DEPARTMENT OF COMPUTER SCIENCE & ENGINEERING,
SHARDA SCHOOL OF ENGINEERING AND TECHNOLOGY,
SHARDA UNIVERSITY, GREATER NOIDA

HEALTH INSURANCE SETTLEMENT USING BLOCKCHAIN

A project report submitted

in partial fulfillment of the requirements for the degree of

Bachelor of Technology in Computer Science and Engineering

by

ATAMJEET SINGH KOHLI (2019001786)

MANISH RAI (2019003752)

ARSHI RAIES (2019620291)

Supervised by:

DR. MAYANK KUMAR GOYAL

Associate Professor

May, 2023

CERTIFICATE

This is to certify that the report entitled **"Health Insurance Settlement Using Blockchain"** submitted by **"Atamjeet Singh Kohli (2019001786), Manish Rai (2019003752) and Arshi Raies (2019620291)"** to Sharda University, towards the fulfillment of requirements for the award of the degree of **"**Bachelor of Technology in Computer Science and Engineering**"** is record of bonafide final year Project work carried out by them in the **"**Department of Computer Science & Engineering, Sharda School of Engineering and Technology, Sharda University**"**. The results/findings contained in this Project have not been submitted in part or full to any other University/Institute forward of any other Degree/Diploma.

Signature of the Guide:
Name: Dr. Mayank Kumar Goyal
Designation: Associate Professor (CSE)

Signature of Head of Department
Name: Prof. (Dr.) Nitin Rakesh
Place: Sharda University
Date

Signature of External Examiner
Date:

ACKNOWLEDGEMENT

A major project is a golden opportunity for learning and self-development. We consider ourselves very lucky and honored to have so many wonderful people lead us through in completion of this project.

First and foremost, we would like to thank **Dr. Nitin Rakesh**, HOD, CSE who gave us an opportunity to undertake this project. We are grateful to **Dr. Mayank Kumar Goyal** for his guidance in our project work. **Dr. Mayank Kumar Goyal**, who in spite of being extraordinarily busy with academics, took timeout to hear, guide and keep us on the correct path. We do not know where we would have been without his help.

The CSE department monitored our progress and arranged all facilities to make life easier. We choose this moment to acknowledge their contribution gratefully.

Name and signature of Students:

Atamjeet Kohli (2019001788)

Manish Rai (2019003752)

Arshi Raies (2019620291)

ABSTRACT

A health record of any individual is needed to get information about the individual, like what kind of medical history they have, and data regarding treatment in the past, allergies, scans and test results, etc. Right now, there are only EHR presents, which store data of the individual, but they have many issues with them, like the fact that they can be tempered with or modified, which can ultimately be really harmful for the patient. So, there is a need for a solution that can resolve these issues. We are presenting a solution or a framework that can be used to transform and prevent these problems by using the features provided by blockchain technology, like security, privacy, transparency, confidentiality, and the most important of them all is decentralization. We are also using another technology known as IPFS. The use of IPFS along with blockchain will efficiently help in reducing the problems faced by today's EHRs systems. During Medical emergencies, Health Insurance plays a critical function in providing us with coverage for medical bills. However, preventing data breaches and safeguarding the data is not guaranteed right now. The most serious concern in this industry is the fraudulent use of health-care data. Transparency, which is a major concern in the health field, is provided by Blockchain Technology. In this article, we build an insurance claim model that will use Blockchain to assist our system preserve openness for both the insurer and the enterprise. This suggested concept eliminates the need for a middleman and provides direct interaction between the insurance, hospital, and firm. IPFS is a decentralized file storage system that allows users to securely exchange huge files. Our studies focus on merging IPFS and blockchain to store the patient's confidential data in a distributed file system called Blockchain technology stores IPFS and the cryptographic addresses of the files.

CONTENTS

LIST OF FIGURES

LIST OF ABBREVIATIONS

EHR	Electronic Health Records
IPFS	Inter Planetary File System
dApps	Decentralized applications

CHAPTER1: INTRODUCTION

The healthcare industry generates a large amount of data every day, and the security and privacy of this data is crucial. Conventional contractual methods for storing this data are not entirely safe, and data breaches and manipulations are a significant concern. The blockchain technology, known for its security, transparency, and decentralization, provides a promising solution for the healthcare industry. In this context, a health insurance system that achieves data security, immutability, and transparency using smart contracts, IPFS, and blockchain technology is presented.

Blockchain technology stores data hashes and transaction metadata in a chain of blocks, making it unchangeable and secure. Smart contracts facilitate different blockchain system operations and enable the application of business strategy in blockchain technology. IPFS is a decentralized file storage system that allows for secure exchange and storage of large files, including personal information, insurance policy details, and medical health records. Using a content-addressed approach, IPFS provides a hash value that can be securely saved, and data is separated and hashed before being stored on a dispersed network. The address of the file is contained in the cryptographic hash produced by IPFS, and a hash table that is distributed is kept up by IPFS. In this way, blockchain technology, IPFS, and smart contracts provide a secure and decentralized healthcare data management system.

1.1 Problem Statement

The healthcare sector faces significant challenges when it comes to managing health records and insurance settlements. The problem of data breaches and privacy violations in the healthcare industry is a major concern, and traditional electronic health records (EHRs) have proven to be vulnerable to tampering and modification. This not only compromises patient confidentiality but also puts their health at risk. Therefore, there is an urgent need to develop a secure and trustworthy health record management system. Blockchain technology offers a promising solution to these issues by providing security, privacy, transparency, and decentralization. By using blockchain, healthcare providers can store and manage patient health records securely, and patients can have control over who can access their data. In addition, the integration of Interplanetary File System (IPFS) can further enhance the security and efficiency of the system by allowing large files, such as medical images and test results, to be stored in a decentralized file system.**[2]** Furthermore, the use of blockchain technology can also revolutionize health insurance settlement by creating a more transparent and efficient system. By using smart contracts and blockchain-based insurance claim models, the need for intermediaries can be eliminated, and direct communication between insurers, hospitals, and patients can be established.

This can lead to faster and more accurate claim settlements, reducing the burden on both healthcare providers and patients. In summary, the use of blockchain technology for health record management and insurance settlement can address the critical challenges faced by the healthcare industry and provide a secure and efficient solution for managing patient data and insurance claims.

1.2 Existing Work

In recent trends, we have heard about blockchain technology and how it is being used in all fields, including healthcare. Blockchain offers improved user experience, safety of data, and the authority of the user to use the system to their convenience.**[13]** The aim is to provide software that is cost-effective and easy to use, with data integrity and security of the user's data. Blockchain technology offers an untampered platform for storing user records, which is particularly useful for confidential and sensitive information, such as health records. Health records are sensitive information, making them valuable to cybercriminals. But as EHR is a digital ledger, its security can be compromised or breached, which can harm the patient being treated.

If a cybercriminal gains access to one's health data, they could alter these records, leading to doctors misunderstanding the patient's medical history and potentially endangering the patient's health. Although there are laws to regulate the cybersecurity of health data, the most stringent of these rules don't apply across every service in every state, and accidents can still happen. Therefore, there is a need to implement better technology to safeguard the patient's data, and one such technology is blockchain. A blockchain-based EHR can be used to secure the privacy of the patient's health data and also give them control over their data.

A blockchain is the interconnection between the blocks which each of them connected to each other creating a chain of blocks. Each block stores some data as well as hash of the previous block and hash of the next block **[3]**. These hashes are the one that would be changed if someone tries to change or tamper the data ultimately chaning the hash of that block and then the previous block would not be able to identify and connect to the next block. That is how it is secure from tampering.

- Decentralized: Unlike traditional centralized storage systems, in blockchain, the patient's record data will be stored in all the nodes of the network, making health records decentralized.
- Immutable: If the records are not stored in one place and are present in every node of the network, tampering with them in one node will result in changing every other node of the network. Technically, there is also something called a hash function provided to every node, making tampering with them impossible.
- Transparent: All transactions are recorded in a ledger, so nothing will be hidden if changed or when a transaction happens.

The use of blockchain technology in the healthcare industry can also have a significant impact on insurance-related processes [7]. For example, when a patient undergoes a medical procedure, the cost is usually covered by their insurance provider. However, the insurance claim process can be slow and complex, often involving multiple intermediaries, which can lead to delays and errors. By using a blockchain-based system, insurance companies can automate the claims process and streamline the verification of patient information. This would lead to faster claim settlements and reduced administrative costs. Smart contracts are a piece of code to validate certain specific action written in them and then trigger the operation that is intended to be performed if the validation is correct.

They can also be used to automate the process of verifying insurance eligibility and payment amounts. In addition to improving the efficiency of insurance processes, blockchain can also help to prevent fraud. Insurance fraud is a significant problem in the healthcare industry, and it can be difficult to detect and prevent using traditional methods. By using blockchain technology, insurance companies can create an immutable record of all transactions, making it more difficult for fraudulent claims to go unnoticed **[4]**.

Moreover, blockchain technology can also help to eliminate the need for intermediaries in insurance processes, such as brokers and third-party administrators, who can increase costs and complexity. By using a blockchain-based system, insurance companies can create a decentralized network that allows for direct interactions between patients, healthcare providers, and insurance providers**.** Overall, the use of blockchain technology in the healthcare industry has the potential to revolutionize the insurance process, leading to faster claim settlements, reduced administrative costs, and improved fraud detection.

The project as there will be some parties like patients, doctors/hospitals, admin and insurance agency. Patients can register themselves directly to the website. Admin is the main head who can add new doctors and as well as insurance agency to the blockchain project. They all will have their roles like patient can store their medical data, can book appointments with the desired doctor. Doctors can check their appointments and do the treatment of the patient. After the treatment is done. Admin can generate the bill for the treatment of that particular patient.

The generated bill then can be paid directly to the hospital by the patient, or they can chose to claim it if they had insurance with the insurance agency connected with the hospital. If patient choses for the claim, insurance agency can check or validate if the claim is false or true, and then can pay the bill to the hospital that will then automatically updates the bill generated at the patient side as bill paid.

