A PROJECT REPORT ON

A Blockchain based cryptocurrency and development of an e-wallet

SUBMITTED TO THE SAVITRIBAI PHULE PUNE UNIVERSITY,
PUNE IN THE FULFILLMENT OF THE REQUIREMENTS FOR THE
AWARD OF THE DEGREE
OF

BACHELOR OF ENGINEERING (COMPUTER ENGINEERING)

SUBMITTED BY

Pranav Waikar	Exam No.: B150574350
Pratik Deshmukh	Exam No.: B150574336
Rohan Patel	Exam No.: B150574346
Aditi Kulkarni	Exam No.: B150574264
Sudam Pawar	Project Guide

DEPARTMENT OF COMPUTER ENGINEERING
STES'S SINHGAD INSTITUTE OF TECHNOLOGY AND SCIENCE
49/1, WESTERLY BYPASS ROAD, OPP. MUMBAI BENGALURU,
NARHE, PUNE, 411041

SAVITRIBAI PHULE PUNE UNIVERSITY
2018 -2019

Sinhgad Institutes

CERTIFICATE

This is to certify that the project report entitles

"A Blockchain based cryptocurrency and development of an e-wallet"

submitted by

Pranav Waikar	Exam No.: B150574350
Partik Deshmukh	Exam No.: B150574350
Rohan Patel	Exam No.: B150574350
Aditi Kulkarni	Exam No.: B150574350

are bonafide students of this institute and the work has been carried out by him/her under the supervision of Prof. S.G.Pawar and it is approved for the partial fulfillment of the requirement of Savitribai Phule Pune University, for the award of the degree of Bachelor of Engineering (Computer Engineering).

(Prof. S.G.Pawar)	**(Prof. G.S.Navle)**
Guide	Head
Department of Computer Engineering	Department of Computer Engineering

(Dr. R.S. Prasad)

Principal

Sinhgad Institute of Technology and Science, Narhe

ACKNOWLEDGEMENT

We express our gratitude to our guide Prof. S.G.Pawar for his competent guidance and timely inspiration. It is our good fortune to complete our project under his able competent guidance. This valuable guidance, suggestions, helpful constructive criticism, helped us keep interest in the problem during the course of presenting this project successfully.

We would like to thank our Project Coordinator Prof. S. M. Chitalkar and all the Teaching, Non-Teaching staff of our department.

We are very much thankful to Prof. G.S.Navle, Head, Department of Computer Engineering and also Dr. R. S. Prasad, Principal, Sinhgad Institute of Technology and Science, Narhe for providing all necessary facilities and guidance.

We thank to those who have directly or indirectly helped us to complete project report successfully.

Pranav waikar (B150574350)
Pratik Deshmukh (B150574350)
Date: Rohan Patel (B150574350)
Place: Pune Aditi Kulkarni (B150574350)

ABSTRACT

The regular currency has grown to reveal many drawbacks such as unavailability; it's proneness to be stolen and the fact that it is regulated strictly by an authority. Cryptocurrencies bypass most of our regular currency's drawbacks. Cryptocurrencies have emerged as a boastful financial system. They depend upon secure distributed ledger data structure. Mining plays an important part in this system.

Mining helps add records of all past transactions to the ledger known as blockchain, which in turn allows users to have a currency with secure, robust consensus for every transaction that occurs in that block. Cryptocurrencies lack a central authority since they are designed as a peer-to-peer system. And every transaction has a record of it stored on every block thus eliminating any misuse.

Basically, cryptocurrency is a decentralized ledger which maintains a growing tamper-proof data structure blocks which hold batches of individual transactions. The verified blocks are then added to the chain in a linear and chronological order. This forms a blockchain which is the core part of our cryptocurrency.

Cryptocurrencies are the need of the future and they are helping shape the future of banking, financial institutions and the advent of Internet of Things.

Keywords: - Blockchain, cryptocurrency, distributed ledger, wallets.

Contents

List of Abbreviations

POW	Proof-of-Work
POA	Proof-of-Authority
POS	Proof-of-Stake
SHA	Secure Hashing Algorithm
ECC	Elliptical Curve Cryptography
SDLC	Software Development Life Cycle
HTML	Hyper Text Markup Language
CSS	Cascading Style Sheet
UUID	Universally Unique Identifier
KMS	Key Management Services

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Background

The blockchain is a transaction database which has information about every transaction ever executed in the past and works on the Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on the network to edit the ledger in a secured way which is shared over a distributed network of the computers. For making any amount of changes to the block of data, all the nodes present in the network run algorithms to evaluate,verify and match the transaction information with its history. If the majority of nodes agree in favour of the transaction, it is approved and a new block gets added to the existing chain. The individual blocks are identified by a hash which is generated using a secure hash algorithm(SHA-256) cryptographic hash algorithm on the header of the block. Every block contains a hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called Genesis block.

The first block 0 created in 2009 is referred as Genesis block in Blockchain. It is encoded within bitcoin client software and can't be tampered. All the node always knows the hash and structure of genesis block which is secure root.

A block contains three major parts: One being the data of the block, the second being the hash of the said block and the last being the hash of the previous block.

The term private blockchain (permissioned ledger) refers to Blockchain that requires authentication of participant identities and authorization of participant's permission-level of access on the Blockchain. This writing will use Private Blockchain to refer to Permissioned Ledger as well. The term public blockchain (permissionless ledger) refers to Blockchain that does not require approval or authorization for access.

Mining validates transactions and adds them to this public ledger. When a new transaction takes place, the miner checks if the currency belongs to the payer, or if the payer is trying to double spend. A malicious user may create multiple nodes and try to validate an invalid transaction.

To prevent this, miners are required to solve a resource-intensive task. Resource intensiveness makes it expensive for a malicious user to create enough false identities to outnumber benign users and validate an invalid transaction. The resource-intensive task can be any of the following: Proof of Work, Proof of Stake, or Proof of Retrievability.

1.2 Objective

The main objective is as follows:

- To study the current block chain systems.
- To create a better cryptocurrency system.

1.3 Relevance

The blockchain is a newly emerging area of research. This report tells all about how the blockchain system operates in the real world and how the system can get attacked and some solutions to those problems. The blockchain has the potential to overthrow all the government, management middlemen for transactions.

The technology is now used for elections in the Sierra Leone 2018. The election was successful. The data was completely secure and no one was able to tamper with the results.It was very successful in terms of security but not in privacy to be maintained in the election. The blockchain has unique ability to solve the double spending problem. The system can help to solve property and asset transfer as well as a tracking system. This system will not only give the verifiable result but also it will be fast cheap.

1.4 Organization of report

The further chapters of the report are structured as:

Chapter 2: Literature survey, which gives an overview of existing methodologies used in the concerned domain.

Chapter 3: Problem definition, which depicts the inferences from the Literature review that have been moulded to form a statement that can be used to address various problems related to the topic.

Chapter 4: System Requirement Specification, which entails the software development model, reasons to choose the stated model along with functional and non-functional requirements of the project.

Chapter 5: Design phase, which represents the proposed architecture with different UML diagrams which can further be used to describe the system.

Chapter 6: Planning phase, represents phase of planning every move for designing system. The design model is taken into consideration. Cost and risk management is also part of this phase.

Chapter 7: Implementation, explains the details about the construction of the project like Algorithms, Software used, Programming languages utilized, platforms, tools etc.

Chapter 8: Testing, reveals all the relevant testing procedures to be performed, their results and related outcomes along with test cases, technical reviews, testing plans, etc.

Chapter 9: Result and Discussion, entails the results and findings of the project in an analytical format.

Chapter 10: Conclusion, which was derived as a result of the implementation of project.

1.5 Summary

- The blockchain is decentralized distributed ledger technology. It was used in Bitcoin for the first time.
- The cryptographic security, public ownership and digital incentives are the main features of blockchain.
- There are various types of blockchain and various consensus protocols to regulate the blockchain.

Chapter 2

Literature Review

2.1 Introduction

The blockchain is a distributed and decentralized ledger that stores data as transactions and that is publicly shared across all the nodes of its network[1]. Now let see what is ledger, Ledger is a record that stores all the transaction of an organization. Ledger is distributed in the network. Each copy of the record is stored in this transaction book.

Blockchain technology backs up Bitcoin and other cryptocurrencies to this day, but there's been a recent groundswell of interest from a variety of industries in making distributed ledger technology work, especially in business. Here's a primer on what blockchain technology is, how it works, and where it is showing the most promise in business.

By design, a blockchain is resistant to modification of the data. It is "an open, distributed ledger that can record transactions between two parties efficiently and in a verifiable and permanent way". For use as a distributed ledger, a blockchain is typically managed by a peer-to-peer network collectively adhering to a protocol for inter-node communication and validating

new blocks. Once recorded, the data in any given block cannot be altered retroactively without alteration of all subsequent blocks, which requires a consensus of the network majority. Although blockchain records are not unalterable, blockchains may be considered secure by design and exemplify a distributed computing system with high Byzantine fault tolerance. Decentralized consensus has therefore been claimed with a blockchain.

Blockchain was invented by Satoshi Nakamoto in 2008 to serve as the public transaction ledger of the cryptocurrency Bitcoin. The invention of the blockchain for Bitcoin made it the first digital currency to solve the double-spending problem without the need for a trusted authority or central server.[2] The Bitcoin design has inspired other applications, and blockchains which are readable by the public are widely used by cryptocurrencies. Private Blockchains have been proposed for business use. Some marketing of blockchains has been called "snake oil". Blockchain has the following use cases:

- Cryptocurrency: Cryptocurrency is the digital medium of exchange. a digital currency in which encryption techniques are used to regulate the generation of units of currency and verify the transfer of funds, operating independently of a central bank.

- Wallets: It is an object that stores the public key and private key of an individual transaction. The public key is the address of the wallet. It helps to sign the transaction.

- Mining: There is the concept of miners in the blockchain. Miners are the vendors who verify the signature. It takes the unconfirmed transaction to verify it and check it whether it is legal or not.

- Bitcoin: Bitcoin is the first decentralized cryptocurrency which is es-

tablished in 2009. It is a digital and global money system currency. It allows people to send or receive money across the internet, even to someone they don't know or don't trust. Money can be exchanged without being linked to a real identity. The mathematical field of cryptography is the basis for Bitcoin's security.

2.2 History

The popular discussion on mainstream media recently is often to separate blockchain technology from Bitcoin. Influential individuals in a financial domain like Jamie Dimon as well as institutions like Goldman Sachs are saying that blockchain is here to stay, maybe not so much the coins and tokens. What does this separation really mean? I will try to capture the key concepts and events that have transpired in the past decade in this fast moving space.

2.2.1 Blockchain 1.0, Grandpa Bitcoin

Wei Dai's was one of the first noted researchers to introduce the proposal of b-money that introduced the idea of creating money through solving computational puzzles and decentralized consensus, but the proposal itself was low in implementation details. In 2005, Hal Finney introduced a concept of "reusable proofs of work", a system that used ideas from b-money together with Adam Back's computationally difficult Hashcash puzzles to create a concept for a cryptocurrency, but was also run on centralized trusted back-end systems.Blockchain finally took root with the Bitcoin whitepaper written by visionary Satoshi Nakamoto in 2009. The whitepaper outlines the details required for a protocol that establishes a decentralized currency, operate it on

a trustless network that is not controlled by individuals with a bias towards a particular country, state or governing body.

2.2.2 Blockchain 2.0, Child prodigy Ethereum

Enter Vitalik Buterin, one of the writers for Bitcoin Magazine that tried to popularize the technology in early 2012. He witnessed first-hand the problems in the Bitcoin implementation like wasteful mining hardware, the centralized mining community, and lack of network scalability. In 2013, the then 19-year-old Vitalik described his vision for Ethereum by extending the concept of Bitcoin beyond just currency. He proposed a platform where developer community and entrepreneurs to build a distributed application (Dapps) for the Blockchain network. He referred to this concept of trust beyond just currency as 'smart contracts' or even blockchain-based "decentralized autonomous organizations" (DAOs).

2.2.3 Blockchain 3.0, The Killers

The newer technologies obviously boast about the ability to improve on capabilities of Bitcoin and Ethereum networks while overcoming their limitations witnessed. We should see them deliver on their vision and differentiated ability least with regards to transaction time and scale in 2018. It would be hard for me to do justice to each of the competitors in this piece

2.3 History of working

Blockchain technology is probably the best invention since the internet itself. It allows value exchange without the need for trust or a central authority. Imagine you and I bet Rs50 on tomorrow's weather in San Francisco. I

bet it will be sunny, you that it will rain. Today we have three options to manage this transaction:

- We can trust each other. Rainy or sunny, the loser will give Rs50 to the winner. If we are friends, this could be a good way of managing it. However, friends or strangers, one can easily not pay the other.

- We can turn the bet into a contract. With a contract in place, both parties will be more prone to pay. However, should either of the two decide not to pay, the winner will have to pay additional money to cover legal expenses and the court case might take a long time. Especially for a small amount of cash, this doesn't seem like the optimal way to manage the transaction.

- We can involve a neutral third party. Each of us gives Rs50 to a third party, who will give the total amount to the winner. But hey, she could also run away with all our money. So we end up with one of the first two options: trust or contract.

- Neither trust nor contract is an optimal solution: We can't trust strangers, and enforcing a contract requires time and money. The blockchain technology is interesting because it offers us a third option which is secure, quick, and cheap.

- Blockchain allows us to write a few lines of code, a program running on the blockchain, to which both of us send Rs50. This program will keep the Rs100 safe and check tomorrow's weather automatically on several data sources. Sunny or rainy, it will automatically transfer the whole amount to the winner. Each party can check the contract logic, and once it's running on the blockchain it can't be changed or stopped.

This may be too much effort for a Rs50 bet, but imagine selling a house or a company.

- This piece explains how the blockchain works without discussing the technical details in depth, but by digging just enough to give you a general idea of the underlying logic and mechanisms.

The Basics of Bitcoin:

The most known and discussed application of the blockchain technology is Bitcoin, a digital currency that can be used to exchange products and services, just like the U.S. dollar, euro, Chinese yuan, and other national currencies. Let's use this first application of the blockchain technology to learn how it works. "Bitcoin gives us, for the first time, a way for one Internet user to transfer a unique piece of digital property to another Internet user, such that the transfer is guaranteed to be safe and secure, everyone knows that the transfer has taken place, and nobody can challenge the legitimacy of the transfer.

The consequences of this breakthrough are hard to overstate." One bitcoin is a single unit of the Bitcoin (BTC) digital currency. Just like a dollar, a bitcoin has no value by itself; it has value only because we agree to trade goods and services to bring more of the currency under our control, and we believe others will do the same. To keep track of the amount of bitcoin each of us owns, the blockchain uses a ledger, a digital file that tracks all bitcoin transactions.

The ledger file is not stored in a central entity server, like a bank, or in a single data center. It is distributed across the world via a network of private computers that are both storing data and executing computations. Each of these computers represents a "node" of the blockchain network and has a copy of the ledger file.

If David wants to send bitcoins to Sandra, he broadcasts a message to the network that says the amount of bitcoin in his account should go down by 5 BTC, and the amount in Sandra's account should increase by the same quantity. Each node in the network will receive the message and apply the requested transaction to its copy of the ledger, updating the account balances.

The fact that the ledger is maintained by a group of connected computers rather than by a centralized entity like a bank has several implications:

- In our bank system we only know our own transactions and account balances; on the blockchain, everyone can see everyone else's transactions.
- While you can generally trust your bank, the bitcoin network is distributed and if something goes wrong there is no help desk to call or anyone to sue.
- The blockchain system is designed in such a way that no trust is needed; security and reliability are obtained via special mathematical functions and code.

We can define the blockchain as a system that allows a group of connected computers to maintain a single updated and secure ledger. In order to perform transactions on the blockchain, you need a wallet, a program that allows you to store and exchange your bitcoins. Since only you should be able to spend your bitcoins, each wallet is protected by a special cryptographic method that uses a unique pair of distinct but connected keys: a private and a public key.

If a message is encrypted with a specific public key, only the owner of the paired private key can decrypt and read the message. The reverse is also true: If you encrypt a message with your private key, only the paired

public key can decrypt it. When David wants to send bitcoins, he needs to broadcast a message encrypted with the private key of his wallet. As David is the only one who knows the private key necessary to unlock his wallet, he is the only one who can spend his bitcoins. Each node in the network can cross-check that the transaction request is coming from David by decrypting the message with the public key of his wallet.

To send bitcoin you need to prove that you own the private key of a specific wallet as you need the key to encrypt your transaction request message. Since you broadcast the message only after it has been encrypted, you never have to reveal your private key.

Tracking Your Wallet Balance:

Each node in the blockchain is keeping a copy of the ledger. So, how does a node know your account balance? The blockchain system doesn't keep track of account balances at all; it only records each and every transaction that is verified and approved. The ledger, in fact, does not keep track of balances, it only keeps track of every transaction broadcasted within the bitcoin network . To determine your wallet balance, you need to analyze and verify all the transactions that ever took place on the whole network connected to your wallet.

This "balance" verification is performed based on links to previous transactions. In order to send 10 bitcoins to John, Mary has to generate a transaction request that includes links to previous incoming transactions that add up to at least 10 bitcoins. These links are called "inputs." Nodes in the network verify the amount and ensure that these inputs haven't been spent yet. In fact, each time you reference inputs in a transaction, they are deemed invalid for any future transaction. This is all performed automatically in Mary's wallet and double-checked by the bitcoin network nodes; she only

sends a 10 BTC transaction to John's wallet using his public key.

So, how can the system trust that input transactions are valid? It checks all the previous transactions correlated to the wallet you use to send bitcoins via the input references. To speed up the verification process, a special record of unspent transactions is kept by the network nodes. Thanks to this security check, it is not possible to double-spend bitcoins.

Owning bitcoins means that there are transactions written in the ledger that point to your wallet address and haven't been used as inputs yet. All the code to perform transactions on the bitcoin network is open source; this means that anyone with a laptop and an internet connection can operate transactions. However, should there be a mistake in the code used to broadcast a transaction request message, the associated bitcoins will be permanently lost.

Remember that since the network is distributed, there is no customer support to call nor anyone who could help you restore a lost transaction or forgotten wallet password. For this reason, if you are interested in transacting on the bitcoin network, it's a good idea to use the open source and official version of bitcoin wallet software (such as Bitcoin Core) and to store your wallet's password or private key in a very safe repository. If this happens, there will be disagreement among the network nodes regarding the order of transactions each of them received.

So the blockchain system has been designed to use node agreement to order transactions and prevent the fraud described above. The bitcoin network orders transactions by grouping them into blocks; each block contains a definite number of transactions and a link to the previous block. This is what puts one block after the other in time. Blocks are therefore organized into a time-related chain that gives the name to the whole system.

Mining Bitcoin:

In order to send bitcoins, you need to reference an incoming transaction to your own wallet. This applies to every single transaction across the network. So, where do bitcoins come from in the first place? As a way to balance the deflationary nature of bitcoin due to software errors and wallet password loss, a reward is given to those who solve the mathematical problem of each block. The activity of running the bitcoin blockchain software in order to obtain these bitcoin rewards is called "mining" and it's very much like mining gold. Rewards are the main incentive for private people to operate the nodes, thus providing the necessary computing power to process transactions and stabilize the blockchain network.

Because it takes a long time for a typical computer to solve a block (about one year on average), nodes band together in groups that divide up the number of guesses to solve the next block.Working as a group speeds up the process of guessing the right number and getting the reward, which is then shared among group members.These groups are called mining pools.[3]

Some of these mining pools are very large and represent more than 20 percent of the total network computing power. This has clear implications for network security, as seen in the double-spend attack example above. Even if one of these pools could potentially gain 50 percent of the network computing power, the further back along the chain a block goes, the more secure the transactions within it become. However, some of these mining pools with substantial computing power have decided to limit their members in order to safeguard overall network security.

Since the overall network computing power is likely to increase over time due to technological innovation and the increasing number of nodes, the blockchain system recalibrates the mathematical difficulty of solving the next

block to target 10 minutes on average for the entire network. This ensures the network's stability and overall security. Moreover, every four years the block reward is cut in half, so mining bitcoin (running the network) gets less interesting over time.

To encourage nodes to keep operating, small reward fees can be attached to each transaction; these rewards are collected by the node that successfully includes such transactions in a block and solves its mathematical problem. Due to this mechanism, transactions associated with a higher reward are usually processed faster than those associated with a low reward. What this means is that, when sending a transaction, you can decide if you'd like to process it faster (more expensive) or cheaper (takes more time). Transaction fees in the bitcoin network are currently very small compared with what banks charge, and they're not associated with the transaction amount.

2.4 Layered architecture of blockchain

We always refer the Blockchain as "The Blockchain not Blockchain" because it's not the single technology that emerged from somewhere it is a collection of other algorithms and protocols that put together to form a single technology called The Blockchain. Most interesting part is when the first time Idea of The Blockchain is represented in its white paper given by Satoshi Nakamoto[4]. In this white paper, he never mentioned "The Blockchain" it was only mentioned as a keyword called "chain of blocks" in it.

He only referred to the technology of the Bitcoin. Later Large corporations starting understanding the power of technology behind the Bitcoin then it is been named as Blockchain. Satoshi Nakamoto never invented Blockchain but He is the first person who represented such idea of The Blockchain. The

technology that completes the blockchain is already in existence way before its main implementation started. The only thing that Satoshi Nakamoto did is put all those technical concepts in one box and gave birth to this technology which later named as Blockchain.

If we have to understand the concepts of the blockchain then we say it as 3 Layer model of a Software that completes blockchain and that's it if as these layers mainly define The Blockchain software architectural level.

2.5 Consensus protocols

The purpose of this protocol is to define the trust within the system. There are different parameters types of consensus protocol. Following are some important consensus protocol:

2.5.1 Proof Of Work (POW)

PoW mechanism uses the solution of puzzles to prove the believability of the data. The puzzle is usually a computationally hard but easily verifiable problem[4]. When a node creates a block, it must resolve a PoW puzzle. After the PoW puzzle is resolved, it will. be broadcasted to other nodes, so as to achieve the purpose of consensus, In various blockchain frameworks, the block structure may fluctuate in detail. Ordinarily, in Bitcoin, each piece contains PrevHash, nonce.

PoS component utilizes the confirmation of responsibility for demonstrating the believability of the information. For a piece or exchange, clients are required to pay a specific measure of digital currency. On the off chance that the square or exchange made can, in the long run, be approved, the digital currency will come back to the first hub as a reward. Else, it will be fined.

In the PoW, it needs a considerable measure of estimation, bringing about a misuse of processing power. Despite what might be expected, PoS component can enormously diminish the measure of calculation, in this manner expanding the throughput of the whole blockchain framework.

2.5.2 Proof Of Stake (POS)

Proof of stake (PoS) is a sort of calculation by which a digital money blockchain organize expects to accomplish appropriated accord. In PoS-based cryptographic forms of money, the maker of the following block is picked through different mixes of arbitrary choice and richness or age (i.e the stake).[5] Interestingly, the calculation of Proof of-work-based cryptographic forms of money, for example, bitcoin utilizes mining; that is, the understanding of computationally concentrated riddles to approve exchanges and make new blocks.

Proof-of-Stake (PoS) consensus protocol, first actualized by Peercoin, relies upon market forces rather than sheer handling energy to secure the system. The concept generally involves increasing the chance of a node's success in minting new digital tokens in proportion with the number of digital tokens already owned by the node. The method of reasoning is that the more computerized tokens a node possesses, the more personal stake the node will have in securing the system. To dispatch an attack, the attacker should sufficiently secure computerized tokens to succeed.

This outcomes in value climb for the token, making the attack financially unsustainable. Regardless of whether the attack was to succeed, the harm from attack will make a debasement of the tokens bringing about considerable monetary misfortune to the assailant. Compare Proof-of-Work, Proof-of-Stake has the upside of securing the system without utilizing handling power

as an obstruction of attack and brings down the hindrance of passage by removing favorable circumstances related to utilizing the specific hardware.3 On the other side, there is no punishment to miners for voting on every one of the chains when a fork emerges which can bring about the network not ready to achieve agreement (Nothing at Stake).

Proof-of-Stake is additionally presented to the sort of assaults unimaginable on Proof-of-Work outlines. For example, for Proof-of-Stake outline, it is conceivable to play out a long-term attack in which the longest fork can be supplanted by a chain recreated from the beginning block. This can't occur in Proof-of-Work as an attacker can just depend on sheer utilization of vitality with a specific end goal to subvert the longest fork. Proof-of-Stake is additionally once in a while actualized without anyone else as this will bring about a lasting preferred standpoint to the wealthiest partner.

2.5.3 Proof Of Authority (POA)

In PoA-based systems, transaction and blocks are approved by affirmed accounts, known as validators. Validators run programming enabling them to place exchanges in blocks. The procedure is mechanized and does not require validators to be always checking their PCs. It, be that as it may, requires keeping up the PC uncompromised. The term was popularised by Gavin Wood, fellow benefactor of Ethereum and Parity Technologies.

With PoA people procure the privilege to wind up validators, so there is a motivation to hold the position that they have picked up. By appending notoriety to personality. validators are boosted to maintain the exchange procedure, as they don't wish to have their characters joined to an adverse notoriety.[5] This is viewed as more strong than PoS, as: In PoS, while a stake between two parties might be even, it doesn't consider each gathering's

aggregate possessions. This implies incentive can be uneven.

In the meantime, PoW utilizes a colossal measure of figuring power, which, in itself brings down motivator. It is likewise defenseless against assault, as a potential assailant would just need 51% of the mining assets (hash rate) to control a system, despite the fact that this isn't anything but difficult to do. Then again, PoA just permits non-consecutive block acceptance from anyone validator, implying that the danger of genuine harm is limited. PoA is suited for private systems however not for open systems where trust ought to be distributed.

