possible contribution to the network. This Neural Network is trained on a dataset which was manually created to suit our blockchain. Since, the entire blockchain is available to all the participating miners, it is easy for

the AI model to get the required data. It analyses this data and selects the best miner for the current state of the blockchain based on specific criteria.

While picking a miner, the AI takes care of the following factors:

1. Every participating node in the mining process gets a fair chance to get mine a block and get the reward.
2. A single miner cannot mine consecutive blocks when more than one miner is present. This ensures diversity of miners.
3. Miners who have invested more time and money in the blockchain get a better chance to mine a block. This demotivates the miners from committing frauds as there's a possibility that they might lose their investments.
4. Miners who have recently joined the network are also prioritised by the algorithm to ensure the fair participation of all miners.

If a miner is not selected by the AI algorithm for mining a block, that miner simply cannot mine that particular block, which reduces the chances of creating forks in the chain.

AI-PoS over PoW and PoS

Since this approach does not make an extensive use of proof-of-work, AI-PoS can be considered computationally inexpensive. The full node (for miners) can be run on any internet connected device with ample memory. Anyone can get involved in the mining process without staking any initial funds, and still get a fair chance at mining the reward.

The AI algorithm makes sure that the rich do not monopolize the network and ensures fairness in the network. Along with this, the basic security provided by PoW and PoS is maintained.

Process Model used for Project:

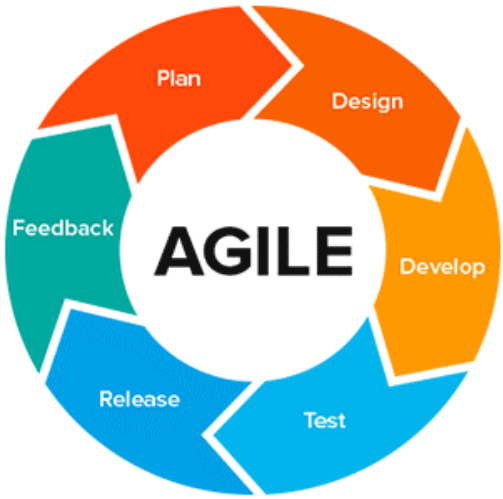

Fig. 6 Analysis of project

This project uses the agile model as the process model for development. In software development, agile practices approach discovering requirements and developing solutions through the collaborative effort of self-organizing and cross-functional teams. This project required strong collaboration and rigorous testing every step of the way. Agile practice is well suitable with this project as it heavily relies on research and exploring areas that have never been seen before. We faced one-of-kind problems and they have been solved in an organised manner by collaboration.

Feasibility Study:

a. Technical Feasibility

This project requires a computer installed with required libraries which can be easily be downloaded from the internet. This project was made using basic text editors. The final product can be used on any browser.

b. Legal Feasibility

After study of basic copyrights and law, the proposed system does not conflict with legal requirements, protection regulations and the proposed venture is acceptable in accordance with the laws as we are not violating any.

c. Financial Feasibility

This project was made using easily available free open source software which makes it cost-effective and economical.

Cost Analysis:

This project is made using free open source software and libraries. Hence, total cost is 0.