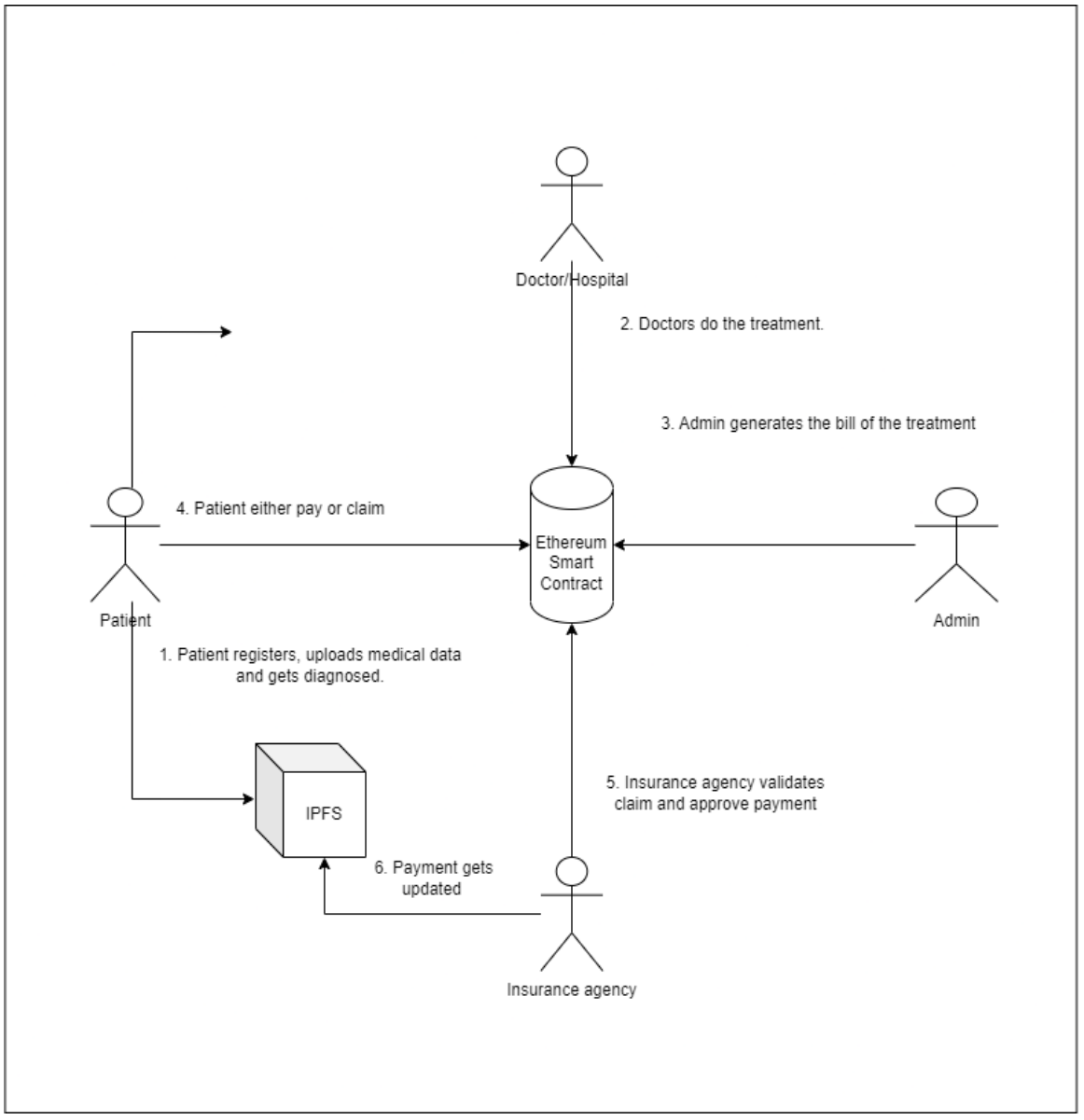


Fig 1. Overview of the project

1.3 Expected Outcome

Research paper submitted to ICCS Conference 2023
Acceptance Notification: By 30th April
A working project model/website

1.4 Hardware & Software Specification

1.4.1 Hardware Requirements

CPU: Intel® Core i7 12th Gen@2.1Gh
GPU: 6GB
RAM: 16GB

1.4.2 Software Requirements

Display: Standard monitor
OS: Windows Operating System
Language: JavaScript, solidity

1.4.3 Tech stack Requirements

- Ethereum ledger
- Metamask
- Truffle
- Ganache
- IPFS Kubo

1.5 Other Non-Functional Requirements

- **Reliability:** The probability of the software functioning faultlessly for a fixed period is called reliability.
- **Maintainability:** This means how long it usually takes, how easy it is, and how rapidly a software can be fixed or restored after an error occurs.
- **Recoverability:** It is the capability of a software to recuperate from a crash or failure and recommence regular functioning.
- **Performance:** Performance means how quickly a system can respond to a particular user's action while managing a specific workload.
- **Serviceability:** This feature shows how simple it is to provide service when it is required.

1.6 Report Outline

Chapter 2 focuses on the previous work done on the use of blockchain in the insurance settlement as well as the health record management of the patient, proposed system, and feasibility of our project.

Chapter 3 focuses on the proposed model, how it proceeds, what are the requirements and system features, and what technologies are required to build our project.

Chapter 4 provides the results and outputs of our work.

Chapter 5 finally concludes the whole project and report and discusses about the future scope of the proposed system.

CHAPTER 2: LITERATURE SURVEY

The blockchain technology used in the healthcare industry has become increasingly popular in recent years. One of the key applications of blockchain in healthcare is in health record management. Blockchain can provide a secure, decentralized, and tamper-proof platform for storing and sharing health records. By using blockchain-based electronic health records (EHR), patients can have more control over their health data and healthcare providers can access more complete and accurate patient information.

In addition to health record management, blockchain can also be used for health insurance settlement. Health insurance claims involve multiple parties, including patients, healthcare providers, and insurance companies. The current system for processing and settling health insurance claims is often slow, inefficient, and prone to errors. By using blockchain technology, insurance claims can be processed more quickly and securely, reducing administrative costs, and improving the accuracy and transparency of the claims process **[6]**.

Several studies have shown the potential benefits of using blockchain in health record management and health insurance settlement. For example, a study published in the International Journal of Medical Informatics found that using blockchain-based EHR can improve data privacy, data security, data integrity, and data interoperability. Another study published in the Journal of Medical Systems found that using blockchain for health insurance claims processing can improve claims accuracy, reduce administrative costs, and increase patient satisfaction. **[10]**.

So, ultimately it can be said that the blockchain technology can be of great help in the healthcare sector as it not only provides transparency and security but also comes with a lot of features that can be used to make the performance of the health care industry better and more efficient, the promising results of existing studies suggest that blockchain has a bright future in healthcare.

2.1 Existing Work

In this section, today's condition of health care systems is described all over the world. In present, many countries of the world like United Nations, Russia, United States, etc., they all use some kind of electronic health record. And India also has A-HMIS which is an information management system. The goal of this project is to combine all the medical information present in all medical facilities coming under AYUSH government programmed. But right now, in the present time, there is no solution that is available for it. The majority of the nation's medical facilities and also the facilities all over the world still follow the traditional centralized approach to store the data of the patient. And simultaneously, there is no standard defined and as it is medical data, it has to follow some government laws.

So, conclusively, the issues present in today's time with the patient record container systems are security, nation or global scalable architecture, and privacy of their data. EHRs were not designed to manage multi-institutional, lifetime medical records.**[2]**

To counter this issue, people have come up with many ways, and one of the ways that we are discussing here is to implement a technology named Blockchain. Martíez proposed a system architecture and provide implementation for the interoperability and end-to-end communication between personal health devices following the ISO/IEEE11073 standard and electronic health records following the ISO/EN13606 standard.**[13]** A blockchain is nothing but a distributed ledger which has many features like immutability, transparency etc., which make it one of the best candidates that can be used in containing the health data of patients. But technology is still new and in evolution phase, not much work or research has been done in this field. Work and research are being done in the implementation and use of this technology in medical data storage.

Many people have come up with different strategies to tackle the issue of storage of medical data. In general, the big idea is to have the blockchain at the core of the system, and just store the patient's data. Although blockchain is a promising technology it still has some drawbacks like we can't store data in huge volume in the blockchain network as every block in blockchain is limited to 1MB of space. And it is clear that 1MB of space would not be enough to store patient's data, it shows its inefficiency as the technology. To tackle this issue, people tried using a new technology named IPFS, it can be implemented parallel to the blockchain network. What it does is, it shrinks or compresses the data before storing it on the blockchain network.

In the current system, insurance agents manage the insurance claim procedure between the healthcare providers and the insurance company. Important papers including information about patients, health-related data, and insurance policy records may be purposefully or unintentionally leaked by insurance agents. The manual insurance claim procedure takes an enormous amount of time and effort to complete. From the over 1000 papers hit during the search on Google scholar before 2016, only about 45 % covered the Distributed Ledger technology and explained in detail its implementation. **[2]**

Read/write operations in a conventional distributed database are controlled by a centralized system. These records might be modified. Data theft and data tampering, which occur when records are housed on a central server, pose a danger to privacy and record authentication with the development of technology and an increase in the volume of records. Access control and data integrity are thus key issues in the healthcare and insurance industries. Claim fraud is a problem that insurance businesses must deal with as well. Bogus information may be given by the policyholder in order to pay for bogus claims. It is now difficult to identify fraud, which can lead to losses for the business and lengthen the time it takes to execute transactions and settle payments since more sources may need to be consulted.

A Flaws in current system:

1)The existing environment involves a lot of paperwork, and it's possible to manipulate information at every level, which costs the insurance sector a lot of money. Data might end up being inaccurate and soiled.

2)The whole insurance sector involves a variety of stakeholders, including policyholders, physicians, and hospitals, among others. As a result of the engagement of different stakeholders, the entire claim flow functions independently, which makes it more difficult to share records.

3)Handling insurance claims take an enormous amount of time and money since there are so many different stakeholders, which makes the customers unhappy.

4)Updating the patient information is laborious. Insurance companies don't have accessibility to all of the patient data, which results in incorrect policy assignments and higher processing costs.

5)There is a security risk associated with having customer and policyholder information maintained on a single server.

6)Insurance providers, healthcare and clearinghouses are involved in the whole process of claim of the insurance. Clearinghouses may intentionally or unintentionally leak critical health records. **[5]**

2.2 Proposed System

In this section, the design of our setup and implementation of our setup is discussed. Our setup is a user application which has an easy-to-understand User Interface. There are different features defined for different types of users, like patients can register themselves, book an appointment, upload their documents, and for doctors as well, they can register themselves, would have appointments booked for them etc.

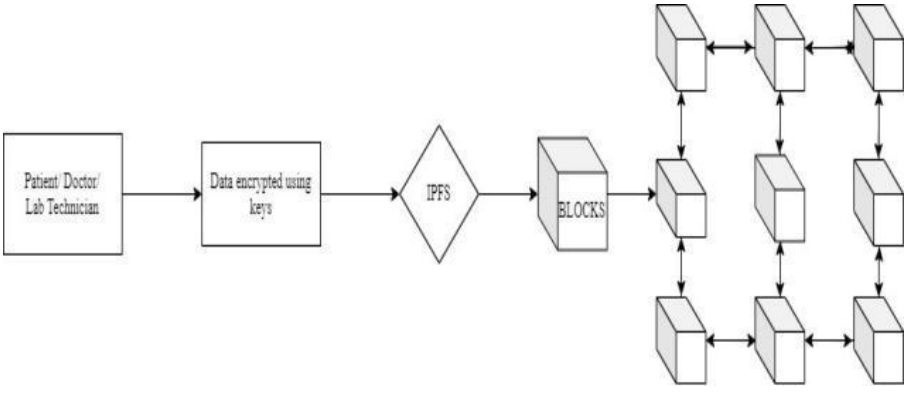


Fig 2: Framework Model

We can’t directly store the data on the network as for every user there will be huge amount of data and it will continue to increase in future, and blockchain would not be able to handle that much data when the number of user increases. So, there is a need for some way to shrink the data before storing on the network. IPFS is used to solve that issue. So, every data that is going to be stored on the blockchain network is going to go through IPFS. The records will be having a has a hash value that is stored in UI (still in exp phase). Then, after the addition of the data, the blockchain network will store all this info with the hashes of the transactions done with their respective time stamp. When the block is ready to be added to the network, a new and unique hash gets created with their respective time stamp. Also, there is storage available for those transactions that weren’t complete, they are stored in the memory buffer and remains there until some new transaction appear.