2.6 Cryptocurrency

A cryptocurrency (or cryptocurrency) is a digital asset designed to work as a medium of exchange that uses strong cryptography to secure financial transactions, control the creation of additional units, and verify the transfer of assets.[6] Cryptocurrencies are a kind of alternative currency and digital currency (of which virtual currency is a subset). Cryptocurrencies use decentralized control as opposed to centralized digital currency and central banking systems. The decentralized control of each cryptocurrency works through distributed ledger technology, typically a blockchain, that serves as a public financial transaction database.

Bitcoin, first released as open-source software in 2009, is generally considered the first decentralized cryptocurrency. Since the release of Bitcoin, over 4,000 altcoins (alternative variants of Bitcoin, or other cryptocurrencies) have been created.[6]

2.7 Wallets

It is an object that stores the public key and private key of an individual transaction. The public key is the address of the wallet. It helps with the transaction. basically, the wallet is a core object with three main components. We balance the cryptocurrency in the wallet. For doing the transaction we require a private key and public key. The private key is only for the sender and public key is used by the receiver. When we combine both the private key and public key then we got a signature which is used to decrypt the data which is sent by the sender.

1.Private key: It is for the first individual. Used to generate a signature

2.Public Key: It is for the Second individual. It contains the address of the wallet.

2.8 Litrature review table:

The table 2.1 specifies the literature review in terms of general idea, advantages and limitations of related papers.

Table 2.1: Literature Survey

ID	Title	General idea	Advantages and limitations
1	Blockchain and Cryptocurrencies: Model, Techniques, and Applications [2018]	A survey of current cryptocurrencies to understand blockchain and its different types.	Advantages:Provides different incentive models, ecosystem and applications of the blockchain.Explains blockchain in a layered architecture. Limitations:Does not provide any solid architecture for its stated application.
2	Blockchain: Future of Financial and Cyber Security[2016]	This paper explains the concept, characteristics, need for Blockchain and how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking.	Advantages:The decrease in device cost and increases computing power. Limitations: If any attack was done by an attacker then there will be a loss of all bitcoins, we can't recover it because the government is not involved in.

3	A Brief Survey of Cryptocurrency Systems[2017]	It evaluates the strengths, weaknesses, and possible threats to all major mining strategy. It outlines how Cryptocurrencies mine, where they have comparable performance and assurance, and where they have unique threats and strengths.	Advantages: Currently, major Cryptocurrencies use Proof of Work, Proof of Stake or a combination of the both for mining. A combination of the both is found to be effective. Typically memory intensive hash functions have been found to be faster mining algorithms. Limitations: A majority of hash algorithms are CPU-intensive and the others are memory intensive. While Proof of Work is resource intensive, Proof of Stake cannot act independently. Cryptocurrencies are still experimenting with their mining protocols and algorithms to optimize their performance. No full proof algorithm has been found yet.

4	Bitcoin: A Peer-to-Peer Electronic Cash System[2008]	A distributed peer to peer system working under blockchain framework.	Advantages:Cryptocurrency without any central authority and successful POW mechanism. Limitations: The cost of POW consensus protocol will keep increasing as more people join the network.
5	Trust Your Wallet : a New Online Wallet Architecture for Bitcoin [2017]	It introduces a wallet which is highly secured by Multiple signatures.	Advantages:The scalability of disaster recovery centre. Limitations: If we lost one of the key then we are not able to recover that key.
6	A survey on the security of blockchain systems [2017]	Detail survey of the security issues in current systems and existing solutions.	Advantages:A careful comparison between Bitcoin and ethereum.Also different aspects of system vulnerability. Limitations: Cryptocurrency will need more methods to achieve security and privacy.

2.9 Gap analysis

- There is a need of currency with proof-of-authority but without central point of failure.
- There is a scope for development of a generalized public blockchain API.
- A cryptocurrency with hybrid consensus protocol is needed which provides better security.
- A secure and high availability e-wallet for easy to facilitate transactions of the cryptocurrency developed using the above stated API.

2.10 Summary

- In this chapter, we have discussed six different papers and different algorithms used to secure the transaction A survey of current cryptocurrencies to understand blockchain its different types.
- It outlines how Cryptocurrencies to mine, where they have comparable performance and assurance, and where they have unique threats and strengths.
- It attempts to highlights role of Blockchain in shaping the future of banking. A distributed peer to peer system working under the blockchain framework.
- Performing gap analysis gives us idea where the current system can be improved.

Chapter 3

Problem Definition

3.1 Problem Statement

To create a de-centralized blockchain based cryptocurrency and an e-wallet to access currency.

3.2 Aim

1. Creating a cryptocurrency with proof-of-authority but without central point of failure.
2. Generalized public blockchain API.
3. A hybrid consensus protocol for blockchain.
4. A secure and high availability e-wallet for easy to facilitate transactions.

3.3 Objective

The objective of this project to create a de-centralized blockchain based cryptocurrency and an e-wallet to access currency. The project entails creating a generalized blockchain API which can later be used for further development in the blockchain field of applications. This blockchain API will be used to construct a cryptocurrency from scratch. Implement a new hashing function for the blockchain which will take data and create a fixed length output.

Implementing a highly secure and personal e-wallet system to access and control the said cryptocurrency. This e-wallet system will let the user control and transact the currency efficiently. It provides the user with full authority over the token currencies. The aim is also to make the currency secure, easy to access, fast and as cheap to avail as possible.

3.4 Feasibility

A distributed peer-to-peer transaction database has been created to form the base of our blockchain based cryptocurrency. It is very feasible to use the generalized blockchain API to create any other application with blockchain as its base.

Today's technology allows us to supplement the working of a blockchain based cryptocurrency. It uses cloud services as well as the internet to reach its goal. It can be used in many scenarios as the currency can be effectively used as a token currency, It can be used as chips like in casinos or as betting tokens.

The project uses Nodejs to implement the functionalities of the currency. Since Nodejs is asynchronous it faces no major issues in implementing its

functionality. Nodejs is asynchronous and is also used in Bitcoin which works perfectly without facing any major fatal issues.

It is really easy for miners to mine for the system. They can easily add themselves in the mining roster. A simple installation of the mining client enables anybody to mine the currency and verify transactions. It enables many miners to sustain a functioning business model. Since the scalability of this system is practically unlimited, it can expand as much as possible.

The network and space requirements of the system are negligible in today's world since the technology already exists for the system to work, the internet speed also is readily available. The cloud storage prices are also cheap so it becomes very feasible to make the system function effectively.

3.5 Scope

The scope of this project spans from creating a blockchain based cryptocurrency. To do this we have to create a hash function. A hash is a one-way function that takes any sized input data and produces a fixed length output. These hash computations should be quick and easy, but reversal should require brute algorithm.

Any change in the input should propagate through the entire output so that outputs for similar input have no predictable similarity. Mining is a brute-force algorithm and should be designed so that the number of blocks mined per day remains approximately constant in order to control the rate of introduction of new currencies, which are unlocked when a block is mined.

SHA 256 is a set of Secure Hash Functions that has six algorithms, which produce digests 256 bits. SHA 256 satisfies the requirement of unidirectional hashes where any change in the input, however insignificant, leads to a com-

pletely different hash.

The user will be given access to an e-wallet with a generated address, which will act as a public key. The wallet will then also create a private key, which can be used to sign the transaction, thus proving ownership. The payer sends money to the payee's address and signs it using the payer's private key.

3.6 Summary

In this chapter, we have discussed the problem statement, aim, objectives, feasibility and scope for this system. These definitions give a clear understanding of what the system is and what are the expectations of the system.

Chapter 4

System requirement specification

4.1 SDLC model

We are using Incremental model for SDLC. Incremental Model is a process of software development where requirements are broken down into multiple standalone modules of the software development cycle.

1. Requirements of the system are clearly understood.
2. The team is not well skilled or trained in technology.
3. Model is more suitable for web application based products.
4. The development environment is stable.

Incremental Model helps to deliver the sequence of releases on an incremental basis which speeds up the progress of development of each function. Each developed functionality gets delivered to the end users one after another. The first increment is always a base feature and other features added

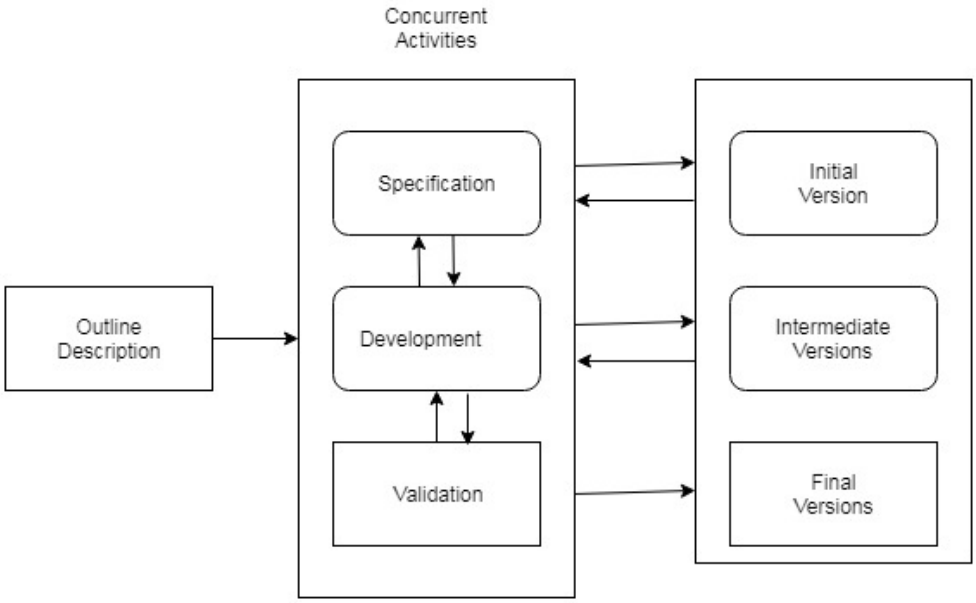


Figure 4.1: Incremental model

in next increments with new releases in case client requests to add any new feature after reviewing of the first release. This process is carried out till the complete product developed.

4.2 Functional requirements

- User registration: The user should be able to create an account after submitting valid information. The information should be saved in the database.
- User login: The user should be able to log in into his account using the same information provided at registration. The login should be successful if the provided values match with the registered values.
- Profile updating: The user should be able to update its email id and

password.

- Transaction capability: Users should be able to carry out transactions successfully.
- Key management: Wallet should deal with private keys complexity automatically.
- Balance request: The user should be able to request its balance at any time.
- Key generation: The public and private keys generation availability.

4.3 Non-functional requirements

- Performance: The system should provide fluent performance. It should be able to handle multiple transactions and still maintain the system.
- Safety: All care must be taken in order to ensure that every access to information is within the bounds of the law. No illegal methods are used to manipulate the data.
- Scalability: The system should be able to scale up to any number of nodes without any problem. It should be able to manage an economy withstanding the change of scalability.
- Accuracy: The system needs to be accurate and should provide an accurate balance to every user.
- Privacy: The system should be able to provide privacy with encryption distributed blockchain network.

- Availability: The system should be available to the client. It means that the system should always provide a response to the client.
- Reliability: The system should always produce the same results upon providing the same input operations consistently.
- Robustness: The system should be robust in the case of user unintentionally or deliberately perform an unexpected operation
- Integrity: The system should have strong integrity constraints as they will help the system to structure and handle the data in a more appropriate manner.
- Usability: The degree of usability of the system should be high. Any class of user should be able to use the system.
- Adaptiveness: The system should be able to adapt to the different system and device and operational environments.

4.4 User interface

- User registration: The user initiates the processes of registering with the system. The user enters essential data gets login credentials for the wallet.
- User login: The user logs in with login credentials into the wallet.
- Balance request: user requests his current balance from his wallet.
- Send coin: The user is able to initiate a transaction to send coins.
- View public key: The user can view his public address, using which currency can be received.

4.5 Hardware interface

- Processor: Intel core 2 duo or above
- Speed: 2.4GHZ
- RAM: 4GB or above
- Hard disk: 20GB or above

4.6 Software interface

1. Platform:
    - Operating system: Windows 7 or above, Linux, MAC.
2. Front-end:
    - HTML
    - CSS
    - Javascript
3. Backend:
    - Node.js: Node.js is an open source server environment. It is free and runs on various platforms. Node.js uses JavaScript on the server.
    - MongoDB: MongoDB open-source cross-platform document-oriented database program. It is a NoSQL database program uses JSON-like documents with the scheme.

4.7 Communication interface

1. The user will access the wallet as a web application..
2. The blockchain nodes will communicate with each other using web sockets.

4.8 Summary

- In this chapter, we have discussed system requirements,functional, non-functional requirements, backend and user interface.
- We are using Incremental model for SDLC. Functional requirements for user registration, user login, profile updating, transaction capability, key management, balance request, key generation.
- Non-functional requirements for performance, safety and scalability.

Chapter 5

Design phase

5.1 Proposed System Architecture

As shown in figure 5.1, suppose party A wants to transfer some currency over to party B. Then by the wallet interaction, party A can start the transaction over to party B. The transaction is represented online as a block.

The block is then broadcasted to every party in the network. The network as a whole will approve the transaction to be valid or invalid by using the distributed ledger. Then by some consensus protocol block will get added to the distributed ledger. In this way, the transaction for transferring money from A to B is completed successfully.

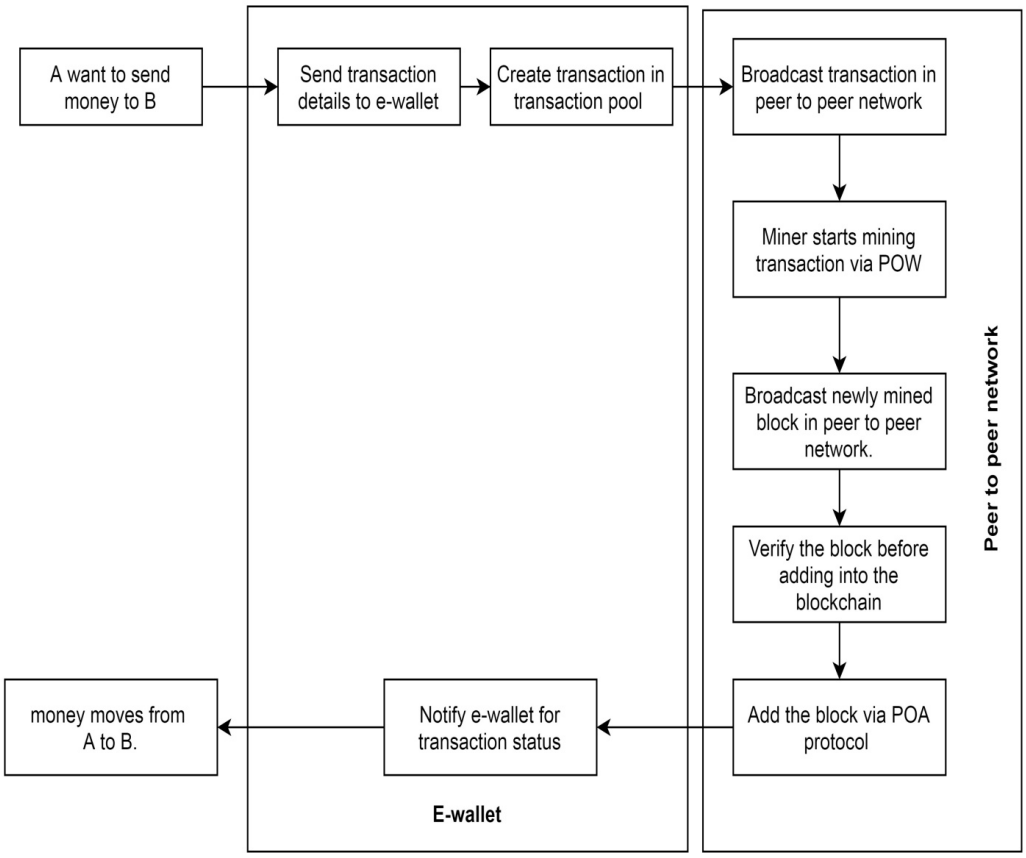


Figure 5.1: Proposed System Architecture

5.2 Use case diagram

A use case diagram represents a use case and a user's interaction with the system. A use case diagram depicts the different types of users a system can have and different ways in which these users can interact with the system.

Figure 5.2 shows us the use case of our system. The user has to interact with the wallet for accessing cryptocurrency. The wallet enables users to launch transactions. The wallet admin manages the wallet functionalities as well as the users for the system. The miner user interacts with cryptocurrency model for verification and validation of any transaction.

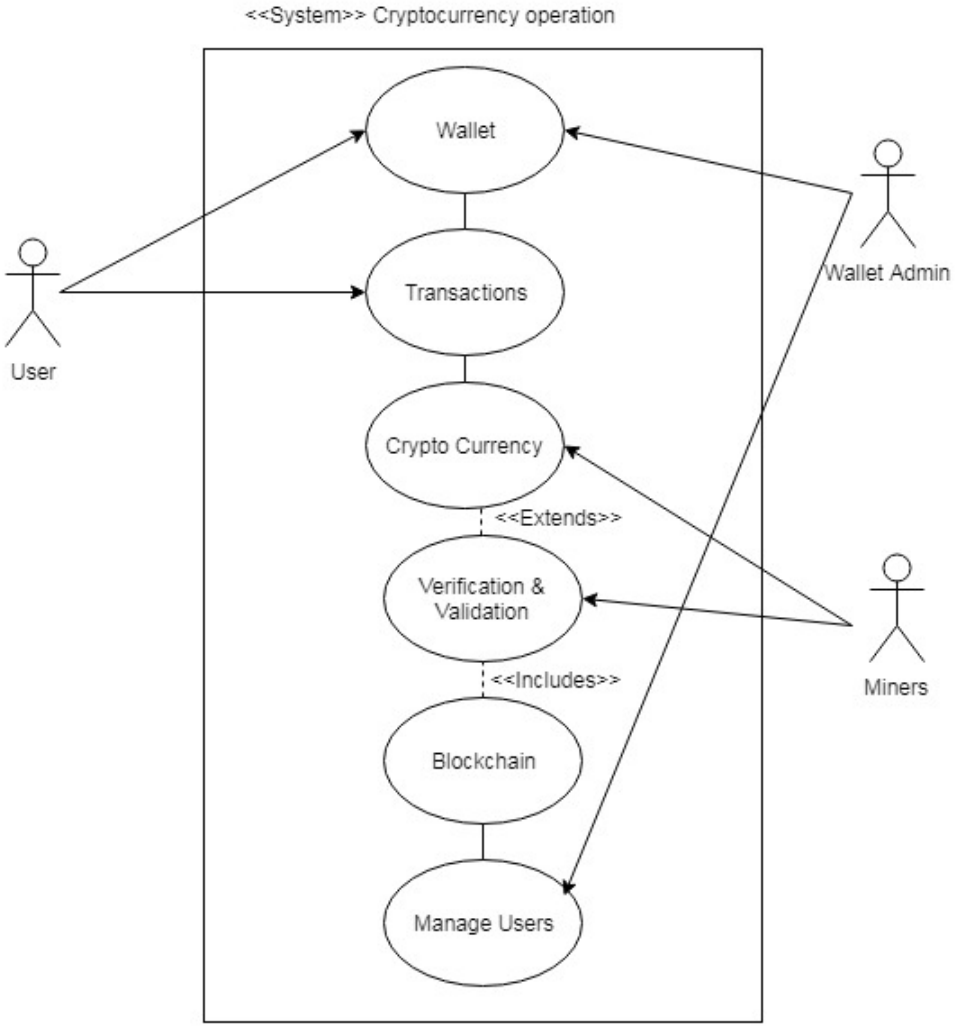


Figure 5.2: Use Case Diagram

5.3 Activity Diagram

Fig 5.3 shows an activity diagram of our system. The Unified Modeling Language uses the Activity diagram for modeling both the computational and organizational processes. Activity diagrams describe the dynamic aspects of

a system. Activity diagrams show the overall flow of control.

In this diagram, it is shown that user visits the wallet, then registers and performs the login activity. After the login user can start transactions. If transactions are successful then transaction details are shown in a receipt and balance is also displayed. If the transaction fails then failure receipt and errors are displayed to the user.

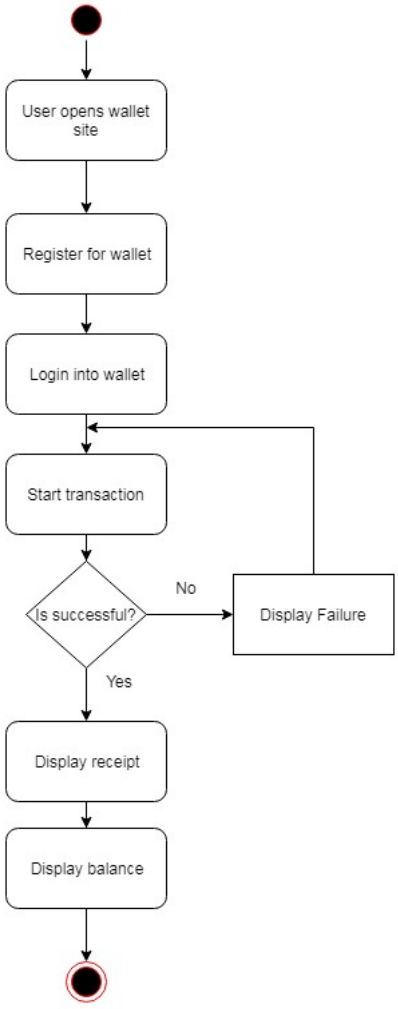


Figure 5.3: Activity Diagram

5.4 Sequence Diagram

Sequence diagrams are popular dynamic modeling solution. It focuses on the sequence of messages that are exchanged, along with their respective occurrence specifications on the lifeline. The object interactions are shown arranged in a time sequence. Lifeline is a named element which represents an individual participant in the interaction. Sequence diagrams are sometimes called event diagrams or event scenarios.

Figure 5.4 shows us that user will the first login into the wallet. Then wallet can create a transaction on behalf of the user. The transaction then is sent to the cryptocurrency model for processing. After processing successfully the new transaction block will be added to the system and blockchain will be updated. Cryptocurrency model then gets an acknowledgment status. Then the status and transaction details are recorded with the wallet. The wallet than will show the resulting receipt to the user at the end.

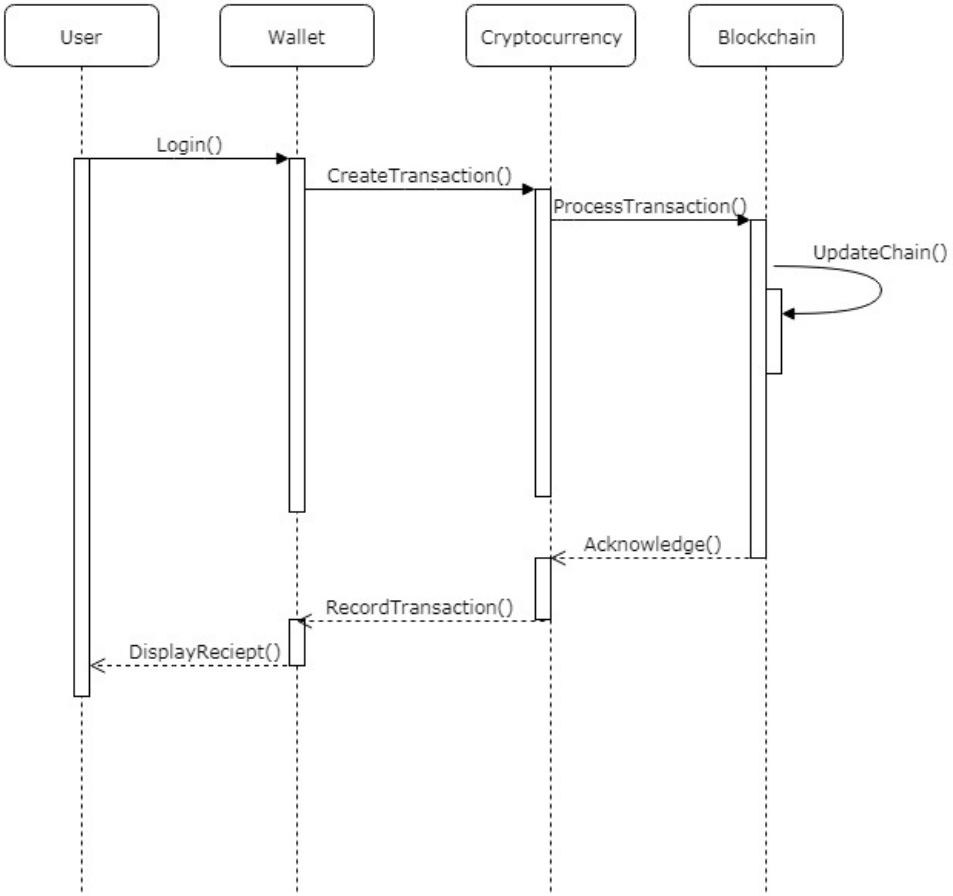


Figure 5.4: Sequence diagram

5.5 State Chart

A state chart shows the outcomes from different classes in response to external stimuli. It is also known as Harel state chart or state machine diagram. This UML diagram model the dynamic flow of control from state to a state of a particular object within a system.

Figure 5.5 shows us the user first opens the wallet. After opening the transaction is started by the user. Processing transaction takes place after

that. Finally, the result is displayed back to the user.