WORKFLOW DESIGN

Work Flow Design

• **Data Flow Diagram:**

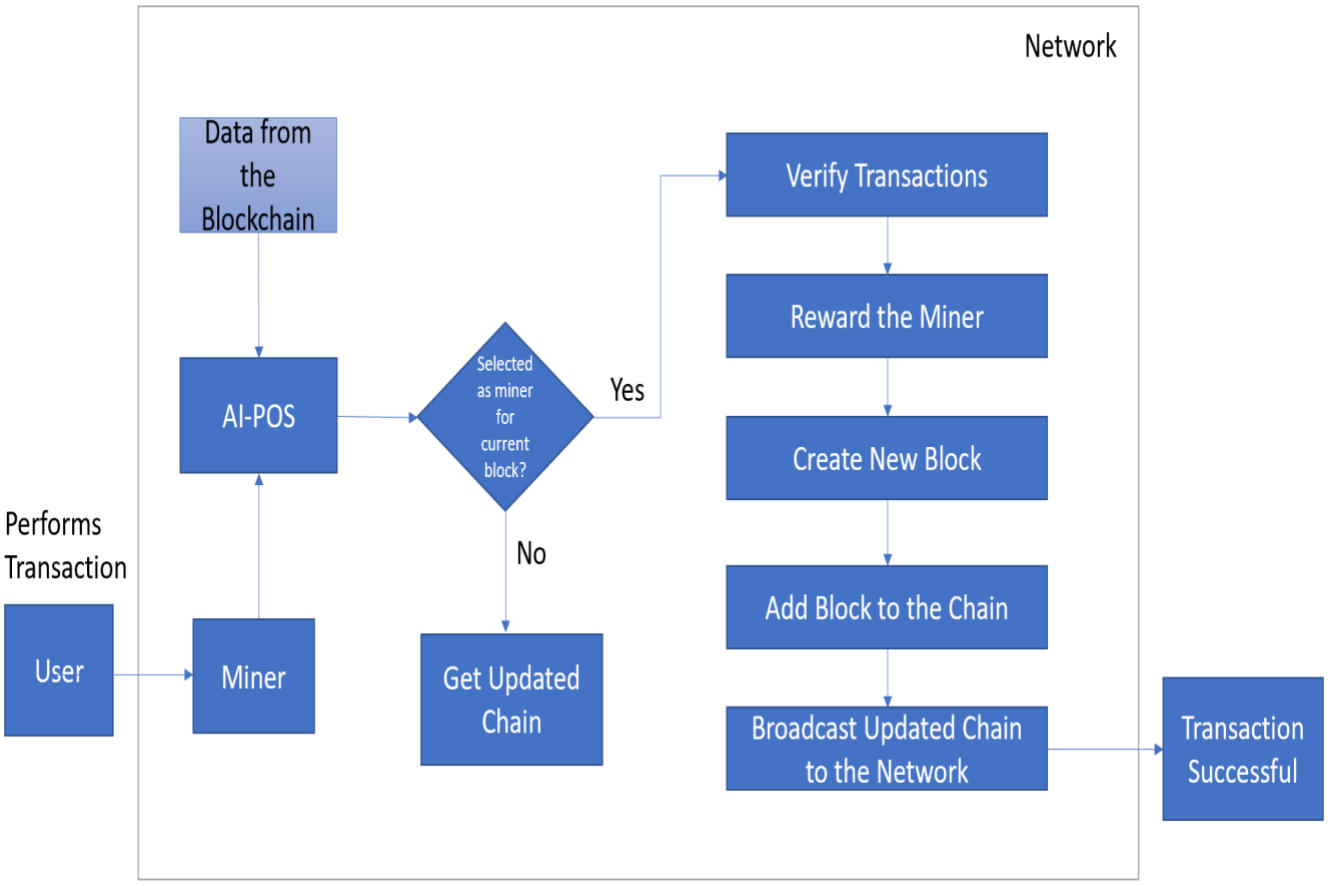

Fig. 7 Data Flow Diagram

SCREENSHOTS OF APPLICATION

SCREENSHOT OF APPLICATION

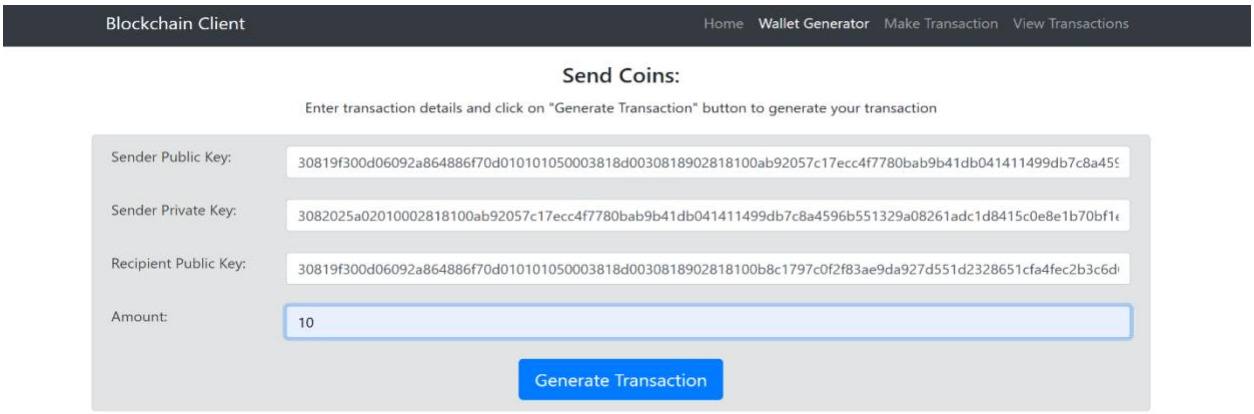

Fig. 8.1 Client Wallet:

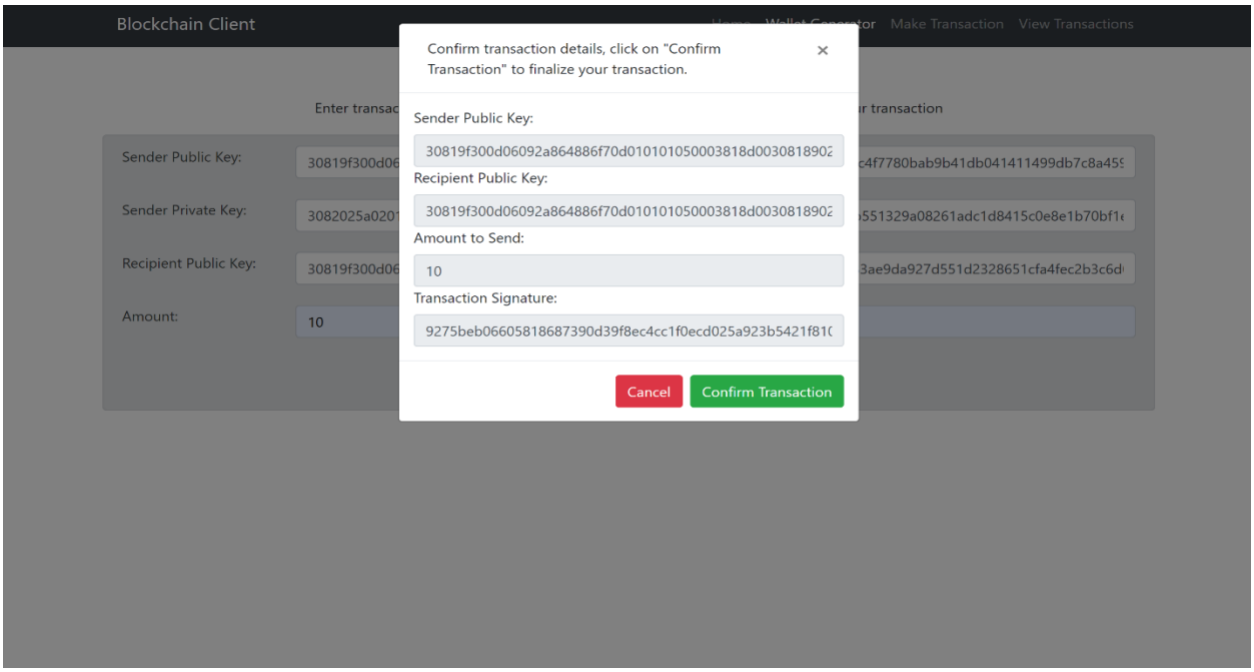

Fig. 8.2 Transaction Notification:

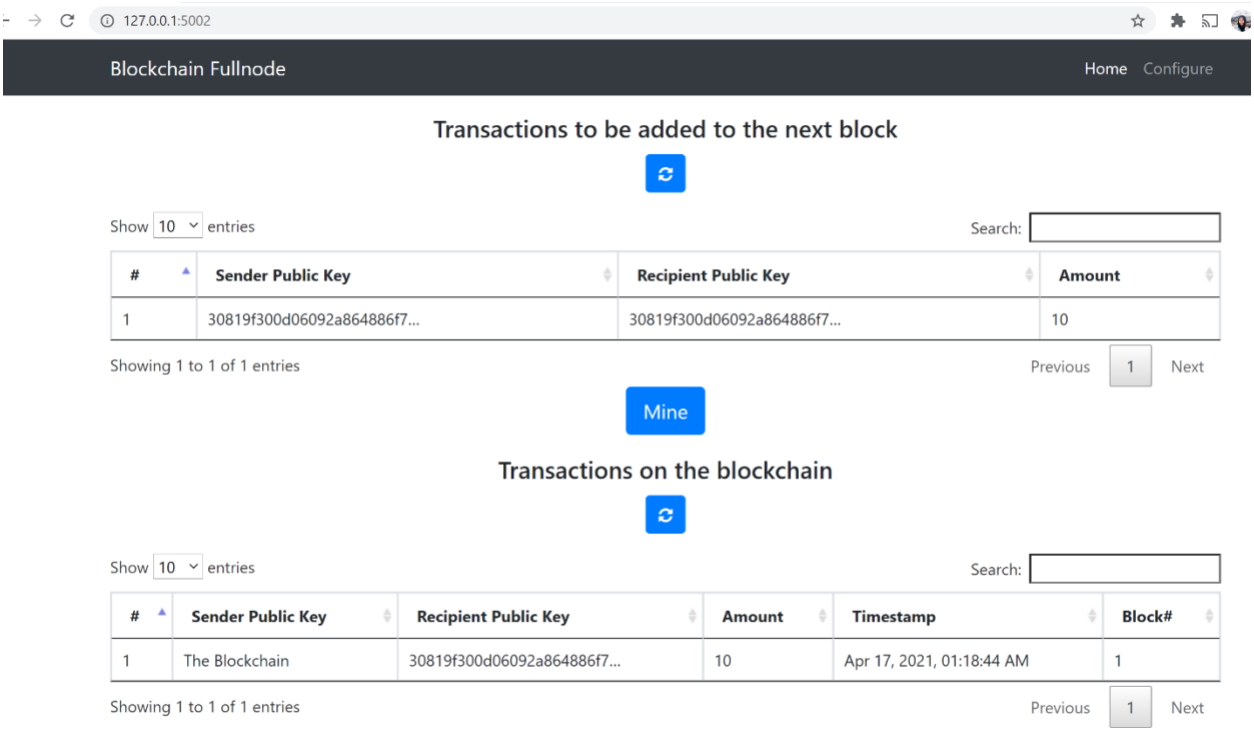

Fig. 8.3 Mining Performed:

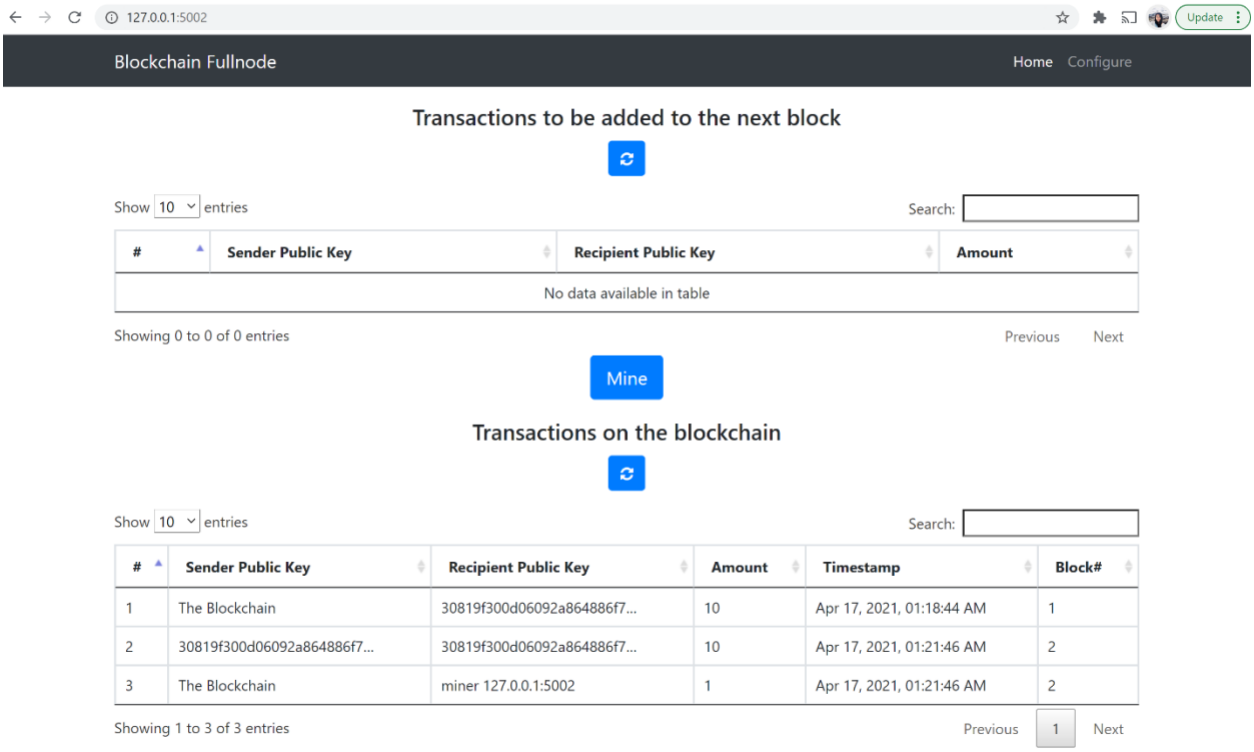

Fig. 8.4 Transaction added to Blocks of Records:

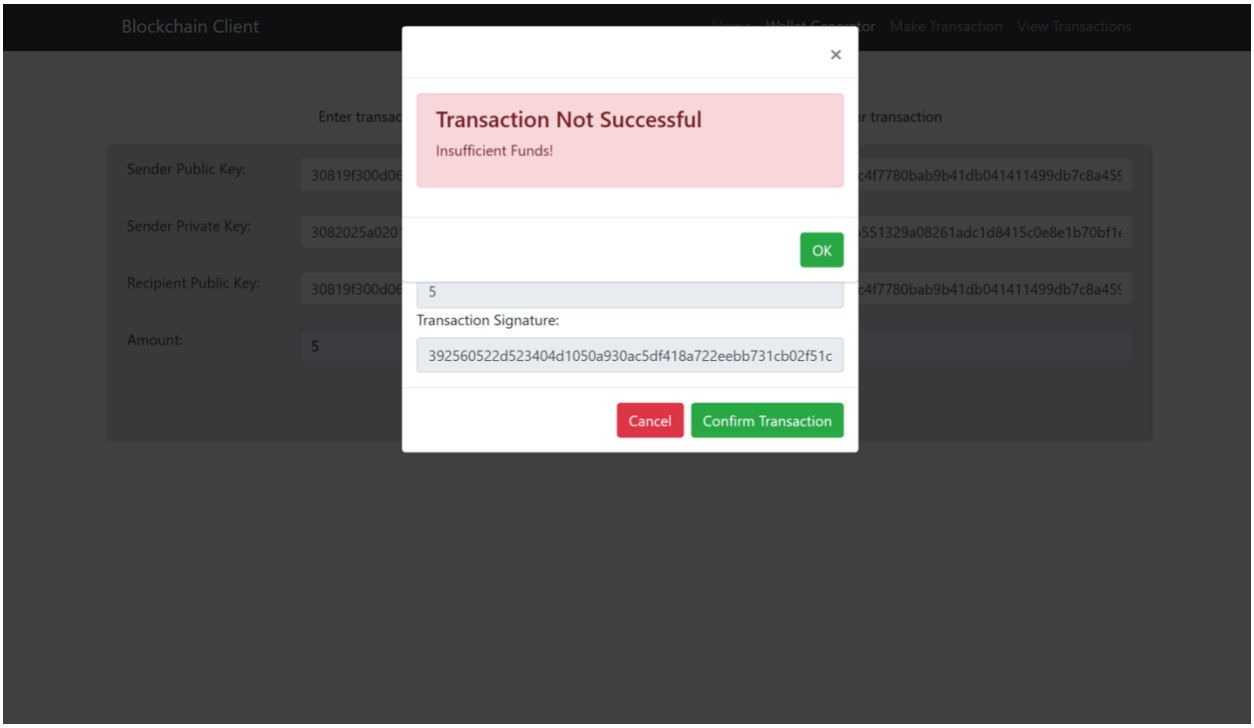

Fig. 8.5 Invalid Transaction alert:

TIMELINE TABLES

Timeline Tables

The following tables gives the project plan for Phase 1, 2 & 3 of our Project:

ACTIVITY	EFFECT IN PERSON MONTHS (2019)	DELIVERABLE
PHASE 1 DESIGNING BLOCKCHAIN	AUGUST - SEPTEMBER	Designing Blockchain
	OCTOBER	Implementing Blockchain
	NOVEMBER	Resolving Errors and Testing

ACTIVITY	EFFECT IN PERSON MONTHS (2020)	DELIVERABLE
PHASE 2 DESIGNING AI and INTERGRATION	JUNE	Creation of Dataset
	JULY	Training AI Model
	AUGUST - SEPTEMBER	Integrating AI with Blockchain
	OCTOBER - NOVEMBER	Adding AI based Mining

ACTIVITY	EFFECT IN PERSON MONTHS (2021)	DELIVERABLE
PHASE 3 FINAL TESTING and PAPER PRESENTATION	JANUARY - MARCH	Improving AI Model and Testing
	APRIL - MAY	Presentation of Paper on Project Application

FUTURE SCOPE

Future Scope

The project requires more refinement in terms of training the AI model against the designed blockchain in order to make the model much more defined and accurate. The other scope of this project can be migrating the entire project over mobile application for easy use and better portability.

For achieving these two task, we need to first make numerus transaction in order to create a better dataset on which we can train our AI model. A much better and refined dataset will give our AI model the knowledge of real time transactions and based on that data we can specify miner with much accurate credit scores.

In order to migrate onto a mobile application require proper understanding of how to design mobile application using various tools and how to design a proper environment for Blockchain and AI model to work efficiently. This could be very helpful in future for all the users as it will give the liberty of making transaction using their cellular devices.

CONCLUSION

Conclusion

Blockchain is one of the most developing and innovative technology which is expanding its horizon just not in the field of cryptocurrency but also in every field like voting system, banking sector, energy sector and many more. Blockchain provided the power back to the user instead of any anonymous central party. The decentralised ideology has changed the way users used to interact with the internet and this made Blockchain a key part of web 3.0 revolution. In this literature survey we introduced Basic Blockchain framework, its key features, some important terminologies , what is Cryptocurrency, Hashing and Hash functions, Mining, Miners, Proof of work v/s proof of stake, Mining pools and other fundamentals of Blockchain Technology and Cryptocurrency. We also discussed about the numerous advantages and disadvantages about the revolutionary technology. With above discussing and knowledge, advancement and development of the business and tech industries looks very promising because of Blockchain Technology. Apart from industries, general users will also be benefited by advanced blockchain technology due to the decentralised nature of the technology.

REFERENCE

Reference

1. http://www.caict.ac.cn/english/yjcg/bps/201901/P020190131402018699770.pdf
2. https://www.slideshare.net/bhargavamin1/whitepaper-on-new- research-on-hashin
3. https://bitcoin.org/bitcoin.pdf
4. https://www.quora.com/What-is-SHA-256
5. https://intellipaat.com/blog/tutorial/blockchain-tutorial/what-is-bitcoin-mining/
6. https://www.investopedia.com/terms/m/mining-pool.asp
7. https://bitcoin.stackexchange.com/questions/11471/what-are-the-advantages-and-disadvantages-of-pooled-mining
8. Blockchain Exhumed by Dr.DhirenPatel, Mr. JayBothra, Mr. Vasudev Patel
9. Securing Images with Fingerprint Data using Steganography and Blockchain by S. Pramothini, Y.V.V.S. Sai Pavan, N. Harini
10. https://blockgeeks.com/guides/hypothetical-attacks-on-cryptocurrencies/
11. Bitcoin and Cryptocurrency Technologies by Arvind Narayanan, Joseph Bonneau, Edward Felten, Andrew Miller, Steven Goldfeder
12. https://blockchainlab.com/pdf/Hyperledger%20Whitepaper.pdf
13. https://github.com/ethereum/wiki/wiki/White-Paper#ethereum
14. https://ethereum.org/wallets/

15. Blockchain in Depth by Saransh Kotha, Pearl Patel
16. https://consensys.net/blog/news/90-ethereum-apps-you-can-use-right-now/