

GENERALISED IMMUTABLE LEDGER (GILED)

A Project Report

Submitted By

Harsh Bari - 190303105153
Meet Kiran - 190303105230
Kapil Tiwari - 190303105110
Aditya Raj - 190303105526

in Partial Fulfilment For the Award of

the Degree of

BACHELOR OF TECHNOLOGY

COMPUTER SCIENCE & ENGINEERING

Under the Guidance of

Prof. Nidhi Patel

Assistant Professor



PARUL UNIVERSITY

VADODARA

March - 2023



PARUL UNIVERSITY

CERTIFICATE

This is to Certify that Project - 3 -Subject code 203105450 of 8th Semester entitled “Generalised Immutable Ledger (GILED)” of Group No. PUCSE_137 has been successfully completed by

- HARSH BARI- 190303105153
- MEET KIRAN- 190303105230
- KAPIL TIWARI- 190303105110
- ADITYA RAJ- 190303105526

under my guidance in partial fulfillment of the Bachelor of Technology (B.TECH) in Computer Science and Engineering of Parul University in Academic Year 2022- 2023.

Date of Submission :-

Assistant Prof. Nidhi Patel,

Project Guide

Head of Department,

Dr. Amit Barve

CSE, PIET

Project Coordinator:-

Dr. Kruti Sutaria

Parul University

External Examiner

Acknowledgements

“The single greatest cause of happiness is gratitude.”

-Auliq-Ice

Behind any major work undertaken by an individual there lies the contribution of the people who helped him to cross all the hurdles to achieve his goal. It gives us the immense pleasure to express our sense of sincere gratitude towards our respected guide **Prof. Nidhi Patel**, (Assistant Professor) for her persistent, outstanding, invaluable co-operation and guidance.

It is our achievement to be guided under her. She is a constant source of encouragement and momentum that any intricacy becomes simple. We gained a lot of invaluable guidance and prompt suggestions from her during entire project work. We will be indebted of her forever and we take pride to work under her.

Also we would like to express our deepest gratitude towards **LAKSHMIKRISHNASAI ALLE(3rd year BTech CSE Student: 2022-23)** and **SHIVANSHU SHASHIDHAR PANDEY(Final year BTech CSE Student: 2022-23)** for providing us with sufficient resources whenever needed.

We would like to thank to Prof. Dr. Amit Barve (HOD CSE Dept.) for providing us with this opportunity.

CSE Department,

Harsh Bari - 190303105153

Parul University

Meet Kiran - 190303105230

Vadodara, Gujarat.

Kapil Tiwari - 190303105110

Date:

Aditya Raj - 190303105526

Abstract

Centralized database are very important for any organization, their applications can be found in a variety of contexts. Most businesses, both either public or private, deploy centralised databases. These databases contain all of the information that can be calculated about the firm, including client records, internal transactions, historical and present performance assessments, and future predictions. These databases are essentially the foundation of a certain organisation.

Nevertheless, the problem with these centralised databases is that some persons or a certain set of people inside the organization have complete access to them due to which they tries to temper with the data. Corruption has been highlighted as the problem. Also if these types of manipulations occur then it is very difficult to identify it. While it is challenging for an outsider to change the data, anyone inside the organisation can do so with relative ease. Now, in this situation, the organization's owner—whether an individual or the government—as well as its clients are in peril since these manipulations are executed so deftly that only the person doing the manipulating is aware of the changes, while the owner and the client are unconscious of them. Government-related industries are more likely to exhibit these things.

Table of Contents

Acknowledgements	iii
Abstract	iv
Table of Contents	v
List of Tables	viii
List of Figures	ix
1 Introduction	1
1.1 Problem Statement	1
1.2 Aim	1
1.3 Objectives	1
1.4 Scope	2
2 Literature Review	3
2.1 Package Delivery System Based on Blockchain Infrastructure	3
2.2 Proof of Existence Using Blockchain	3
2.3 Vaccination System using Blockchain Technology: A Prototype Development . . .	4
2.4 A Track Donation System Using Blockchain	4
2.5 What is your Distributed (Hyper) Ledger ?	4

2.6 BlockchainAs a Service (BaaS) Framework for Government Funded Projects e-Tendering Process Administration and Quality Assurance using Smart Contracts	5
2.7 Blockchain-based e-Tendering System	5
2.8 Creating value in equity crowdfunding platforms using blockchain technology	5
2.9 Blockchain-Watermarking for Compressive Sensed Images	5
2.10 Secured voting through Blockchain technology	6
2.11 Certificate validation using blockchain	6
2.12 Fighting COVID-19 and helping economy reopen by using blockchain technology	6
2.13 A Blockchain-Based Medical Data Sharing and Protection Scheme	7
2.14 Blockchain-based Website Solution for Controlling the Authorized Sale of Drugs in Peru.	7
2.15 Removing the Trusted Third Party in a Confidential Multiparty Registered eDelivery Protocol Using Blockchain.	7
2.16 TrustedChain: A Blockchain-based Data Sharing Scheme for Supply Chain.	7
2.17 Cost Fairness for Blockchain-Based Two-Party Exchange Protocols	8
2.18 Data Security Based on Blockchain Digital Currency	8
2.19 Movie Rating System based on Blockchain	8
2.20 Detection of Tampered Images Using Blockchain Technology	8
3 Experimental setup and Methodology	13
3.1 Tools And Technology	13
3.1.1 Desktop Application	13
3.1.2 Network Connectivity	13
3.2 Modules	13
3.2.1 Login and Registration	13
3.2.2 My /Add /Join Organization	15
3.2.3 Add Miners	17

3.2.4	Creating Ledgers	18
3.2.5	Types of operations on ledger	21
3.2.6	Ledger Verification	22
3.2.7	Generate Database	23
3.3	Network Structure	26
3.3.1	Ledger	27
3.3.2	Organisation	27
3.3.3	Transactions	28
3.3.4	Unlocking	28
3.3.5	Registries	29
3.4	UML Diagrams of Project	30
3.4.1	Activity Diagram	30
3.4.2	Sequence Diagram	32
3.4.3	Use Case Diagram	34
3.5	Algorithms	36
3.5.1	Hash value while adding new block	36
3.5.2	Hash value of lock request	38
3.5.3	Hash value of unlock request	40
3.5.4	Validate Hash	42
4	Conclusion and Future Scope	44
4.1	Conclusion	44
4.2	Future Scope	44

List of Tables

2.1	Table of Comparision 1	9
2.2	Table of Comparision 2	10
2.3	Table of Comparision 3	11
2.4	Table of Comparision 4	12
3.1	Hash Level v/s Time(in secs)	20

List of Figures

3.1	Login	14
3.2	Register	14
3.3	Forget Password	15
3.4	My Organisation	16
3.5	Creating Organisation	17
3.6	Add Miners	18
3.7	My Ledgers	19
3.8	Creating ledger	19
3.9	Operations on ledger	21
3.10	Ledger Verification	22
3.11	Database	23
3.12	Ledger	24
3.13	Network Structure	25
3.14	Ledger	26
3.15	Organisation	26
3.16	Transactions	26
3.17	Unlocking	26
3.18	Registries	26
3.19	Activity Diagram	30
3.20	Sequence Diagram	32
3.21	Use Case Diagram	34
3.22	Add Block Hash Algorithm	36
3.23	Lock Ledger Hash Algorithm	38
3.24	Unlock Ledger Hash Algorithm	40
3.25	Algorithm for validate function	42

Chapter 1

Introduction

As we see in our daily life that in the government sector the files or the details are manipulated by the worker who works there due to which the civilians are facing problems as we see in government hospitals the bills of the patient are manipulated, in a municipal corporation the data are manipulated. So if we use the concept of blockchain in the government sector then it becomes very difficult for the manipulator to manipulate the data.

A transaction cannot be changed once it has been recorded since it is an immutable public digital ledger. Blockchain is always safe because of the encryption function. The ledger is updated automatically, allowing for quick and transparent transactions. No intermediate cost is necessary because the system is decentralized. Participants in a transaction authenticate and verify its legitimacy.

1.1 Problem Statement

There are many organizations running which has centralized database and which are not secured. There are chances of mutations in the databases. The central authority lies within a single hand or single group. There are high possibilities of the data being tempered if the person handling it is corrupt.

1.2 Aim

To provide a trusted database in the network with the help of blockchain technology using Cryptographic algorithms

1.3 Objectives

- To create a secured network among trusted people

- To create a multipurpose generalized ledger structure
- To create immutable ledger using that ledger structure
- To create a trust among the network and secure the data using cryptographic signatures

1.4 Scope

- Building a software that provides a generalized ledger which is impractical to be mutated without the support of more than 50

Chapter 2

Literature Review

2.1 Package Delivery System Based on Blockchain Infrastructure

Today, millions of shipments are shipped every day, and since they are vulnerable to assaults like phishing, the information associated to such goods has to be safeguarded. Additionally, the majority of the existing package delivery systems are built on centralised platforms, making them open to many types of assaults.

In this study, we propose a blockchain-based delivery system for packages, which would increase security by preserving information integrity but also user & data verification. Among the basic characteristics is indeed the capacity of validation and also the maintenance of data protection, that in conventional platforms would hardly be guaranteed [1].

2.2 Proof of Existence Using Blockchain

This project's main goal is to provide a Proof-Of-Existence of any kind of file or record on the Blockchain platform. After submission, we will upload the file's distinctive signature and all of its related data to the Private Decentralized Public Ledger.

Records kept here can be retrieved at a later time to demonstrate that the relevant file existed at the specified time and date and that the relevant data was posted. The signature on the document cannot be replicated, and no computational or technical method can be used to change the prior data. POE can therefore be used to demonstrate the presence of any file in judicial proceedings. It may also be a crucial component of any business, which will undoubtedly keep records of transactions, bonds, client information, personnel information, etc [2].

2.3 Vaccination System using Blockchain Technology: A Prototype Development

today vaccinations are becoming a legal requirement for citizenship however there have been instances where citizen data has been altered in order to link the vaccination records of healthcare providers with one another.

Here project aims for developing a vaccination system by blockchain as the architecture for data storage the system uses a permissioned blockchain to safeguard patient data preventing unauthorised users from accessing the network three network participants nodes that validate and upload data to the blockchain are part of the design this satisfies the prerequisite The system was successfully built as a prototype for future enhancement and to research or minimise the issues and challenges in blockchain in order for a blockchain network to be fault-tolerant [3].

2.4 A Track Donation System Using Blockchain

Charities now confront a challenging fundraising situation. Mostly because they are not very open over time it become harder to tell if donations were going to the correct places or if they were funding shady campaigns or something else else donors, thus have less confidence in these organisations however there are some legitimate charities who have a harder time raising money at a high cost with the help of blockchain as a technology a decentralised database offering safety and lucidity while removing the need for middlemen between contributors and charity this probing suggested an idea for aforementioned issue block chain enables donors to trace all gifts and see the total amount sent smart contracts are used for all donations the outcomes of the blockchain track donation method lower the possibility of encountering questionable campaign donations or terrorist projects for people to donate money a website was made [4].

2.5 What is your Distributed (Hyper) Ledger ?

Following the 2008 debut of Bitcoin, blockchain technology has gained prominence and seen several applications. Some of these initiatives now extend beyond cryptocurrencies, and there is a significant demand for projects that use blockchains to provide solutions that satisfy particular business objectives. As a result, the challenge of identifying the blockchain technology that best suits the project requirements has emerged. With an emphasis on Hyperledger, the top software ecosystem allowing the collaborative construction of unique distributed ledgers, this effort seeks to advance things further by extending the framework to private blockchains [5].

2.6 BlockchainAs a Service (BaaS) Framework for Government Funded Projects e-Tendering Process Administration and Quality Assurance using Smart Contracts.

Tenders must be used when bidding on government-funded projects due of the lack of openness this approach is cumbersome and encourages dishonesty in order to make managing public projects simple and transparent this article suggests employing blockchain as a service. This provides an immutable ledger that allows various stakeholders to follow a proper guide of rules and also no one can imitate or temper with the data [6].

2.7 Blockchain-based e-Tendering System

In most cases, governments and businesses employ the tendering procedure to get goods or services from manufacturers or service providers. Although it is the most used technology, e-tendering has less security. We'll look at how smart contracts, which are built on the Ethereum blockchain, may be used to create a distributed e-tendering system in this essay. For each process' implementation, many algorithms are utilised. Implementing a fair, open, and transparent tendering system is the primary goal of this study [7].