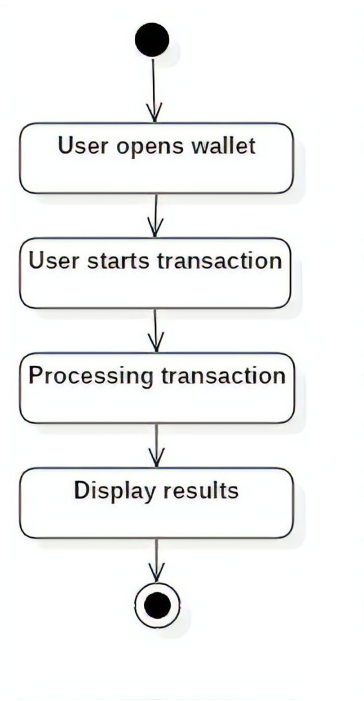


Figure 5.5: State Chart

5.6 Swimlane Diagram

A swimlane diagram is a visual element used in process flow diagrams or flowcharts that visually distinguishes job sharing and responsibilities for sub-processes of a business process. Swimlanes may be arranged either horizontally or vertically.

As shown in figure 5.6, user access the wallet website and authenticates himself by referencing the database. After a successful login, the user can input transaction details and then start a transaction. The important details are verified with database and transaction is created in cryptocurrency network. The miners will then verify and validate the transactions. After that

block gets added into blockchain. The changes are acknowledged by cryptocurrency model. The transaction details are recorded into the database. The result is displayed to the user by the wallet.

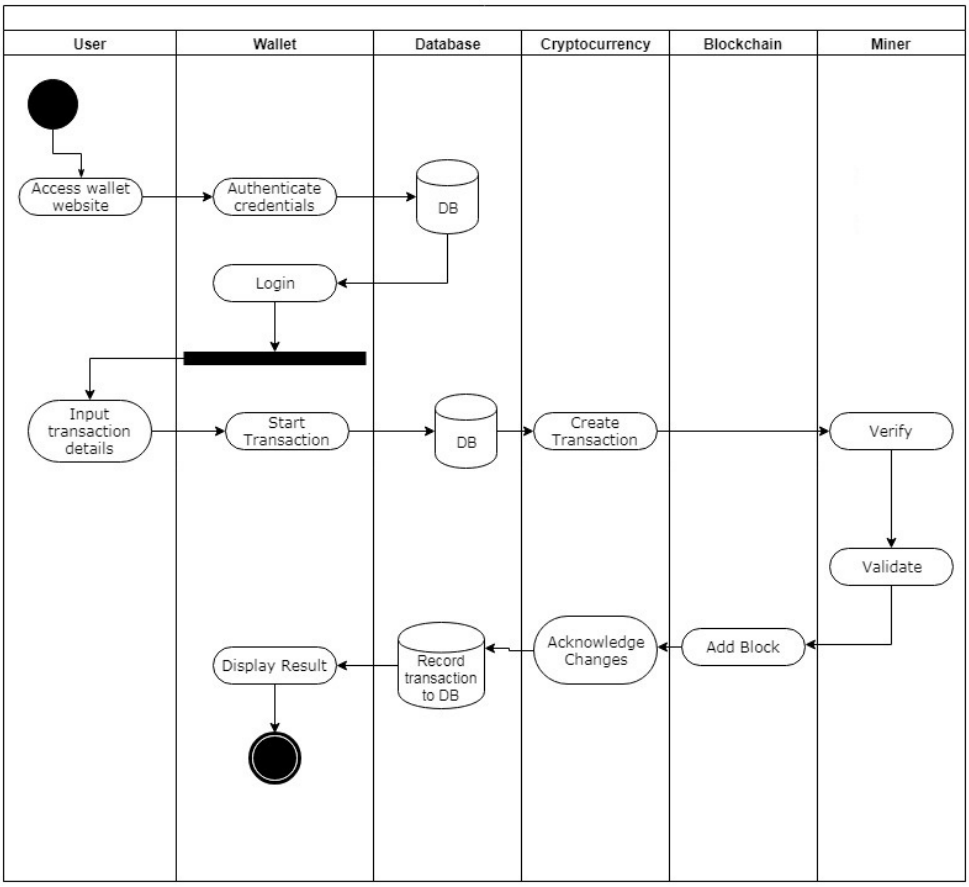


Figure 5.6: Swimlane Diagram

5.7 Deployment Diagram

Figure 5.7 shows the deployment diagram of our system. Deployment diagram shows the overview of the system in terms of the deployment of different software artifacts to the targets of deployment. We have to realize

the major elements of a software system in terms of artifacts. The blockchain resides on many nodes and its services are made available via web services. The miner clients are connected to blockchain and cryptocurrency using web services. The wallet resides on a web server and connected to a database server. The client can access the web server by using a simple browser on any device.

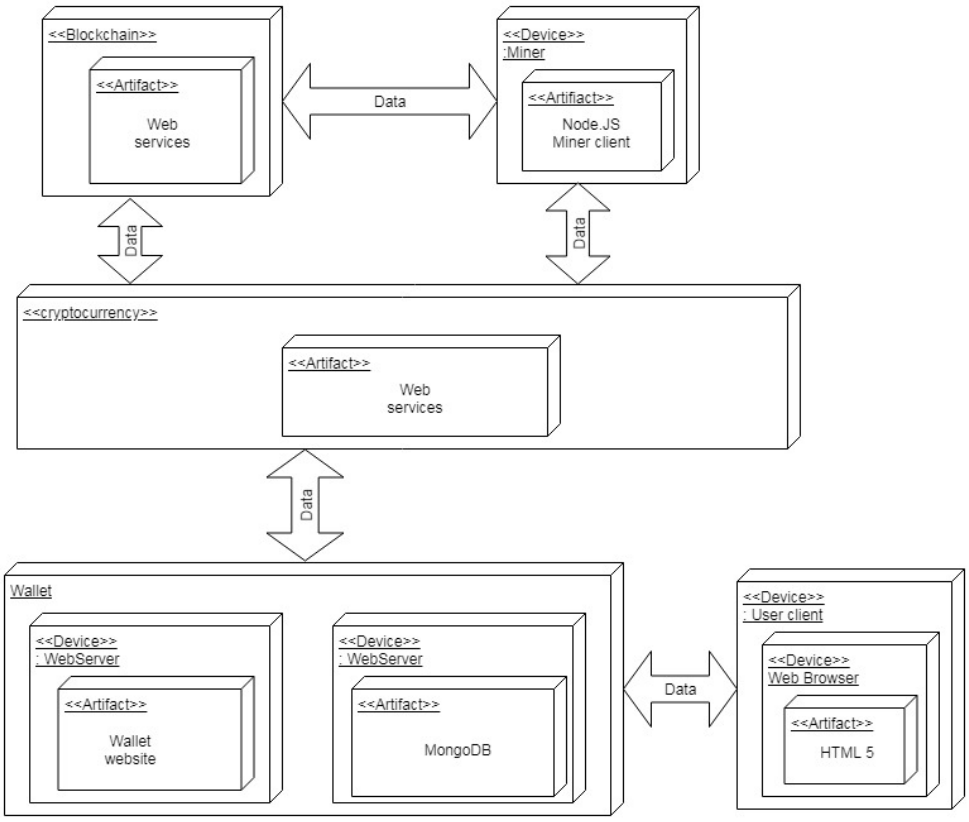


Figure 5.7: Deployment Diagram

5.8 Class Diagram

Fig 5.8 shows the class diagram of our system. This diagram shows the different classes used in the system. It displays relationships between various objects. A class contains variables and functions. The objects of a particular class are used to access the elements of that class.

The classes 'Block' and 'Blockchain' provide full functionality for a generalized blockchain.The class 'Transaction' and 'TransactionPool' provides functionality for cryptocurrency model and mining incentive respectively. The class 'Wallet' allows users to use cryptocurrency by providing identification and keys for users.

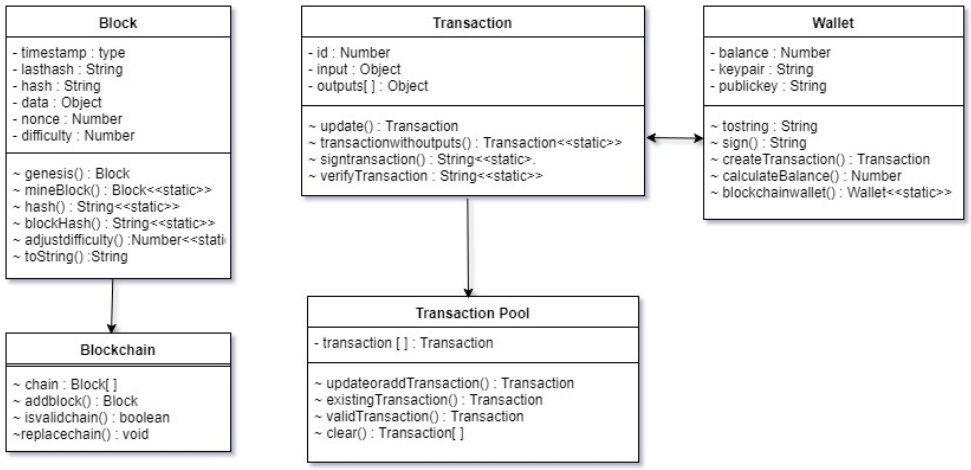


Figure 5.8: Class Diagram

5.9 DFD Diagrams

A data flow diagram is responsible for mapping out the flow of information in a particular system. Whenever we want to create only an overview of a data system we prefer DFD. It maps all the steps from input to generating

an output.

- DFD – Level 0: Figure 5.9 suggest us a simple data flow. User data is given to a decentralized system and the system then shares the data with different services to obtain the results.

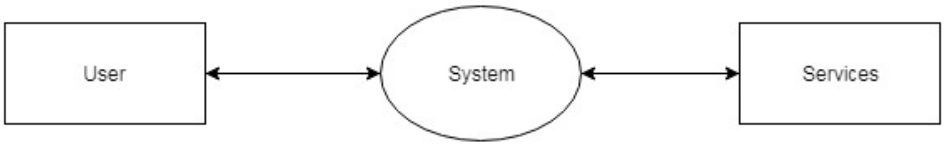


Figure 5.9: Data Flow Diagram (Level 0)

- DFD – Level 1: figure 5.10 suggest a general data flow scenario. User registers his data with the wallet. The wallet then accepts transaction details as input. The transaction is created in cryptocurrency network. The data is verified and validated by miners. The output block is then added to the blockchain. The end results are displayed back to the user.

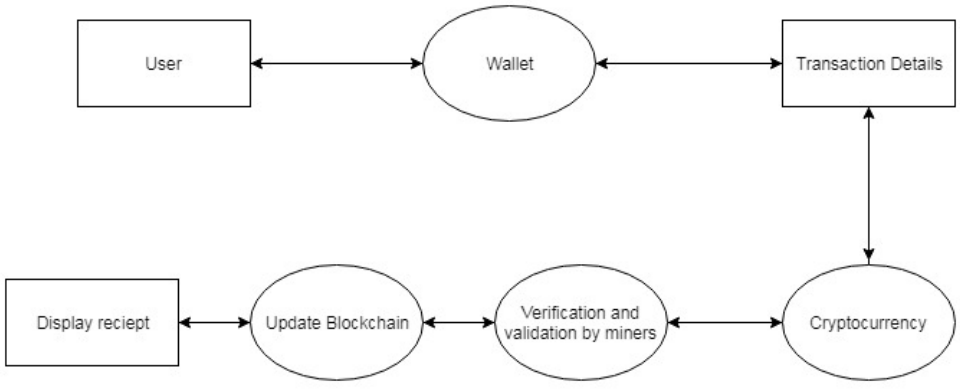


Figure 5.10: Data Flow Diagram (Level 1)

5.10 Summary

In this chapter, we have proposed the system architecture by using different diagrams like use case diagram, activity diagram, sequence diagram, state chart, swimlane diagram, deployment diagram, class diagram and DFD diagram. Each UML diagram helps to model the system.

Chapter 6

Planning phase

6.1 Frontend

- A wallet as a web app: It is an object that stores the public key and private key of an individual transaction. The public key is the address of the wallet. It helps with the transaction. basically, the wallet is a core object with three main components. We balance the cryptocurrency in the wallet. For doing the transaction we require a private key and public key. The private key is only for the sender and public key is used by the receiver. When we combine both the private key and public key then we got a signature which is used to decrypt the data which is sent by the sender. Private key: It is for the first individual. Used to generate a signature. Public Key: It is for the Second individual. It contains the address of the wallet.

Figure 6.1: Creation of Digital Signature

- Transaction: The transaction includes the timestamp. A timestamp is accepted as valid if it is greater than the median timestamp of previous 11 blocks, and less than the network-adjusted time + 2 hours. "Network-adjusted time" is the median of the timestamps returned by all nodes connected to you. Here we give timestamp as an input, also some cryptocurrency and senders public key after giving this input to the transaction we got the output which contains some amount (Cryptocurrency), the address of the receiver. It shows how much currency send by the user.

6.2 Backend

- Blockchain API: The Blockchain Wallet API provides a simple interface Merchants can use to programmatically interact with their wallet.

  To use this API, you will need to run a small local service which is responsible for managing your Blockchain Wallet. The application then interacts with this service locally via HTTP API calls.

- Cryptocurrency model: The cryptocurrency model is responsible for managing transaction and transaction pools. The cryptocurrency will

make transactions and help them broadcast among peer to peer network. It will send transaction into a transaction pool from where miners can start verifying transactions. When a miner will share the solution, the solution is broadcasted to the network for verification. After verification, the successful transaction should be added as a new block and should be removed from the unconfirmed transaction pool. The cryptocurrency model works with both HTTP web socket protocols to transfer and share the data and services among the nodes.

- Web server- For blockchain and cryptocurrency: We will use a Node.js web server. It will connect nodes by web socket. It also gives HTTP API interface for service. Peer to peer network will need Node.js as a web server. Node.js has a built-in module called HTTP, which allows Node.js to transfer data over the HyperText Transfer Protocol (HTTP). To include the HTTP module, use the require() method. The HTTP module can create an HTTP server that listens to server ports and gives a response back to the client. Use the createServer() method to create an HTTP server.

  The function passed into the HTTP.createServer() method, will be executed when someone tries to access the computer on port 8080. If the response from the HTTP server is supposed to be displayed as HTML, you should include an HTTP header with the correct content type. The first argument of the res.writeHead() method is the status code, 200 means that all is OK, a second argument is an object containing the response headers. The

- Database server- For the wallet: For wallet transaction and management here we use MongoDB as a database. To create a database in

MongoDB, start by creating a MongoClient object, then specify a connection URL with the correct IP address and the name of the database you want to create. MongoDB will create the database if it does not exist, and make a connection to it. MongoDB waits until you have created a collection (table), with at least one document (record) before it actually creates the database (and collection). You can check if a database exists by listing all databases in your system.

6.3 Coding Languages

- HTML: Hypertext Markup Language (HTML) is the standard markup language for creating web pages and web applications. With Cascading Style Sheets (CSS) and JavaScript, it forms a triad of cornerstone technologies for the World Wide Web. Web browsers receive HTML documents from a web server or from local storage and render the documents into multimedia web pages. HTML describes the structure of a web page semantically and originally included cues for the appearance of the document. HTML can embed programs written in a scripting language such as JavaScript, which affects the behaviour and content of web pages. The inclusion of CSS defines the look and layout of content.

- CSS: Cascading Style Sheets (CSS) is a style sheet language used for describing the presentation of a document written in a markup language like HTML. CSS is a cornerstone technology of the World Wide Web, alongside HTML and JavaScript. CSS is designed to enable the separation of presentation and content, including layout, colors, and fonts. This separation can improve content accessibility, provide more flexibility and control in the specification of presentation characteristics,

enable multiple web pages to share formatting by specifying the relevant CSS in a separate .css file and reduce complexity and repetition in the structural content. Separation of formatting and content also makes it feasible to present the same markup page in different styles for different rendering methods, such as on-screen, in print, by voice (via speech-based browser or screen reader), and on Braille-based tactile devices. CSS also has rules for alternate formatting if the content is accessed on a mobile device.

- Node.js: It is an open-source, cross-platform JavaScript run-time environment that executes JavaScript code outside of a browser. Historically, JavaScript was used primarily for client-side scripting, in which scripts written in JavaScript are embedded in a webpage's HTML and run client-side by a JavaScript engine in the user's web browser. Node.js lets developers use JavaScript to write Command Line tools and for server-side scripting running scripts server-side to produce dynamic web page content before the page is sent to the user's web browser. Consequently, Node.js represents a "JavaScript everywhere" paradigm, unifying web application development around a single programming language, rather than different languages for server side and client side scripts.

- MongoDB: MongoDB is a free and open-source cross-platform document-oriented database program. Classified as a NoSQL database program, MongoDB uses JSON-like documents with schemata. MongoDB is developed by MongoDB Inc. and is published under a combination of the GNU Affero General Public License and the Apache License.MongoDB provides high availability with replica sets. A replica set consists of two

or more copies of the data. Each replica set member may act in the role of the primary or secondary replica at any time. All writes and reads are done on the primary replica by default. Secondary replicas maintain a copy of the data of the primary using built-in replication. When a primary replica fails, the replica set automatically conducts an election process to determine which secondary should become the primary. Secondaries can optionally serve read operations, but that data is only eventually consistent by default.

6.4 Algorithms

1. Secure Hashing Algorithm (SHA)-2: The SHA version 2 provides various different hash functions with various output bit length input. The SHA-256 is a novel hash function which works on 32bit words respectively. SHA-256 has ability work on x86 as well as x86-64 based architecture.

2. Consensus protocols: The process of achieving single data value among the distributed or decentralized system is known as consensus protocol. The main goal is to achieve reliability in the system of unreliable nodes. These are also known as mining algorithms. The system will use a hybrid model of proof-of-work and proof-of-authority. The Proof-of-work uses a computational puzzle which needs to be solved by random guessing. Once the solution is found anyone can check the answer easily for authenticity. The proof-of-authority provides comparatively fast transaction through consensus mechanism of identity as a stake

3. Elliptic curve cryptography(ECC): ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over

finite fields. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators, and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme.

4. Universally Unique Identifier (UUID): UUID is also known as GUID. It is a 128-bit number used to identify information in computer systems. When generated according to the standard methods, UUIDs are for practical purposes unique, without depending for their uniqueness on a central registration authority or coordination between the parties generating them, unlike most other numbering schemes. While the probability that a UUID will be duplicated is not zero, it is close enough to zero to be negligible.

6.5 Advantages

1. No central point of failure, unlike regular currency.
2. Full control over digital tokens by the owner.
3. Secure, available, fast, cheap and reliable.
4. Every transaction is verified by every peering in the network.
5. Trust is in-built in the Peer to Peer system.

6.6 Cost Estimation

The cost estimation is an important phase in planning. The cost estimation allows us to estimate and manage the resources efficiently which are required for the project. Product cost estimation:

– The product cost estimation deals with the cost of only the end product and its functioning cost in the future if deployed. Following are the cost estimation for complete deployment of the project for 1 year of intense operation in standalone mode.

Table 6.1: Product cost estimation

Srno	**Service name and function**	**Cost in dollar**
1	AWS Gateway 53 (Domain name)	10
2	AWS EC2 T2 unlimited instance	430
3	AWS Elastic load balancer	300
4	Total	750

Project cost estimation: The project cost estimation deals with the cost of making the project. The costing deals with the cost of developing a prototype and other documentation activities.

Table 6.2: Project cost estimation

Srno	**Service name and function**	**Cost in rupee**
1	Paper publication in open access journal (Sem-I)	2500
2	Paper publication in open access journal (Sem-II)	2500
3	Documentation printing	2000
4	AWS prototype deployment and testing	500
5	Total	7500

6.7 Risk Management

The risk is the uncertainty which is associated with a future event which may or may not occur and a corresponding potential for loss. The risk management goes long way in the project help project manager to predict problems and act accordingly.

Table 6.3: Risk management

Srno	**Type of risk**	**Risk**	**Solution**
1	Time-related risk	Incorrect time estimation for delivery of modules	The team should be in continuous communication and follow the deadlines placed by the university.
2	Financial risk	Improper tracking of finances for AWS	The cost of testing the functionality on AWS cloud should be monitored by AWS Cloud watch with billing alerts.
3	Technical risk	Improper implementation of the process	The team should always validate the resultant module with the requirements in mind.
4	Operational risk	Lack of sufficient training	The team should always reach out for different study resources and industry experts opinions.

5	Operational risk	Performance issue	The team should always use memory optimization as the distributed ledger has huge memory requirements.

6.8 Timeline chart

The figure 6.2 represents the timeline chart for the project activities. The chart clearly shows the stages and their respective completion period. The project activities must be followed in timely manner to ensure success of this project.

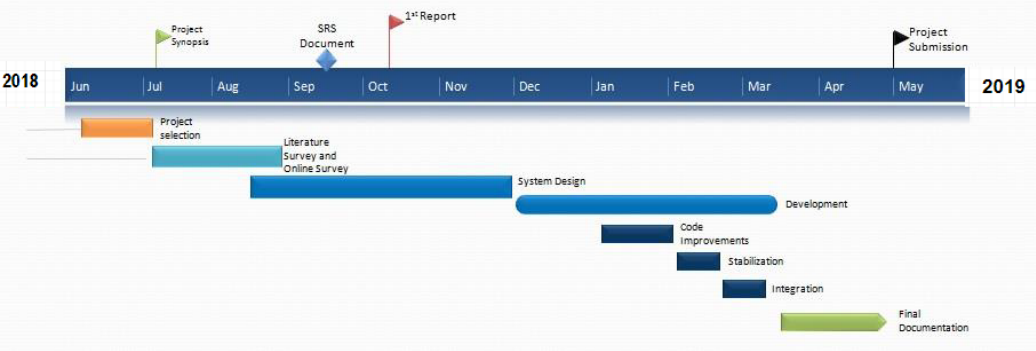


Figure 6.2: Timeline chart

6.9 Reusability of the project

In light of the above efficient examination on the security and flow blockchain, we list a couple of future bearings to mix up inquire about endeavors into this region. The most prominent accord instrument utilized as a part of blockchain is PoW. A noteworthy weakness of PoW is the misuse of registering resources. To take care of this issue, we are attempting to build up a half and half agreement instrument of PoW and PoA.

The blockchain API itself is generalized. It can be used to craft any sort of foundational model for various blockchain applications. The cryptocurrency API is also very robust and can easily be fine-tuned for a private currency exchange or banking like platform easily. The front-end application can easily be changed to form a new wallet for another cryptocurrency. In this way, individual modules are written can be reused for various purposes.

6.10 Summary

- In this chapter, we have discussed the frontend in which we show how the wallet works along with its transaction process. And the backend consists of discussion about the different algorithms used to implement this system.
- Discussed different coding languages that we have used in our project. Different algorithms are used like Secure Hashing Algorithm (SHA), consensus protocols, Elliptic Curve Cryptography(ECC), Universally Unique Identifier (UUID).
- Risk management deals with the assesment of associated risks and risk management strategies.

Chapter 7

Implementation

7.1 Generalized blockchain

The generalized implementation means only the blockchain constraints are taken into consideration irrespective of the data that is being stored. The main advantage is that the blockchain can easily be adapted to any other application. The blockchain is simply the data blocks linked to each other.

In blockchain, blocks are added one after another in consecutive order arranged by their timestamp. Each block contains SHA256 hash of its own as well as a hash of the previous block. Tempering with the block data in any matter would make the chain invalid immediately.

7.1.1 The Block class

The block represents the unit structure of the block. The timestamp field contains the time of block creation. The lasthash field contains the hash of the last block added into blockchain. The hash contains the SHA256 hash of the block itself. The data can be anything related to the application which

we want to store in a distributed environment. The nonce is the number of iterations it took to find the answer of POW consensus protocol. The difficulty is the difficulty level of POW consensus protocol.

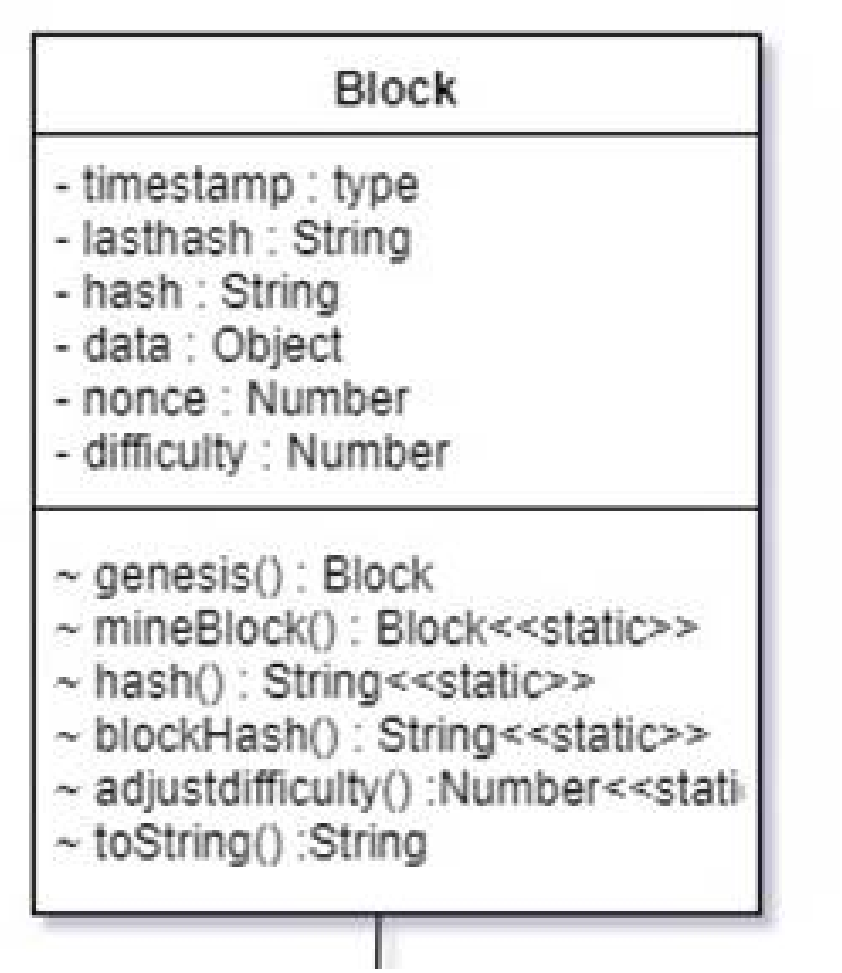


Figure 7.1: Class diagram of 'class Block'

The genesis method provides the genesis block which is the first block in the blockchain. The mineBlock method provides the mining algorithm which is a POW consensus protocol. This method allows solving the computation which helps to add the block in the blockchain. The blockHash method allows

you to calculate the hash of the block provided block details as an input. The adjust difficulty method allows to dynamically change the difficulty of POW consensus protocol according to mining rate. The difficulty increased or decreased accordingly to keep the economy stable.