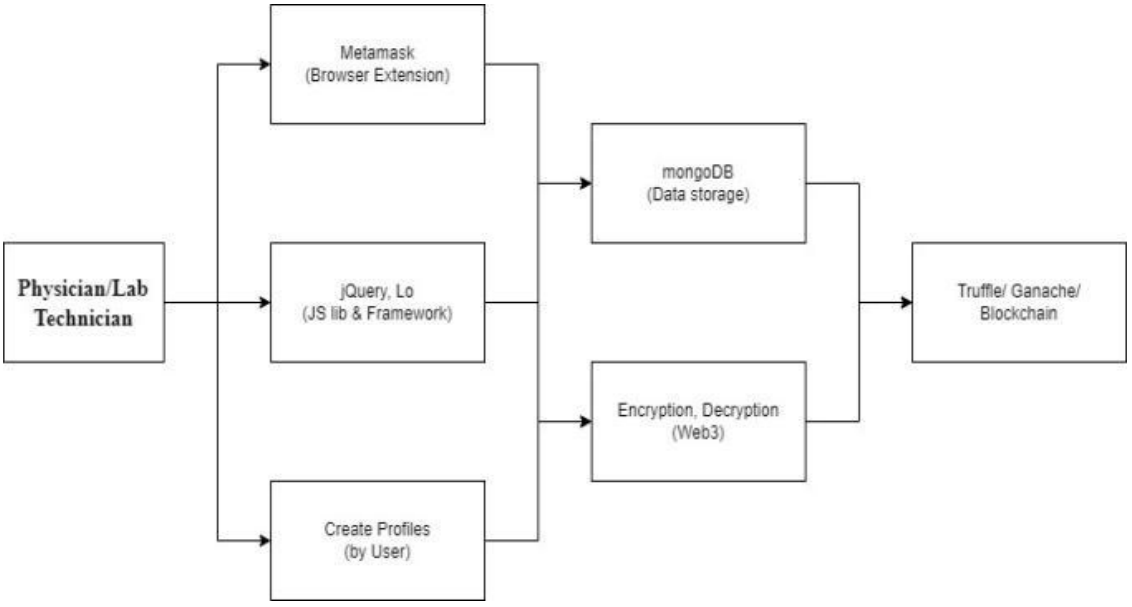


Fig 3: Technology Used in Our System

It is made sure that the data like timestamp of data uploaded and block’s timestamp cannot be altered. To download the data from the network, the user has to validate and verify their credentials. And the data present in the blockchain will not be altered, as one change in hash of data, it will result in making it a completely new file and with it its timestamp will also be changed. This feature of the combined system gives user to trust the system completely as they are immutable in nature.

There is one more hindrance or restriction in the system i.e., to give the user freedom to make changes to their file system, and for that we can have a backup somewhere. It means when the data is being stored on the IPFS, a backup of the IPFS will be done. Then, it will be connected making it a coupled resource in nature. So, when a user or patient will want their file to be deleted, it will be deleted locally, as it is not possible to delete the files from the whole network. The user or patient does not need to worry about their file still being present in the network, as it will be restricted and can’t be viewed by others.

One more issue is when patient wants to update the file, it would not be possible to do it without changing the hash of previous file that was uploaded. So, for this, it was decided that every uploaded file would be a complete independent entity and at the same time all the hash of all the files uploaded by a patient will be in a collection and will be maintained. The privacy of user's file should be maintained too as it would be stored at multiple nodes on the network. The provided solution is to not let the user to fill a personal identifier to their file.

The file identification would be limited to hash collection, their private key, and timestamp mapped for every other hash being maintained in the network. Ultimately resulting in making the user's data impossible to find or trace. We looked at ways to implement a blockchain-based system that would process claims in real time, more transparently, and independently in the medical insurance sector. For storing the outcome, smart contracts were utilized and added to the distributed ledger (a blockchain platform).

The demands made by the stake holders are handled via methods in smart contracts. Smart contracts are the piece of code that are used for the validation of the certain specific thing as specified in the program and then if the validation comes to be true, then it triggers some action that is also specified in that piece of code. They can help to reduce the false number of claims of insurance, which is one of the major problems in the healthcare and insurance industry [22]. Smart contracts will be helpful in automating the process of validation of insurance claims by identifying the patient health records if they are correct or not.

A. Core Members of the Proposed Model

Insurance Companies includes Policy Holders, Hospitals (Service Providers to Policy Holders), New Policy Applications, Claiming, and Getting Refunds for the Same. In order for any of the two organizations to get reimbursement for treating the patient, the hospital may submit an insurance claim.

B. Various Components in the Model

Roles that are automated by smart contracts determine which data may be accessed. The outcomes of each transaction's execution are tracked by a distributed ledger. Cryptographic techniques are used to authenticate users and grant access to resources **[19]**. Smart contracts are used in the framework to power the transactions.

Every smart contract has specific rules that must be followed in order for transactions to be added to the blockchain. Depending on the outcome of the validating block, nodes will be adding a block to the medical insurance blockchain after validating a transaction. Smart contracts are used in the framework to power the transactions.

C. Registration

A minimum of one primary account, such as [EOA], to be held by every stakeholder. Alternatively, the insurance provider may create the account by calling eth.createAccount(), which produces the key pair needed to connect to the network. Each account's addresses, which is generated from the owner's public key, is used to index all of the accounts. In our situation, smart contracts handle identity authentication and management in a decentralized manner.

D. Insurance Model

The situation when the primary transactions are routine insurance procedures, such as client registration, claim filing by either the policyholder or the hospital, processing of refunds, etc. As a result of all transactions being transparent and traceable per evidence, the qualities of blockchain make guarantee that policyholders do not fraudulently accuse insurance companies of providing subpar services. The suggested framework process is shown in Figure 4.

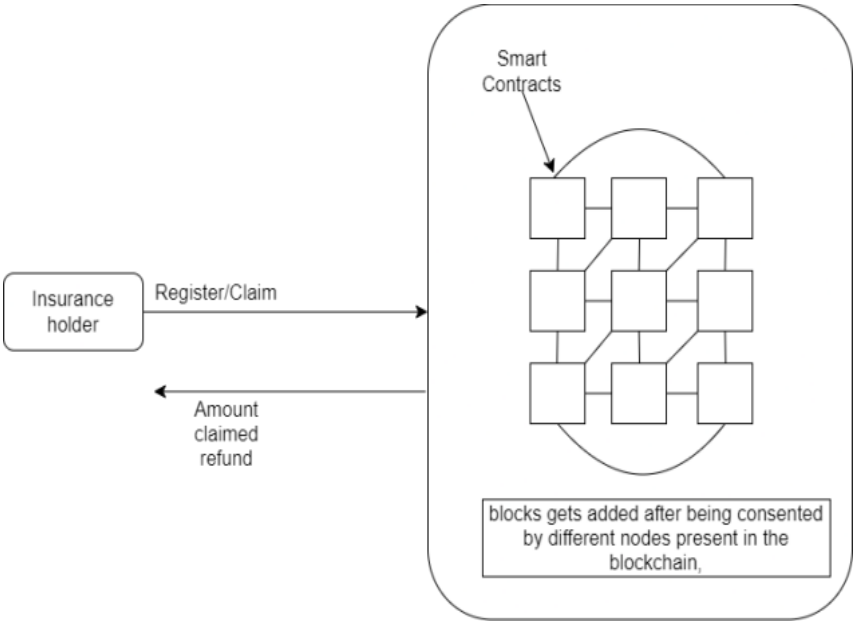


Fig 4: Architecture of Insurance Model

A transaction that takes place should comply with the requirements set out by the smart contract; otherwise, the transaction will be placed in uncle block until a period of time before being deleted. Objects can be either a client's or a policy's characteristics. Rules are programmed into smart contracts, and each transaction that takes place must comply with them. If it doesn't, the transaction will be placed in uncle block until a while before being deleted.

E. Retrieval of Policy Holder Details

Either the person who owns the policy or an insurance agent can get client information. To access some information, the user must give an insurance agent (ida) a session key. That key is no longer usable when the session expires. The insurance representative will not register any alterations to the policies details made at that meeting until the policyholder has signed them.

F. Claim Processing

The customer (policyholder or hospital) submits a transaction to the insurance company under the blockchain network model that has been presented.

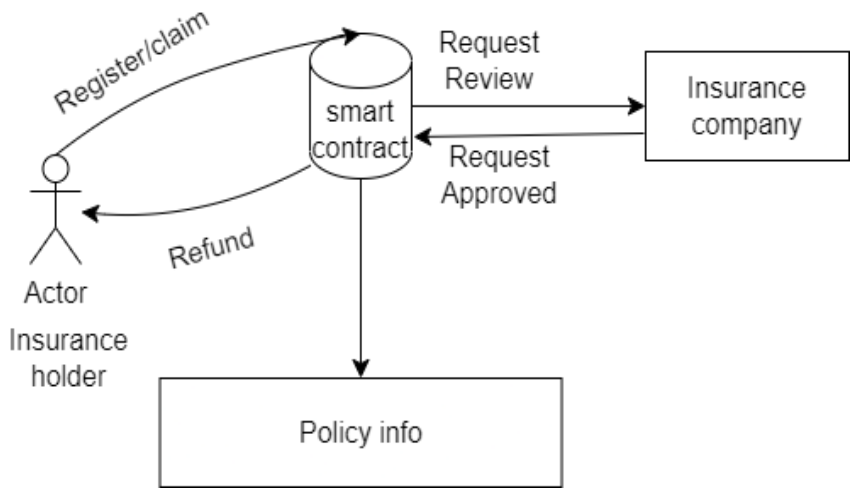


Fig 5: Model for Claim processing

As seen in Figure 5, a smart contract processes the claims request appropriately. For a legitimate policyholder, the insurance provider will cover hospital expenditures. For the claim, the policyholder must sign a message with his or her private key. The insurance company will use the Elliptic Curve Cryptography method ecrecover() to decode the data. If the blockchain has the address that was retrieved, a smart contract will verify the payment amount and send the ethers to the hospital's account. If a transaction is genuine, the peer nodes conduct its Proof of Work consensus then add it to the blockchain.

Message Signed with:

0xfa9jsk35n633k2afdjl239gn45kslf493lfms467lrmd0acfa85ec45038ed5358b991ca4539b
d55dc4126cb128b087476c71e65b72adb0b0ef947439d32e93nfsl399nfsj3l22n3k44a3b0b
9d8ce838dd7975291b.This signed message will be sent to the smart contract as (64,64,4)

bits, which the smart contract will then use to decrypt the message using ecrecover (hash value,r,s,v) transferring ethers to the hospital's fund in accordance with the policyholder's approval. All of this takes place under a smart contract, where each transaction is readily available and immutable. cryptanalysis methods.

2.3 Feasibility Study

2.3.1 Technical feasibility: The technological tools and software resources required are:

- Any standard PC or laptop
- Windows Operating System or Ubuntu or MacOS.
- IPFS Kubo, Metamask, Truffle Ganache,
- The technical abilities needed are manageable, and all these software and tools are freely accessible.

Therefore, the proposed model is technically feasible.

2.3.2 Resource feasibility: Resources that are essential for the project include:
A programming device like a laptop or a computer.
Programming tools that are freely available. Programming individuals
So, the project model has the needed resource feasibility.

CHAPTER 3: SYSTEM DESIGN AND ANALYSIS

3.1Project Perspective

In this project we are focusing to develop to decentralized software in which we decentralized the health record data so the data breaches and the altering the data is not possible so the data is safe and secure and only the right person can access the health record only the person can access the record when the permission is given to that person for the admin and in this software doctor can upload the data and can view the data doctor can upload the clinical reports and patients can also view the records and access all the data

3.1 Performance Requirements

In this project we are using the Ethereum platform to develop the decentralized software and many more dependencies which will need the high amount of performance

- A minimum 2 GB of GPU is recommended for optimal performance.
- A minimum 8GB RAM
- Windows/Linux Operating System
- A CPU with Intel Core i5 10^{th} gen
- Programming Language JavaScript, solidity

3.2 System Features

- Stores the patients data
- Validate the patient data
- Only the assigned person and doctor can view and edit the patient data

3.3 Methodology

The fact that companies maintain several, disjointed patient health records is the primary issue with the existing health care system. By storing health record transactions on Blockchain to establish a smart ecosystem, the Proposed System seeks to address the present issues facing the health care sector. The motive is to provide the patient or individual with the authority to be in control of their own personal health data and no other third party can access it without their consent or authorization if the consent if provided. Blockchain technology is used by EHR Framework to store records securely and uphold a single source of truth. To access a patient's medical information and add the transactions to the decentralized system, the stakeholders will need to ask for permission. A blockchain-based solution enables widespread availability, trust in the information system, cost-

effectiveness, and data secrecy trust in the information system.