2.8 Creating value in equity crowdfunding platforms using blockchain technology

Crowdfunding for injustice permits investors to purchase shares in businesses or initiatives. But occasionally, a firm or initiative loses interest. This essay aims to demonstrate how blockchain-based distributed ledger technology might help to resolve a few of the problems with stock crowd funding. Through to the designing of a crowd funding platform that uses a deconcentrated ledger to track the transactions that took place there and has the ability to load and implement smart contracts, it was possible to confirm that block chain can create value in this type of platform, being able to mitigate or even solve a few of the problems associated with this kind of crowd sourcing [8].

2.9 Blockchain-Watermarking for Compressive Sensed Images

The security of photographs, one of the most used forms of multimedia, has grown to be a serious issue for open networks on a broad scale. In order to ensure privacy, this research suggested a block chain content protection system. A complete security protection of the huge picture facts obtained on compressive sensing may be accomplished via copyrighting, blockchain, as well as

other dependable authentication mechanisms [9].

2.10 Secured voting through Blockchain technology

The primary way to alter that destiny of the nation is through electing. Electronic voting have taken the role of manually operated voting machines (EVM). Voters are still troubled by the issues even after replacement. issues such as names missing from the voter list, lost votes, etc. So keep the election system temper-free, we recommend integrating a decentralised method. The blockchain is one of those decentralised platforms. Utilizing the solidity language, our project is being built on the Ethereum platform. This initiative offers several opportunities for safeguarding the electoral process and promoting global wellbeing. [10].

2.11 Certificate validation using blockchain

In today's digital age, everything is digitalized, including academic certificates like the SSLC and HSC that are given to students in educational institutions. It is challenging for students to hold onto their degree diplomas. Verification and validation of certifications are time-consuming and difficult for the organisation and institution. Our project will contribute to a safe storage of a certification in the blockchain network. The paper certificates are first transformed into digital versions. A hash code value for such certificate is created using the chaotic algorithm. The certifications are then kept on the blockchain. We can offer a more safe and efficient digitally signed validation by utilising blockchain based technology. [11].

2.12 Fighting COVID-19 and helping economy reopen by using blockchain technology

A sound solution is required to address several issues, including health data collecting and monitoring, data privacy management, immutable data record, global identification, and cross-regional cooperation, while the international community is coping with the COVID-19 pandemic and economic reform strategy. We created the Green Pass solution in order to address these issues by utilising distributed ledger technology, decentralised identification, verified credentials, and distributed storage. Community-level COVID-19 mitigation and economic challenges that have reopened [12].

2.13 A Blockchain-Based Medical Data Sharing and Protection Scheme

The process of a disease's onset, progression, and treatment are all documented in an electronic health record (EHR), which gives it significant medical significance. Data exchange and privacy preservation are crucial issues in EHR due to the private and sensitive nature of medical data for patients. Given that it possesses the qualities like decentralisation & tamper resistance, distributed ledger technology may offer a potential solution to the issues listed above [13].

2.14 Blockchain-based Website Solution for Controlling the Authorized Sale of Drugs in Peru.

Medicines are seen to be a crucial part of our lives. Unfortunately, such adulteration of these drugs causes significant negative effects on the health care and economic sectors. In Peru, such issue is quite important. In this project, we present a concept that intends to deploy technology that offers a solution that gives consumers trustworthy data on the origin and legitimacy of these items in Peru. Details on the drug's composition, pharmaceutical form, active ingredients, and other pertinent information will be available. This technique seeks to publish them in a way that ensures their immutability. [14].

2.15 Removing the Trusted Third Party in a Confidential Multiparty Registered eDelivery Protocol Using Blockchain.

People nowadays are indeed very interested in assisting people in need, yet many are unsure if their efforts will actually be successful. Therefore, under such circumstances, we may create a legitimate and transparent application for donations that will be beneficial to the surrounding community. taking use of the immutable data registry that the blockchain technology provides. These suggestions include approaches for recorded delivery, fair payments, digital contract signatures, and verified notifications. Due to this concept, those who want to assist the poor will be more ready to approach them and give them money [15].

2.16 TrustedChain: A Blockchain-based Data Sharing Scheme for Supply Chain.

management in supply chain, which is utilized in business, entails the circulation and storage of raw materials as well as work-in-progress from either the point of source towards the site of demand. Data sharing across stakeholders is a crucial project since it increases the efficiency of various

workflows among stakeholders. This study suggests Trusted Chain, a supply chain data sharing system based on blockchain, which offers the following two benefits: (A) Trust: built on blockchain to enable parties with mistrust for one another to handle data cooperatively. (b) Security: Offers a secure architecture that saves order forms in a distributed database (DDB) [16].

2.17 Cost Fairness for Blockchain-Based Two-Party Exchange Protocols

Many a times people faces unfair means of money exchange/digital goods in online mode of transaction. Because there are no where mention about notion of fairness. Blockchains can increase transparency even during trade of digital products, ensuring that nobody is taken advantage of by a dishonest counterpart in a two-party trade. This can be achieved through smart contracts. The conversion value of two different digital goods is assigned and that is used while exchanging the goods. [17].

2.18 Data Security Based on Blockchain Digital Currency

There are many of the advantages of blockchain technology. Mainly it a distributed ledger and database and due to it it is immutable. This property of the blockchain brings trust to the user. But at the same time there are also some of the hidden dangers of data security. This article focus on the how to protect the data security of digital currency in blockchain transactions [18].

2.19 Movie Rating System based on Blockchain

For any movie, the success or failure is decided by the ratings and reviews of the people. The use of digital media as a classification method, where people read evaluations about films, has become more prevalent as a result of recent marketing trends, or the ratings rated before making any decision to watch a movie. But now a days people try to buy the ratings or manipulate the reviews. The idea behind our article is make this review and ratting system in distributed ledger. Blockchain gives us the opportunity to decentralize the data on which not any single authority have the access. Also they are temper proof and this brings a trust over a movie and the movie will sell in market [19].

2.20 Detection of Tampered Images Using Blockchain Technology

Now a days the images are being published very often on the web but the problem is that there are high chances of the image to be get manipulated. Using blockchain technology, it provides: a) immutable ledger(no one can manipulate it. b) adding data to blockchain provides a block a unique identity. If anyone tries also to temper it, we can verify it with its unique identity .Blockchain helps the user to register their block(image) at their own name and further if anyone tries to visit [20].

Ref. No.	Year	Description	Methodology
[1]	2018	Package Delivery System which helps security in data integrity and verification of both users.	System flows in following manner: Created, Accepted, Handed, Delivered, Finished.
[2]	2019	Concept which provides the proof of existence of any file or record in system.	Hash is generated using sha-256 which gets associated with each record.
[3]	2021	System to protect patient's vaccination data from being tempered.	System works in following way: Requirement Gathering, System Design, System Implementation and Network Testing.
[4]	2021	A system to track donation which allows doners and the organisation knows the flow of money.	The important sequence of the work flow is: user selects project, transfer fund, receives confirmation and creates a unique id for the transaction.
[5]	2021	It is a framework which aims at extending private blockchain with the help of Hyperledger that leads to software eco-system supporting collaborative development of customized distributed ledgers.	Different types of hyperledgers are been introduced like: Hyperledger Besu, Hyperledger Fabric, Hyperledger Indy and any more.

Table 2.1: Table of Comparison 1

Ref. No.	Year	Description	Methodology
[6]	2021	System which provides solution towards corruption using Blockchain as service and makes the process transparent.	This system has following elements: Tendering organising (for organizing the events), Blockchain Network (provides platform), Bidder and Citizen.
[7]	2020	System to provide decentralization and provide security to e-tendering process.	It contains the algorithms to conduct e-tendering, publishing bids and selecting Winner.
[8]	2021	System proposed to introduce how Distributed ledger aims to provides security in crowd funding platforms.	Proposed system is loads all the transaction to the blockchain netowrk which further cannot be tempered.
[9]	2022	System proposed to protect the privacy, integraty and availability.	The system uses Blockchain, compressed sensing, interplanetery file system.
[10]	2019	Provides a platform on decentralised system to do voting.	Tools used in the system are: Ethereum, wallet account and smart contract account.
[11]	2022	This project helps to validate certifcate and generates a hash code.	This system works by creating digital certificate and work on hash code generation.

Table 2.2: Table of Comparision 2

Ref. No.	Year	Description	Methodology
[12]	2020	Provides a solution to manage personal data vault with ownership.	It works by gathering important test data and then check its geo-location then finally stores on blockchain.
[13]	2019	Provides Electronic health records that helps in data sharing with multiple hospitals.	It makes uses of blockchain, network, proof of stake.
[14]	2020	System to provides reliable information of the originality of the drug.	The system uses Drug query, Validation of transaction, drug management and management of users and permission.
[15]	2020	System proposed to remove third party for in between eDelivery for effective payment and low cost delivery.	Uses 3 Steps: Creation, Accept and Finish.
[16]	2020	Provides trusted environment based on blockchain that allows data to be shared in distributed way.	It makes uses of smart contract and etherium
[17]	2020	System to define the cost fairness	Provides framework to for data trading.

Table 2.3: Table of Comparision 3

Ref. No.	Year	Description	Methodology
[18]	2020	System proposed to secure data on blockchain.	Core technology used in the system are: Distributed storage, Consensus mechanism, smart contract and cryptography.
[19]	2021	System used to store movie reviews which cannot be tempered in future.	System uses smart contract in which people adds the review and then it is sent to blockchain network.
[20]	2019	System proposed serves two purpose: first is to register ownership and copyrights of authors and second is to avoid insertion of raw image data into blockchain.	Registering the image has algorithm which takes image and owner id and Checking image algorithm takes only image and verifies it.

Table 2.4: Table of Comparision 4

Chapter 3

Experimental setup and Methodology

3.1 Tools And Technology

3.1.1 Desktop Application

We have used **visual studio** application for creating desktop application. In this the code is written in C# language.

3.1.2 Network Connectivity

We have used **Firebase** for creating the network. All the online activities like data sharing is done through this only.

3.2 Modules

3.2.1 Login and Registration

Basic step needed for almost every application.