7.1.2 The Blockchain class

The blockchain class is a representation of an array of block objects. The blockchain has 3 main methods. The addblock method is to append the new block at the end of the chain. The isValidChain method accepts the incoming chain determines if the given chain is valid or not. The replaceChain method replaces the chain with the new valid chain.

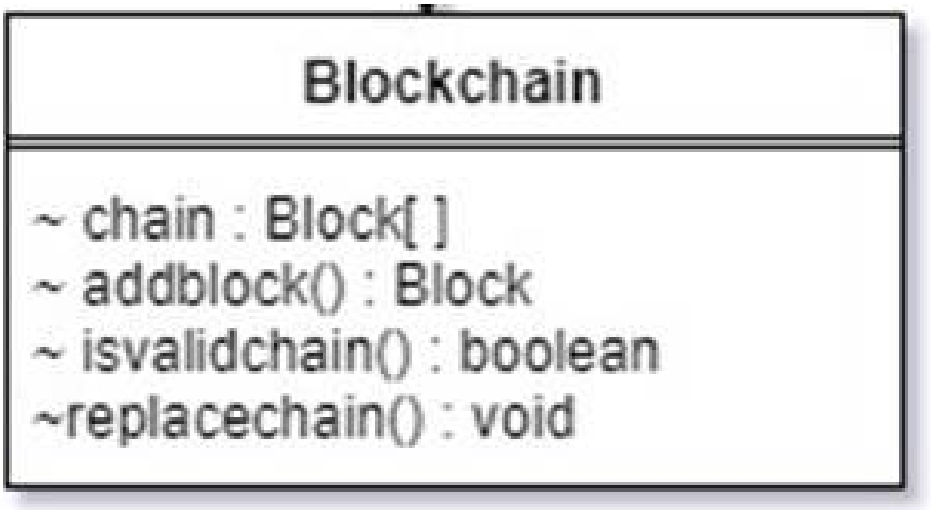


Figure 7.2: Class diagram of 'class Blockchain'

7.1.3 Algorithm for general blockchain

The fig below represents the flowchart for the operation of the blockchain based systems. At the time of creation of blockchain, the first block ie genesis

block is added into the chain. To add subsequent blocks, new data accepted from the user. The last block of the chain is acquired hash difficulty fields are extracted from it. The default nonce value is zero. The current timestamp is then acquired. The SHA256 hash is generated taking data, nonce, difficulty, lasthash, timestamp as an input.

The condition for POW consensus protocol is the generated hash value should have a prefixed number of zeros equal to the difficulty level. The POW is like solving the computational puzzle. Till the desired condition is achieved, the nonce timestamp changes every time new hash value is generated. After a successful attempt, the value is stored as a hash of that block block is added at the end of the chain.

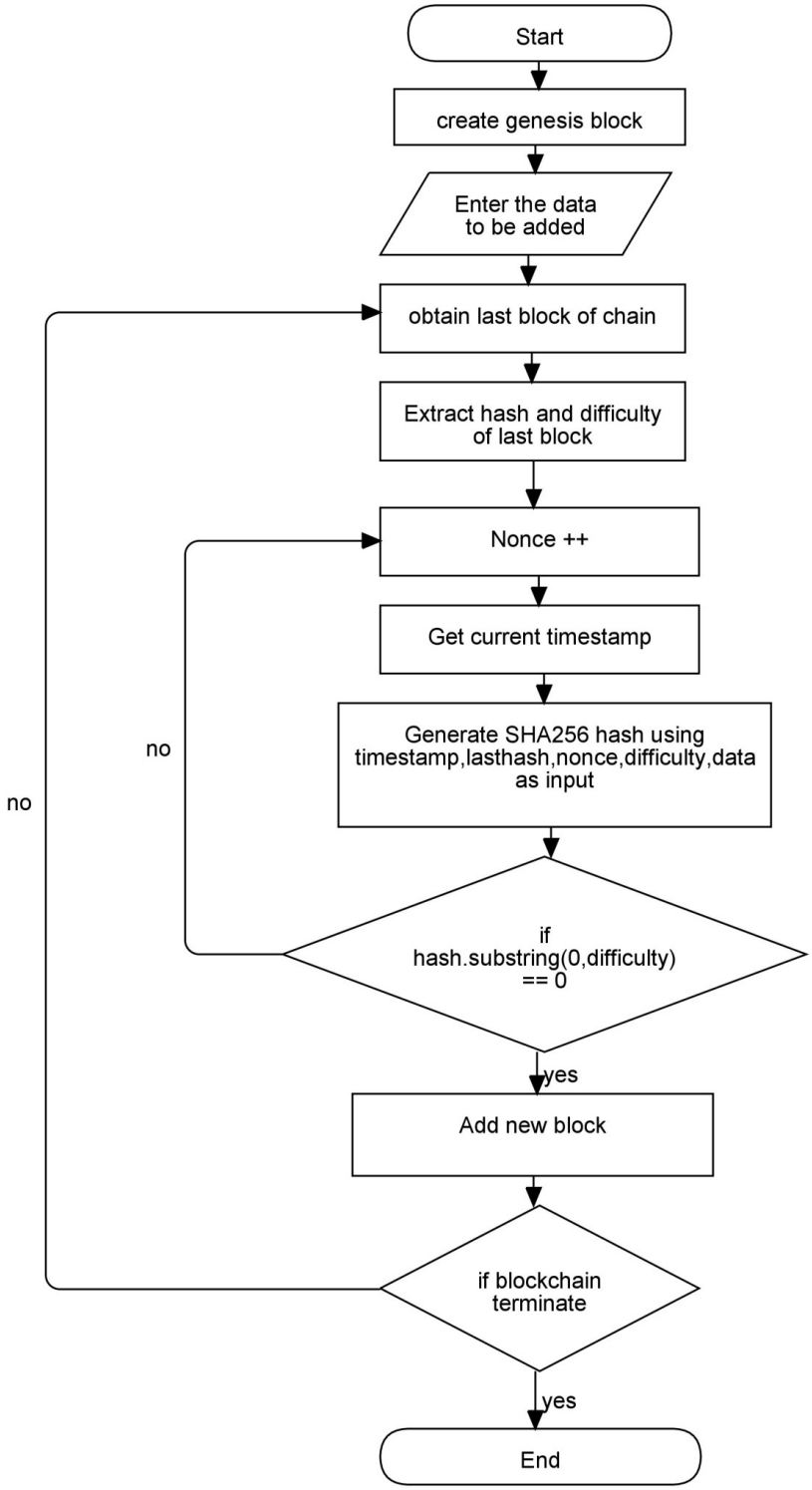


Figure 7.3: Blockchain Flowchart

7.1.4 Algorithm for chain validation replacement

This algorithm takes action when a new chain is sent to a node after it is connected as a peer or when a new block is added at the end of the chain. The fig below shows the flowchart for chain validation replacement.

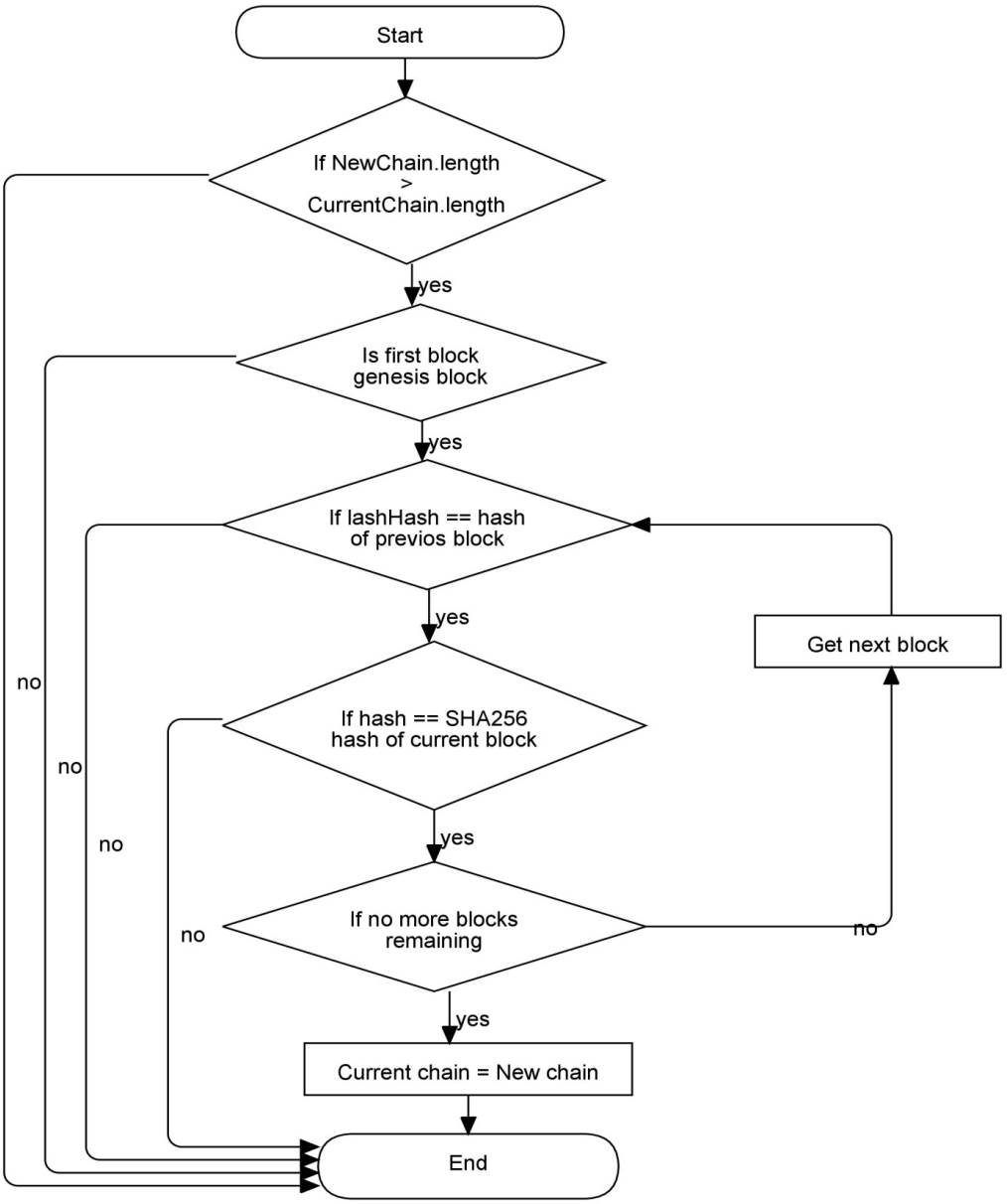


Figure 7.4: Chain validation and replacement

The length of the chain is checked if it is not longer than the current chain then its invalid. Every node has a definition of genesis block. The first block is checked whether it matches with the definition of genesis block. For all blocks in the chain, the lasthash field must contain has of the previous block. The hash of each block is calculated verified whether the hash field contains the appropriate hash. If all conditions are satisfied then the current chain is replaced by a new chain.

7.1.5 Algorithm for dynamic difficulty mining

The algorithm is useful to adjust the difficulty of mining so that the economy user waiting time can be monitored easily. The fig below shows the flowchart for the same. At the time of adding a new block; the timestamp of the last mined block is extracted. The difference between 2 timestamps is compared with the mining rate. If the mining rate is greater then, the difficulty is increased otherwise decreased. Again system waits for the addition of new block again new mining difficulty level.

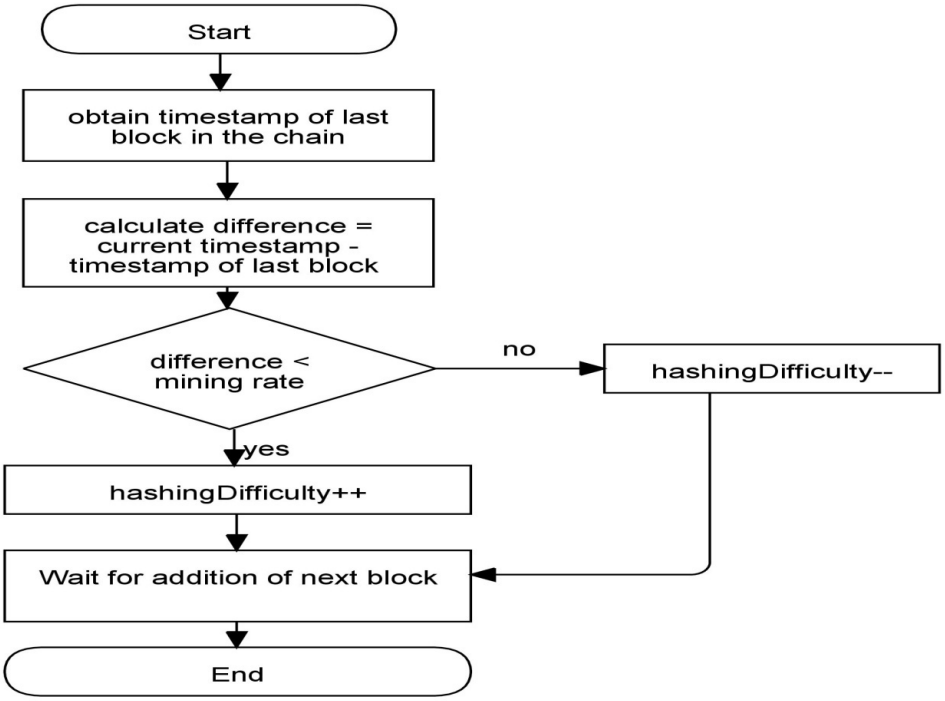


Figure 7.5: Dynamic difficulty mining

7.1.6 API endpoints

The table 7.1 describes the API points to be used for blockchain related requests. It states the request type, name of endpoint, input type and description for the functionality of that endpoint.

Table 7.1: API endpoints for blockchain

Srno	Request type	Name	input	Description
1	GET	blocks	null	The endpoint provides the blockchain as a response.
2	POST	mine	data:data	The endpoint takes data as an input and returns new blockchain as a response.

7.2 Cryptocurrency model

The generalized blockchain is utilized to store the data of the transaction. The cryptocurrency model uses the blockchain technique to store manipulate the data of transactions. The cryptocurrency model facilitates the creation mining of transactions. The model allows sharing the transaction with multiple miners so that they could try to mine simultaneously the one who wins will receive the reward. Also, the transaction data is shared between multiple nodes among those.

7.2.1 The Transaction class

The transaction class facilitates the transaction data processes. The fig below shows the class diagram for this class. The data members are id,

input outputs. ID is just a unique number which is generated using Universally Unique Identification (UUID). Inputs contain the fields like timestamp, amount of transaction, public key of sender wallet, digital signature of the sender using this data private key. The outputs is an array of objects which defines the remaining balance public key of sender wallet, public key of recipient amount to be transferred.

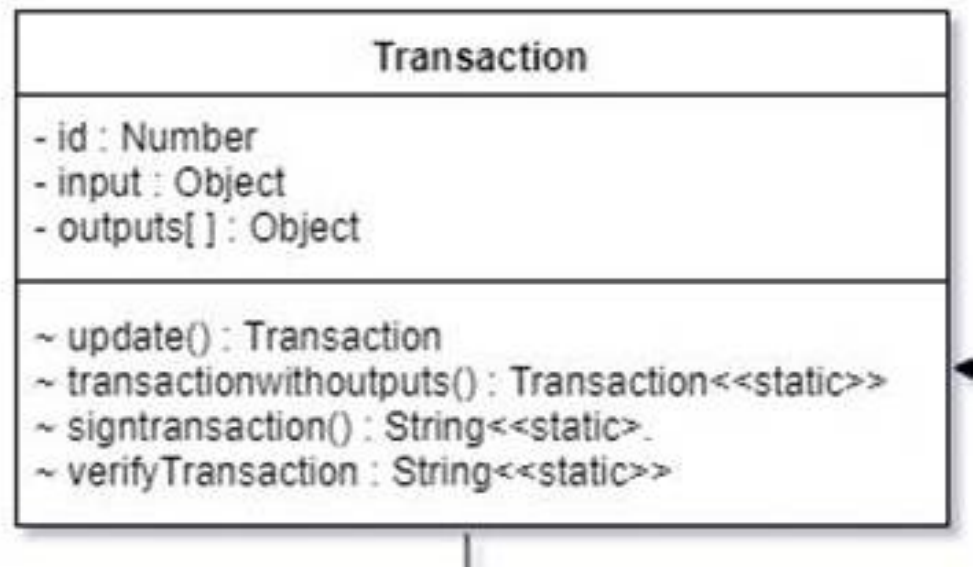


Figure 7.6: Class diagram of 'class Transaction'

The update method allows adding additional entries in the outputs. The transactionWithOutputs method allows creating the outputs object. The signTransaction method generates the digital signature for the sender using transaction data his private key. The verifyTransaction method checks for the correctness of digital signature generated. The signature is verified using the public key of sender the signature itself.

7.2.2 The TransactionPool class

The TransactionPool class facilitates the storage area for newly created user transactions. The TransactionPool is synchronized across the miner nodes. Every node has the ability to mine transaction from TransactionPool.

The transaction is an array of transaction objects. The updateoraddTransaction method allows to update the transaction while it is in the transactionPool has not started mining if their needs multiple transactions to the same recipient. The existingTransaction method facilitates checking whether transaction exists or not in TransactionPool. The validTransaction method checks for the validity of the transaction. The validation is of signature, amount to be transferred correctness of outputs object.

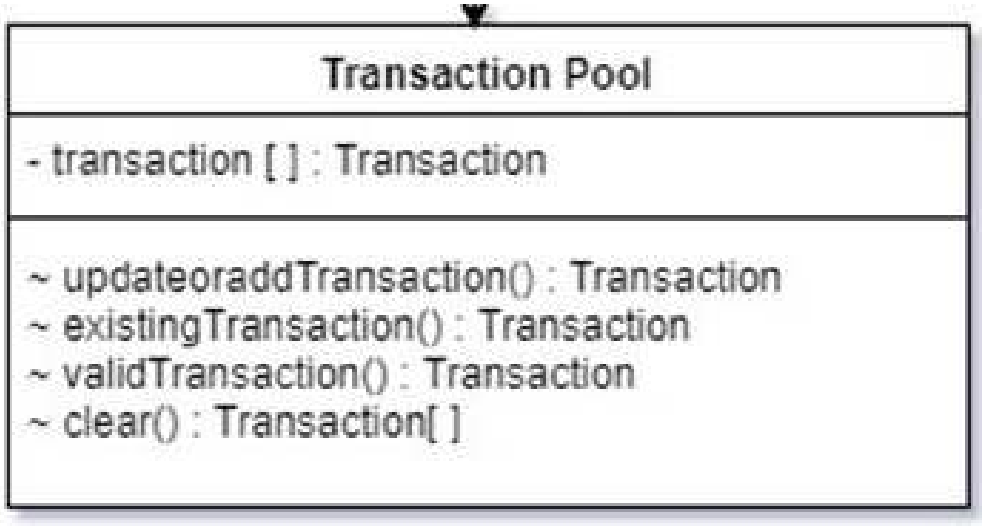


Figure 7.7: Class diagram of 'class TransactionPool'

7.2.3 The Wallet class

The Wallet class facilitates a wallet structure for every user of blockchain. The wallet provides service for the user as well as miners. The fig below shows

the class diagram for the same. The balance, keypair public key are data members. The balance stores the current balance of the user. The keypair is the combination of public key private key. The public key is the hexadecimal encoded version of the real private key.

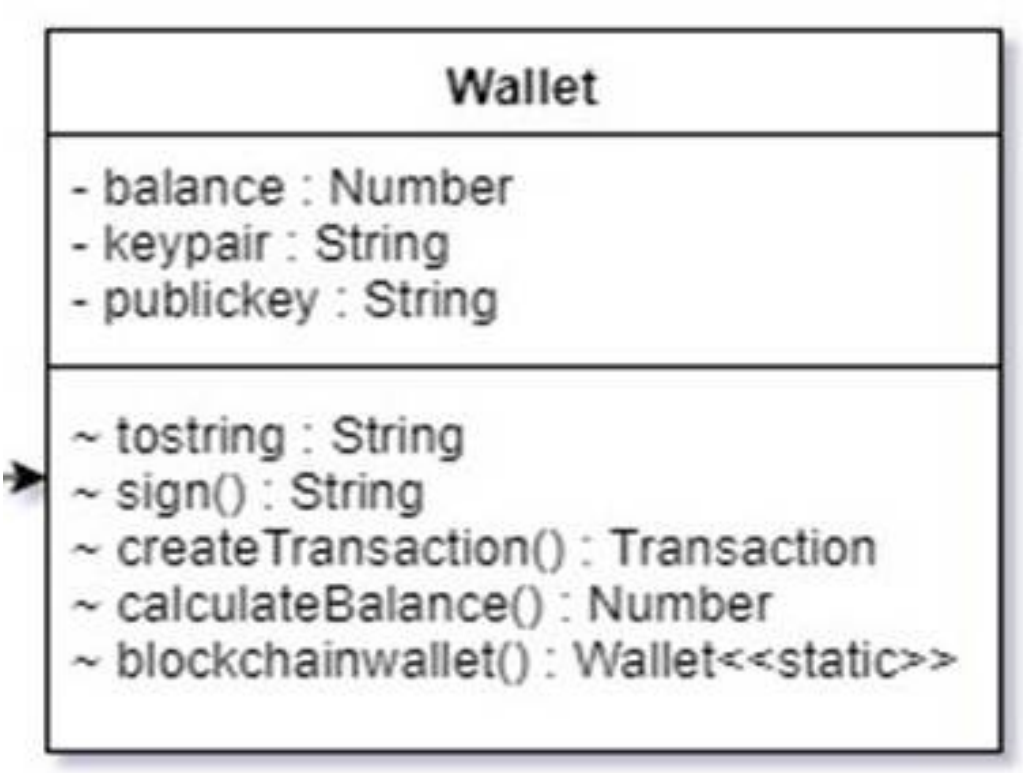


Figure 7.8: Class diagram of 'class Wallet'

The signing method generates the digital signature of the wallet user. The createTransaction method creates a new transaction or updates the existing transaction. The calculateBalance method calculates the current balance of the wallet user by traversing auditing through blockchain. The blockchain-Wallet method provides a blockchainWallet instance which will transfer the reward transaction to the miner.

7.2.4 Algorithm to calculate balance

The algorithm is used to calculate the current balance of the user using the blockchain transaction data. The fig below shows the flowchart for the same. The public key is needed as input. The transactions with the given public key are filtered out from the blockchain. The transactions are sorted according to the timestamp given. The amount if credited then added else if debited then subtracted while calculating. This process is continued till the end of the chain balance is generated as output.

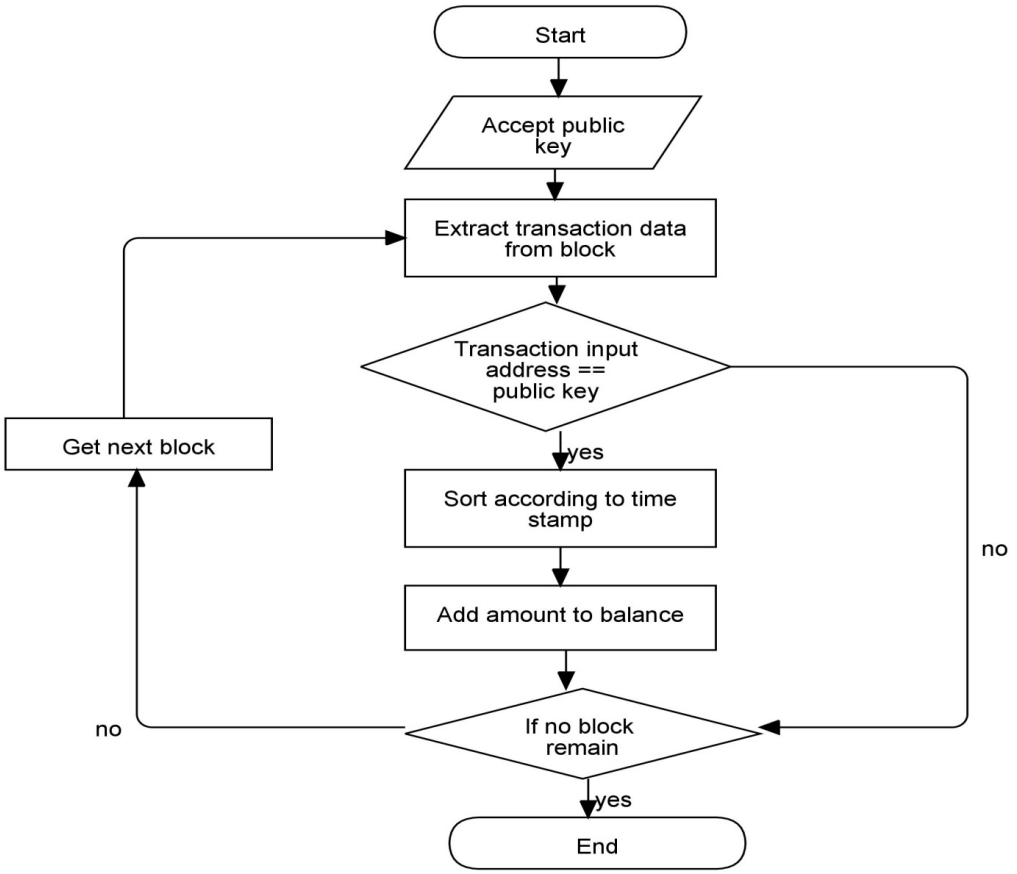


Figure 7.9: Calculate balance

7.2.5 Algorithm to create transaction

The algorithm is used to create a new transaction or update existing transaction. The fig below shows the flowchart for the same. The balance is calculated first to verify the user has needed appropriate balance. If the balance is not enough then the transaction is not created. If the balance is enough then it is checked whether transaction already exists or not. If a transaction already exists then it is updated updated transaction is broadcasted into the network. If the transaction does not exists then a new transaction is created with its UUID, the remaining balance is calculated and added as data of the transaction. The sender recipient address, balance, amount signature data used to create a new transaction. The transaction is broadcasted to the network using transactionPool.