In this section, we will discuss the design and implementation of our setup, which is a blockchain-based system for processing medical insurance claims in real-time. The system features an easy-to-understand user interface with different functionalities for different types of users, such as patients who can register themselves, book appointments, and upload documents, and doctors who can register themselves and have appointments booked for them.

To address the challenge of storing large amounts of data for each user, which would be too much for the blockchain to handle, we use the InterPlanetary File System (IPFS) to shrink the data before storing it on the network. Each record is assigned a hash value, which is stored in the user interface. After the data is added, the blockchain network stores all the information with the hashes of the transactions and their respective timestamps. A new and unique hash is created with its respective timestamp when the block is ready to be added to the network. Transactions that weren't completed are stored in a memory buffer until new transactions appear.

The system ensures that the data's timestamp and block timestamp cannot be altered. To download data from the network, the user must validate and verify their credentials. The data stored in the blockchain cannot be altered since any change in the hash of the data would result in creating a completely new file with a new timestamp. This immutability feature of the combined system gives users complete trust in the system.

To address the issue of giving users the freedom to make changes to their file system, we create a backup of the IPFS when data is being stored on it. The backup is then connected to make it a coupled resource. When a user or patient wants to delete their file, it will be deleted locally, as it is not possible to delete files from the entire network. The user or patient does not need to worry about their file still being present on the network, as it will be restricted and cannot be viewed by others.

To address the issue of updating files, we make every uploaded file a complete independent entity, and all the hashes of all the files uploaded by a patient are collected and maintained. The user's privacy must also be maintained since their file would be stored at multiple nodes on the network. We solve this by not letting the user fill in personal identifiers in their file. The file identification is limited to the hash collection, their private key, and the timestamp mapped for every other hash being maintained in the network, making the user's data impossible to find or trace.

The system also features smart contracts added to the distributed ledger to handle demands made by stakeholders in the medical insurance sector. The roles that are automated by smart contracts determine which data may be accessed. The outcomes of each transaction's execution are tracked by a distributed ledger. Cryptographic techniques are used to authenticate users and grant access to resources. Smart contracts are used in the framework

to power the transactions. Every smart contract has specific rules that must be followed for transactions to be added to the blockchain. Depending on the outcome of the validating block, nodes will be adding a block to the medical insurance blockchain after validating a transaction.
In terms of registration, each stakeholder must hold at least one primary account, such as EOA, and every account's address is generated from the owner's public key and used to index all accounts. Smart contracts handle identity authentication and management in a decentralized manner.

Finally, the framework's insurance model comprises primary transactions, such as client registration, claim filing by either the policyholder or the hospital, processing of refunds, etc. The blockchain's transparency and traceability ensure that policyholders do not fraudulently accuse insurance companies of providing subpar services. The suggested framework process is shown in Figure 1.

The use of blockchain technology for health record management and insurance settlement has the potential to revolutionize the healthcare industry by improving efficiency, security, and transparency. Here is a possible methodology for implementing this technology:
Identify the stakeholders: Identify all the parties involved in the healthcare system, including patients, healthcare providers, insurance companies, and regulatory bodies. Determine their respective roles, responsibilities, and data requirements.

Design the blockchain system: Design a blockchain-based system that can securely and efficiently store, manage, and share health records and insurance claims data. Choose the appropriate blockchain protocol and consensus mechanism based on the specific needs of the stakeholders.

Develop the smart contracts: Develop smart contracts that automate the insurance settlement process based on predefined rules and conditions. These contracts should be transparent, secure, and immutable to ensure that all parties can trust the results.
Integrate the system with existing infrastructure: Integrate the blockchain system with existing healthcare and insurance infrastructure, including electronic health record (EHR) systems, claims processing systems, and regulatory compliance frameworks. Ensure that the system complies with relevant laws and regulations.

Test the system: Conduct thorough testing of the blockchain system to ensure that it functions as intended and meets the requirements of all stakeholders. This should include functional testing, security testing, and performance testing.
Launch and monitor the system: Launch the system and monitor its performance, reliability, and security over time. Continuously evaluate the system's effectiveness and make adjustments as needed to ensure that it continues to meet the needs of all stakeholders.
The use of blockchain technology for health record management and insurance settlement has the potential to revolutionize the healthcare industry by improving efficiency, security, and transparency. Here is a possible methodology for implementing this technology:

Identify the stakeholders: Identify all the parties involved in the healthcare system, including patients, healthcare providers, insurance companies, and regulatory bodies. Determine their respective roles, responsibilities, and data requirements.
Design the blockchain system: Design a blockchain-based system that can securely and efficiently store, manage, and share health records and insurance claims data **[23]**. Choose the appropriate blockchain protocol and consensus mechanism based on the specific needs of the stakeholders.

Develop the smart contracts: Develop smart contracts that automate the insurance settlement process based on predefined rules and conditions. These contracts should be transparent, secure, and immutable to ensure that all parties can trust the results.
Integrate the system with existing infrastructure: Integrate the blockchain system with existing healthcare and insurance infrastructure, including electronic health record (EHR) systems, claims processing systems, and regulatory compliance frameworks. Ensure that the system complies with relevant laws and regulations **[21]**.

Test the system: Conduct thorough testing of the blockchain system to ensure that it functions as intended and meets the requirements of all stakeholders. This should include functional testing, security testing, and performance testing.

Launch and monitor the system: Launch the system and monitor its performance, reliability, and security over time. Continuously evaluate the system's effectiveness and make adjustments as needed to ensure that it continues to meet the needs of all stakeholders. By following this methodology, healthcare organizations can leverage the power of blockchain technology to improve health record management and insurance settlement processes, resulting in greater efficiency, security, and transparency for all stakeholders.

3.4.1 Blockchain

Blockchain is a distributed database, where the information is checked by other network users. It has historically been used to handle bitcoin transaction data, but it can be utilised in a number of healthcare-related contexts, including the maintenance of electronic health records, the administration of prescription (and related fraud prevention), and insurance coverage. Blockchain employs cryptographic proofs to confirm records rather than third-party verification. This cryptographic validation is performed by a network of users who all follow a set of pre-established norms. By guaranteeing there is just one "right" account of the events, integrity is introduced without the consent of all of the nodes, data is kept in the database and cannot thereafter be modified. This approach works by using a hash to tie each group of the database's records (referred to as a "block") to the one before it, so that altering one block would change the hashing of all succeeding blocks. The present healthcare record systems are susceptible to integrity vulnerabilities as well as cyberattacks, such as the WannaCry assault in 20177 that compromised computers at 80 of a 237 NHS trusts as well as more than 250,000 machines in 150 countries. More recently, 1.5 million Singaporeans' personal information was stolen due to a cyberattack on

SingHealth, the country's primary healthcare provider. Enough security measures must always be put in place to safeguard healthcare systems so they are not still a target for hackers.**[3]** A Blockchain secures data using public-key cryptography. Each user receives an private key and public key and after being individually encrypted in one direction (hash). Both parties may use these parties involved in a transaction the writer signs and the recipient confirms using their respective private keys, and transactions are sent to a recipient using public keys. This enables the recipient to confirm the reliability of the information chain. Additionally, any potential of hacking is eliminated because only the recipient may view the information delivered. Additionally, the system can let the addition of parts of authoritarian logic to process, authenticate, and approve access to the data that is secured therein, streamlining the permission procedures for patients and medical professionals. This is referred to as a "smart contract," which works as a block of computer code that runs once certain specific predetermined conditions are satisfied, guaranteeing the safety of the system and allowing authorised access. Blockchain is suited for the healthcare industry because of its capacity to build smart contracts. Strict rules regulate how sensitive data may be handled in this industry, which has become more crucial with the recent addition of the GDPR (General Data Protection Regulation).**[3]**

Fig 6. Blockchain**.**

3.4.1 Ethereum

The well-known virtual currency Bitcoin has the same blockchain technology as Ethereum, a decentralised blockchain platform. The idea behind Ethereum was to create a trust-free smart contract framework with open-source capabilities and programmable blockchain functionality. The first version of Ethereum appeared in 2015. Additionally shared is the peer-to-peer networking that gives this technology its decentralised nature. Additionally, this system employs ethers, a unique cryptocurrency. This cryptocurrency supports transfers between accounts connected to the Ethereum network. Ethereum offers the Solidity programming language, which enables programmers to build their own blockchains.[16]. Ethereum is considered to be a second-generation blockchain technology that offers a more advanced and versatile approach to creating decentralized applications (dApps) and smart contracts. Unlike Bitcoin, which is primarily used as a digital currency, Ethereum provides a broader range of use cases for developers and entrepreneurs seeking to build decentralized solutions for various industries, including finance, supply chain, and

gaming. One of the key features of Ethereum is its ability to execute smart contracts autonomously without the need for intermediaries, such as banks or legal institutions. This allows for faster, more efficient, and cost-effective transactions compared to traditional methods. Furthermore, Ethereum's decentralized nature ensures that there is no central point of control, making it less susceptible to manipulation or censorship. This also means that it is highly secure, transparent, and immutable, making it an ideal platform for businesses and individuals who value privacy and security. Ethereum also offers a range of tools and frameworks that enable developers to create complex applications on the blockchain, including the Truffle Suite, Web3.js, and the Ethereum Virtual Machine (EVM). These tools make it easier for developers to deploy and manage decentralized applications, making Ethereum a popular choice for blockchain-based projects.In conclusion, Ethereum has revolutionized the blockchain industry by providing a more advanced, versatile, and secure platform for decentralized applications and smart contracts. As more developers and entrepreneurs continue to explore the possibilities of this technology, we can expect to see even more innovative use cases emerge in the coming years **[1]**.

3.4.2 IPFS

A technology called IPFS makes advantage of a peer-to-peer networking to store data. Highly secure storage is offered, as opposed to data kept on IPFS is shielded against modification. Since altering the identification is the only way to change data saved on IPFS, the data is protected from tampering by applying a cryptographic identity **[9]**. Every data file stored on IPFS contains an encrypted hash value. It stands out and is used to identify files that are stored on the IPFS. The IPFS protocol is a suitable choice for retaining sensitive and significant data because of its secure storage mechanism. The resulting cryptographic hash can be kept on the application decentralized to lessen the laborious computational operations. A technology called IPFS makes advantage of a peer-to-peer networking to store data. Highly secure storage is offered, as opposed to data kept on IPFS is shielded against modification. Since altering the identification is the only way to change data saved on IPFS, the data is protected from tampering by applying a cryptographic identity **[11]**. Every data file stored on IPFS contains an encrypted hash value. It stands out and is used to identify files that are stored on the IPFS. The IPFS protocol is a suitable choice for retaining sensitive and significant data because of its secure storage mechanism. The resulting cryptographic hash can be kept on the application decentralised to lessen the laborious computational operations The IPFS protocol uses peer-to-peer networking, which contains an IPFS object, a data structure that holds links and data. The data is unstructured binary data, and the link is an array **[17]**. The following is how the IPFS protocol works:

- IPFS assigns a special cryptographic hash to each file it stores.
- The IPFS forbids the existence of duplicate files.
- A node within the network maintains its own indexes and stores material.