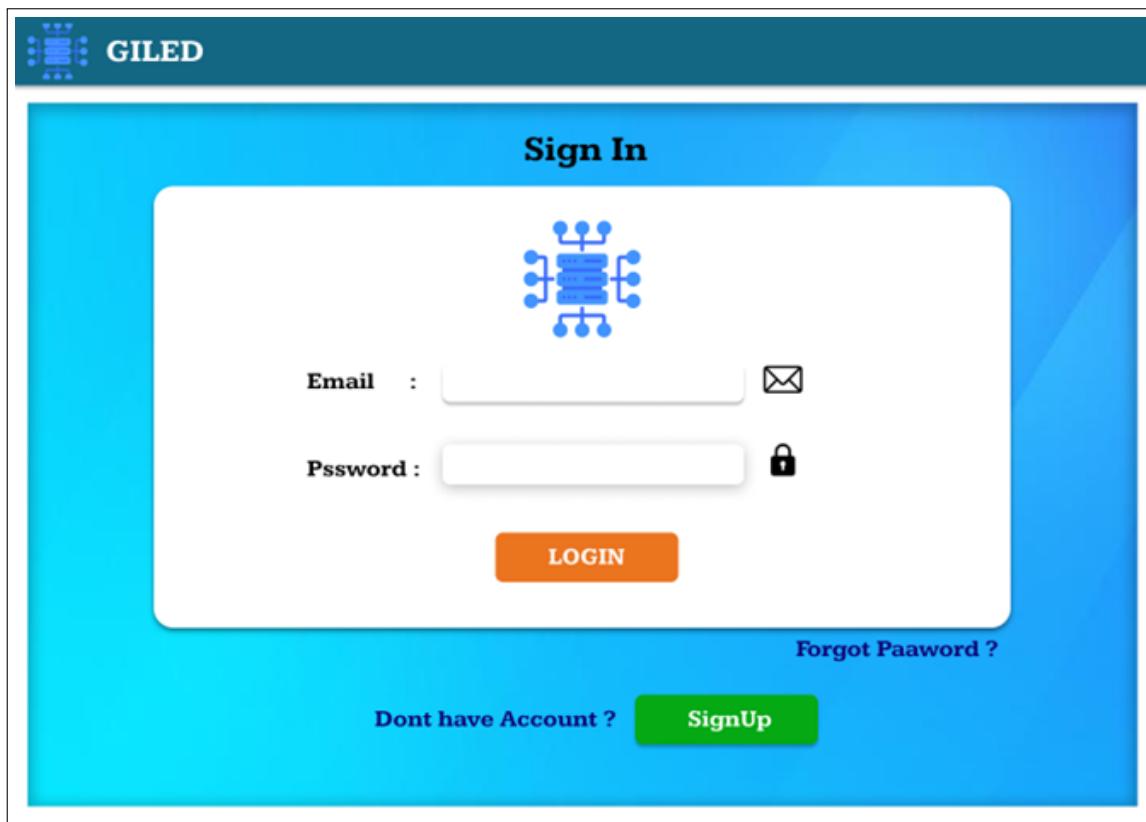


Figure 3.1: Login

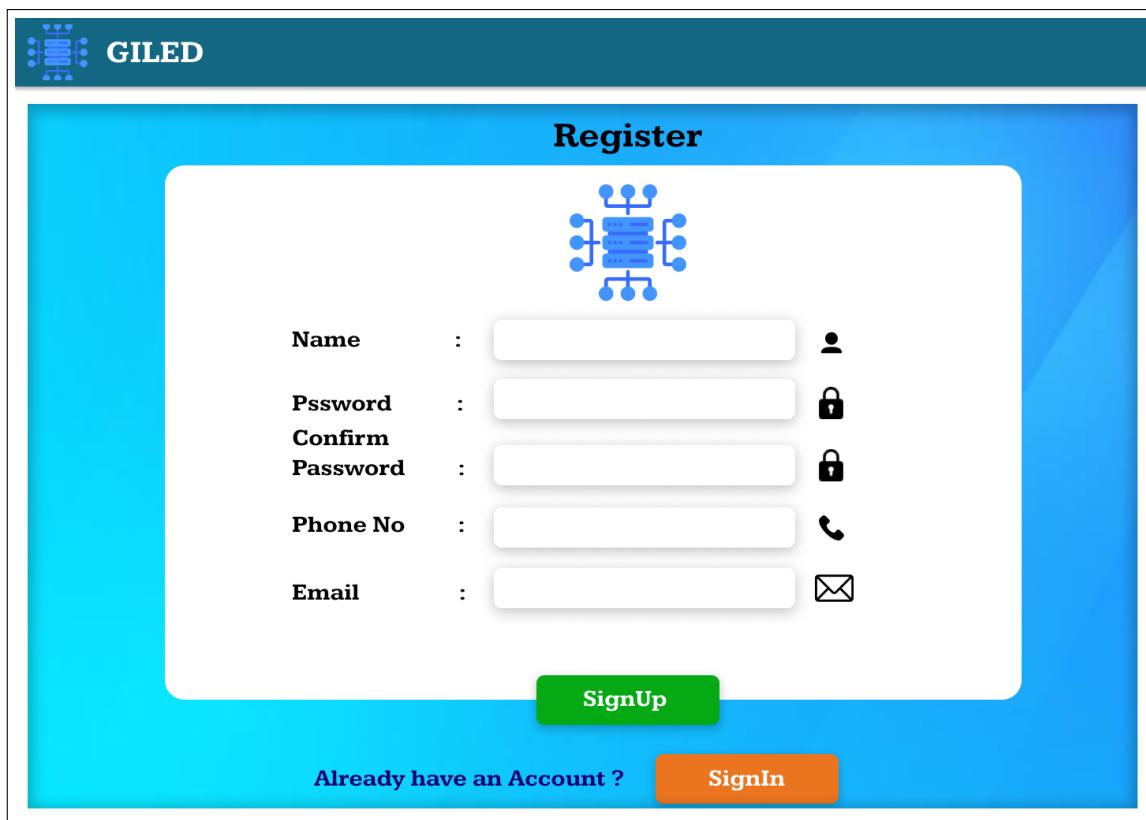


Figure 3.2: Register

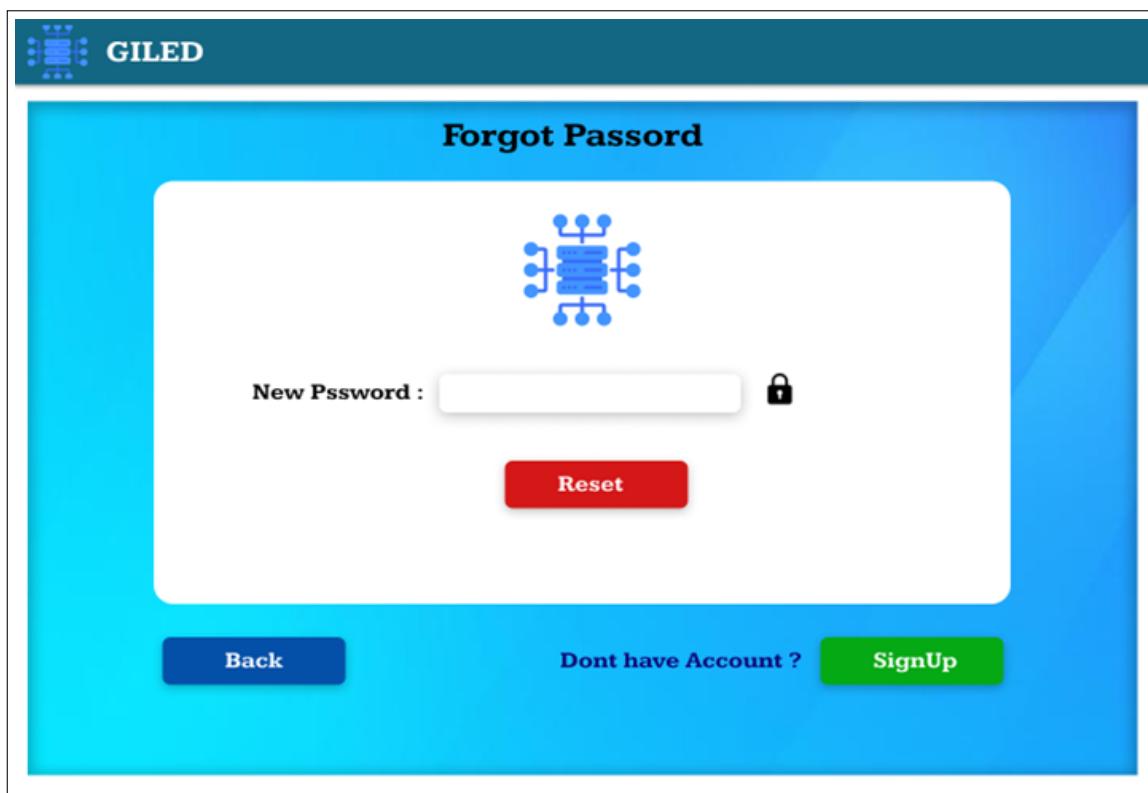


Figure 3.3: Forget Password

3.2.2 My /Add /Join Organization

Creating organization is a way to form a group/organization. This organization will be created by registering the details about the organization. Each organization will have unique invitation link using which trusted miners can be added in the organization.

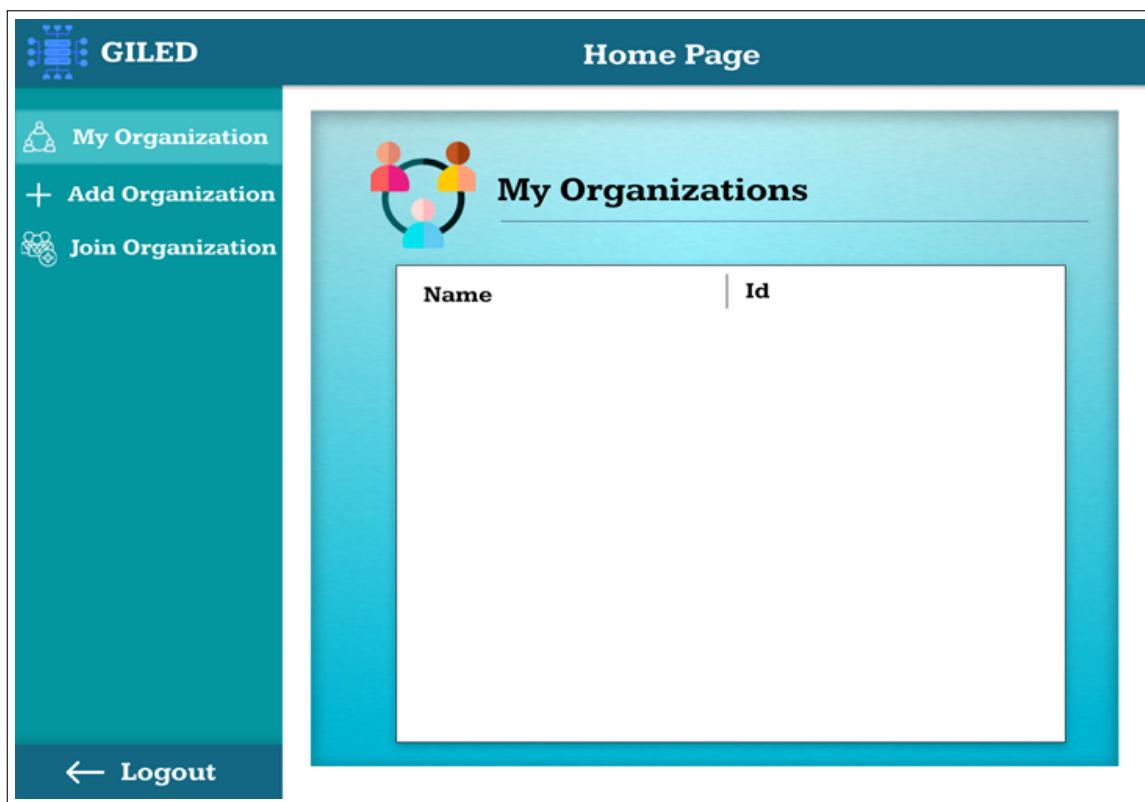


Figure 3.4: My Organisation

- After login we will be redirected to home page
- My organization page will be opened by default where we can see the organizations listed in white box which user are part of.
- If we want to perform operations on the organizations listed in the white box then we can double click on it and that Organization ledger Page will be opened up.



Figure 3.5: Creating Organisation

- If we want to register a organization in the app we need to go to Add Organization page.
- There we need to fill the details related to particular organization
- Finally after filling the details we can register particular Organization in the app by clicking on create Organization button

3.2.3 Add Miners

In this step the miners(users) area able to join the organization. For this purpose, the miners need organization id. If the miner enters any invalid organization id or already joined in the organization then it will show error.



Figure 3.6: Add Miners

- If any member(minor) wants to join particular organization that person needs to enter organization's id to Join in it
- miner can ask organization id from the Owner of particular Organization
- Every Organization has Unique id

3.2.4 Creating Ledgers

Within an organization an individual can create one or more ledgers (generalized form). This is actual structure to enter data. This ledger would be reflected in every miner's screen who ever joins the organization.