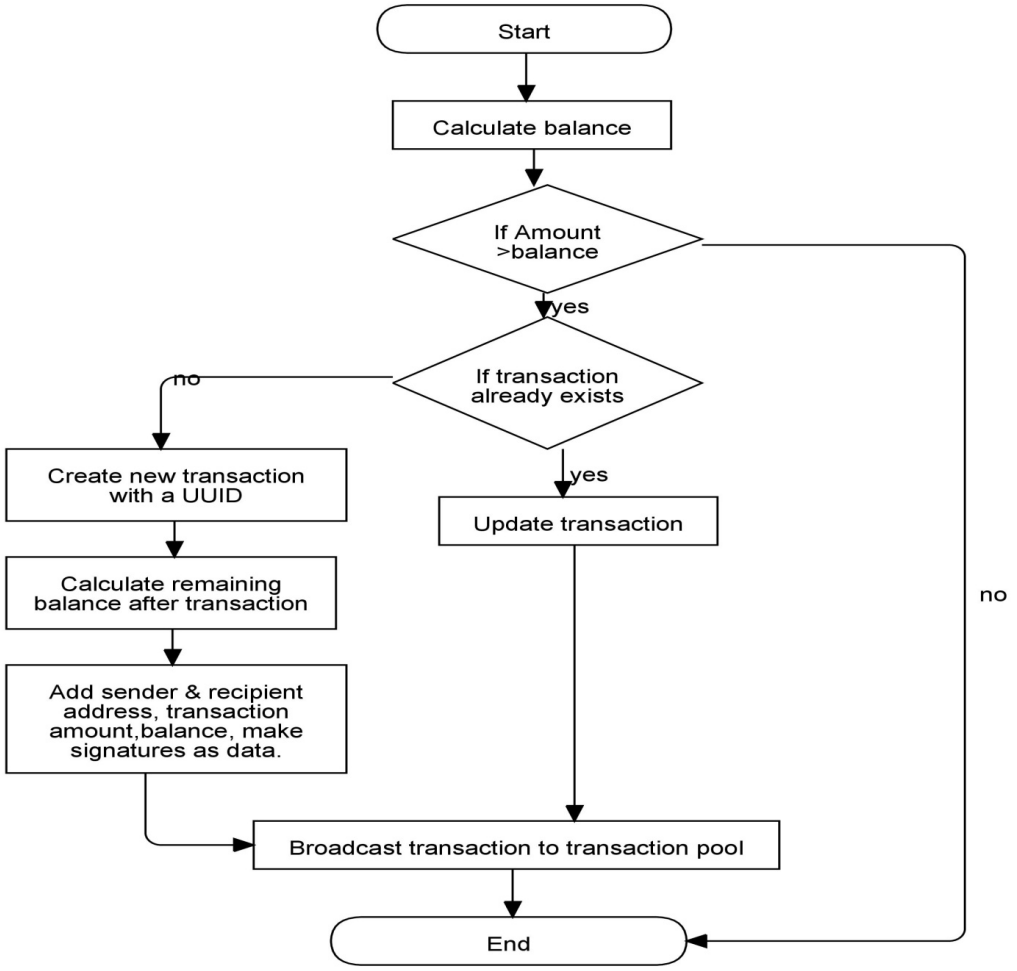


Figure 7.10: Create a transaction

7.2.6 Algorithm to mine transaction

The algorithm is used to mine a transaction of the user from the transaction pool. The fig below shows the flowchart for the mining process of the transaction. The transaction is acquired from transaactionPool the output amounts are calculated again for the validity. If invalid then it is rejected. If valid then the digital signature is checked for the correctness using the transaction data public key of sender wallet. If invalid then the transaction

is rejected. If valid then the mining starts using POW consensus protocol. After that reward transaction for a miner is created. All this information stored in the block then added to the blockchain. This newly added block is broadcasted over the network.

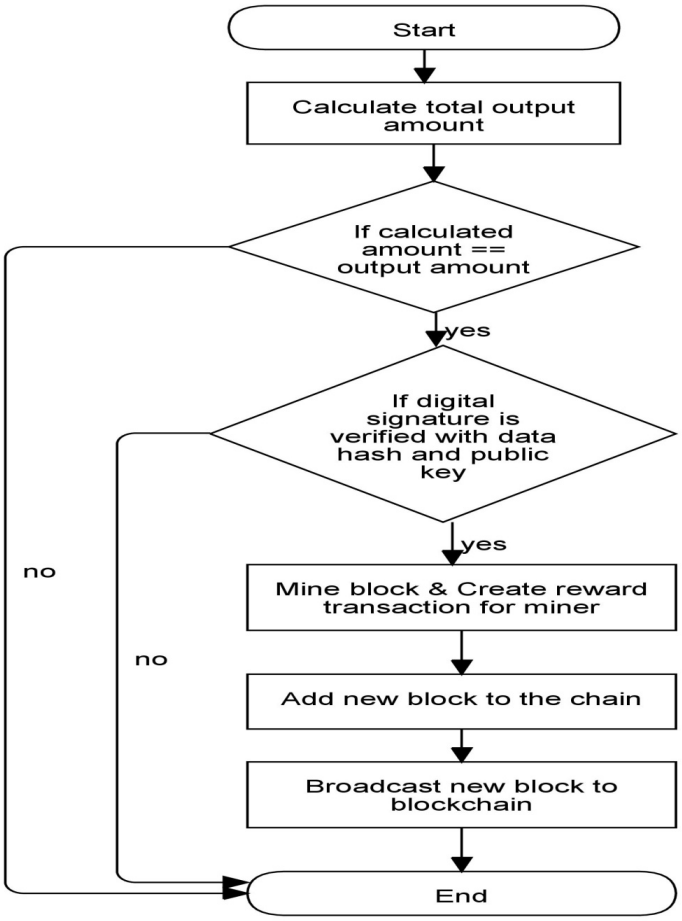


Figure 7.11: Mine transaction

7.2.7 Algorithm to broadcast to peers

The algorithm is used in peer to peer network to transfer different types of messages around the peers. The message can contain the new chain or transaction data or clear transaction message to clear the transactionPool.

The fig. 7.12 shows the flowchart for the same. The message type to set depends on the data to be sent across. Then the message is sent to the peer. This process is repeated for all the peer nodes in the network.

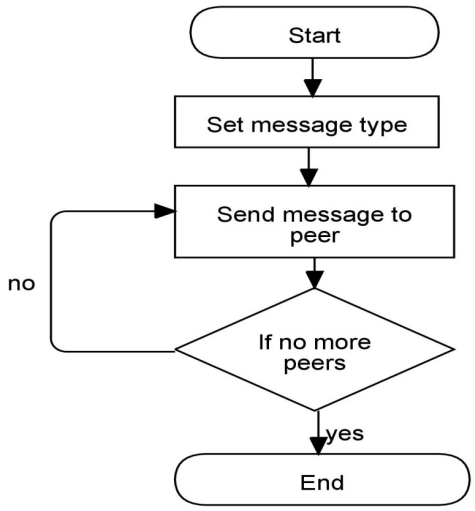


Figure 7.12: Broadcast messages to peers

7.2.8 API endpoints

The table 7.2 describes the API points to be used for cryptocurrency related requests. It states the request type, name of endpoint, input type and description for the functionality of that endpoint.

Table 7.2: API endpoints for cyrptocurrency

Srno	**Type**	**Name**	**input**	**Description**
1	GET	transactions	null	The endpoint provides the current blockchain as a response.
2	POST	transact	recipient: address, amount: amount	The endpoint takes recipient and amount to be transferred as input and returns all the transactions in the TransactionPool.
3	GET	mine-transaction	null	The endpoint mine-transaction returns the newly mined transaction block as output.
4	GET	public-key	null	TThe endpoint returns the public key of current wallet instance.

5	GET	balance	null	The endpoint returns the balance of current wallet instance.

7.3 Wallet for cryptocurrency

The wallet is an interface between the user the cryptocurrency. The nodes which are involved in blockchain ie miners can directly contribute in the processing of blockchain. The users which do not want to use cryptocurrency without investing in blockchain with resources, they can use such an online wallet. The online wallet facilitates an easy interface for users. The wallet can provide some other services to reduce complexity of the system.

The wallet is an online platform. Users can create an account secure it with a password. The user profile is automatically generated saved by the wallet. The wallet provides private key management services which help the user manage the private public key. The wallet also shows past transaction as well as pending transactions from transactionpool. The features like address book help the user save contact details for faster payment.

7.3.1 User system

The user management is a very important function on any platform. The wallet needs efficient secure access to the system. The registration step allows the user to create an account with the wallet. Wallet saves user details on

the database. As per the need, the details are fetched from the database to process.

- Registration system: The registration system allows the registration of the users to the wallet. The user details such as email-id, mobile number, name, and password are accepted from the user. The accepted fields are validated against the validation criteria. Once validated the user details are stored inside a document database as a new document.

  The password field is not stored directly as it implies security risks for the user data. The password field is instead stored as a bcrypt hash. Upon providing correct password bcrypt provides a mechanism for checking the correctness of password.

- Login system: The login system needs the email-id and password as input from the user. Using email-id as a filter, the correct document is acquired from the database. The encrypted hashed password then compared with the user provided a password. The bcrypt compare function allows comparing hashed password real password string gives result true if password matches.If the result is true then using the passport module express session, the user session is created on a database cookie for the same is created on the client side. The session is successfully created for the user for the specified time period.

- Logout system: At the time of log out, simply the created session cookie is destroyed. The database entry of active session is removed. The cookie created on the client side is deleted or made expired.

7.3.2 Address book

The address book is a simple CRUD (Create, Read, Update, and Delete) application. The public keys are really long hard to remember for the user. The address book allows the user to save the public key of the user with a nickname. This drastically helps the user in contact management. The storage allows the user to save once use it multiple time. The nickname allows the user to easily identify the desired keys in an efficient way.

The entries can easily be added. The nickname keys are taken as input from user added into the database. The added entry can be edited to change the nickname or the public key itself. The entry can also be removed from the database if desired.

7.3.3 Key management policy

The key management policy is the method of providing services and assistance to the user regarding the private key. Private key management is a challenge for a naïve user. Private Key is big in length contains lots of numbers, letters symbols. The slightest change in private key results in failure of the transaction. The private key must be accurate. If the private key is lost then it is impossible to access the currency related to the wallet. If the private key is stolen, then it may result in currency theft. The private key cannot be regenerated or recovered. The safety security is of crucial importance.

- Automatic key management policy: The automatic key management is the policy provides seamless access to the cryptocurrency. The private keys are encrypted with the randomly generated system key. Both the encrypted key system key are saved into the database. Whenever a

user makes a transaction, the private key is decrypted and used to sign transaction without the user even knowing. In this way, the naïve user is isolated from the complexity of managing a private key. The private keys are also secured as they are stored in an encrypted format.

- Non-recoverable passphrase key management policy: The private key is long in length very hard to remember. But in automatic mode, the user may feel insecure because if an attacker has profile password of the user then the attacker can easily steal the cryptocurrency. To avoid this, the private keys are encrypted with the custom user passphrase. The passphrase can contain any combination of letters, numbers, and symbols. It can also be viewed as a transaction password. The private keys are encrypted with user passphrase stored in the database. At the time of the transaction, the user needs to put in the passphrase to decrypt the key. If the passphrase is lost then it is not possible to decrypt the key. This may generate an issue of accessibility to the wallet.

- Recoverable passphrase key management policy: In this policy, even if the passphrase is lost, it can be recovered. The private key is encrypted with both user passphrase and the system key. If the user passphrase is lost, then the private key is decrypted using the system key. The decrypted private key then again encrypted with the new user passphrase. In this way, the high availability of key is ensured. The private key can never be lost with this method.

- Cold wallet key management policy: Some users use cryptocurrency as a form of digital gold rather than cryptocurrency. They keep their stored currency till they achieve higher real-world value then they sell

that currency. Such users tend to keep their private keys to their selves and do not want their keys stored or shared anywhere else. For those users, whenever they are transacting they need to provide their private key while transacting. If the key is lost, then it can never be recovered.

7.3.4 Routines for change in key management policy

The wallet allows users to change their key management policy anytime they want. By default, the wallet uses the automatic key management policy. The user can change policy to whatever suitable for him whenever he desires. The following fig shows the policy migration routines needed to perform for changing the key management policy. The procedures are described in table 7.3.

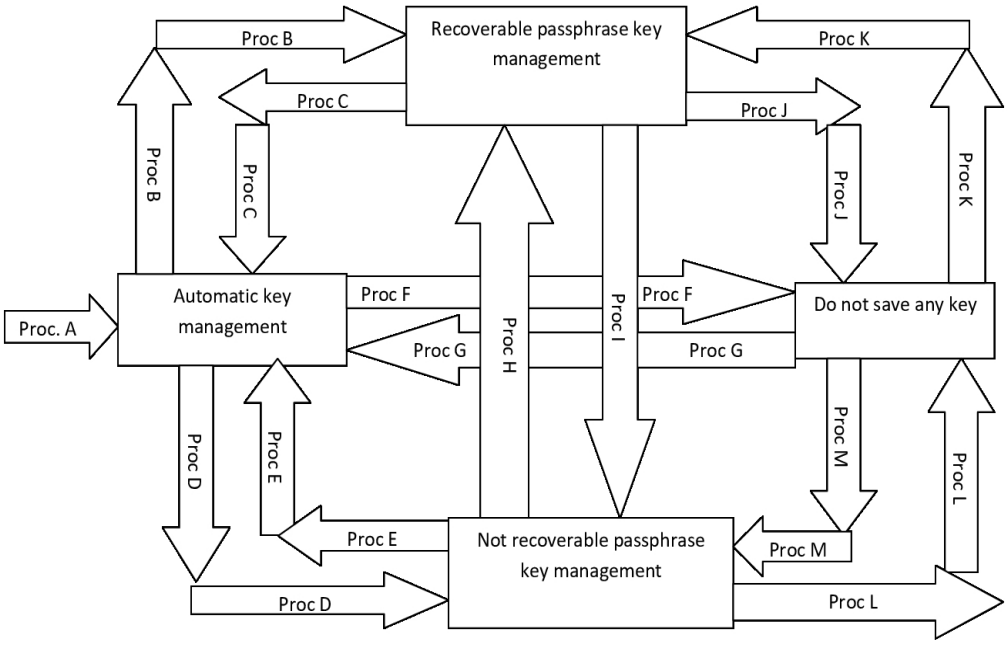


Figure 7.13: Key management

Table 7.3: Key management routines

Procedure	**Procedure**
Proc A: Step 1: Generate a system key Step 2: Encrypt private key with the system key Step 3: save encrypted key and system key Step 4: save encrypted key as a backup	Proc B: Step 1: decrypt the encrypted private key Step 2: encrypt private key with user passphrase Step 3: save the encrypted private key
Proc C: Step 1: decrypt private key with user passphrase Step 2: encrypt private key with the system key Step 3: save encrypted key and system key	Proc D: Step 1: decrypt private key with the system key Step 2: encrypt private key with user passphrase Step 3: Save encrypted key Step 4: Remove system key and backup private key

Proc E: Step 1: Decrypt private key with user passphrase Step 2: Generate a system key Step 3: Encrypt private key with the system key Step 4: save system key and encrypted private key	Proc F: Step 1: Decrypt private key with the system key Step 2: show private key Step 3: Remove encrypted private key and system key
Proc G: Step 1: Accept private key Step 2: Generate a system key Step 3: encrypt private key with the system key Step 4: save system key and encrypted private key	Proc H: Step 1: Accept user passphrase Step 2: decrypt private key with user passphrase Step 3: generate a system key Step 4: encrypt private key with the system key Step 5: save system key and encrypted private key as a backup

Proc I: Step 1: remove the backup system key Step 2: remove encrypted private key backup	Proc J: Step 1: accept user passphrase Step 2: decrypt the encrypted key Step 3: show private key Step 4: remove system key, the backup encrypted key and encrypted key
Proc K: Step 1: Accept private key Step 2: Accept user passphrase Step 3: encrypt private key with a passphrase Step 4: save the encrypted private key Step 5: Generate a system key Step 6: encrypt private key with the system key Step 7: save system key and encrypted backup private key	Proc L: Step 1: accept user passphrase Step 2: decrypt private key with user passphrase Step 3: display private key Step 4: remove encrypted private key

Proc M: Step 1: Accept private key Step 2: Accept user passphrase Step 3: encrypt private key with user passphrase Step 4: save the encrypted private key	

7.3.5 Algorithm for the wallet

This is the general flow of the wallet server. The wallet server first generates a proof-of-authority (POA) digital signature. The POA signature is then verified. If verification is successful wallet server is initialized otherwise terminated. In this way, the online wallet service will always be verified. After successful verification, the wallet server is started at the determined port. On that specific port, the server starts providing services to different clients.

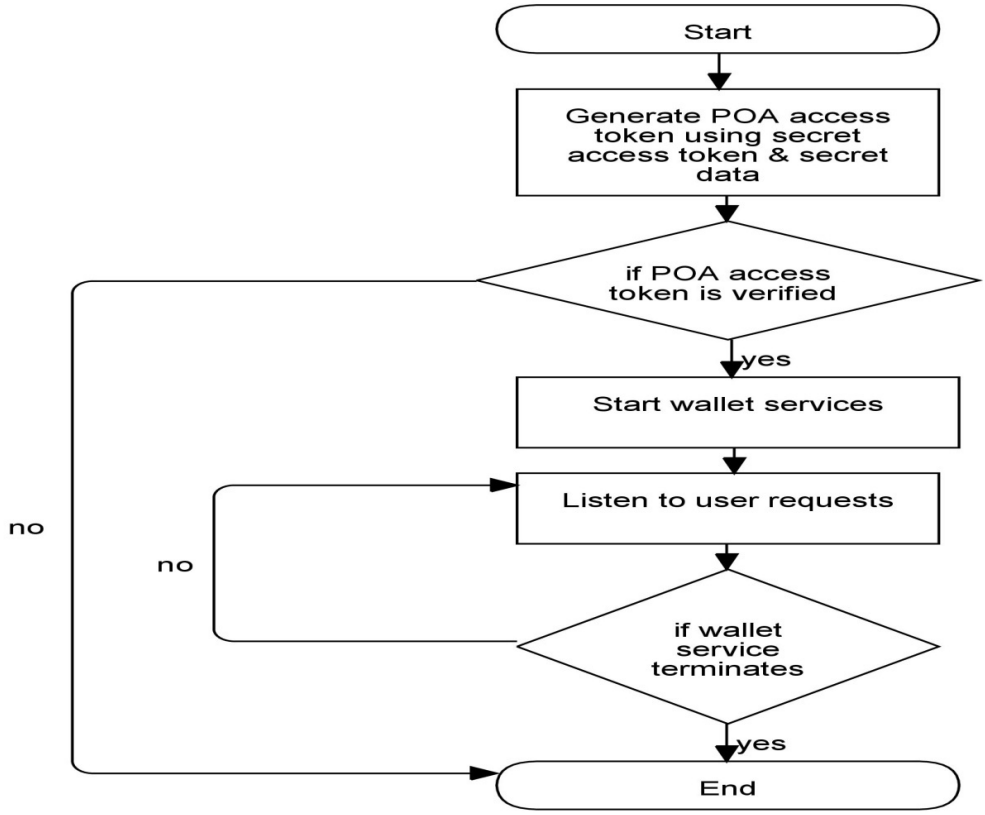


Figure 7.14: Wallet flowchart

7.3.6 API endpoints

The table 7.4 describes the API points to be used for e-wallet related requests. It states the request type, name of endpoint, input type and description for the functionality of that endpoint.

Table 7.4: API endpoints for wallet

Srno	**Type**	**Name**	**input**	**Description**
1	GET	create-user	null	The endpoint provides a new wallet as a response.
2	POST	get-user-balance	publicKey: Public key	The endpoint takes recipient and amount to be transferred as input and returns all the transactions in the TransactionPool.
3	POST	launch-user-transaction	publicKey: Public key, privateKey: private key, recipient: address, ammount: amount	The endpoint takes public key, private key, amount and recipient address and generates transaction for that user. It return transaction details as JSON response.

4	POST	get-completed-user-transactions	publicKey: Public key	The endpoint provides the transaction details of all the debited completed transactions for the user in the blockchain.
5	POST	get-pending-user-transactions	publicKey: Public key	The endpoint provides the transaction details of all the debiting pending transactions for user in transactionPool.
6	POST	get-completed-credit-user-transactions	publicKey: Public key	The endpoint provides the transaction details of all the credited completed transactions for user in blockchain.
7	POST	get-pending-credit-user-transactions	publicKey: Public key	The endpoint provides the transaction details of all the crediting pending transactions for user in transactionPool.

8	GET	do-mine-transactions	null	The endpoint returns the newly mined transaction details as JSON response.

7.4 Summary

- The project is implemented in 3 modules. The blockchain, the cryptocurrency model around the blockchain and the e-wallet website.
- Each module has its own responsibilities. The upper module relies on the services provided by lower modules.
- The services of each module are exposed via an API endpoint.
- The e-wallet interacts with these exposed modules and provides an easy interface to the users.

Chapter 8

Testing

8.1 Functional testing

Functions (or features) are tested by feeding them input and examining the output. Functional testing ensures that the requirements are properly satisfied by the application. This type of testing is not concerned with how processing occurs, but rather, with the results of processing. It simulates actual system usage but does not make any system structure assumptions.

Table 8.1: Functional Testing.

TC-ID	**Test case**	**Test step**	**Expected**	**Actual**	**Result**
TC 01	Check login	Click on the login button and enter Email-id and Password	The user should be able to login Successfully	Login Successful	Pass
TC 02	Check Registration	Click on the Register button and fill all required information	The user should get a Successful message	Register Successfully	Pass

TC 03	Change Password	Click on Profile Dropdown list and Select change password	The user should get Password changed message Successfully	Password Changed Successfully	Pass
TC 04	Change Key Management	Click on Profile Dropdown list and select Change key Management	It should display the current policy and other option	It displays Current policy and other option	Pass
TC 05	Transact	Click on the transact and fill the recipient and amount field	It should ask recipient and amount also passphrase or private key if required	It displays current balance and Appropriate field	Pass

TC 06	Credits-Completed Transaction	Click on Credits Dropdown list and select Completed transactions	It should display all completed credit transactions	Display a list of transactions with their attributes	Pass
TC 07	Credits-Pending Transaction	Click on Credits Dropdown list and select Pending transactions	It should display all Pending credit transactions	Display list of Pending transactions with their attributes	Pass

TC 08	Debits-Completed Transaction	Click on Debits Dropdown list and select Completed transactions	It should display all completed debit transactions	Display a list of completed transactions with their attributes	Pass
TC 09	Check login	Click on the login button and enter Email-id and Password	The user should be able to login Successfully	Login Successful	Pass
TC 10	Debits-Pending Transaction	Click on Debits Dropdown list and select Pending transactions	It should display all Pending debit transactions	Display list of pending transactions with their attributes	Pass

TC 11	Tools-Address Book edit	Click on Tools Dropdown list and select Address-book and click on edit	It should modify entry in the address book	It displays a successful message and modified entry	Pass
TC 12	Tools-Address Book delete	Click on Tools Dropdown list and select Address-book and click on delete	It should delete entry in the address book	It displays a successful message and removed entry	Pass

TC 13	Tools-Address Book trans-act	Click on Tools Dropdown list and select Address-book and click on Transact Now	It should fill public key auto-matically in transact page	It displays name of the recipient and filled his public key as the recipient	Pass
TC 14	Tools-Recover passphrase	Click on Tools Dropdown list and select Recover pass-phrase	It should display success message on recovery	It displays an ap-propriate message on recovery	Pass
TC 15	Home page	Click on Home Page	It should display the main landing page	Displayed main land-ing page	Pass

8.2 Performance testing

Performance testing, a non-functional testing technique performed to determine the system parameters in terms of responsiveness and stability under various workload.

Table 8.2: Performance Testing.