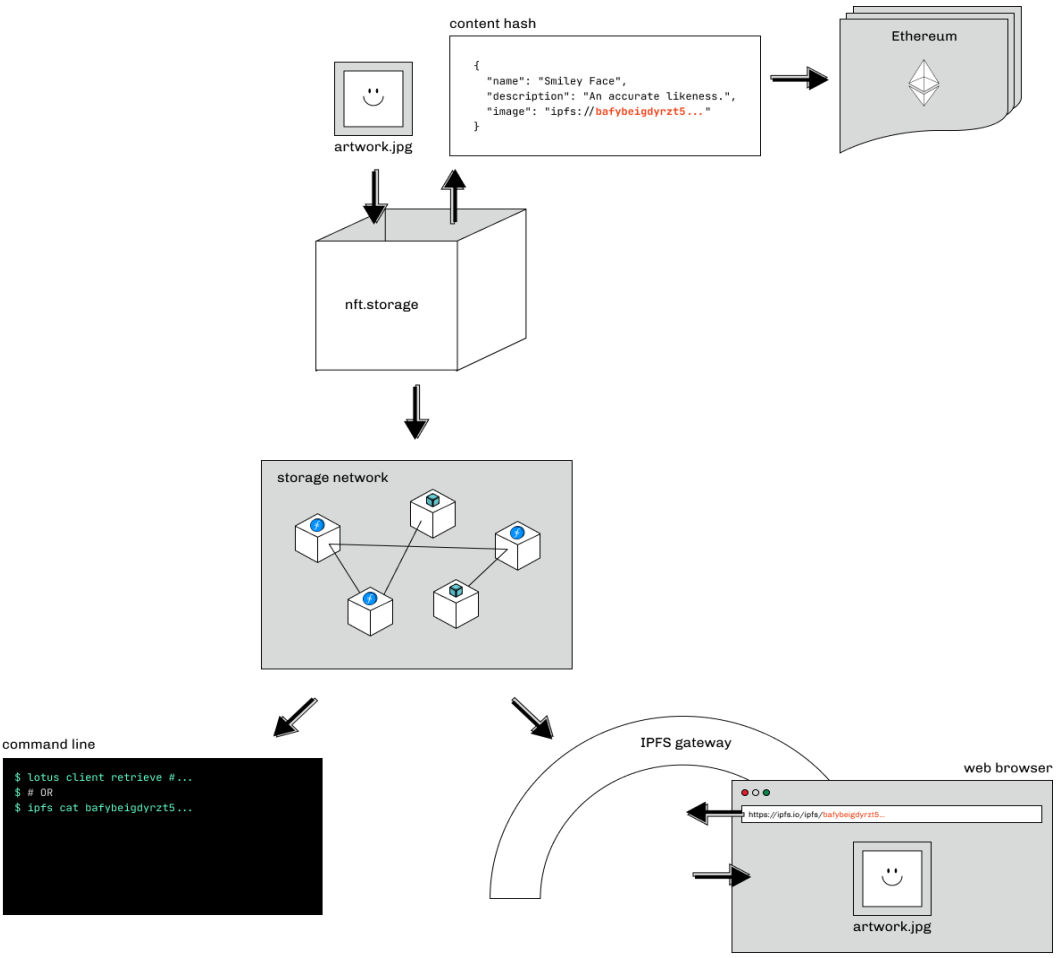


Fig 7: IPFS working

3.4.3 Ganache

In order to build decentralised applications on both Corda and Ethereum, Ganache is utilised as a top-tier development tool to administer your own private blockchain network. Ganache is quite advantageous to all stages of the development cycle and has a variety of possible benefits. One of Ganache's key advantages is that you can develop, test, and implement your smart contract and decentralised application projects in a controlled and safe environment. You have two different versions of Ganache to pick from, depending on the features you need. The Ganache UI is a desktop application that can assist Corda and Ethereum development tasks. The Ganache-CLI, a command-line tool that focuses on Ethereum development, offers an alternative. The fact that Ganache is available for Windows, Mac, and Linux is also notable.

Ganache is a popular development tool that enables developers to manage their own private blockchain network and create decentralized applications on Corda and Ethereum. Its various features make it an essential tool for developers in all stages of the development cycle.

One of the key benefits of using Ganache is the ability to create, test, and execute smart contract and decentralized application projects in a secure and predictable environment. With Ganache, developers can easily simulate real-world scenarios and test their projects before deploying them to the public blockchain. Ganache offers two different versions depending on the developer's needs. The Ganache UI is a desktop program that supports both Corda and Ethereum development tasks, while the Ganache-CLI is a command-line tool that is specifically designed for Ethereum development **[13]**. Both versions are available on Windows, Mac, and Linux, making it accessible to developers across different operating systems.

Overall, Ganache's flexibility and ease of use make it an excellent choice for developers who want to streamline the development process and focus on creating high-quality decentralized applications.

3.4.4 Metamask

Meta mask is a browser extension,and used as a cryptocurrency wallet which enables you to store tokens, use dapps, and trade Ethereum. By integrating with MyEtherWallet, MetaMask eliminates the requirement for users to give private keys at the time of each transaction, whether creating, holding, or transferring tokens. Users can store and organise their Ether, Bitcoin, and other cryptocurrencies using a cryptocurrency wallet, which is an online or digital wallet. A cryptocurrency wallet enables transactions using cryptocurrencies, prevents asset theft, and enables users to convert cryptocurrencies to real money when necessary. Today, MetaMask is the most frequently used non-custodial cryptocurrency wallet in the world. With monthly users exceeding 30 million, MetaMask is the one of the most famous blockchain wallet.
In addition to providing a secure platform for storing and managing cryptocurrencies, MetaMask also simplifies the process of sending and receiving cryptocurrency payments. Users can easily send and receive Ether, Bitcoin, and other digital assets using MetaMask. The wallet also supports many ERC-20 tokens, which are tokens that are built on the Ethereum blockchain.

Furthermore, MetaMask provides a great user experience with an intuitive interface that makes it easy for users to manage their accounts, view transaction history, and monitor the value of their assets. Additionally, MetaMask offers a range of features such as integration with hardware wallets, the ability to create multiple accounts, and custom network support. All of these features make MetaMask a great choice for anyone looking to securely manage their cryptocurrencies and interact with the world of decentralized applications.

3.4.5 Truffle

Truffle is a comprehensive development framework and testing suite that provides an ecosystem for Ethereum dApp development. It enables developers to create, compile, and

deploy smart contracts on the Ethereum blockchain with ease [4]. With Truffle, developers can write, test, and deploy their contracts, as well as build front-end interfaces for their dApps.
One of the biggest advantages of using Truffle is that it simplifies the generation of smart contracts and makes the development process more accessible to all levels of developers. Truffle utilizes the Ethereum Virtual Machine (EVM) as its foundation, which is a runtime environment for smart contracts on the Ethereum blockchain [8].
Truffle also manages the entire lifecycle of smart contracts, including compilation, deployment, and testing. This allows developers to focus on other project-related tasks, such as developing front-end interfaces or building complex business logic, without worrying about the low-level details of smart contract deployment and management.
Furthermore, Truffle supports custom deployments, allowing developers to deploy their smart contracts to various blockchain networks, such as private or test networks, or even the main Ethereum network. This provides flexibility for developers and enables them to test their dApps in various environments before deploying to production.
Overall, Truffle has become a popular choice among Ethereum developers due to its ease of use, flexibility, and robustness. Its active community and comprehensive documentation make it an attractive option for those looking to develop decentralized applications on the Ethereum blockchain.

Basically truffle provide or setup the ecosystem for development for testing framework and asset pipeline. With a sizable community, Truffle is a well-liked Ethereum dApp building framework. Additionally, Truffle seeks to make the generation of smart contracts simpler and more accessible by using the EVM (Ethereum virtual machine) as a foundation. Additionally, truffle offers a number of benefits: Any smart contracts that are used in your dApps and their artefacts are managed by truffle. While Truffle takes care of this, you can focus on other project-related tasks. dApps with custom deployments, difficult library coupling, etc.

3.4.6 Smart Contracts

The piece of program needed to execute any action on the blockchain is known as a smart contract. This programme is run whenever a user sends transactions They immediately run on the blockchain, making them impervious to hacking and modifications of any type [14]. The smart contract.They commonly use the Solidity programming language, which allows programmers to write whatever kind of operation they want to carry out on a blockchain. Coders can use EVM bytecode to compile their essential operations after writing them in code; this is discussed in greater detail in the section below. After compilation, they might be run and put to use on Ethereum. JavaScript and python is a programming language both are encapsulated with solidity programing language offered by Ethereum for creating smart contracts.**[16]**

Smart contracts are a key component of the Ethereum blockchain ecosystem. They enable the automation of transactions and the execution of complex agreements without the need

for intermediaries, making the process more efficient and cost-effective **[15]**. The advantages of using smart contracts extend beyond cost and efficiency savings; they also enhance transparency and security by ensuring that transactions are recorded on an immutable ledger that cannot be altered.

Solidity is the most popular programming language used for creating smart contracts on the Ethereum blockchain [10]. It is a high-level programming language that is designed to be easy to learn and use for developers with experience in C++, Python, or JavaScript. Solidity provides a wide range of tools and features for writing smart contracts, including data types, functions, control structures, and libraries.

After writing the smart contract code, developers can compile it into EVM bytecode, which is the low-level language that can be executed by the Ethereum Virtual Machine (EVM). The EVM is a critical component of the Ethereum network that allows smart contracts to run on the blockchain. The EVM is responsible for executing smart contracts in a secure and deterministic manner.

In addition to Solidity, developers can also use JavaScript and Python to create smart contracts on the Ethereum network. JavaScript is a popular language for creating front-end web applications, and its integration with Solidity enables developers to create more complex smart contracts. Python, on the other hand, is a versatile language that is widely used for scientific computing, data analysis, and artificial intelligence applications. Its integration with Solidity enables developers to create more sophisticated smart contracts that can interact with other systems and data sources.

Overall, smart contracts and the Ethereum blockchain platform provide a powerful tool for creating secure, efficient, and transparent applications for a wide range of use cases.

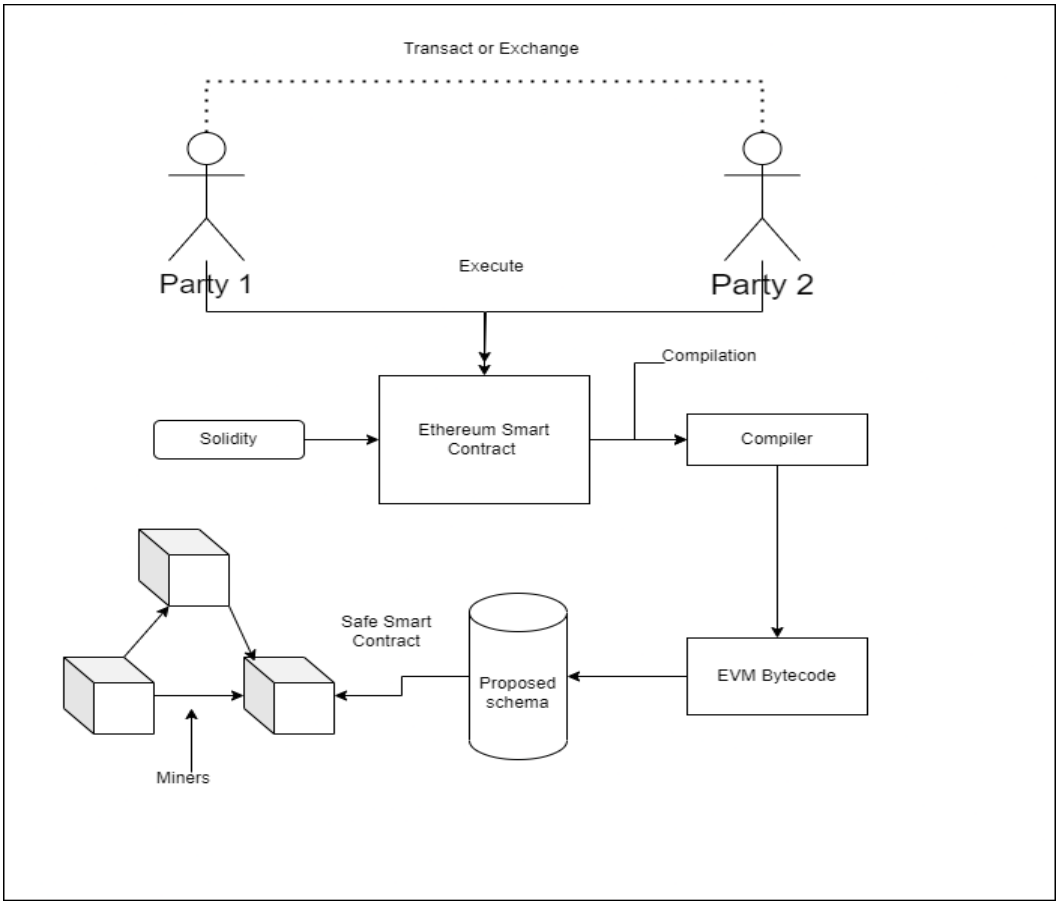


Fig 8: Validation done by smart contract

As shown in the above figure that is how the ethereum smart contracts are used in the blockchain. Smart contracts are small piece of codes which are used to trigger certain specified action when triggered as written.