Figure 3.7: My Ledgers

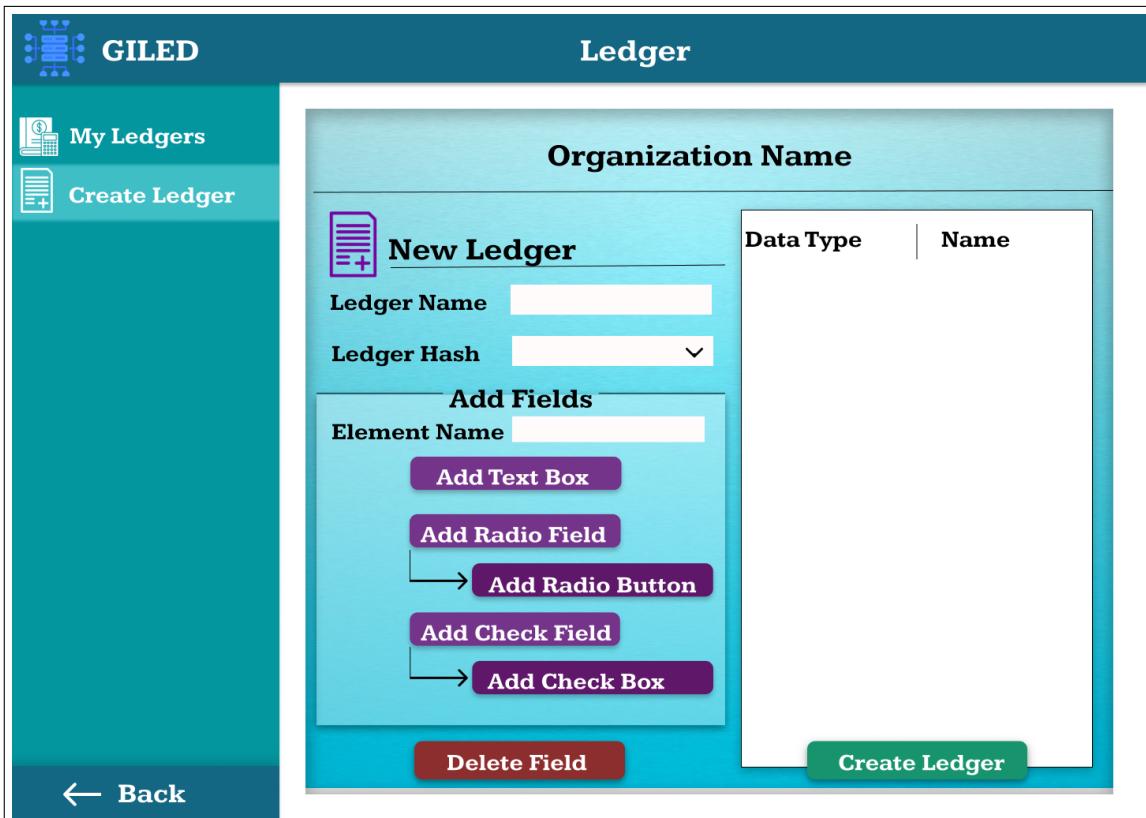


Figure 3.8: Creating ledger

- Here you will be able to make dynamic form with text field, radio button and check box and in that blank drop box , we have to select the hashing level that how much time and processing speed will be required to calculate the value of nonce (The bigger the number, the more time and the more processing power.) and create.
- As per user format a dynamic form can be created and it is shown in the white box as we create the form then after formatting the structure of the form we can click on create ledger to create the ledger of that particular Organization.
- Selecting **Ledger Hash** decides the level of security you are giving in the generation of the hash value. The more level you choose the time it takes to generate the hash.

Below is the table given which shows the hash level and approximate time taken to generate the hash value.

Level	Time(in secs)
0	0-5
1	5-10
2	10-15
3	15-20
4	20-25
5	25-30
6	30-35
7	35-40
8	40-45
9	45-50

Table 3.1: Hash Level v/s Time(in secs)

3.2.5 Types of operations on ledger

- Add Data: Used to add new data/block to ledger
- Update Record: Used to change the data which is already present on ledger.
- Lock Record: If a record is locked then no updation is possible on that record.
- Unlock Record: If need to open the lock of an locked record, we need permission of more than 50
- Lock Ledger: If the ledger is locked then no new data will be able to insert/update.
- Unlock Ledger: If need to open the lock of the ledger, we need permission of more than 50

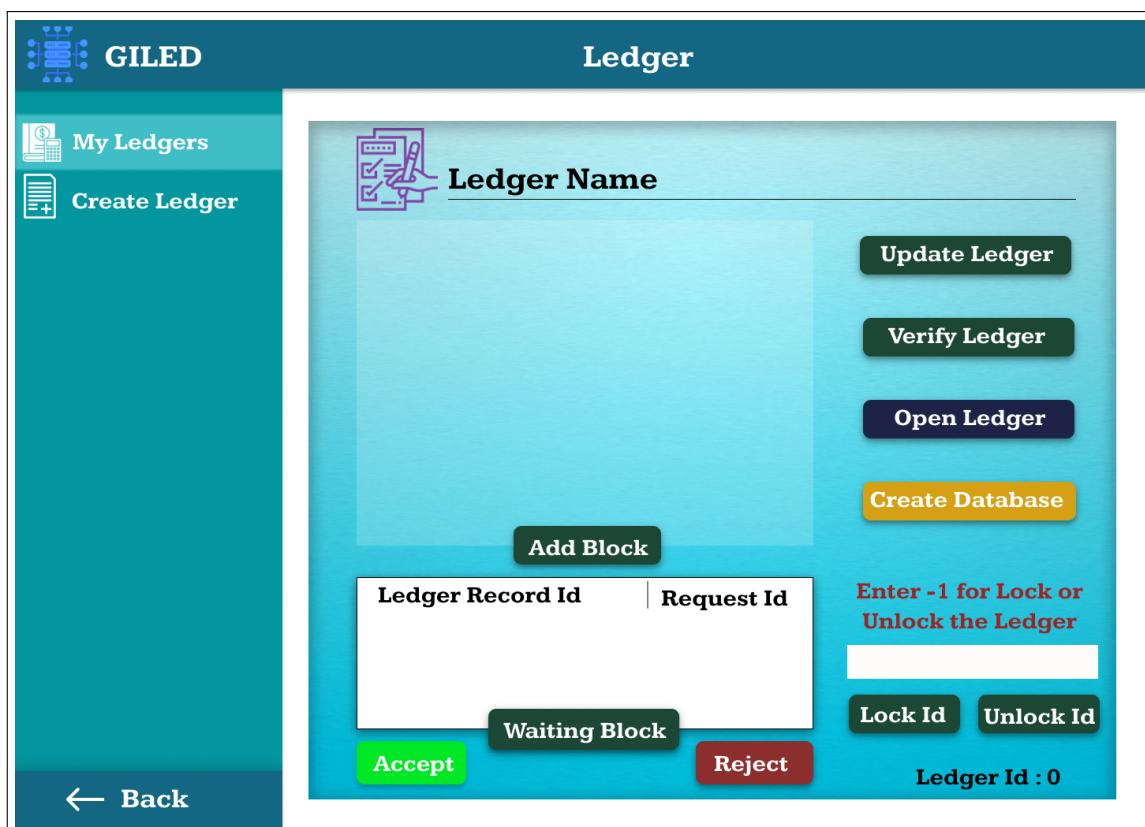


Figure 3.9: Operations on ledger

- In the Ledger Page, there will be ledger name and in the box which is below it , there will be a dynamic form whose data has to be sent
- Update ledger means to fetch the data from online network to the local ledger.
- And then in the textbox which is below in that, the particular id of the ledger has to be written.(if you want to lock or unlock that partciular record, else keep it blank)

- NOTE:- ledger has id = -1 (if you want to lock/unlock the ledger)

3.2.6 Ledger Verification

- **verify ledger** hashing will check that whether there has any unwanted manipulation occurred.
- **Create database** means create a final database using ledger in which there will be data which are important for the user
- If user wants to see the ledger then click ”**open ledger**“ button and it will show the ledger in Excel sheet.
- **Waiting block** is for voting that any update should be allowed or not. All these the request will be shown there. if allow then accept else reject it.
- There is also ledger id shown at bottom right.

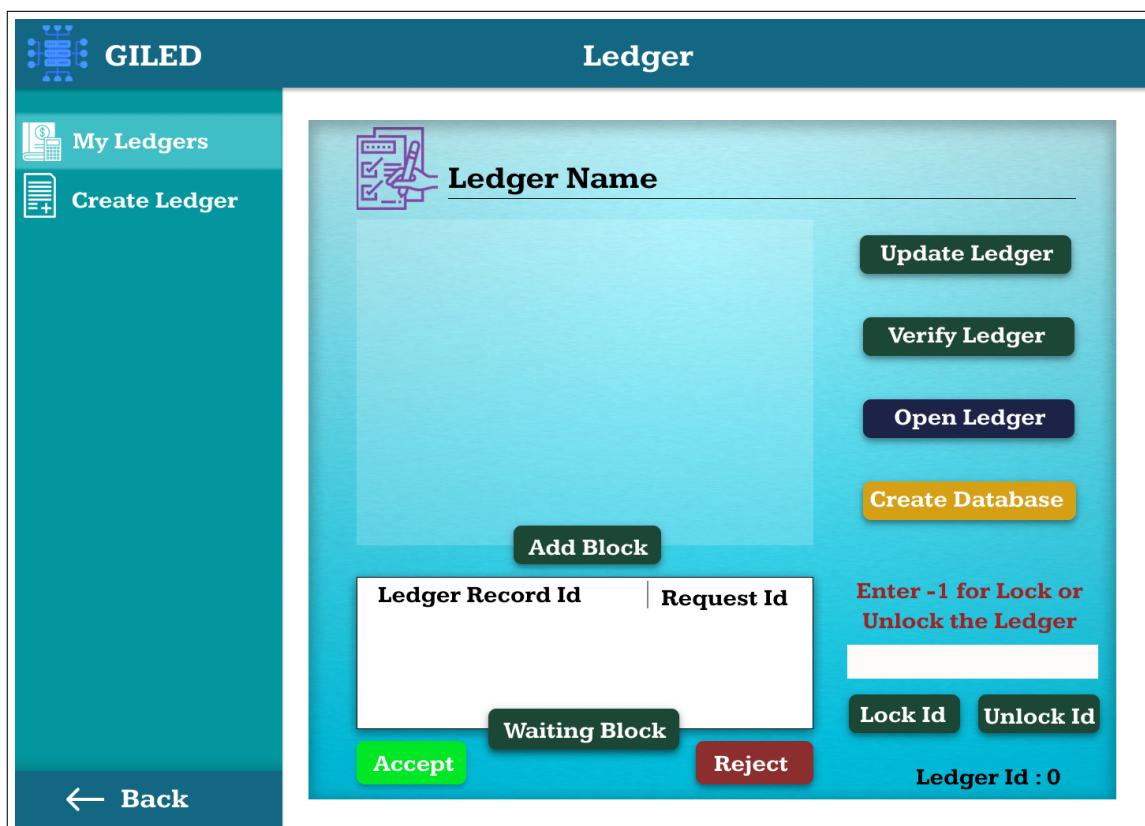


Figure 3.10: Ledger Verification

The ledger present in the local machine of each miners needs to be verify. This is done by verifying the hash value. It may possible that data in one miners is corrupted so for verification purpose, the ledger presented in the miner's machine will be passed to a verification process. The

output of the verification process will be a data set. If the ledger is verified successfully then, then only it will be eligible for creating database. If the ledger fails in verification, then it will also show the entry number where it is being manipulated.

3.2.7 Generate Database

The final operation performed on the ledger. This is the required output of the user. This contains only the final and required result only. This is generated by the ledger after its verification. This database generated is completed free from any unwanted manipulation.