TC-ID	**Test case**	**Expected outcome**	**Actual outcome**	**Result**
TC 01	Loading time	Should within 60 seconds	Successfully loaded within 15 seconds	Pass
TC 02	Loading of the style sheet	It should load all the style sheets	Successfully loaded all style sheets	Pass
TC 03	Loading of static file like images	It should load all image files within 60 seconds	Failed to load within 15 seconds	Failed

TC 04	Mobile friendliness	It should adapt to all mobile devices or different resolution devices	It displays mobile-friendly version of the website , adapted to screen resolution automatically	Pass
TC 05	Server behavior	It should show high availability	Got response for all consecutive requests without failure	Pass
TC 06	URL format	It should have a standard informative URL format	All URLs were descriptive about their functionality	Pass

8.3 Unit and integration testing

Unit testing is a level of software testing where individual units/ components of software are tested. The purpose is to validate that each unit of the software performs as designed. Integration testing is a level of software testing where individual units are combined and tested as a group. The

purpose of this level of testing is to expose faults in the interaction between integrated units.

Table 8.3: Test cases for block module testing

TC-ID	**Test case**	**Expected outcome**	**Actual outcome**	**Result**
TC 01	Sets 'data' to match function	String "data" should appear in the data field of the new block	String "data" appear in the data field of the new block	Pass
TC 02	Sets 'last hash' to match the hash of the last block	The last hash field of the new block should contain a hash of the previous block	The last hash field of new block contains a hash of the previous block	Pass
TC 03	Generates a hash that matches the difficulty	The hash should have a number of zero as prefix equal to the value of difficulty	The hash has a number of zero as prefix equal to the value of difficulty	Pass

TC 04	Lowers the difficulty for slowly mined block	The mining difficulty should be lowered by 1	The mining difficulty lowered by 1	Pass
TC 05	Raises the difficulty for quickly mined block	The mining difficulty should be increased by 1	The mining difficulty increased by 1	Pass

Table 8.4: Test cases for blockchain module testing

TC-ID	**Test case**	**Expected outcome**	**Actual outcome**	**Result**
TC 01	Starts with the genesis block	The first block should have genesis values	The first block has genesis values	Pass

TC 02	Adds new block	The new block should be added in to blockchain with specified data	New block added in to blockchain with specified data	Pass
TC 03	validates a valid chain	The incoming chain should be validated correctly	The incoming chain validated correctly	Pass
TC 04	Invalidates the chain with corrupt genesis block	It should invalidate the chain if genetic block doesn't match	Invalidate the chain if genetic block doesn't match	Pass
TC 05	Invalidate corrupt chain	The invalid chain should be rejected	The invalid chain rejected	Pass

TC 06	Replaces the chain with a valid chain	If the chain is valid and it should longer then replace the current chain with a new chain	The chain was valid and shorter but was still replaced with a new chain	Failed
TC 07	Do not replace chain if less than or equal length	It should not replace the current chain	Not replace the current chain	Pass

Table 8.5: Test cases for wallet module testing

TC-ID	**Test case**	**Expected outcome**	**Actual outcome**	**Result**
TC 01	clones the 'sendAmmount' output for a recipient	It should map the sent amount for both sender and recipient	It maps the sent amount for both sender and recipient	Pass

TC 02	calculates the balance for blockchain transactions matching recipients	It should calculate the current balance of recipient by auditing block chain records	It calculates the current balance of recipient by auditing block chain records	Pass
TC 03	calculates the balance for blockchain transactions matching the sender	It should calculate the current balance of sender by auditing block chain records	It calculates the current balance of sender by auditing block chain records	Pass
TC 04	calculates recipient balance only using transactions since its most recent one	It should Calculate the recipient balance by auditing only latest transaction	It Calculates the recipient balance by auditing only latest transaction	Pass

Table 8.6: Test cases for transaction module testing

TC-ID	**Test case**	**Expected outcome**	**Actual outcome**	**Result**
TC 01	Outputs the 'amount' subtracted from wallet balance	It should display an updated balance of sender after a debit transaction	Display updated balance of sender after a debit transaction	Pass
TC 02	Outputs the 'amount' added to the recipient	It should display an updated balance of recipient after a credit transaction	Display updated balance of recipient after a credit transaction	Pass
TC 03	Inputs the balance of wallet	It should allow a transaction with a complete balance of sender	Allow transaction with a complete balance of sender	Pass

TC 04	Validates a valid transaction	It should verify the transaction by auditing blockchain records and signatures	Verify the transaction by auditing blockchain records and signatures	Pass
TC 05	Invalidates a corrupt transaction	It should reject transaction by auditing blockchain records and signatures	Reject transaction by auditing blockchain records and signatures	Pass
TC 06	Does not create a transaction	It should not prevent transaction where the amount is less than current balance	Did not prevent transaction when the amount was less than current balance	Failed

TC 07	Subtract nextAmmount from senders output	It should update the sender balance by subtracting nextAmmount	Update the sender balance by subtracting nextAmmount	Pass
TC 08	Outputs an amount for nextReciepient	It should update the recipient balance by adding nextAmmount	Update the recipient balance by adding nextAmmount	Pass
TC 09	Reward the miner's wallet	The miner should receive correct mining reward	The miner receive correct mining reward	Pass

Table 8.7: Test cases for transaction-pool module testing

TC-ID	**Test case**	**Expected outcome**	**Actual outcome**	**Result**
TC 01	Add a transaction to the transaction-pool	It should add new transaction into the transaction-pool	Add new transaction into the transaction-pool	Pass
TC 02	Updates a transaction in a pool	It should update existing transaction into the transaction-pool	Failed to update existing transaction into the transaction-pool	Failed
TC 03	Clears transaction	It should remove the mined transaction from the transaction-pool	Remove mined transaction from the transaction-pool	Pass
TC 04	shows a difference between valid and corrupt transactions	It should differentiate valid and corrupt transaction	Differentiate valid and corrupt transaction	Pass

TC 05	grabs valid transactions	It should only mine valid transaction	Only mine valid transaction	Pass

8.4 Security testing

Security testing is a type of software testing that intends to uncover vulnerabilities of the system and determine that its data and resources are protected from possible intruders.

Table 8.8: Security Testing

TC-ID	**Test case**	**Expected outcome**	**Actual outcome**	**Result**
TC 01	No user data is gathered anonymously	The system should not gather data without any intention	The system does not gather data without any intention	Pass

TC 02	No unauthorized access to DB	The only an authorized person should be given access to modify the database	An only an authorized person has access to modify the database	Pass
TC 03	No unauthorized write access to blockchain without POA	Without POA signature write to blockchain should fail	Without POA signature write to blockchain should fail	Pass
TC 04	No unauthorized access to the user account	User account should only be accessed with correct authentication detail	User account only access with correct authentication detail	Pass

8.5 Acceptance testing

Acceptance testing is a level of software testing where a system is tested for acceptability. The purpose of this test is to evaluate the system's compliance with the business requirements and assess whether it is acceptable for delivery.

The acceptance testing can be done via various methods. Here online survey

method is used. An online survey is a structured questionnaire that your target audience completes over the internet generally through a filling out a form. Online surveys can vary in length and format. Analytics are performed to achieve insights into data.

The category of users: The figure below depicts that the majority of users entrusted with testing the system were naïve. A fair part i.e. about 24% were beginners and the remaining were fairly competent in using such software.

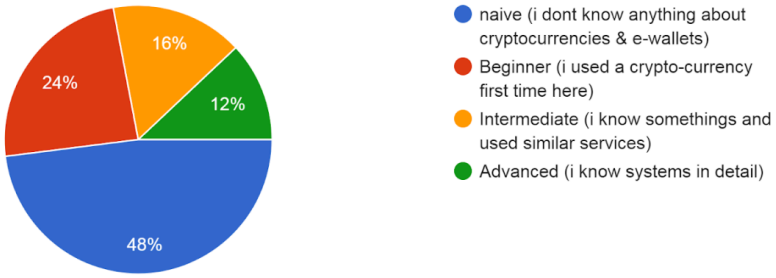


Figure 8.1: Category of users

Address book: As shown in figure below, 98% of the users find the tool of address book helpful.

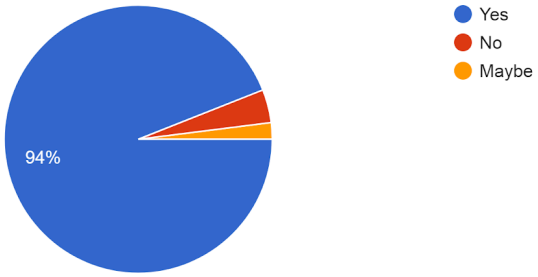


Figure 8.2: Address book

Preferred key management policy: As expected, a majority of users chose the automatic KMS policy. While a fair share chose to have a recoverable passphrase for their operations. A minority of users opted to not save private key any form.

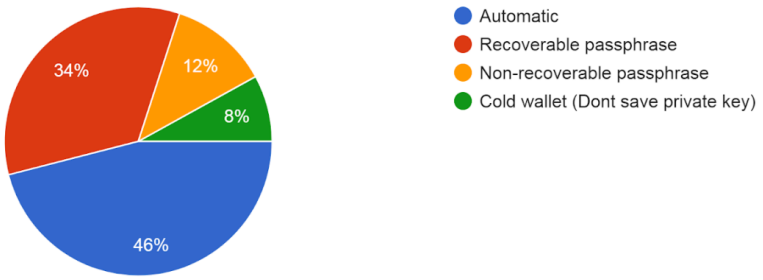


Figure 8.3: Preferred KMS

Ease of use: A whopping 94% of users found the website very easy to use.

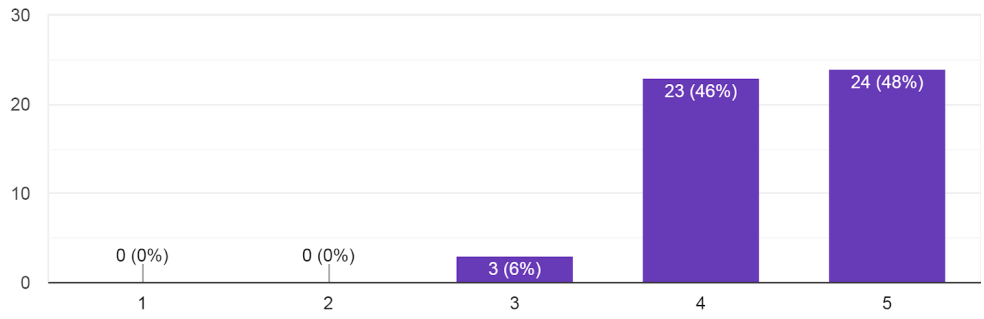


Figure 8.4: Ease of use

Overall satisfaction: Almost all the users were satisfied with their experience when using the webite.

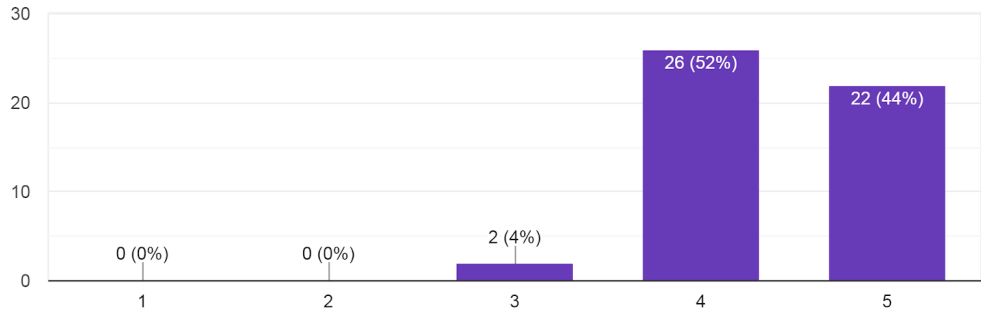


Figure 8.5: Overall satisfaction

Recommendation to other users: Among all the users who were entrusted with testing the website, a major part of them would happily recommend it to others

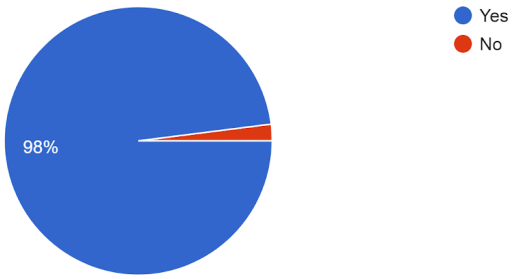


Figure 8.6: Recommendation to other users

8.6 Summary

In this chapter, we have tested our system using different forms of testing. We performed and recorded testing results of different test cases.The product is secure from different types of attacks and external threats. The testing allowed us to record the product performance and efficiency. The outcome of acceptance testing is positive, meaning the users are satisfied with the product.

Chapter 9

Results

9.1 Outcomes

- A generalized blockchain API was created which could be used to create various project models like voting systems, crypto currencies etc.
- A cryptocurrency model was created using the above stated blockchain API with higher security, robustness and availability.
- An e-wallet was designed with reference to the cryptocurrency model to access and control the currency transactions.
- The system was deployed over the cloud platform, which showcased reliable speed, performance and scalability of the system.