CHAPTER 4: RESULT AND OUTPUTS

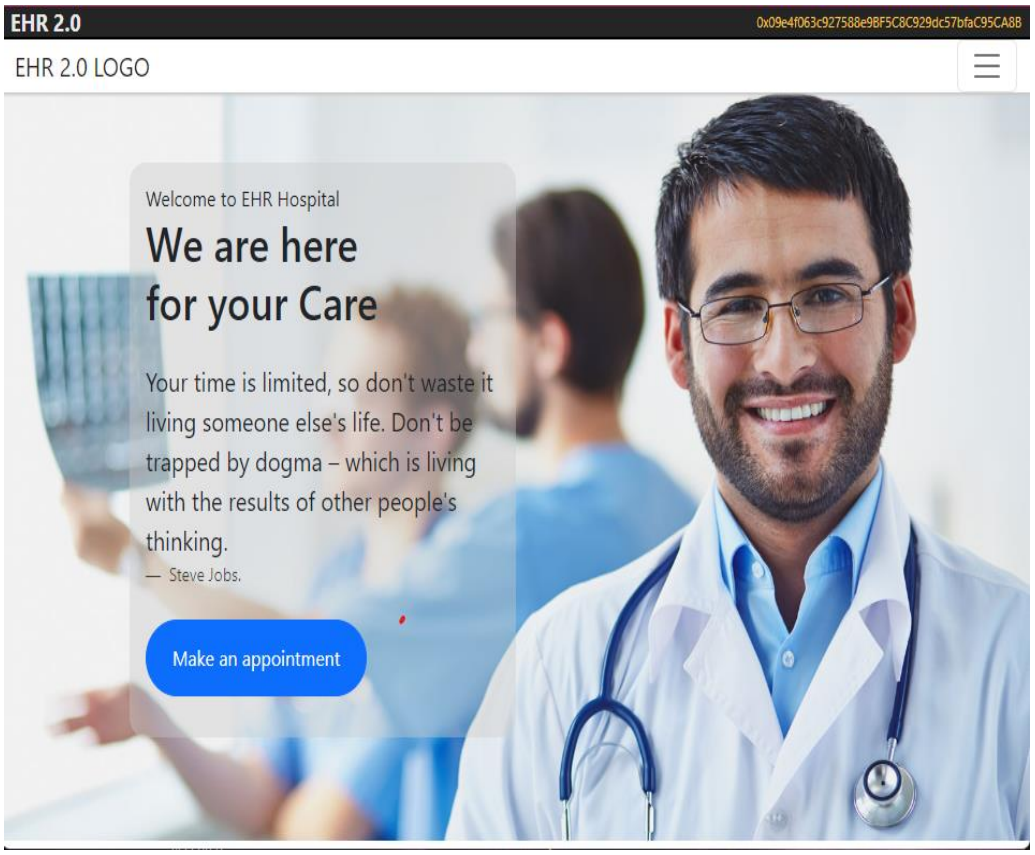


Fig 9. Main website of health record management and insurance settlement using blockchain.

As the project includes the following types of candidates:

1. Admin:- The admin is the one in our project that can include doctors to the blockchain and also the insurance agency to the blockchain. It can do multiple tasks like can see how many doctors and insurance agencies are there. It has a dashboard to see the above said information.
   So, first of all the admin needs to be present, for that we take the public address key from the truffle ganache and add it to the metamask wallet as it is the thing that helps us to connect with the blockchain and name it admin.

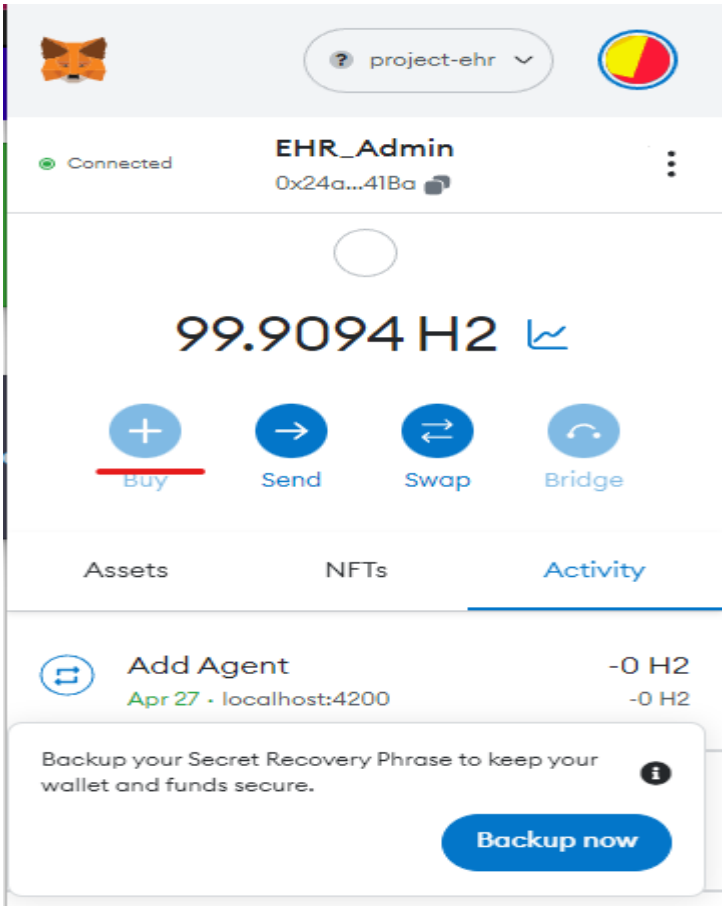


Fig 10. shows the admin account.

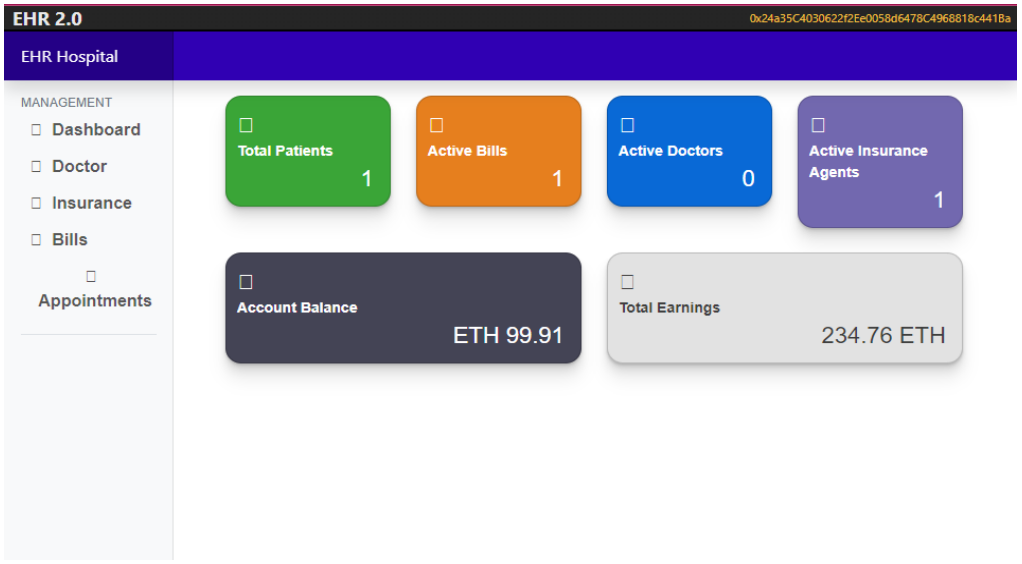


Fig 11. Shows the admin dashboard

Admin dashboard containing the details of no of patients, doctors, insurance agencies, bills and its own balance left.

So, as admin can add doctors, let’s see how the whole process takes place.

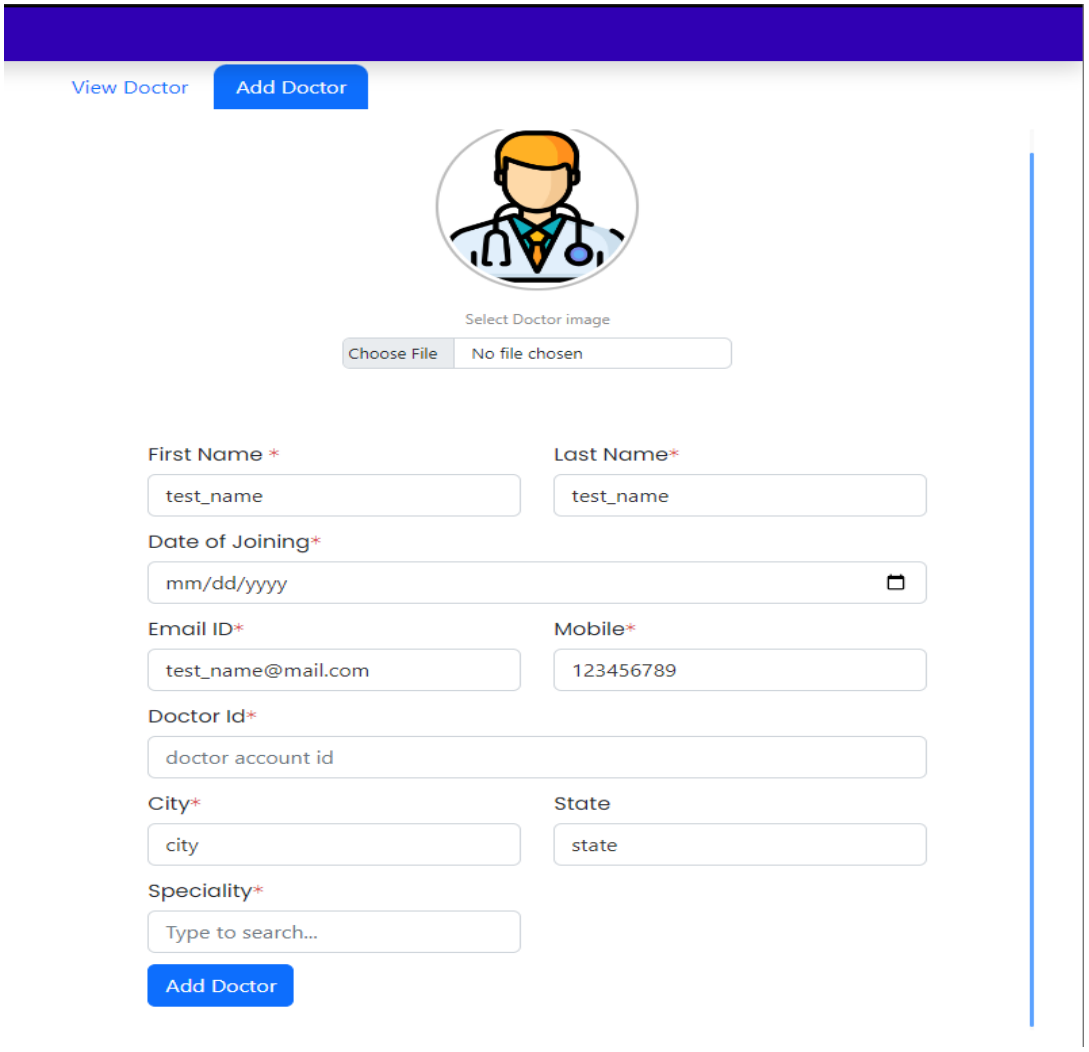


Fig 12. Shows how the doctor can be added to the blockchain.