A	B	C	D	E	F	G	H
1							
2	Id	Lock	name	Gender	Hobby:-Sports	Hobby:-Reading	Hobby:-Cooking
3	0	0	Rohini	Female	N	Y	Y
4	1	0	Null entry	Male	N	N	N
5	2	0	Dhruv	Male	N	N	Y
6	3	0	Rohit	Male	N	N	N
7	4	0	Priya	Female	Y	Y	Y
8	5	0	Geeta	Female	Y	N	Y
9							
10							

Figure 3.11: Database

A	B	C	D	E	F	G	H	I	J	K	L	M
1	28 a7e703ac1	5 testing org		7 Check verification	13	0						
2	Entry No	Previous Hash	Current Hash	Miner Id	Nonce	Id	Lock	name	Gender	Hobby-Sports	Hobby-Reading	Hobby-Cooking
3	0	0 a6036b3312a566c38dd36cb96d86356f8b0d7e171f185ae28a3e		1	10	-1	1	-1				
4	1	1 a6036b3312a566c38dd36cb96d86356f8b0d7e171f185ae28a3e		1	70	-1	1	0				
5	2	2 a72b6b90fb046a943874dc2178a10fd8e07e602d a8aa3669deff1fb285f56445e33ed3aa595759b72434666aea6669b		1	6	-1	-1	1	1			
6	3	3 a8aa3669deff1fb285f56445e33ed3aa595759b72434666aea6669b		1	60	0	0 Harsh	Male	Y	N	Y	
7	4	4 a9e33c98136d73140e05574746f7c6145975151:afcd39220976096297639f60146c85e838ca3ccb82b6c4077ee		1	16	0	0 Tejas	Male	N	Y	Y	
8	5	5 afcd39220976096297639f60146c85e838ca3ccb82b6c4077ee		1	248	0	1	-1				
9	6	6 a8141488751505a9dce646b0d04ac2530e93733a: a2e48b3220e065daa87ee5921539f07ab4d8db8eaef38e017172b;		1	45	0	1	0				
10	7	7 a2e48b3220e065daa87ee5921539f07ab4d8db8eaef38e017172b;		1	64	0	1	-1				
11	8	8 a8936b1b1d4625913c8adbf8e13227d89cd43fa a016b0f0c8cabaf631674af1313eaa862caadfbfb9fad38d96f41259		1	97	0	-1	1	1			
12	9	9 a016bcf0eabaf631674af1313eaa862caadfbfb9fad38d96f41259		1	9	-1	1	-1				
13	10	10 ae38a47296a47b7ebf62eaa9a28cde75c5e8e9b9771a667aca517484a0d02d88714603217fb85e0c502082b65a6d223		1	20	-1	-1	1	1			
14	11	11 a667aca517484a0d02d88714603217fb85e0c502081a91a59ce82610bd936309956a4835c57aa605054a2630a5a0012ee		1	305	0	0 rajiv	Male	N	N	N	
15	12	12 a91e59fc82610bd936309956a4835c57aa605054: ab8bd21940cc1cf0a609ca4ebfa27d03d8c9b4d7b5ea9bd8eaaf9		1	0	1	0 Vilas	Male	Y	N	N	
16	13	13 ab8bd21940cc1cf0a609ca4ebfa27d03d8c9b4d7b5ea9bd8eaaf9		1	191	0	0 Shivani	Female	Y	Y	Y	
17	14	14 a9731903c3aca28285a864a88055e9b91a483ab; a65456b0e88e07950b31199c42c815b284e0705530046b099811		1	13	1	0 Null entry	Female	N	N	N	
18	15	15 a65456b0e88e07950b31199c42c815b284e0705530046b099811: a65b20ae75f1abf162cdff0d450ab3614f80a5eab49cef131474e		1	99	1	0 Null entry	Male	N	N	N	
19	16	16 a65b20ae75f1abf162cdff0d450ab3614f80a5eab49cef131474e		1	158	2	0 Dhruv	Male	N	N	Y	
20	17	17 a5eab271d269971c89f6076662ab8a1b8779f23363 abcf8c8ed4775015cba19845e0fbba8f825c5adaea070f5b9f8081ebf		1	98	0	0 Rohini	Female	N	Y	Y	
21	18	18 a&fc&cd4775015cba19845e0fbba8f825c5adaea070f5b9f8081ebf: ac0d4b5f19a165adc3e4b1d301691ee1c58238&52c937c62e69		1	9	3	0 Raghav	Male	Y	Y	N	
22	19	19 a0ad4b5f19a165adc3e4b1d301691ee1c58238&52c937c62e69		1	53	4	0 Priya	Female	N	Y	Y	
23	20	20 a80fdfe88974ba7a4ub8fa530a24c6b1a843b549 a5a16dfc53129105873d2c04772d7dd024732056a8f2863a049794d		1	93	5	0 Geeta	Female	Y	N	Y	
24	21	21 a5a16dfc53129105873d2c04772d7dd024732056a8f2863a049794d: a870f03570a69bc1758426a3e3cc8799e08743f24182437823150:		1	49	3	0 Rohit	Female	Y	Y	N	
25	22	22 a870f03570a69bc1758426a3e3cc8799e08743f24182437823150: a3d8d353720e12129e604eaa1a830820c7db90259 a3fc5970aa4e7a61a96d23db0f600ebc29b5c5b3e5a96c7c9553e		1	3	3	1	-1				
26	23	23 a3d8d353720e12129e604eaa1a830820c7db90259 a3fc5970aa4e7a61a96d23db0f600ebc29b5c5b3e5a96c7c9553e		1	83	3	0 Rohit	Male	N	N	N	
27	24	24 a3fc5970aa4e7a61a96d23db0f600ebc29b5c5b3e5a96c7c9553e		1	187	3	1	0				
28	25	25 a2af09fc6323e070a71786a6ebbf35c3d83e0fb029 ad45cc8d77fb781c529314f66a8298b500c35a291aede2ec1a7701		1	24	3	-1	1	1			
29	26	26 ad45cc8d77fb781c529314f66a8298b500c35a291aede2ec1a7701		1	20	3	0	Male	N	N	N	
30	27	27 aa8fb6d419bb90c2a227b5f0a6f2fbcae80b04a7e703ac1be1b41b68ad8b5f57aba17910b3a6a2129092e8ff4		1	561	4	0	Female	Y	Y	Y	

Figure 3.12: Ledger

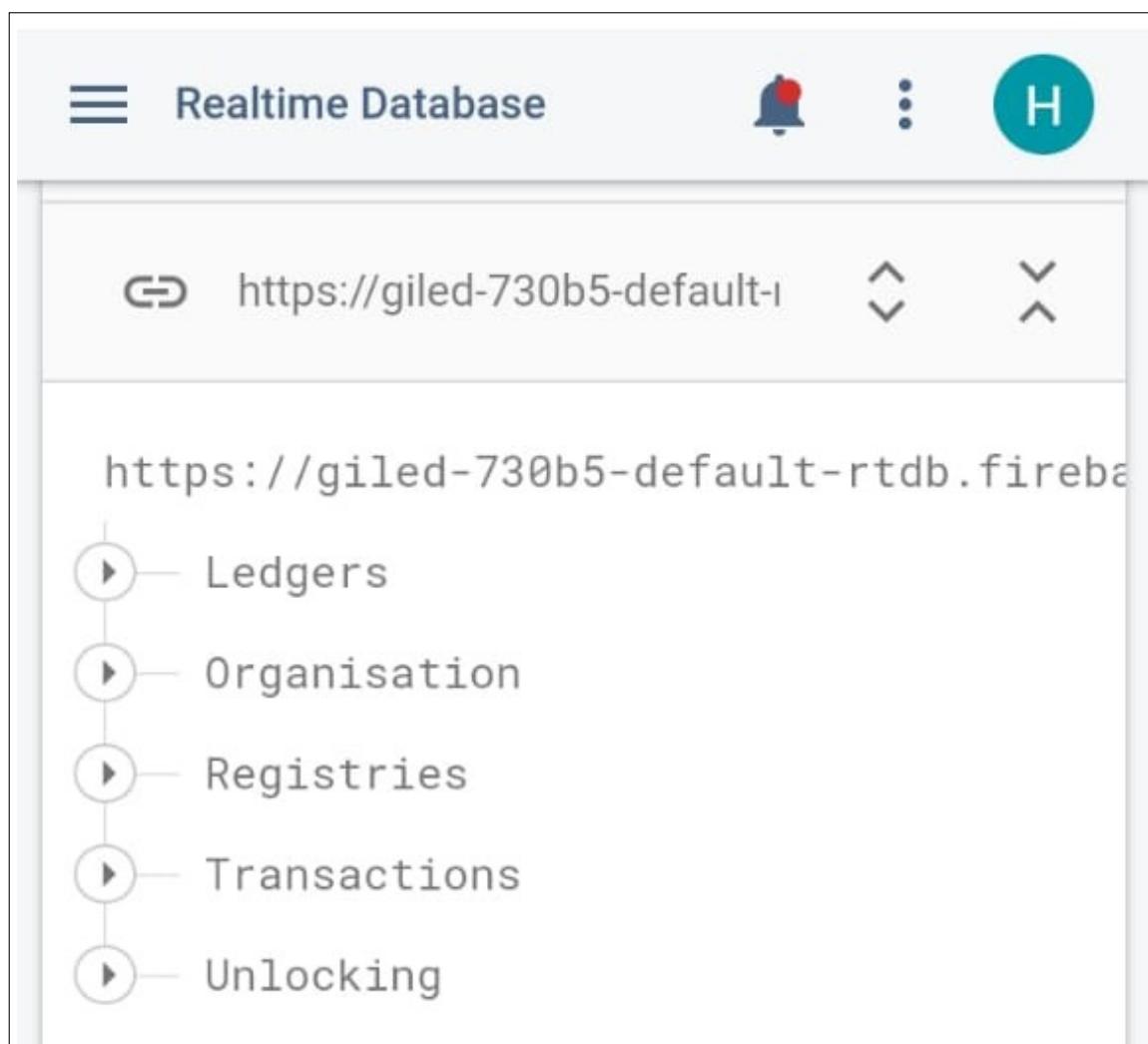


Figure 3.13: Network Structure

3.3 Network Structure



Figure 3.14: Ledger



Figure 3.15: Organisation

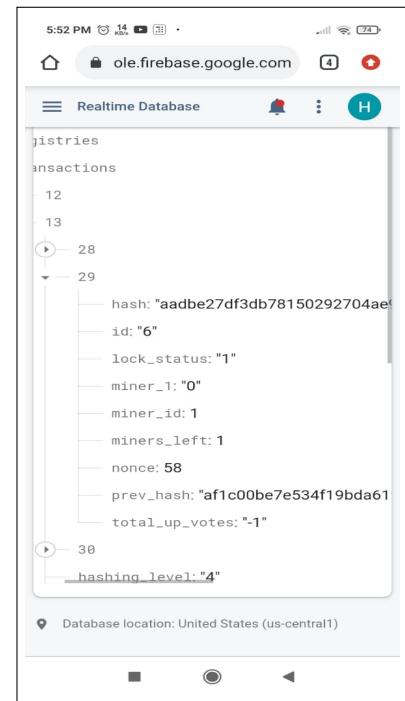


Figure 3.16: Transactions

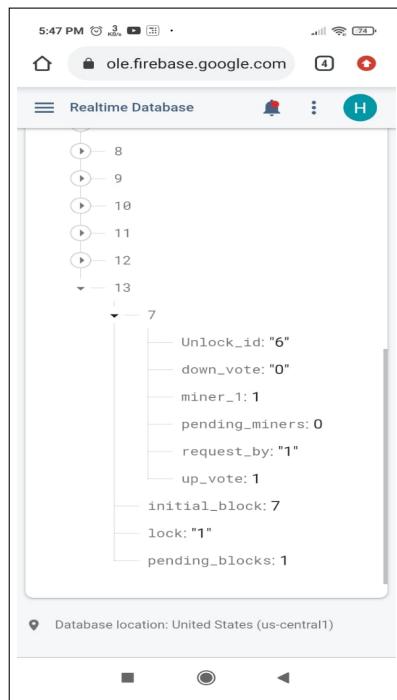


Figure 3.17: Unlocking



Figure 3.18: Registries

3.3.1 Ledger

This is a place where all the structure of ledgers will be stored. Ledger structure means the design of the database. It has the following attributes:

- hashing_level: security level to generate the hash.
- ledger_id: to show the unique id of the ledger.
- ledger_name: name of the ledger.
- miner_id: id of the user who have created the ledger.
- organisation: name of the organisation to which it belongs.
- total_fields: number of attributes the ledger has to store data which are labeled as 0, 1, 2..... and so on.

3.3.2 Organisation

This is a place where the structure of the organisation will be saved. All the details regarding the organisation will be there. It has the following attributes:

- country: from which country it belongs.
- id: unique id of the organisation.
- miner_id: id of the user who have created this organisation.
- name: name of the organisation.
- owner: who is the owner of the organisation.
- place: place where it is located.
- state: in which state is is located.
- total_ledgers: number of the ledgers this organisation has which are listed as ledger_0, ledger_1, and so on.
- total_miner: total number of members in the organisation.
- type: what kind of organisation it is example private or government or anythings else.

3.3.3 Transactions

This is a place where all the data travels. The data which is generated is sent over here to be distributed over the network (means among the other user of the same organisation).

Here all the blocks are accumulated and it makes a chain in sequence. It has the following attributes:

- hash: unique fingerprint of a block which is 64 character (256 bit) long.
- id: sequence number of the block.
- lock_status: it the data of the block locked or unlocked for the updation.
- miner_id: id of the user who had created the block.
- nonce: a number to make the hash value valid.
- prev_hash: hash value of the previous block.
- miner_0, 1, 2,...,n: user ids to whom the block to be sent.
- total_upvotes: number of user who have approved for unlocking (if it is an unlocking request).