9.2 Screenshots

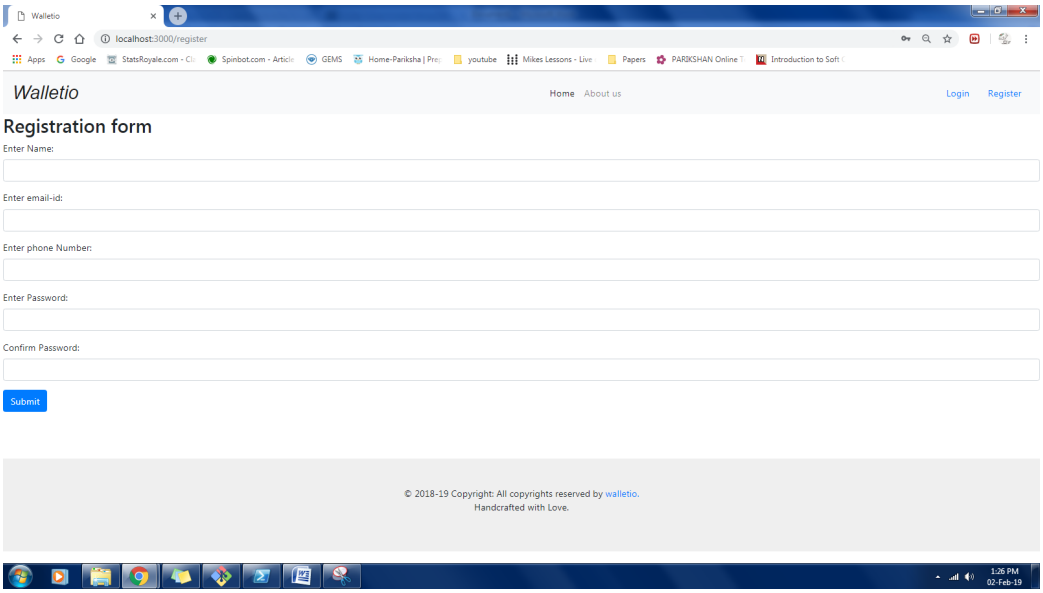


Figure 9.1: Register page

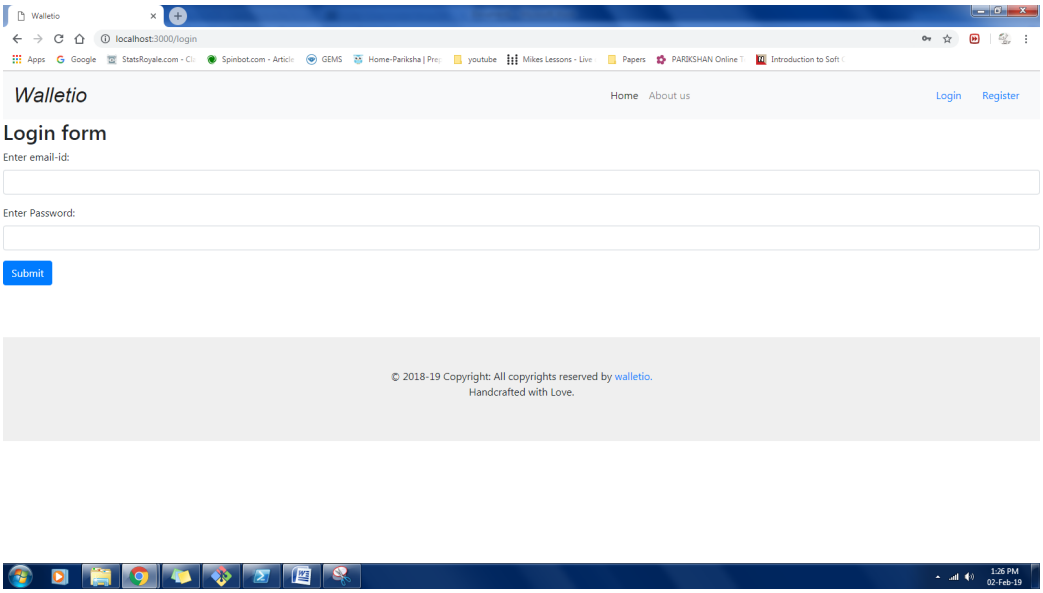


Figure 9.2: Login page

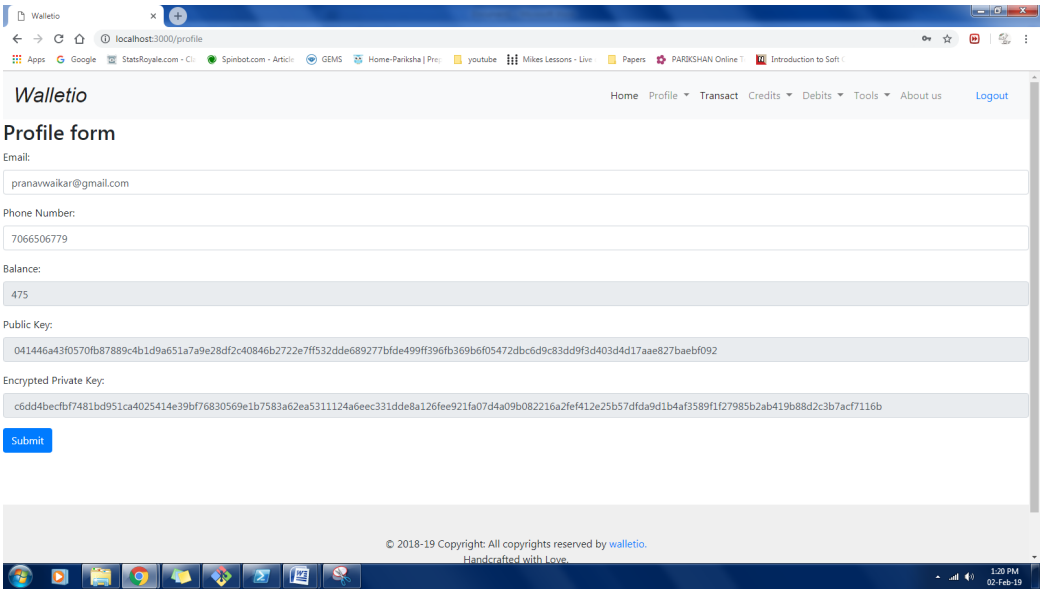


Figure 9.3: Profile page

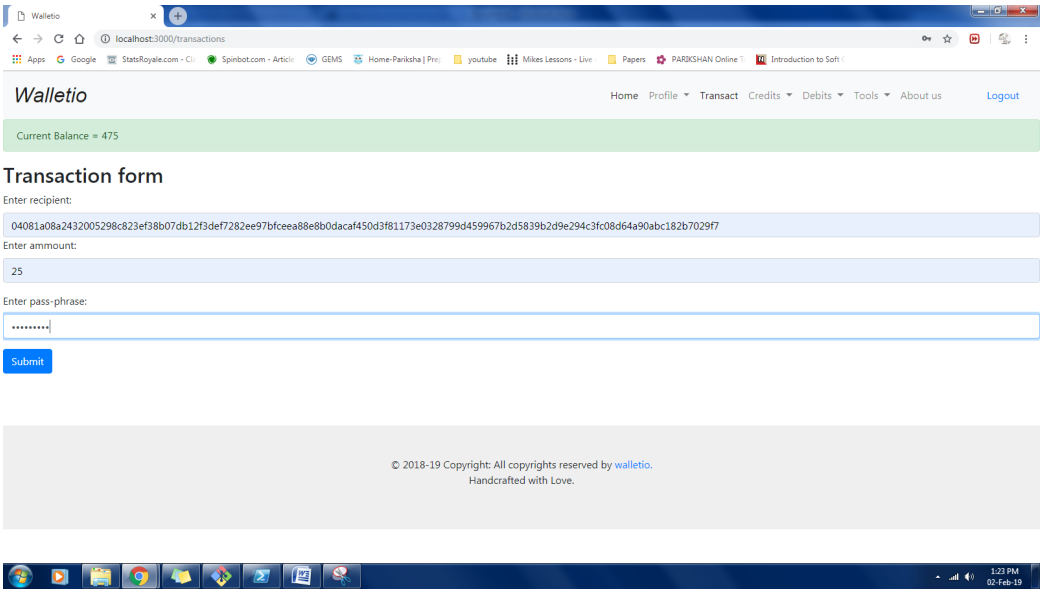


Figure 9.4: Transact page

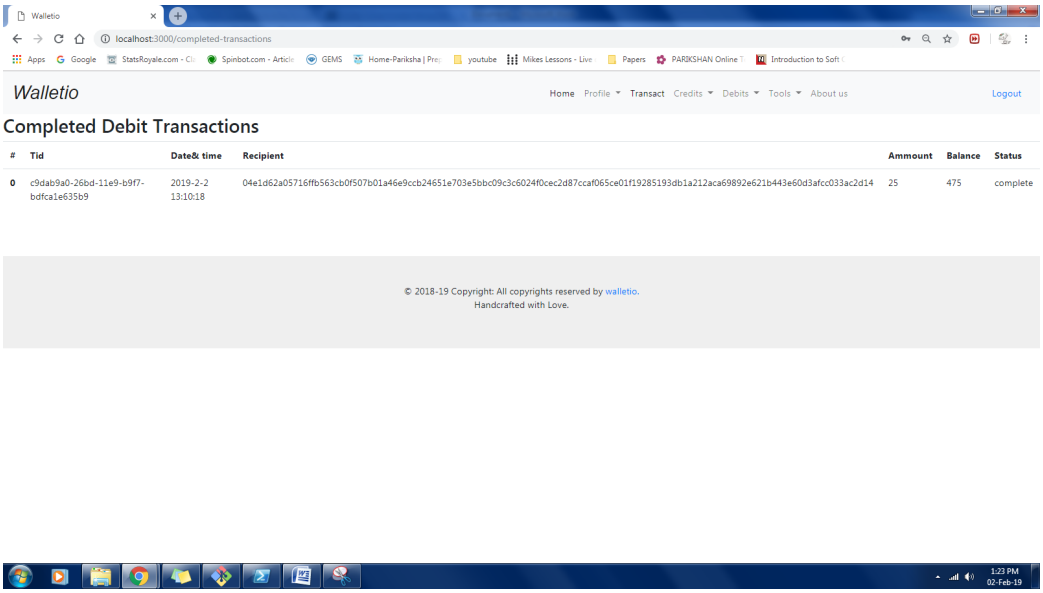


Figure 9.5: Transaction History

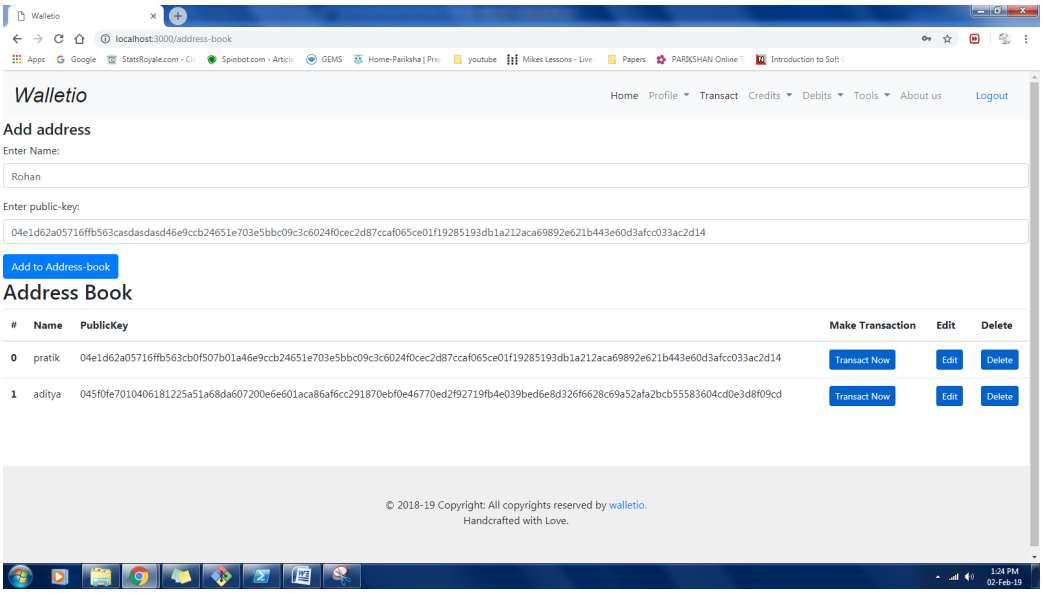


Figure 9.6: Address book

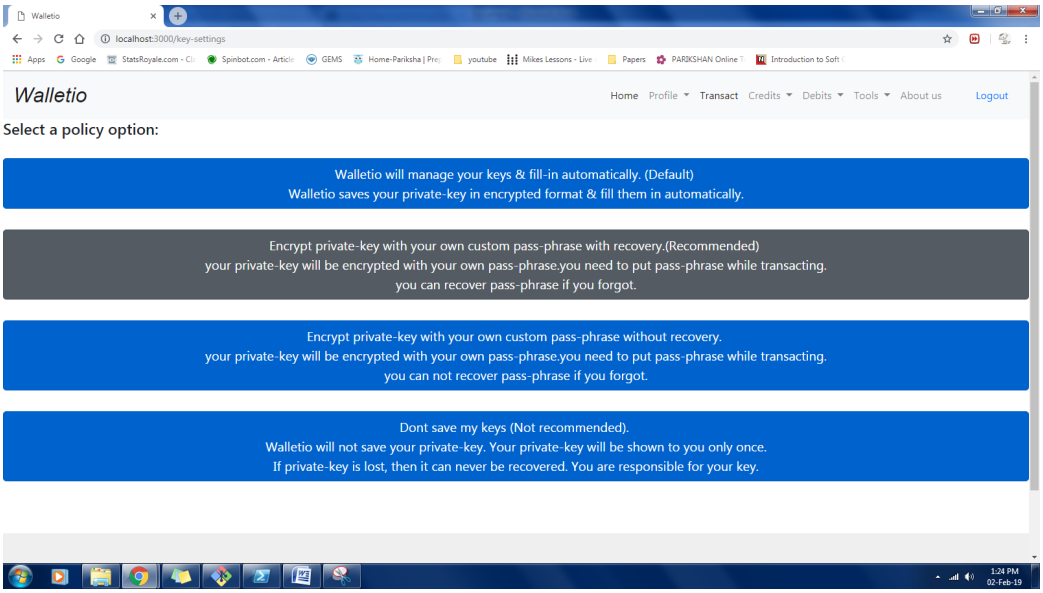


Figure 9.7: Key Management policies

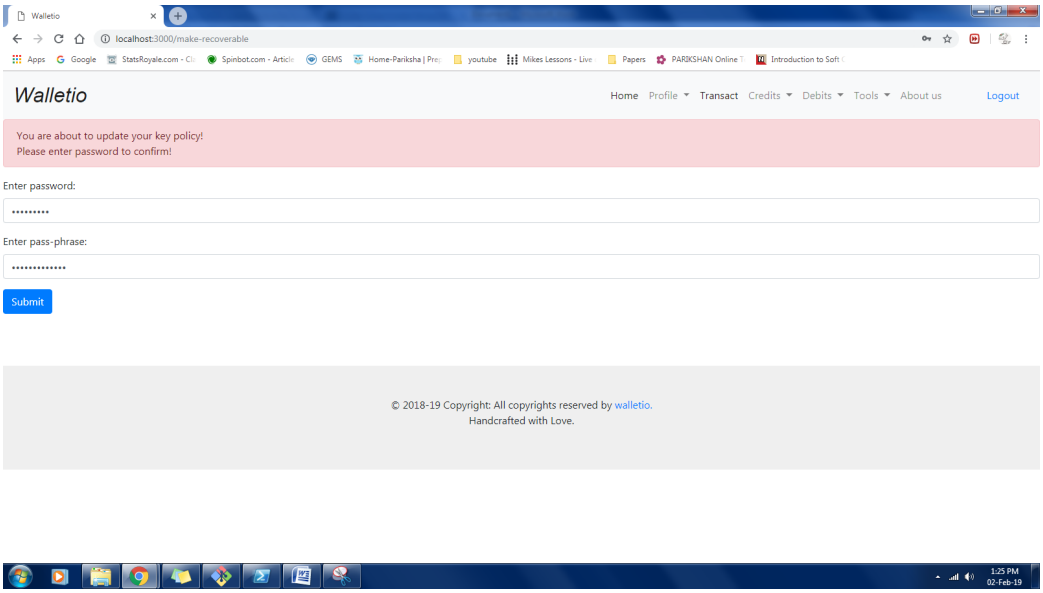


Figure 9.8: Key Management confirmation page

Chapter 10

Conclusions

"A Blockchain based cryptocurrency development of an e-wallet" project led to development of a generalized blockchain API, with the help of which a new cryptocurrency model was implemented along with the development of an e-wallet so as to access the aforementioned cryptocurrency. The main objective of the project was to create a new blockchain based cryptocurrency model which was more secure, robust and faster than the current cryptocurrencies in the market.

The cryptocurrency model was implemented along with a website acting as an e-wallet. The users were then asked to review the website which revealed the usefulness of the address book and Key Management Services(KMS).

This report is a detailed document of the methods used in the implementation of the project along with the relevant theory and practical. It also contains all the testing scenarios, their results and relevant data. This document can be considered for improvement to the cryptocurrency models or the API's used to create them in the future.

Our cryptocurrency model is robust, faster, secure and adaptable compared to the current cryptocurrency models in the market which makes it a

highly viable alternative to the conventional currency models. The e-wallet with its KMS and address-book also will surely help even the naive users to easily make effective use of the e-wallet.

10.1 Future work

1. With a possibility of cryptocurrency being floated on NASDAQ, the credibility of blockchain would be enforced along with its uses as an alternative to the conventional currency.

2. Cryptocurrencies being mathematically complex can further help avoid fraud and hacker attacks, but also easy for consumers to understand. Since it is decentralized it provides the consumer with adequate safeguards to preserve the anonymity of the user.

3. The cryptocurrency automatically regulates the value of its token, based on the number of users in the system, which is not possible with conventional currencies and often leads in a bubble.

4. Online exchange platforms can be used to convert virtual currencies into a physical form which can be further taxes helping in the legalization of cryptocurrencies along with the ability to monitor transactions.

5. The blockchain based API can further be used to create other applications like a voting system or admission process.

6. Blockchain-based cryptocurrencies can be used in the future up and coming Indian companies as payment or tokens.

7. The shadow ban by the Indian government on virtual currencies ay deter new users, but steps are being taken to regulate, monitor and

accept them via the use of regulation, identification, security checks etc.

8. In the case of conventional currencies failing in the future, cryptocurrencies can pose as viable step-in or replacement.

9. Different approaches may be used in consensus protocols and storage mechanisms in the future which might lead to better performance and efficiency.

Appendix A

Published paper list:

- P. Waikar, P. Deshmukh, R. Patel, A. Kulkarni, and S. Pawar, "A Survey on Blockchain based Cryptocurrency an e-Wallet," pp. 10271–10277,2018.
- P. Waikar, P. Deshmukh, R. Patel, A. Kulkarni, and S. Pawar, "A Blockchain based cryptocurrency the development of an e-wallet ," pp. 22251–22258,2019.

List of project competition participated:

- Ideazzz 2K18 project concept competition.
- CSI regional level project competition 2019.

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

A survey on Blockchain based cryptocurrency & an e-wallet

Pranav Waikar [1], Pratik Deshmukh[2], Rohan Patel[3], Aditi Kulkarni[4], Sudam Pawar[5]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[1]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[2]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[3]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[4]

Professor, Department of Computer Engineering, SITS, Narhe, Pune, India[5]

ABSTRACT: The regular currency has grown to reveal many drawbacks such as unavailability; it‘s proneness to be stolen and the fact that it is regulated strictly by an authority. Cryptocurrencies bypass most of our regular currency‘s drawbacks. Cryptocurrencies have emerged as a boastful financial system. They depend upon secure distributed ledger data structure. Mining plays an important part in this system. Mining helps add records of all past transactions to the ledger known as blockchain, which in turn allows users to have a currency with secure, robust consensus for every transaction that occurs in that block. Cryptocurrencies lack a central authority since they are designed as a peer-to-peer system. And every transaction has a record of it stored on every block thus eliminating any misuse. Basically, our cryptocurrency is a distributed database which maintains a growing tamper-proof data structure blocks which hold batches of individual transactions. The verified blocks are then added to the chain in a linear and chronological order. This forms a blockchain which is the core part of our cryptocurrency. A blockchain is a linear chain of Cryptocurrencies are the need of the future and they are helping shape the future of banking, financial institutions and the advent of the Internet of Things.

KEYWORDS: Blockchain, cryptocurrency, distributed ledger, wallets.

I. INTRODUCTION

The blockchain is an appropriated and decentralized record that stores information as exchanges and that is freely shared over every one of the hubs of its system. Presently let see what is a record, Ledger is a record that stores all the exchange of an association. The record is conveyed in the system. Each duplicate of the record is put away in this exchange book.

Blockchain innovation backs up Bitcoin and different digital forms of money right up 'til today, however, there's been an ongoing groundswell of enthusiasm from an assortment of ventures in making appropriated record innovation work, particularly in business. Here's an introduction on what blockchain innovation is, the means by which it works, and where it is demonstrating the most guarantee in the business. By outline, a blockchain is impervious to change of the information. It is "an open, dispersed record that can record exchanges between two gatherings effectively and in an evident and perpetual way Once recorded, the information in some random block can't be modified retroactively without change of every consequent block, which requires an agreement of the system lion's share.

In spite of the fact that blockchain records are not unalterable, blockchains might be viewed as secure by outline and embody a circulated processing framework with high Byzantine adaptation to internal failure. Decentralized accord has subsequently been asserted with a blockchain. Blockchain was developed by Satoshi Nakamoto in 2008 to fill in as the

 DOI:10.15680/IJIRSET.2018.0710001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

general population exchange record of the digital currency bitcoin. The development of the blockchain for bitcoin made it the principal advanced money to take care of the double spending issue without the requirement for a confided in power or focal server. The bitcoin systems have motivated different applications, and blockchains which are coherent by the general population are broadly utilized by cryptographic forms of money. Private blockchains have been proposed for business utilize. Some advertising of blockchains has been designated "a snake oil".
Paper is organized as follows. Section II describes background and current work. The Section III describes the problem definition in detail. Section IV describes the design & methodology for suggested problem definition with UML diagrams. Finally, Section V presents conclusion.

II. LITERATURE SURVEY

Sr no	Paper title	General idea	Advantages & limitations
1	Blockchain and Cryptocurrencies: Model, Techniques, and Applications [2018]	A survey of current cryptocurrencies to understand blockchain & its different types.	**Advantages:** Provides different incentive models, ecosystem & applications of the blockchain. Explains blockchain in a layered architecture. **Limitations:** Does not provide any solid architecture for its stated application.
2	A Brief Survey of Cryptocurrency Systems[2017]	It evaluates the strengths, weaknesses, and possible threats to all major mining strategy. It outlines how Cryptocurrencies mine, where they have comparable performance and assurance, and where they have unique threats and strengths.	**Advantages:** 1. Currently, major Cryptocurrencies use Proof of Work, Proof of Stake or a combination of the both for mining. 2. A combination of the both is found to be effective. 3. Typically memory-intensive hash functions have been found to be faster mining algorithms. **Limitations:** A majority of hash algorithms are CPU-intensive and the others are memory intensive. 2. While Proof of Work is resource intensive, Proof of Stake cannot act independently. 3. Cryptocurrencies are still experimenting with their mining protocols and algorithms to optimize their performance. No full proof algorithm has been found yet.

 DOI:10.15680/IJIRSET.2018.0710001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

3	Blockchain: Future of Financial and Cyber Security[2016]	This paper explains the concept, characteristics, need for Blockchain and how Bitcoin works. It attempts to highlights role of Blockchain in shaping the future of banking.	**Advantages:** 1.The decrease in device cost 2.Increases computing power **Limitations:** 1. If an attack was done by an attacker then there will be a loss of all bitcoins, we can't recover it because the government is not involved in
4	Bitcoin: A Peer-to-Peer Electronic Cash System[2008]	A distributed peer to peer system working under the blockchain framework	**Advantages:** Cryptocurrency without any central authority. Successful POW mechanism. **Limitations:** The cost of POW consensus protocol will keep increasing as more people join the network.
5	Trust Your Wallet : a New Online Wallet Architecture for Bitcoin [2017]	It introduces a wallet which is highly secured by Multiple signatures.	**Advantages:** The scalability of disaster recovery center **Limitations:** If we lost one of the keys then we are not able to recover that key.
6	A survey on the security of blockchain systems [2017]	Detail survey of the security issues in current systems and existing solutions	**Advantages:** A careful comparison between bitcoin and ethereum. Different aspects of system vulnerability **Limitations:** Cryptocurrency will need more methods to achieve security and privacy.

Table 1.1: Literature review

The above table 1.1 describes the literature survey. The table describes about the details about the paper with the general idea of the paper with its advantages & limitations. It helps to understand the workings of the current system & the limitations of the system which are required to overcome for betterment of the system. The next section defines the solution for the limitations.

 DOI:10.15680/IJIRSET.2018.0710001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

III. PROBLEM DEFINITION:

Aim:
To create a de-centralized blockchain based cryptocurrency and an e-wallet to access currency.

Problem statement:
1. Creating a crypto-currency with proof-of-authority but without a central point of failure.
2. Generalized public blockchain API.
3. A hybrid consensus protocol for blockchain.
4. A secure and high availability e-wallet for easy to facilitate transactions.

Objective:
The objective of this project to create a de-centralized blockchain based cryptocurrency and an e-wallet to access currency. The project entails creating a generalized blockchain API which can later be used for further development in the blockchain field of applications. This blockchain API will be used to construct a cryptocurrency from scratch. Implement a new hashing function for the blockchain which will take data and create a fixed length output. Implementing a highly secure and personal e-wallet system to access and control the said cryptocurrency. This e-wallet system will let the user control and transact the currency efficiently. It provides the user with full authority over the token currencies. The aim is also to make the currency secure, easy to access, fast and as cheap to avail as possible.

IV. PROPOSED ARCHITECTURE

As shown in figure 1.1, suppose party A wants to transfer some currency over to party B. Then by the wallet interaction, party A can start the transaction over to party B. The transaction is represented online as a block.
The block is then broadcasted to every party in the network. The network as a whole will approve the transaction to be valid or invalid by using the distributed ledger. Then by some consensus protocol block will get added to the distributed ledger. In this way, the transaction for transferring money from A to B is completed successfully.

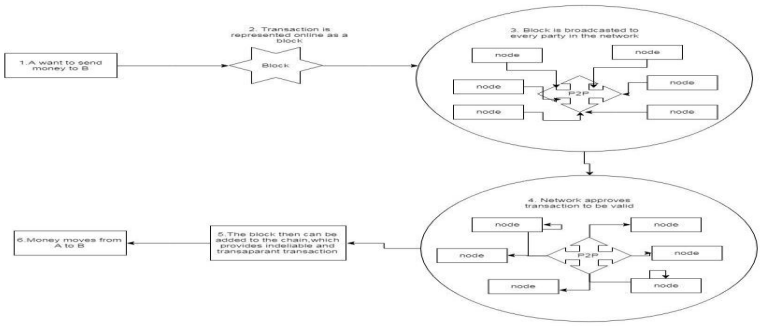


Fig 1.1 System architecture

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

Activity diagram:
In figure 1.2, user access wallet website and authenticate by referencing the database. After a successful login, the user can input transaction details and then start a transaction. The important details are verified with database and transaction is created in cryptocurrency network. The miners will then verify and validate the transactions. After that block gets added into blockchain. The changes are acknowledged by cryptocurrency model. The transaction details are recorded into the database. The result is displayed to the user by the wallet.

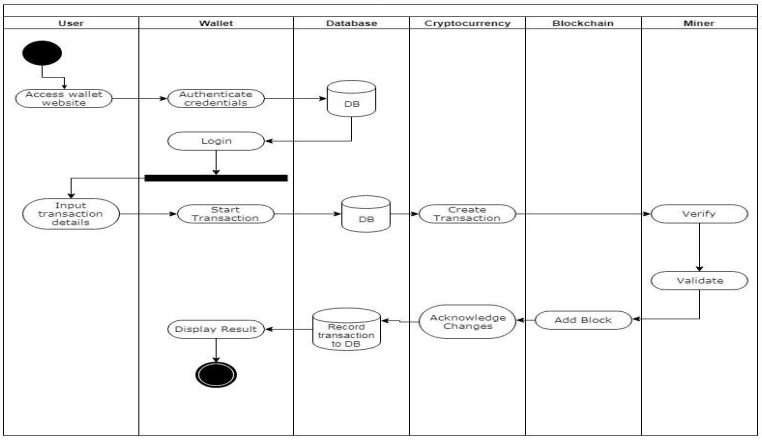


Figure 1.2 Swim lane activity diagram

Algorithms:

1. Secure Hashing Algorithm (SHA)-2:
The SHA version 2 provides various different hash functions with various output bit length & input. The SHA-256 is a novel hash function which works on 32bit words respectively. SHA-256 has ability work on x86 as well as x86-64 based architecture.

2. Consensus protocols:
The process of achieving single data value among the distributed or decentralized system is known as consensus protocol. The main goal is to achieve reliability in the system of unreliable nodes. These are also known as mining algorithms. The system will use a hybrid model of proof-of-work and proof-of-authority. The Proof-of-work uses a computational puzzle which needs to be solved by random guessing. Once the solution is found anyone can check the answer easily for authenticity. The proof-of-authority provides comparatively fast transaction through consensus mechanism of identity as a stake.

 DOI:10.15680/IJIRSET.2018.0710001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

3. Elliptic curve cryptography(ECC):
ECC is an approach to public-key cryptography based on the algebraic structure of elliptic curves over finite fields. Elliptic curves are applicable for key agreement, digital signatures, pseudo-random generators, and other tasks. Indirectly, they can be used for encryption by combining the key agreement with a symmetric encryption scheme. [12]

4. Universally Unique Identifier (UUID):
UUID is also known as GUID. It is a 128-bit number used to identify information in computer systems. When generated according to the standard methods, UUIDs are for practical purposes unique, without depending for their uniqueness on a central registration authority or coordination between the parties generating them, unlike most other numbering schemes. While the probability that a UUID will be duplicated is not zero, it is close enough to zero to be negligible.[8]

5. Dynamic Difficulty mining algorithm:
Figure 1.3 shows the flowchart for dynamic difficulty mining algorithm. This algorithm is used to adjust the mining difficulty of the system automatically as per the specified mining rate. The difficulty parameter suggests how hard the hashing function should be for the proof-of-work algorithms.
The time difference between the last mined block and the newly mined block is compared with the specified mining rate. If the answer is less than the mining rate, the difficulty is increased. If the value is higher then the mining difficulty is decreased. This function is repeated for every new block inclusion into the system.

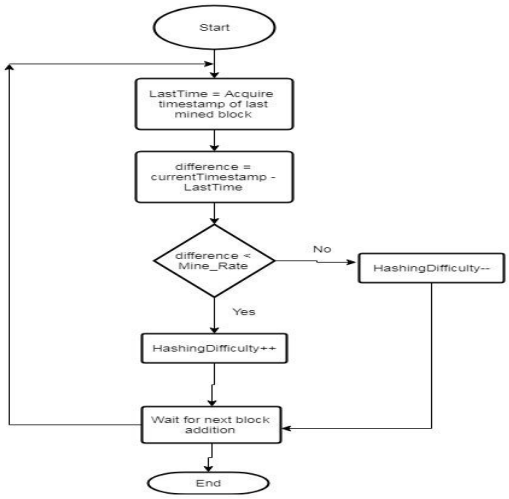


Fig 1.3: Dynamic difficulty mining

 DOI:10.15680/IJIRSET.2018.0710001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 7, Issue 10, October 2018

V. CONCLUSION

Thus, as we have already seen there is a need of a decentralized regulated transaction token or currency without a central point of failure. We have created a cryptocurrency from scratch which can be controlled using an e-wallet.
We have also created a generalized blockchain API which can further be used to develop applications in the blockchain domain. This purpose can be other than a cryptocurrency as well. A new hashing function was implemented to create fixed length output needed. The cryptocurrency is fast, secure and readily available. It implements a hybrid consensus protocol, meaning it combines two proofs to verify and validate transactions in the blockchain system, since PoW is expensive on the resources but not as good as PoS, PoA. Any transaction needs to be verified by miners like all the other prevalent cryptocurrencies. The difficulty of the function to be solved to verify transactions is set to be dynamic and is set such so that it does not cause either inflation or recession of the currency. The system is built as a peer-to-peer system, thus all the users depend on each other for the proper functionality of the system. An efficient data clean-up and detection mechanism has been implemented to improve the execution efficiency of blockchain systems. An e-wallet which is secure, fast and highly accessible has been implemented which can be used by the user to interact and control the cyrptocurrency. This e-wallet creates a public as well as private key bind to the user which can be used in various transactions over the currency.

REFERENCES

[1] Y. Yuan, S. Member, and F. Wang, ―Blockchain and Cryptocurrencies: Model, Techniques, and Applications,‖ IEEE Trans. Syst. Man, Cybern. Syst., vol. PP, pp. 1–8, 2018.
[2] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, ―A Brief Survey of Cryptocurrency Systems.‖
[3] S. Singh, ― Blockchain: Future of Financial and Cyber Security,‖ pp. 463–467, 2016.
[4] S. Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System,‖ Www.Bitcoin.Org, p. 9,2008.
[5] F. Zhu et al., ―Trust Your Wallet: a New Online Wallet Architecture for Bitcoin,‖ 2017.
[6] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ―A survey on the security of blockchain systems,‖ Futur. Gener. Comput. Syst., 2017.
[7] R. Lai and D. LEE Kuo Chuen, Blockchain – From Public to Private, 1st ed., vol. 2. Elsevier Inc., 2018.
[8] http://www.wikiwand.com/en/Universally_unique_identifier
[9] https://hackernoon.com/types-of-consensus-protocols-used-in-blockchains-6edd20951899
[10] https://en.wikipedia.org/wiki/SHA-2
[11] https://en.wikipedia.org/wiki/Blockchain
[12] https://en.wikipedia.org/wiki/Elliptic-curve_cryptography
[13] https://en.wikipedia.org/wiki/Cryptocurrency
[14] https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/
[15] https://coinsutra.com/future-of-bitcoin-cryptocurrency-india/

 DOI:10.15680/IJIRSET.2018.0710001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

A Blockchain based cryptocurrency & the development of an e-wallet

Pranav Waikar [1], Pratik Deshmukh[2], Rohan Patel[3], Aditi Kulkarni[4], Sudam Pawar[5]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[1]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[2]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[3]

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India[4]

Professor, Department of Computer Engineering, SITS, Narhe, Pune, India[5]

ABSTRACT: The blockchain technology underlying the cryptocurrencies have the potential to be the future of finance. It can revolutionize the way all transactions works today. The underlying blockchain technology can provide a solid base for a fully autonomous system that could govern. Its potential is not just about the transactions with the cryptocurrency but can extend far beyond that. cryptocurrencies are cryptographically secure, publically owned by user & highly available. The regular currency has grown to reveal many drawbacks such as unavailability, Cryptocurrencies bypass most of our regular currency's drawbacks. They depend upon a secure distributed ledger data structure. Mining helps add records of all past transactions to the ledger known as the blockchain, which in turn allows users to have a currency with secure, robust consensus for every transaction that occurs in that block. Our cryptocurrency is a distributed database which maintains a growing tamper-proof data structure blocks which hold details of individual transactions. The verified blocks are then added to the chain in a linear and chronological order. This forms a blockchain which is the core part of our cryptocurrency.

KEYWORDS: Blockchain, cryptocurrency, distributed ledger, e-wallets.

I. INTRODUCTION

The blockchain is a transaction database which has information about every transaction ever executed in the past and works on the Bitcoin protocol. It creates a digital ledger of transactions and allows all the participants on the network to edit the ledger in a secure way which is shared over a distributed network of the computers For making any amount of changes to the block of data, all the nodes present in the network run algorithms to evaluate, verify and match the transaction information with its history. If the majority of nodes agree in favor of the transaction, it is approved and a new block gets added to the existing chain. In this, we are using (SHA-256) genetic algorithm to secure the chain. Every block contains a hash of parent block in its own header and the sequence of hashes linking individual block with their parent block creates a big chain pointing to the first block called Genesis block. The term private blockchain (permissioned ledger) refers to Blockchain that requires authentication of participant identities and authorization of participant's permission-level of access on the Blockchain This writing will use Private Blockchain to refer to Permissioned Ledger as well. The term public blockchain (permissionless ledger).Mining validates transactions and adds them to this public ledger. When a new transaction takes place, the miner checks if the currency belongs to the payer, or if the payer is trying to double spend. The resource-intensive task can be any of the following: Proof of Work, Proof of Stake, or Proof of Retrievability.

Paper is organized as follows. Section II describes related work. Section III describes the problem definition. Section IV describes the implementation. Section V describes the testing and result. Finally, Section VI presents the conclusion.

 DOI:10.15680/IJIRSET.2019.0805001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

II. RELATED WORK

no	Paper title	General idea	Advantages	Limitations
1	Blockchain and Cryptocurrencies: Model, Techniques, and Applications [2018]	A survey of current cryptocurrencies to understand blockchain & it's different types.	Provides different incentive models, ecosystem & applications of the blockchain.	Does not provide any solid architecture for its stated application.
2	Blockchain: Future of Financial and Cyber Security[2016]	This paper explains the concept, flows, need for Blockchain and Bitcoin works.	The decrease in device cost and Increases computing power.	If an attack was done by an attacker then there will be a loss of all bitcoins.
3	Bitcoin: A Peer-to-Peer Electronic Cash System[2008]	A distributed peer to peer system working under the blockchain framework.	Cryptocurrency without any central authority.Successful POW mechanism.	The cost of the POW consensus protocol will keep increasing as more people join the network.
4	Trust Your Wallet : a New Online Wallet Architecture for Bitcoin [2017]	It introduces a wallet which is highly secured by Multiple signatures.	The scalability of the disaster recovery center.	If we lost one of the keys then we are not able to recover that key.
5	A survey on the security of blockchain systems [2017]	Detail survey of the security issues in current systems and existing solutions.	A careful comparison between bitcoin and ethereum. Different aspects of system vulnerability.	Cryptocurrency will need more methods to achieve security and privacy.

Table 1. 1: A Literature review [1]

The table above represents the literature review. It explains the paper name with its general idea with some advantages and limitations derived.