Doctor image is necessary in our project and for the doctor id, it can be taken from the truffle ganache.
The public address key that is present there. And then the private key to be added in the metamask wallet to make it a doctor.

Now after the doctor is added, patients can register themselves and book an appointment or store their records as well.

Fig 13. Patient registration.

Patient will be added to the blockchain and that can be visible too to the patient and patient can also edit the details if they wanted to.

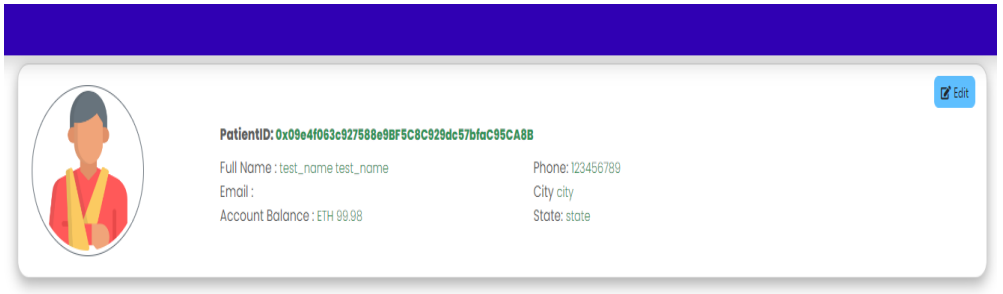


Fig 14. Patient dashboard

After registering themselves patient can book their appointment.

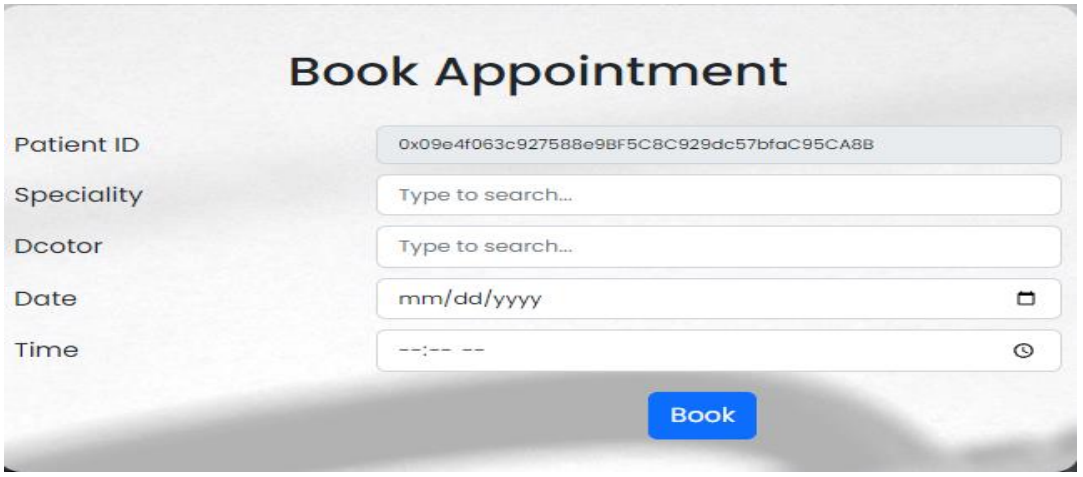


Fig 15. Book appointment for patient

Patient can also select the desired doctor using their name as well as the speciality they work with. After doing the above said thing, the patient will have an appointment on their selected date and time.

Now, we have doctors as well as patients on the blockchain/project. Patient will have their medical data stored as well as appointments but what after the whole procedure of seeing the doctor and getting the treatment is complete. There is now some bill to be paid to the hospital. So patient can settle their bill or they can use the insurance if they have one on them. For this, the blockchain should have another party Insurance agency.

The admin can add the insurance agency to the blockchain using the address key from truffle ganache.

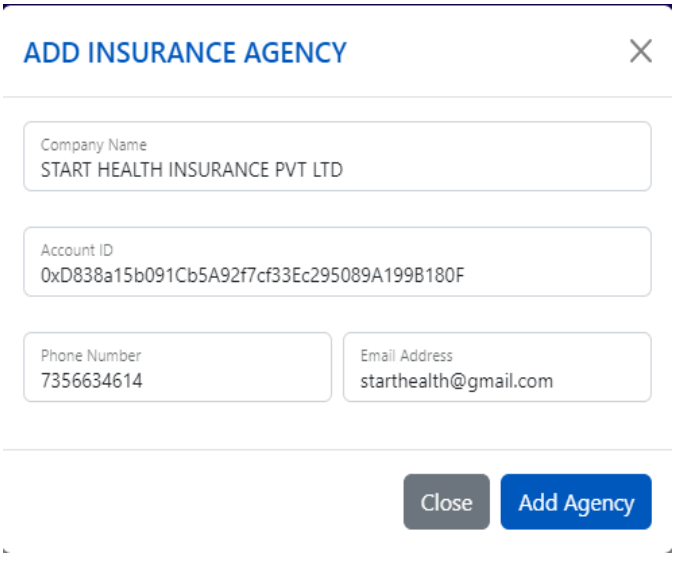


Fig 16. Adding insurance agency to the blockchain.

Then after doing confirmation using the metamask wallet, the insurance agency will be added to the blockchain and it will be shown in the list of insurance agencies.

Fig 17. Insurance agencies present on the blockchain

Now, there would be some bill to generate and that can be done and the procedure would be as follows.

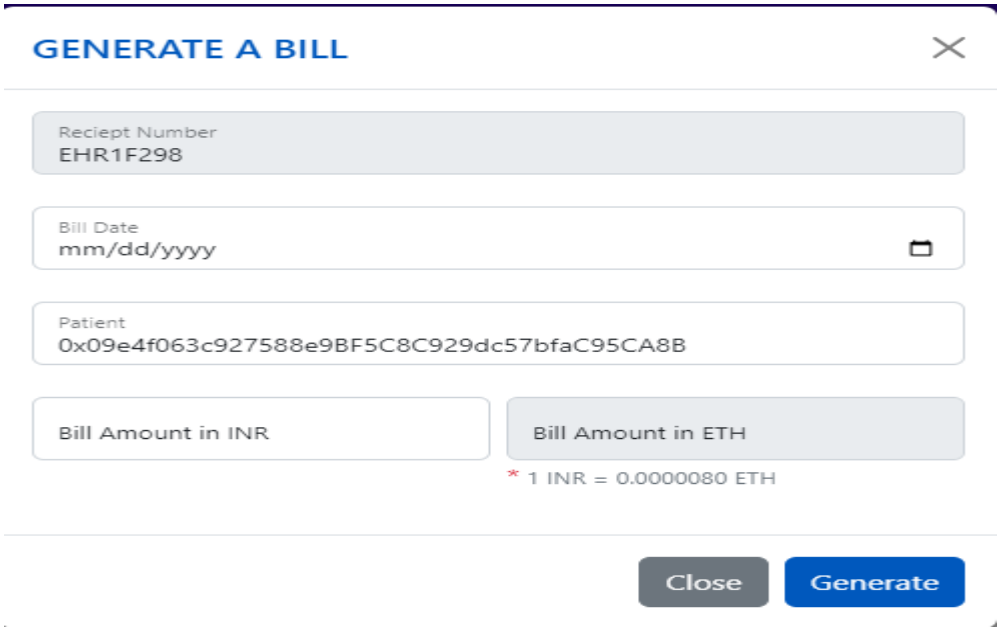


Fig 18. Generating the bill.

The patient detail is added in generating the bill by providing the address key/name of that patient. When the admin clicks on the generate it will request to create the bill for that patient, and the information will be stored on the blockchain. The process of generation will be confirm by metamask in the project. It will give the option to either reject or confirm. On confirming the bill will be generated and if rejected, no bill will be generated.

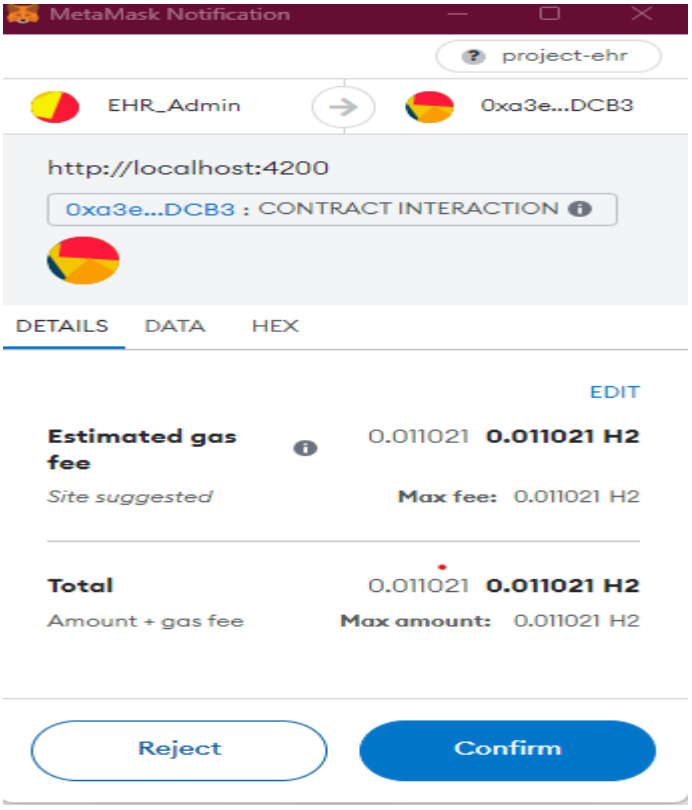


Fig 19. Bill generation confirm or reject by admin

After the generation of the bill of the procedure done for the patient. Generated bills could be accessed by the patient. Patient can either pay or claim the insurance according to their choice.

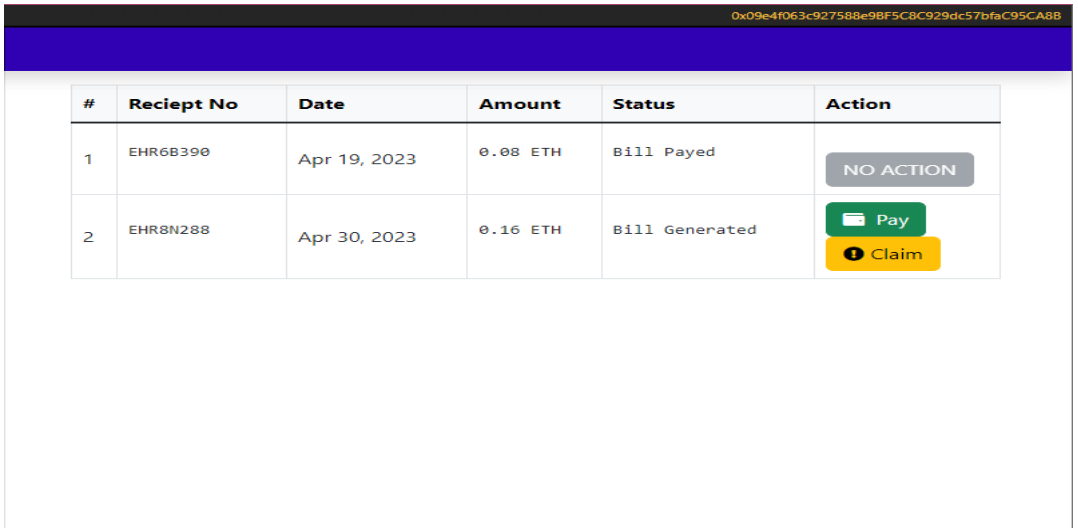


Fig 20. Patient receipts/bills.