Note: As it is decentralised system, data will not be stored here permanently, as soon as all the user fetches the block the data will be deleted from here.

3.3.4 Unlocking

This is the place where all the unlocking request arrives. To lock the data no need to ask permission to anyone but to unlock any data (either record or whole ledger) then we need to send unlocking request to ask everyone about the unlocking of the data. It has the following attributes:

- initial_block: number to be assigned to the block in sequence.
- lock: lock variable used for mutual exclusion.
- pending_block: number of block left for the approval.
- unlock_id: number of sequence used to provide number to block.
- down_vote: number of users who have rejected the unlock request.
- pending_miners: number of user pending to make decision about lock or unlock.
- request_by: id of the user who is willing to unlock record or ledger.
- up_vote: number of users who have accepted the unlock request.

3.3.5 Registries

This is the place to store the user information. It has the following attributes:

- email: email of the user.
- id: unique id of the user.
- password: password to login to system.
- phone_No: contact number of the user.
- total_org: total number of organisation in which the user has joined which are listed as organisation0, organisation1,.....and so on.
- username: name to be displayed on the system.
- total_count: total users.

3.4 UML Diagrams of Project

3.4.1 Activity Diagram

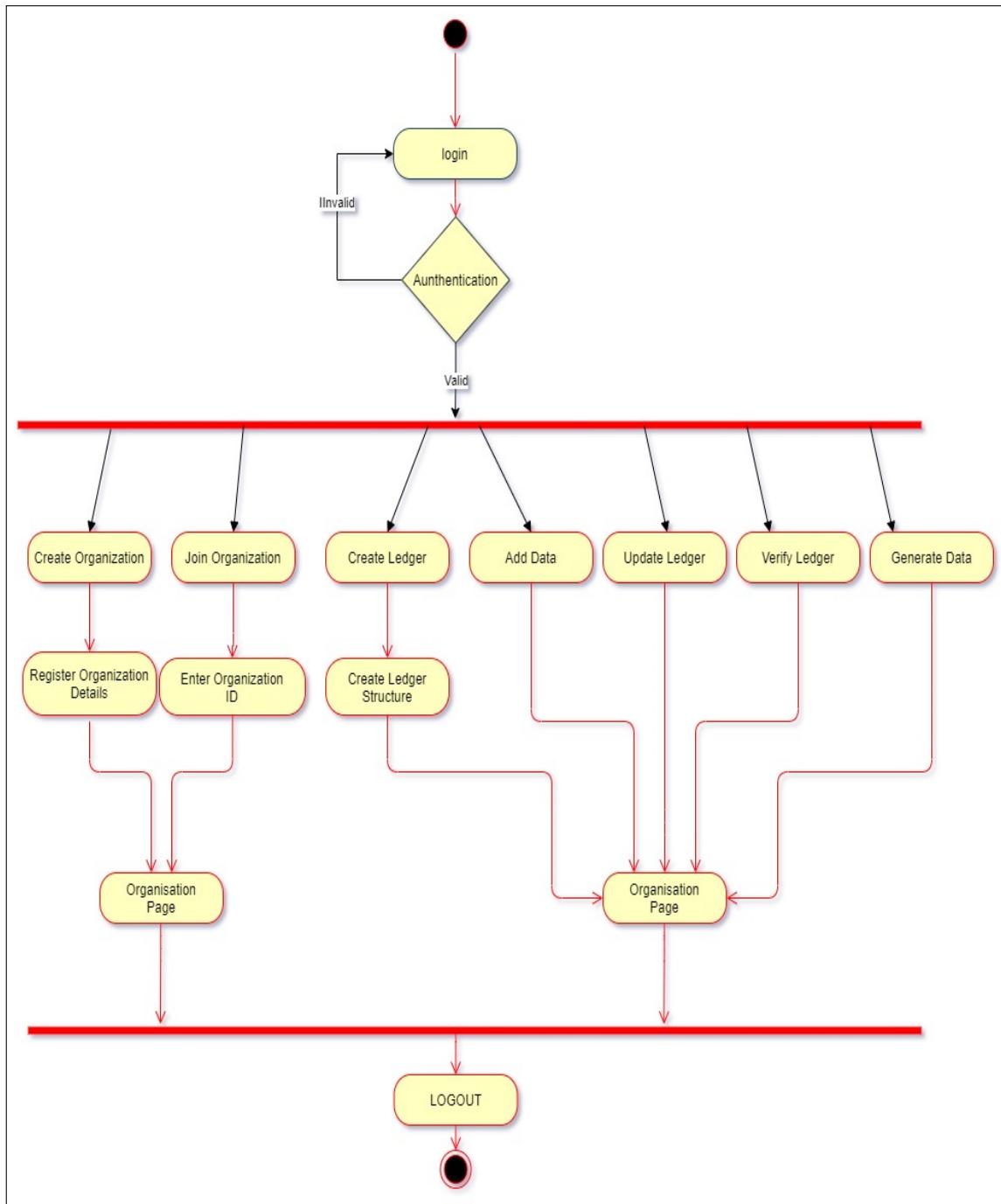


Figure 3.19: Activity Diagram

This is the activity diagram which shows the kinds of operations that can be performed on the system.

1. First of all need to login into the system.
2. If the credentials are valid then will able to enter into the system, else it will be failed and you will be end up on same page.
 - We can create organisation.
 - We can join organisation.
 - We can create ledger structure.
 - Add data to the chain.
 - Update the ledger.
 - Verify Ledger.
 - Create final database.
3. logout.

3.4.2 Sequence Diagram

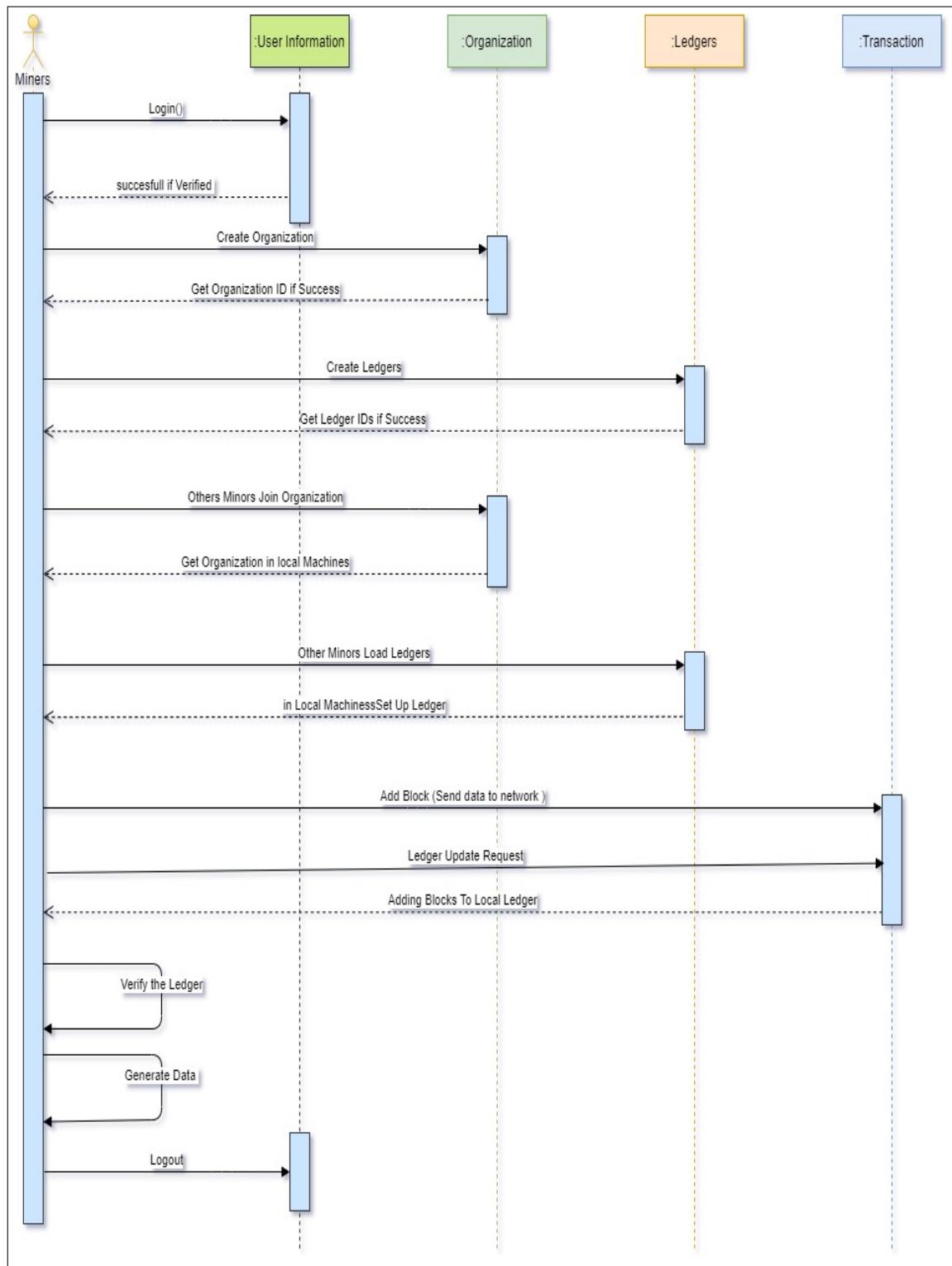


Figure 3.20: Sequence Diagram

This is the sequence diagram of the system which shows the sequence of adding block in the chain (on network).

1. First of all need to login into the system.
2. If the credentials are valid then will able to enter into the system, else it will be failed and you will be end up on same page.
3. Then need to create the organisation (if already created then just need to in it using the organisation id) then will get the organisation id.
4. Create ledger structure (if joined the organisation then ledger structure will be already there in the system).
5. Add other users into organisation.
6. Now we can perform all the operations like add, update or delete the data.
7. To get all the data in the system, we need to update the ledger.
8. Verify the ledger and then create the database (if ledger is not verified then database will not be created).
9. logout.