III. PROBLEM STATEMENT

To create crypto-currency with proof-of-authority but without a central point of failure by creating generalized public blockchain API with a hybrid consensus protocol for blockchain as well as a secure and high available e-wallet for easy to facilitate transactions. [1]

IV. IMPLEMENTATION

The Blockchain: The fig below represents the flowchart for the operation of the blockchain based systems. At the time of the creation of blockchain, the first block ie genesis block is added into the chain. To add subsequent blocks, new data accepted from the user. The last block of the chain is acquired & hash & difficulty fields are extracted from it. The default nonce value is zero. The current timestamp is then acquired. The SHA256 hash is generated taking data, nonce, difficulty, last hash, timestamp as an input. The condition for POW consensus protocol is the generated hash value should have a prefixed number of zeros equal to the difficulty level. The POW is like solving the computational puzzle. Till the desired condition is achieved, the nonce & timestamp changes & every time a new hash value is generated. After a successful attempt, the value is stored as a hash of that block & block is added at the end of the chain. Refer to figure 1.1.

 DOI:10.15680/IJIRSET.2019.0805001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

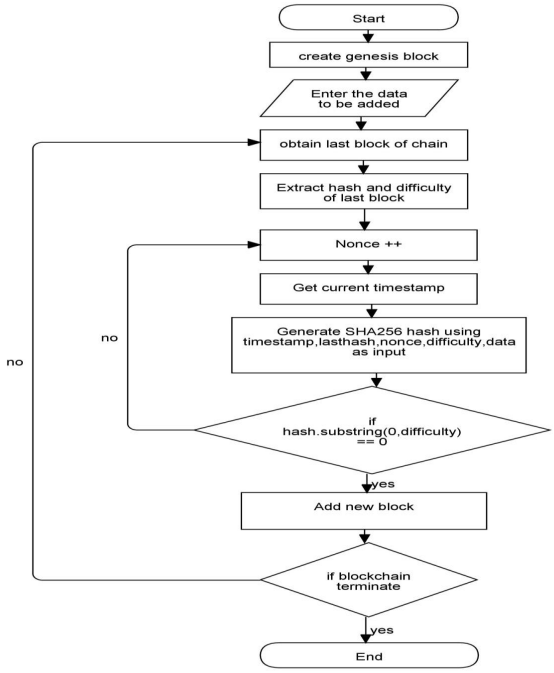


Fig 1.1: Blockchain flowchart

The cryptocurrency: The cryptocurrency model uses the blockchain technique to store & manipulate the data of transactions. The cryptocurrency model facilitates the creation & mining of transactions. The model allows sharing the transaction with multiple miners so that they could try to mine simultaneously & the one who wins will receive the reward. Also, the transaction data is shared between multiple nodes among those.

Creating a transaction: The algorithm is used to create a new transaction or update an existing transaction. The fig below shows the flowchart for the same. The balance is calculated first to verify the user has needed appropriate balance. If the balance is not enough then the transaction is not created. If the balance is enough then it is checked whether transaction already exists or not. If a transaction already exists then it is updated & updated transaction is broadcasted into the network. If the transaction does not exists then a new transaction is created with its UUID, the remaining balance is calculated and added as data of the transaction. The sender & recipient address, balance, amount & signature data used to create a new transaction. The transaction is broadcasted to the network using the transaction pool. Refer to figure 1.2.

 DOI:10.15680/IJIRSET.2019.0805001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

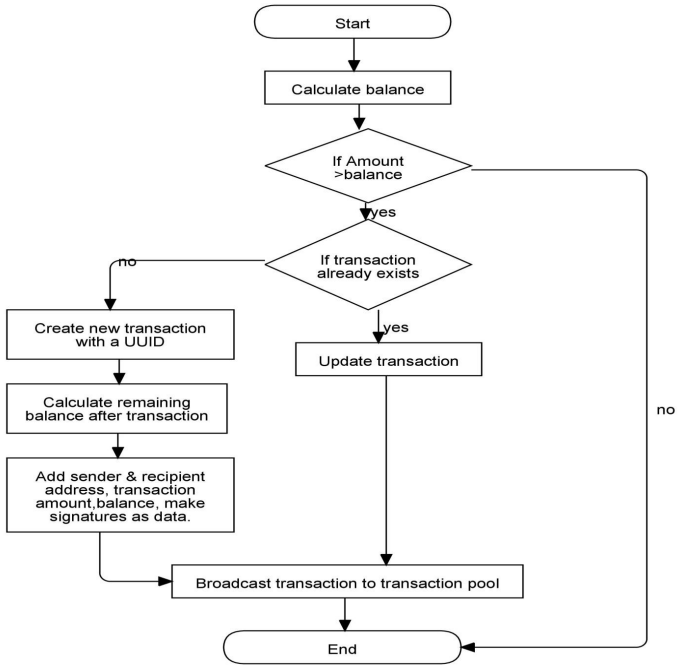


Fig 1.2: Transaction creation flowchart

Mining transactions: The algorithm is used to mine a transaction of the user from the transaction pool. The transaction is acquired from the transaction pool & the output amounts are calculated again for the validity. If invalid then it is rejected. If valid then the digital signature is checked for the correctness using the transaction data & public key of sender wallet. If invalid then the transaction is rejected. Mining starts using POW consensus protocol if valid.
After that reward transaction for a miner is created. All this information stored in the block then added to the blockchain. This newly added block is broadcasted over the network.

The wallet: This is the general flow of the wallet server. The wallet server first generates a proof-of-authority (POA) digital signature. The POA signature is then verified. If verification is successful wallet server is initialized otherwise terminated. In this way, the online wallet service will always be verified. After successful verification, the wallet server is started at the determined port. On that specific port, the server starts providing services to different clients. Refer to figure 1.3.

 DOI:10.15680/IJIRSET.2019.0805001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

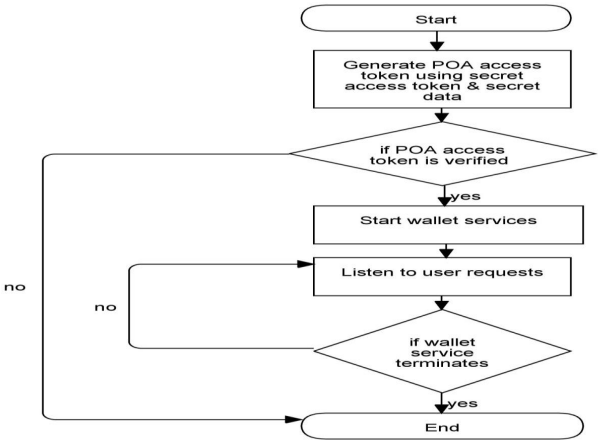


Fig 1.3: wallet flowchart

V. TESTING AND RESULTS

Performance testing: The memory space taken by each block affects performance as it is directly related to bandwidth parameters of the network. In this case each block measures around 100kb in size. It means each transaction upon adding into blockchain will consume 100kb space in memory over all the connected nodes. Another performance measure for a cryptocurrency is a number of transactions per second(TPS). Because of POW algorithm, TPS can be different for different machines. Refer to table 1.2.

Srno	Processor	RAM	TPS rate
1	Intel Core 2 Duo E7500	2 GB	100
2	Intel Core i3-8100	4 GB	106
3	Intel Core i3-6100	4 GB	103
4	Intel Core i7 7700K	8 GB	110
5	Intel Xeon E5-2686 v4 (Broadwell)	16 GB	119

Table 1. 2: Transaction rates

Acceptance testing: Acceptance testing can be done via various methods. Here online survey method is used. An online survey is a structured questionnaire that your target audience completes over the internet generally through a filling out a form.

The category of users: The figure below depicts that the majority of users entrusted with testing the system were naïve. A fair part i.e. about 24% was beginners and the remaining was fairly competent in using such software. Refer to figure 1.4.

 DOI:10.15680/IJIRSET.2019.0805001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

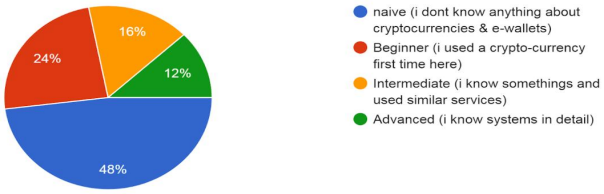


Figure 1.4: Category of users

Error occurrence in the system: The majority of users did not encounter any errors while navigating the system. 96% of users were satisfied with the experience of the system. Refer to figure 1.5.

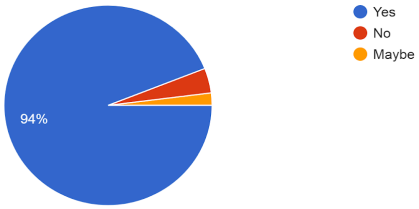


Figure 1.5: Error occurrence

Preferred key management policy: As expected, a majority of users chose the automatic KMS policy. While a fair share chose to have a recoverable passphrase for their operations. A minority of users opted to not save private key any form. Refer to figure 1.6.

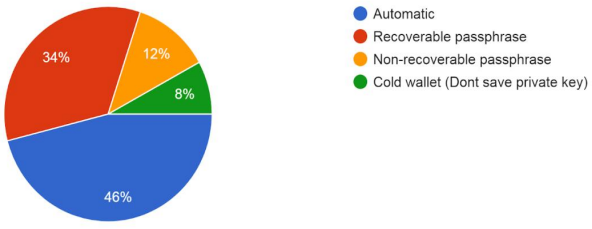


Figure 1.6: Preferred KMS

 DOI:10.15680/IJIRSET.2019.0805001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Ease of use: A whopping 94% of users found the website very easy to use. Refer to figure 1.7.

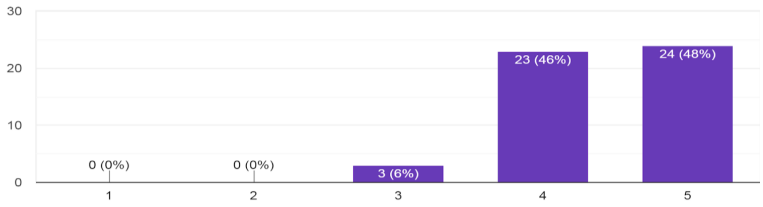


Figure 1.7: Ease of use

Overall satisfaction: Almost all the users were satisfied with their experience when using the website. Refer to figure 1.8.

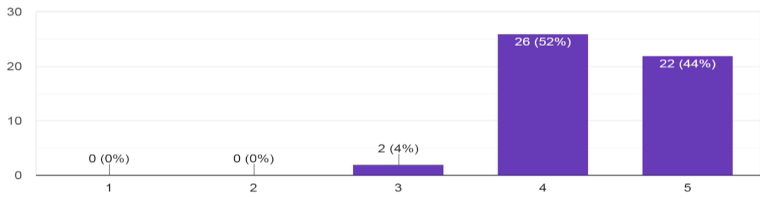
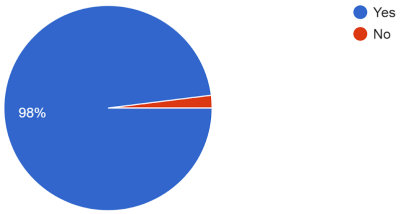


Figure 1.8: Overall satisfaction

Recommendation to other users: Among all the users who were entrusted with testing the website, a major part of them would happily recommend it to others. Refer to figure 1.9.



 DOI:10.15680/IJIRSET.2019.0805001

ISSN(Online): 2319-8753
ISSN (Print): 2347-6710

International Journal of Innovative Research in Science, Engineering and Technology

(A High Impact Factor, Monthly, Peer Reviewed Journal)

Visit: www.ijirset.com

Vol. 8, Issue 5, May 2019

Figure 1.9: Recommendation to others

Outcome: The outcomes of the project are as following:

- A generalized blockchain API was created which could be used to create various project models like voting systems, cryptocurrencies, etc.
- A cryptocurrency model was created using the blockchain API with higher security, robustness, and availability.
- An e-wallet was designed with reference to the cryptocurrency model to access and control the currency transactions.
- The system was deployed over the cloud platform, which showcased reliable speed, performance, and scalability of the system.

VI. CONCLUSION

Thus, "A Blockchain based cryptocurrency & development of an e-wallet" project led to development on a generalized blockchain API, with the help of which a new cryptocurrency model was implemented along with the development of an e-wallet so as to access the said currency. The main objective of the project was to create a new blockchain based cryptocurrency model which was more secure, robust and faster than the current cryptocurrencies in the market. The cryptocurrency model was implemented along with a website acting as an e-wallet to access the currency. The users were then asked to review the website which revealed the usefulness of the address book and Key Management policies (KMS). This report is a detailed document of the methods used in the implementation of the project along with the relevant theory and practical. It also contains all the testing scenarios, their results, and relevant data. This document can be considered for improvement to the cryptocurrency models or the API's used to create them. Our cryptocurrency model is robust, faster, secure and adaptable compared to the current cryptocurrency models in the market which make it a highly viable alternative. The e-wallet with its KMS and address-book also will surely help even the naïve users to easily make effective use of the e-wallet.

REFERENCES

[1]P. Waikar, P. Deshmukh, R. Patel, A. Kulkarni, and S. Pawar, "A Survey on Blockchain based Cryptocurrency & an e-Wallet," pp. 10271–10277, 2018.
[2] Y. Yuan, S. Member, and F. Wang, ―Blockchain and Cryptocurrencies: Model, Techniques, and Applications,‖ IEEE Trans. Syst. Man, Cybern. Syst., vol. PP, pp. 1–8, 2018.
[3] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, ―A Brief Survey of Cryptocurrency Systems.‖
[4] S. Singh, ― Blockchain: Future of Financial and Cyber Security,‖ pp. 463–467, 2016.
[5] S. Nakamoto, ―Bitcoin: A Peer-to-Peer Electronic Cash System,‖ Www.Bitcoin.Org, p. 9,2008.
[6] F. Zhu et al., ―Trust Your Wallet: a New Online Wallet Architecture for Bitcoin,‖ 2017.
[7] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, ―A survey on the security of blockchain systems,‖ Futur. Gener. Comput. Syst., 2017.
[8] R. Lai and D. LEE Kuo Chuen, Blockchain – From Public to Private, 1st ed., vol. 2. Elsevier Inc., 2018.
[9] http://www.wikiwand.com/en/Universally_unique_identifier
[10] https://hackernoon.com/types-of-consensus-protocols-used-in-blockchains-6edd20951899
[11] https://en.wikipedia.org/wiki/SHA-2
[12] https://en.wikipedia.org/wiki/Blockchain
[13] https://www.investopedia.com/tech/most-important-cryptocurrencies-other-than-bitcoin/
[14] https://coinsutra.com/future-of-bitcoin-cryptocurrency-india/
[15] https://github.com/pranavwaikar/cryptocurrency

 DOI:10.15680/IJIRSET.2019.0805001

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

PRANAV WAIKAR

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Survey on Blockchain based Cryptocurrency & an e-Wallet"

in IJIRSET, Volume 7, Issue 10, October 2018

Certificate No: V7110C013
Date: 15th October 2018

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

PRATIK DESHMUKH

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Survey on Blockchain based Cryptocurrency & an e-Wallet"

in IJIRSET, Volume 7, Issue 10, October 2018

Certificate No: V7110C014
Date: 15th October 2018

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

ROHAN PATEL

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Survey on Blockchain based Cryptocurrency & an e-Wallet"

in IJIRSET, Volume 7, Issue 10, October 2018

Certificate No: V7I10C015
Date: 15th October 2018

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

ADITI KULKARNI

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Survey on Blockchain based Cryptocurrency & an e-Wallet"

in IJIRSET, Volume 7, Issue 10, October 2018

Certificate No: V7I10C016
Date: 15th October 2018

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

SUDAM PAWAR

Professor, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Survey on Blockchain based Cryptocurrency & an e-Wallet"

in IJIRSET, Volume 7, Issue 10, October 2018

Certificate No: V7I10C017
Date: 15th October 2018

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

PRANAV WAIKAR

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Blockchain based Cryptocurrency & the Development of an e-wallet"

in IJIRSET, Volume 8, Issue 5, May 2019

Certificate No: V8I5C039
Date: 15th May 2019

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

PRATIK DESHMUKH

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Blockchain based Cryptocurrency & the Development of an e-wallet"

in IJIRSET, Volume 8, Issue 5, May 2019

Certificate No: V8I5C040
Date: 15th May 2019

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

ROHAN PATEL

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Blockchain based Cryptocurrency & the Development of an e-wallet"

in IJIRSET, Volume 8, Issue 5, May 2019

Certificate No: V8I5C041
Date: 15th May 2019

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

ADITI KULKARNI

U.G. Student, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Blockchain based Cryptocurrency & the Development of an e-wallet"

in IJIRSET, Volume 8, Issue 5, May 2019

Certificate No: V8I5C042
Date: 15th May 2019

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

INTERNATIONAL JOURNAL OF INNOVATIVE RESEARCH IN SCIENCE, ENGINEERING AND TECHNOLOGY

ISSN (Online) : 2319 – 8753 ISSN (Print) : 2347 - 6710

IJIRSET

PUBLICATION CERTIFICATE

This is to certify that

SUDAM PAWAR

Professor, Department of Computer Engineering, SITS, Narhe, Pune, India

Published a research paper titled

"A Blockchain based Cryptocurrency & the Development of an e-wallet"

in IJIRSET, Volume 8, Issue 5, May 2019

Certificate No: V8I5C043
Date: 15th May 2019

IJIRSET
Impact Factor: 7.089
www.ijirset.com

Editor-in-Chief
IJIRSET

Sinhgad Technical Education Society
Sinhgad Institute of Technology and Science
Narhe,Pune-41
Sinhgad Institutes
Department of Computer Engineering
Ideazzz 2K18

Certificaate of Participation

This is to certify that Mr./Ms. Pranav Waikar from SITS [Computer] has participated in Ideazzz 2K18 Project Concept Competition under Blockchain domain held on 5th October 2018 at Sinhgad Institute of Technology and Science Narhe, Pune-41.

Faculty Co-ordinator Heads of Department Principal

MASS Technologies HERBALIFE NUTRITION Hackers_Era KasNet

Sinhgad Technical Education Society
Sinhgad Institute of Technology and Science
Narhe,Pune-41
Sinhgad Institutes
Department of Computer Engineering
Ideazzz 2K18

Certificaate of Participation

This is to certify that Mr./Ms. Rohan Patel from SITS [Computer] has participated in Ideazzz 2K18 Project Concept Competition under Blockchain domain held on 5th October 2018 at Sinhgad Institute of Technology and Science Narhe, Pune-41.

Faculty Co-ordinator Heads of Department Principal

MASS Technologies HERBALIFE NUTRITION Hackers_Era KasNet

Sinhgad Technical Education Society
Sinhgad Institute of Technology and Science
Narhe,Pune-41
Sinhgad Institutes
Department of Computer Engineering
Ideazzz 2K18

Certificaate of Participation

This is to certify that Mr./Ms. Aditi from SITS [Computer] has participated in Ideazzz 2K18- Project Concept Competition under Blockchain domain held on 5th October 2018 at Sinhgad Institute of Technology and Science Narhe, Pune-41.

Faculty Co-ordinator Heads of Department Principal

MASS Technologies HERBALIFE NUTRITION Hashem Era KasNet INDIA | USA

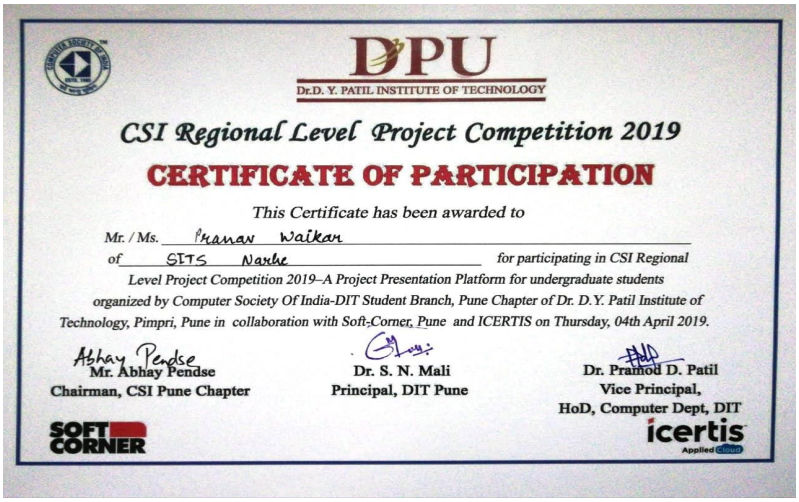
Sinhgad Technical Education Society
Sinhgad Institute of Technology and Science
Narhe,Pune-41
Sinhgad Institutes
Department of Computer Engineering
Ideazzz 2K18

Certificaate of Participation

This is to certify that Mr./Ms. PRATIK from SITS [Computer] has participated in Ideazzz 2K18- Project Concept Competition under Blockchain domain held on 5th October 2018 at Sinhgad Institute of Technology and Science Narhe, Pune-41.

Faculty Co-ordinator Heads of Department Principal

MASS Technologies HERBALIFE NUTRITION Hashem Era KasNet INDIA | USA



DPU
Dr.D. Y. PATIL INSTITUTE OF TECHNOLOGY

CSI Regional Level Project Competition 2019

CERTIFICATE OF PARTICIPATION

This Certificate has been awarded to

Mr. / Ms. Pranav Waikar

of SITS Narhe for participating in CSI Regional Level Project Competition 2019–A Project Presentation Platform for undergraduate students organized by Computer Society Of India-DIT Student Branch, Pune Chapter of Dr. D.Y. Patil Institute of Technology, Pimpri, Pune in collaboration with Soft-Corner, Pune and ICERTIS on Thursday, 04th April 2019.

Mr. Abhay Pendse
Chairman, CSI Pune Chapter

Dr. S. N. Mali
Principal, DIT Pune

Dr. Pramod D. Patil
Vice Principal,
HoD, Computer Dept, DIT

SOFT CORNER

icertis Applied Cloud

DPU
Dr.D. Y. PATIL INSTITUTE OF TECHNOLOGY

CSI Regional Level Project Competition 2019

CERTIFICATE OF PARTICIPATION

This Certificate has been awarded to

Mr. / Ms. Pratik Deshmukh

of SITS Narhe for participating in CSI Regional Level Project Competition 2019–A Project Presentation Platform for undergraduate students organized by Computer Society Of India-DIT Student Branch, Pune Chapter of Dr. D.Y. Patil Institute of Technology, Pimpri, Pune in collaboration with Soft-Corner, Pune and ICERTIS on Thursday, 04th April 2019.

Mr. Abhay Pendse
Chairman, CSI Pune Chapter

Dr. S. N. Mali
Principal, DIT Pune

Dr. Pramod D. Patil
Vice Principal,
HoD, Computer Dept, DIT

SOFT CORNER

icertis Applied Cloud

DPU
Dr.D. Y. PATIL INSTITUTE OF TECHNOLOGY

CSI Regional Level Project Competition 2019

CERTIFICATE OF PARTICIPATION

This Certificate has been awarded to

Mr. / Ms. Rohan Patel

of SITS Narhe for participating in CSI Regional Level Project Competition 2019–A Project Presentation Platform for undergraduate students organized by Computer Society Of India-DIT Student Branch, Pune Chapter of Dr. D.Y. Patil Institute of Technology, Pimpri, Pune in collaboration with Soft-Corner, Pune and ICERTIS on Thursday, 04th April 2019.

Mr. Abhay Pendse
Chairman, CSI Pune Chapter

Dr. S. N. Mali
Principal, DIT Pune

Dr. Pramod D. Patil
Vice Principal,
HoD, Computer Dept, DIT

SOFT CORNER

icertis
Applied Cloud

DPU
Dr.D. Y. PATIL INSTITUTE OF TECHNOLOGY

CSI Regional Level Project Competition 2019

CERTIFICATE OF PARTICIPATION

This Certificate has been awarded to

Mr. / Ms. Aditi Kulkarni

of SITS Narhe for participating in CSI Regional Level Project Competition 2019–A Project Presentation Platform for undergraduate students organized by Computer Society Of India-DIT Student Branch, Pune Chapter of Dr. D.Y. Patil Institute of Technology, Pimpri, Pune in collaboration with Soft-Corner, Pune and ICERTIS on Thursday, 04th April 2019.

Mr. Abhay Pendse
Chairman, CSI Pune Chapter

Dr. S. N. Mali
Principal, DIT Pune

Dr. Pramod D. Patil
Vice Principal,
HoD, Computer Dept, DIT

SOFT CORNER

icertis
Applied Cloud

Bibliography

[1] Y. Yuan and F.-Y. Wang, "Blockchain and cryptocurrencies: Model, techniques, and applications," *IEEE Transactions on Systems, Man, and Cybernetics: Systems*, vol. 48, no. 9, pp. 1421–1428, 2018.

[2] U. Mukhopadhyay, A. Skjellum, O. Hambolu, J. Oakley, L. Yu, and R. Brooks, "A brief survey of cryptocurrency systems," in *2016 14th annual conference on privacy, security and trust (PST)*, pp. 745–752, IEEE, 2016.

[3] S. Singh and N. Singh, "Blockchain: Future of financial and cyber security," in *2016 2nd International Conference on Contemporary Computing and Informatics (IC3I)*, pp. 463–467, IEEE, 2016.

[4] S. Nakamoto *et al.*, "Bitcoin: A peer-to-peer electronic cash system," 2008.

[5] F. Zhu, W. Chen, Y. Wang, P. Lin, T. Li, X. Cao, and L. Yuan, "Trust your wallet: A new online wallet architecture for bitcoin," in *2017 International Conference on Progress in Informatics and Computing (PIC)*, pp. 307–311, IEEE, 2017.

[6] X. Li, P. Jiang, T. Chen, X. Luo, and Q. Wen, "A survey on the security of blockchain systems," *Future Generation Computer Systems*, 2017.