3.4.3 Use Case Diagram

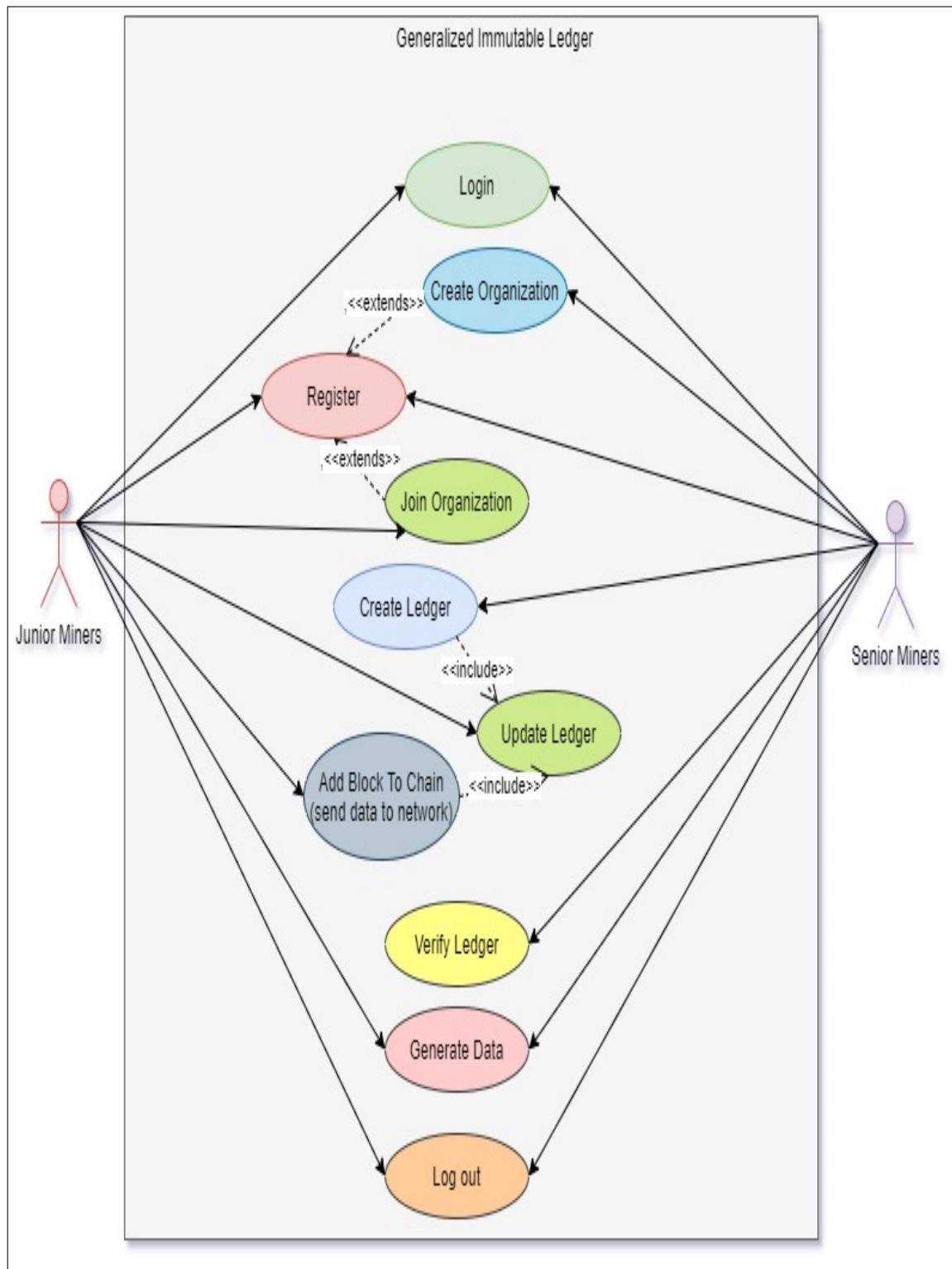


Figure 3.21: Use Case Diagram

This diagram shows the usecases of the system for the members of the organisation.

- Login.
- Register (then create or join organisation).
- Create ledger.
- Add data to blocks.
- Lock record or ledger.
- Unlock record or ledger.
- Verify ledger.
- Generate Database.
- logout.

3.5 Algorithms

3.5.1 Hash value while adding new block

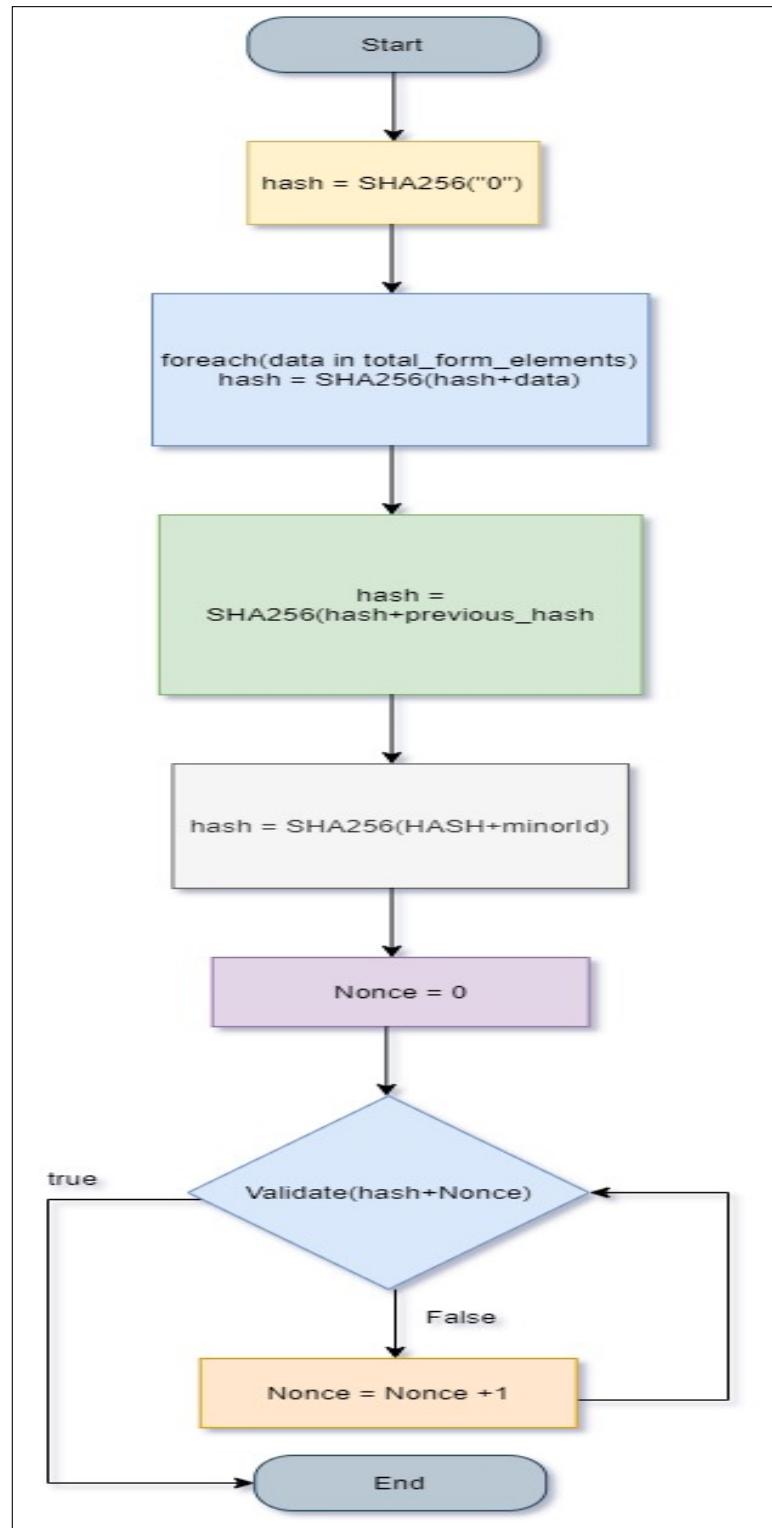


Figure 3.22: Add Block Hash Algorithm

This algorithm used to generate the hash value of the data that has been sent to network.

Each and every time the a new block is added, the new hash will be generated using this algorithm and then added to the network for the further distribution.

The algorithm keeps on looping for the nonce value. The nonce value will be validated from the function named "validate function".

Input

- Attribute Data
- Previous Hash
- User id

Output

- 64 character (256 bits) hash value

3.5.2 Hash value of lock request

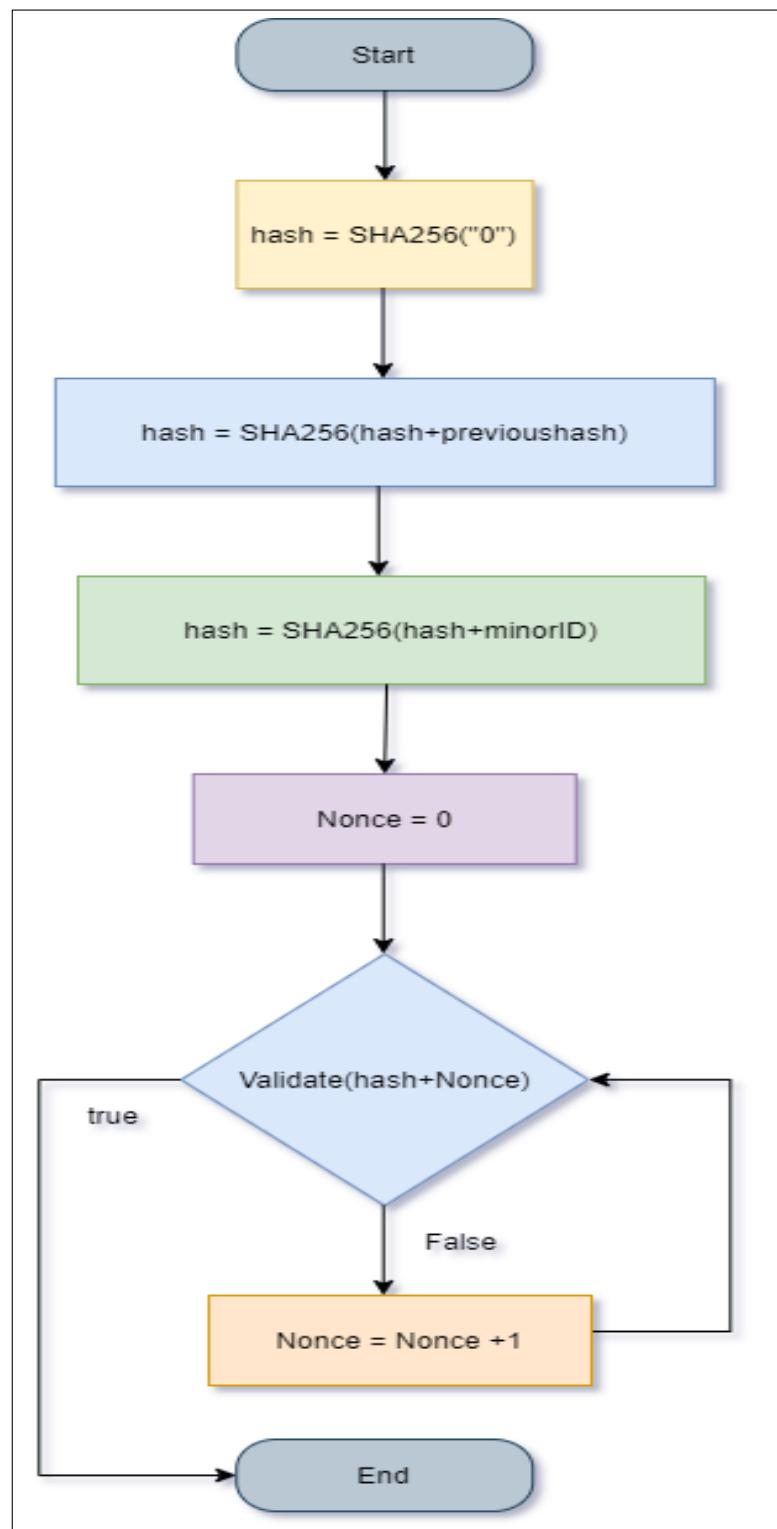


Figure 3.23: Lock Ledger Hash Algorithm

This algorithm used to generate the hash value of the request to lock record or ledger on the network.

Whenever the user wants that the data of the particular record or the ledger itself doesn't changes then new block is added and the hash which is generated is created by this algorithm.

To perform lock operation, we don't the user id of other user users, just the id of the user who is locking the record or data.

Input

- Ledger/record
- Previous Hash
- User id

Output

- 64 character (256 bits) hash value

3.5.3 Hash value of unlock request

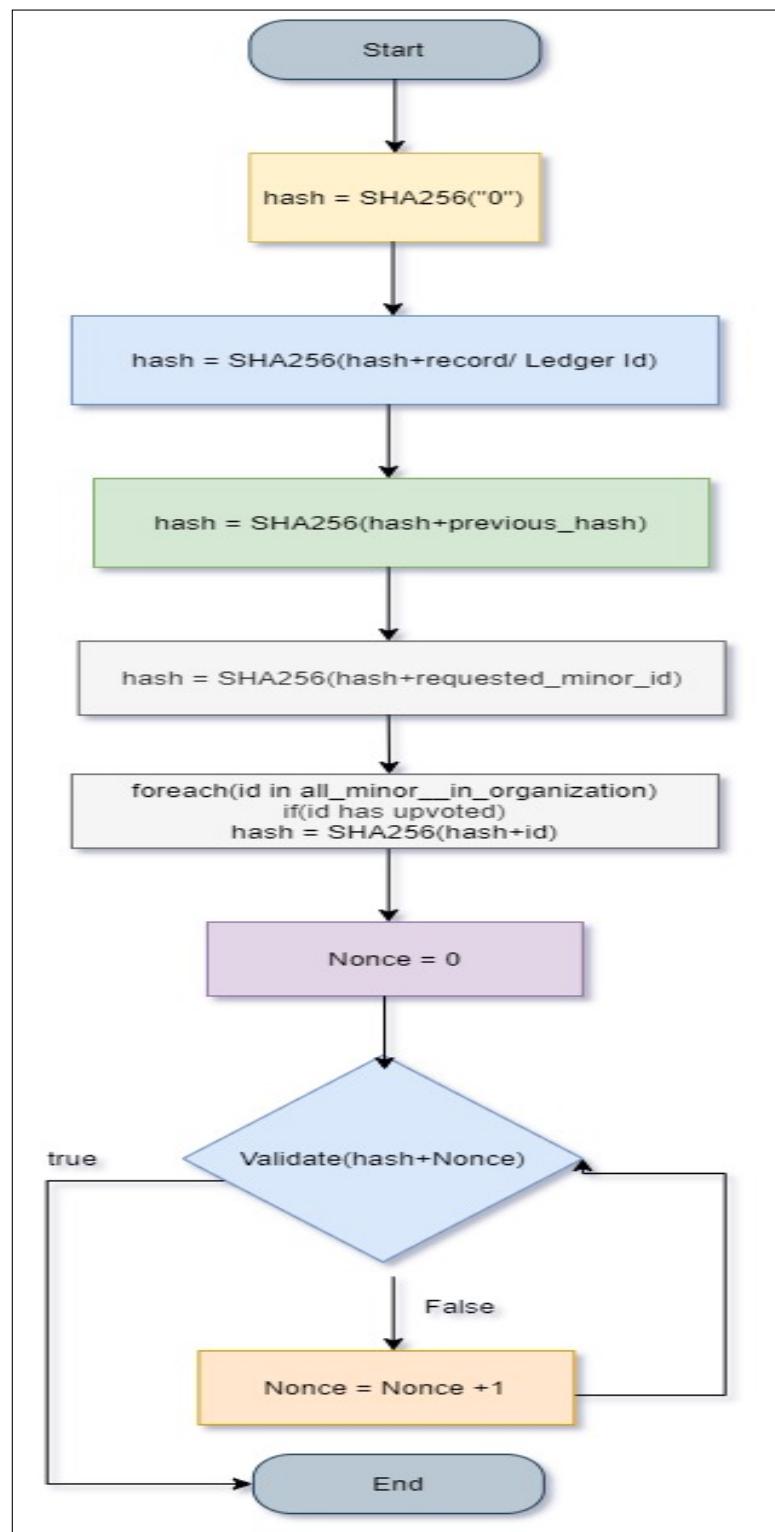


Figure 3.24: Unlock Ledger Hash Algorithm

This algorithm used to generate the hash value of the request to lock record or ledger.

Whenever the user wants to unlock a record or the entire ledger then the request generated will use this hashing algorithm.

In this algorithm, we need the user id of all the members accepting to unlock request.

Input

- Ledger/record
- Previous Hash
- User id
- All user id who supports to unlock the record or ledger

Output

- 64 character (256 bits) hash value

3.5.4 Validate Hash

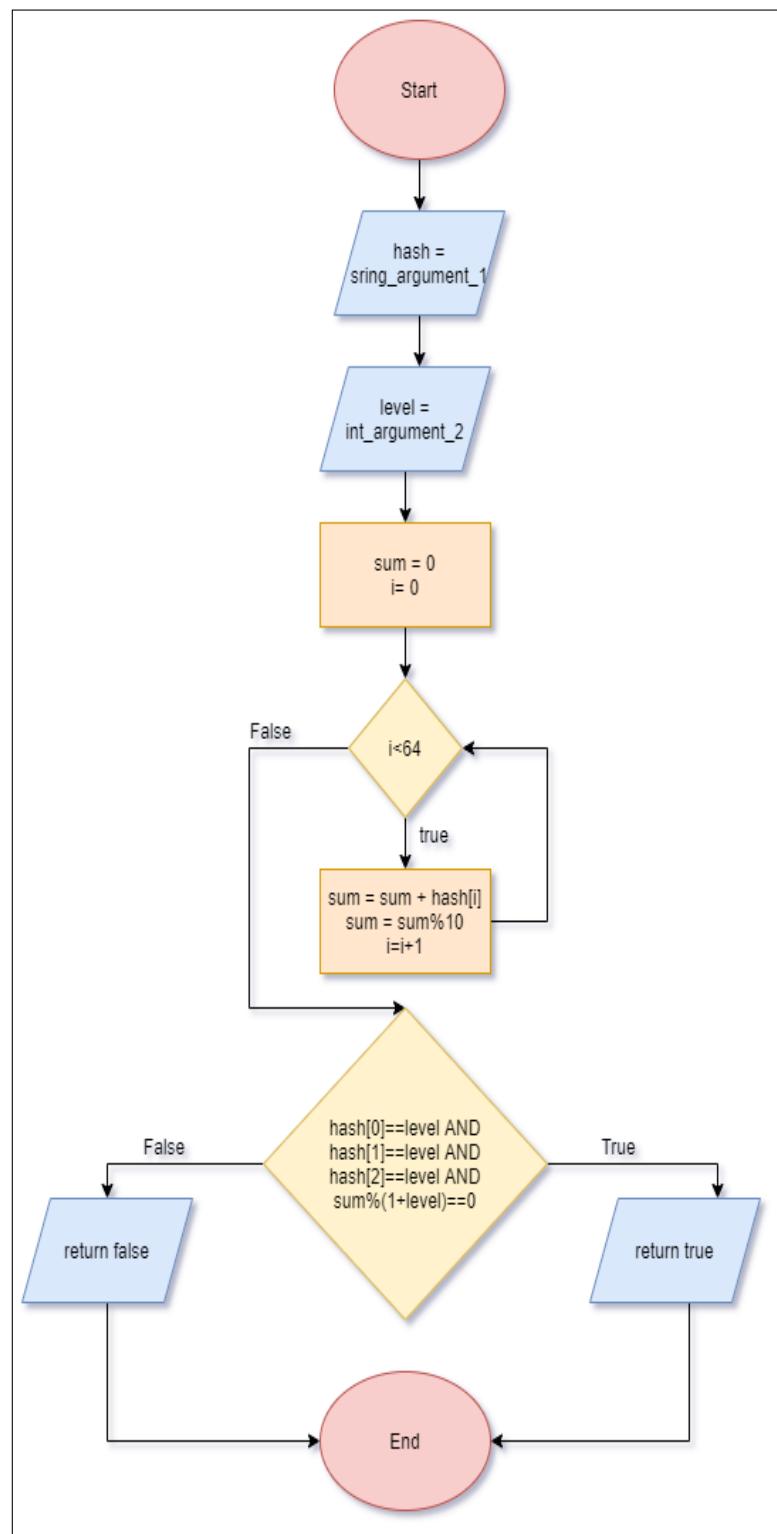


Figure 3.25: Algorithm for validate function

This algorithm used to generate the hash value of the request to lock record or ledger.

Input

- 64 character (256 bits) hash value
- Hashing level

Output

- True if it is valid hash, else false.

Chapter 4

Conclusion and Future Scope

4.1 Conclusion

- Developed to provide a distributed immutable ledger to an organisation.
- Provides a database with complete transparency within the organisation.
- Does not allows unwanted or hidden manipulation due to blockchain.
- Flexible to design the database according to need.
- Changes are based on the permission of majority on the organisation.

4.2 Future Scope

- Currently it is accepting only text box, radio button and check box as input elements, in future we will plan to take more input elements like: image, documents like pdf, word etc.

References

- [1] S. Ngamsuriyaroj, T. Likittheerameth, A. Kahutson, and T. Pathummasut, “Package delivery system based on blockchain infrastructure,” in *2018 Seventh ICT International Student Project Conference (ICT-ISPC)*, pp. 1–6, IEEE, 2018.
- [2] K. Chopra, K. Gupta, and A. Lambora, “Proof of existence using blockchain,” in *2019 International Conference on Machine Learning, Big Data, Cloud and Parallel Computing (COMITCon)*, pp. 429–431, IEEE, 2019.
- [3] M. A. Fiquaro, R. Zahilah, S. H. Othman, M. M. Arshad, and S. M. S. Saad, “Vaccination system using blockchain technology: a prototype development,” in *2021 3rd International Cyber Resilience Conference (CRC)*, pp. 1–6, IEEE, 2021.
- [4] E. Shaheen, M. A. Hamed, W. Zaghloul, E. Al Mostafa, A. El Sharkawy, A. Mahmoud, A. Labeb, M. O. Al Enany, and G. Attiya, “A track donation system using blockchain,” in *2021 international conference on electronic engineering (ICEEM)*, pp. 1–7, IEEE, 2021.
- [5] S. Dalla Palma, R. Pareschi, and F. Zappone, “What is your distributed (hyper) ledger?,” in *2021 IEEE/ACM 4th International Workshop on Emerging Trends in Software Engineering for Blockchain (WETSEB)*, pp. 27–33, IEEE, 2021.
- [6] M. Latha, R. Chinnaian, *et al.*, “Blockchain as a service (baas) framework for government funded projects e-tendering process administration and quality assurance using smart contracts,” in *2021 International Conference on Computer Communication and Informatics (ICCCI)*, pp. 1–4, IEEE, 2021.
- [7] D. Mali, D. Mogaveera, P. Kitawat, and M. Jawwad, “Blockchain-based e-tendering system,” in *2020 4th International Conference on Intelligent Computing and Control Systems (ICICCS)*, pp. 357–362, IEEE, 2020.

- [8] R. Nunes, B. Alturas, and A. L. Fernandes, “Creating value in equity crowdfunding platforms using blockchain technology,” in *2021 16th Iberian Conference on Information Systems and Technologies (CISTI)*, pp. 1–6, IEEE, 2021.
- [9] I. Natgunanathan, P. Praitheeshan, L. Gao, Y. Xiang, and L. Pan, “Blockchain-based audio watermarking technique for multimedia copyright protection in distribution networks,” *ACM Transactions on Multimedia Computing, Communications, and Applications (TOMM)*, vol. 18, no. 3, pp. 1–23, 2022.
- [10] K. Teja, M. Shravani, C. Y. Simha, and M. R. Kounte, “Secured voting through blockchain technology,” in *2019 3rd international conference on trends in electronics and informatics (ICOEI)*, pp. 1416–1419, IEEE, 2019.
- [11] M. D. R. Zainuddin and K. Y. Choo, “Design a document verification system based on blockchain technology,” in *Multimedia University Engineering Conference (MECON 2022)*, pp. 229–244, Atlantis Press, 2022.
- [12] W. Xin, “Fighting covid-19 and helping economy reopen by using blockchain technology,” in *2020 IEEE/CIC International Conference on Communications in China (ICCC Workshops)*, pp. 102–105, IEEE, 2020.
- [13] X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, “A blockchain-based medical data sharing and protection scheme,” *IEEE Access*, vol. 7, pp. 118943–118953, 2019.
- [14] H. M. Garcia, M. M. Cortez, and E. D. Amaya, “Blockchain-based website solution for controlling the authorized sale of drugs in peru,” in *2020 IEEE Engineering International Research Conference (EIRCON)*, pp. 1–4, IEEE, 2020.
- [15] M. Mut-Puigserver, M. A. Cabot-Nadal, and M. M. Payeras-Capellà, “Removing the trusted third party in a confidential multiparty registered edelivery protocol using blockchain,” *IEEE Access*, vol. 8, pp. 106855–106871, 2020.
- [16] G. Le, Q. Gu, Q. Jiang, and W. Lin, “Trustedchain: A blockchain-based data sharing scheme for supply chain,” in *2020 International Conference on Data Mining Workshops (ICDMW)*, pp. 895–901, IEEE, 2020.
- [17] M. Lohr, B. Schlosser, J. Jürjens, and S. Staab, “Cost fairness for blockchain-based two-party exchange protocols,” in *2020 IEEE International Conference on Blockchain (Blockchain)*, pp. 428–435, IEEE, 2020.

- [18] M. Xie, Z. Liao, and L. Huang, “Data security based on blockchain digital currency,” in *2020 3rd International Conference on Smart BlockChain (SmartBlock)*, pp. 5–10, IEEE, 2020.
- [19] D. Saveetha, “Movie rating system based on blockchain,” in *2021 International Conference on Computer Communication and Informatics (ICCCI -2021)*, pp. 5–10, IEEE, 2021.
- [20] N. Jnoub and W. Klas, “Detection of tampered images using blockchain technology,” in *2019 IEEE International Conference on Blockchain and Cryptocurrency (ICBC)*, pp. 70–73, IEEE, 2019.