Either patient can pay their bill directly or can claim. So if the patient chooses to claim their bill.

Fig 21. Patient submitting the insurance claim.

It will further result in following the insurance claim process. That is the insurance agency will check the legitimacy of the bill and checking the records. Ultimately following their procedure of claiming the insurance for the particular insurance policy taken by the insured.

Insurance agency will either accept the claim of the patient or reject it after following their claim verification process for that insurance policy.

Fig 22. Insurance agency accepting claim.

The details will be updated that the insurance claimed is accepted and will be visible on the insurance agency dashboard.

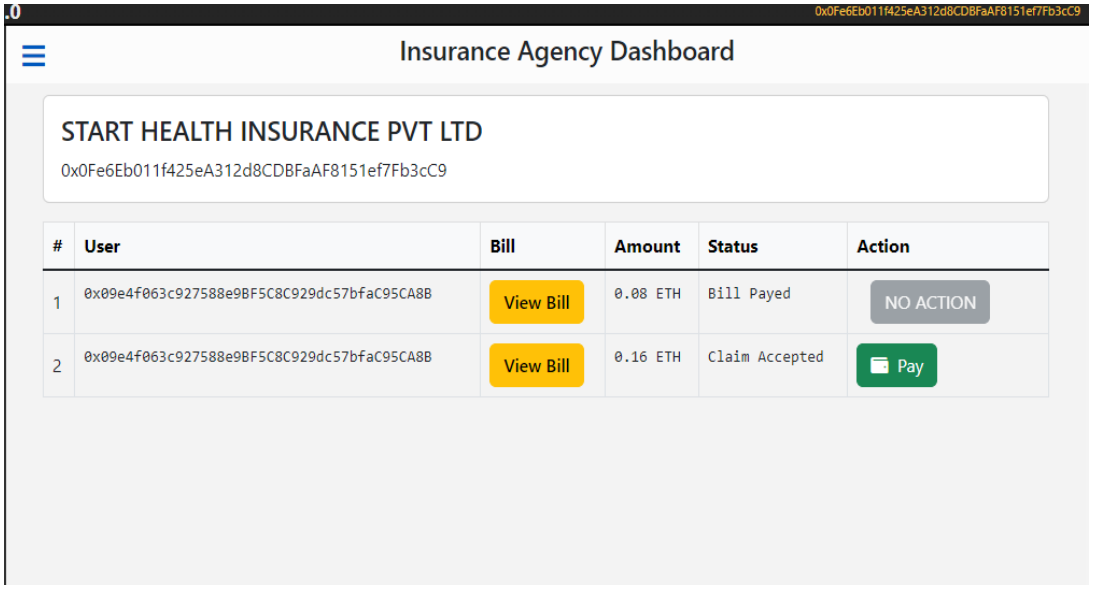


Fig 23. Insurance agency dashboard before paying the claim.

Insurance agency can also view the bill as shown below. As that is the amount that is to be paid to the hospital by the patient using the insurance that they have in the insurance agency.

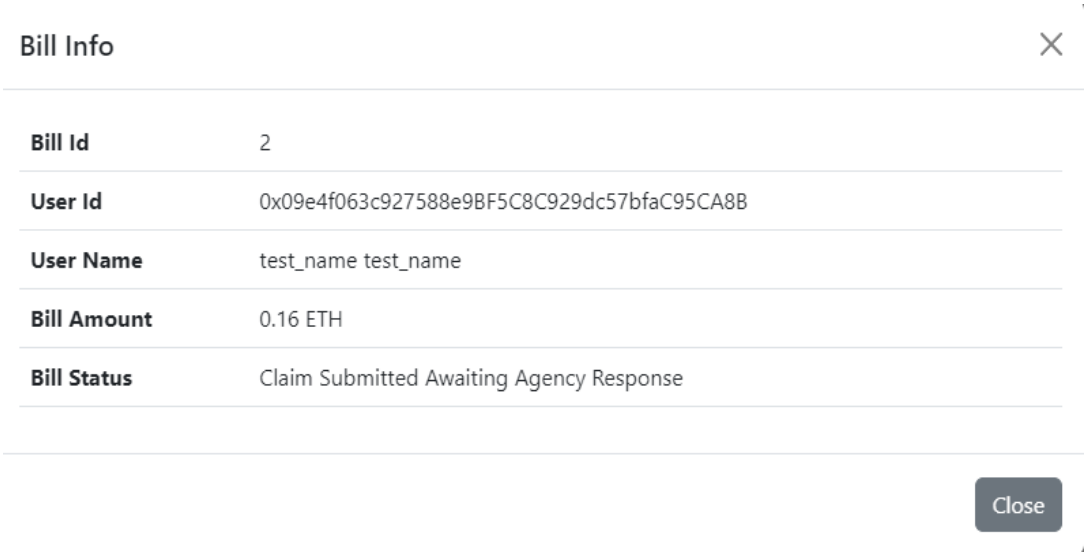


Fig 24. Bill payment Info.

Now, after insurance agency chooses to approve the claim and do the payment of the same. The data will be updated and will be visible on the insurance agency dashboard as well.

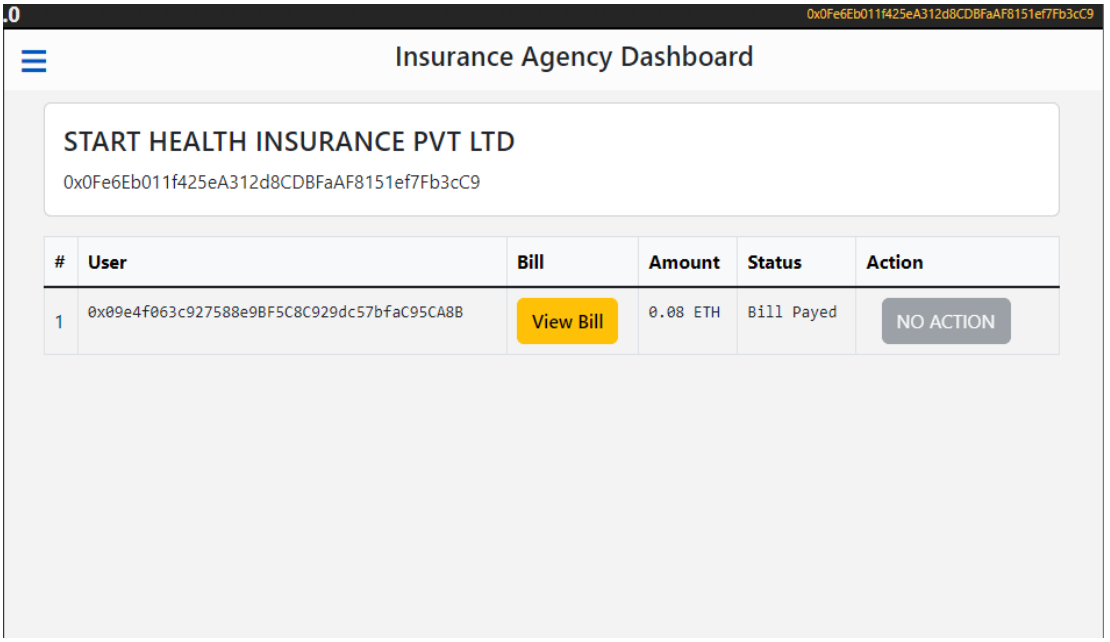


Fig 25. Insurance agency dashboard after payment of claim is done.

And patient also can see that the bill that they claimed for that particular procedure is paid on their own dashboard.

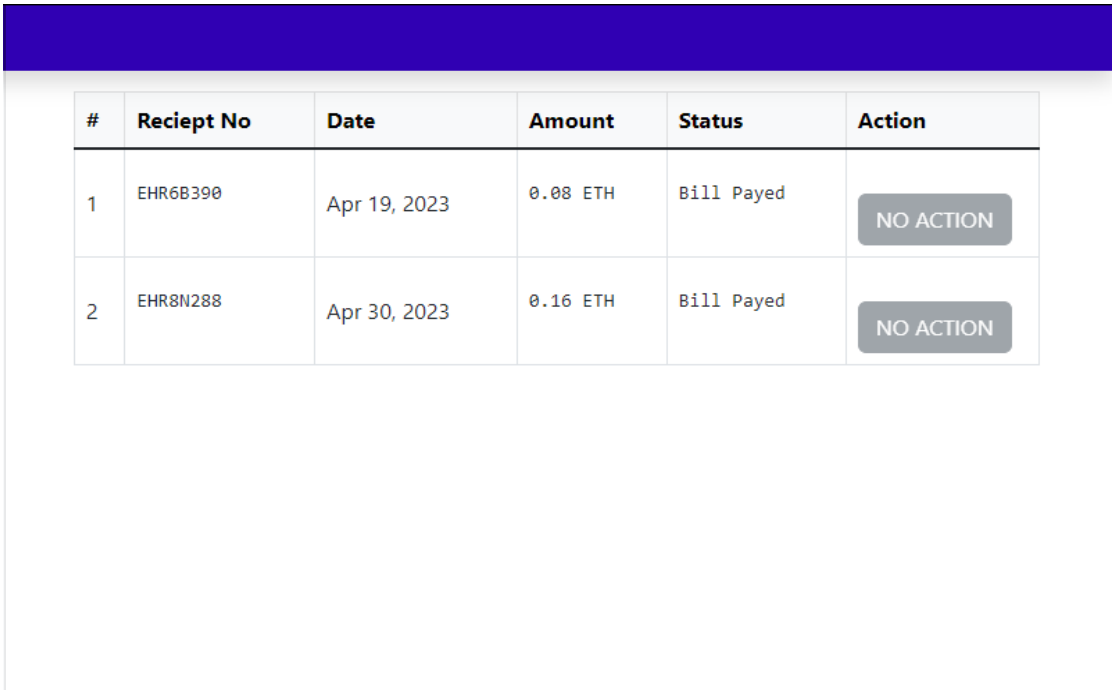


Fig 26. Patient dashboard showing no bill to pay.

CHAPTER 5: CONCLUSION

5.1 Conclusion

Blockchain has potential applications in the healthcare industry. digital health data Despite the expansion of the health industry and technological advancements in Electronic Health Record systems, still had some problems, which this new technology, called blockchain, was able to solve. Our suggested framework combines granular access controls for those data with safe record storage. It develops a system in such a way that simple to use and comprehend for users. Additionally, the framework suggests actions to make sure the system addresses the As it makes use of IPFS's off-chain storing feature, it has no storage problem. Additionally, the system can benefit from role-based authorization because only related and trustworthy individuals have authorization to medical records. This also fixes the Electronic Health Record system's information asymmetry issue. We intend to integrate the billing module into the current framework going forward. In determine how much a person would price for a doctor's appointment on this decentralised system operating on the blockchain, we need to take a few factors into account. Defined laws and regulations that adhere to the fundamentals of the healthcare industry would also be necessary.

The healthcare industry has long been plagued by inefficiencies and inconsistencies in managing health records and insurance settlements. However, the proposed blockchain-based solution provides a promising new approach to address these challenges. By leveraging the security, transparency, and decentralization of blockchain technology, the proposed system can provide patients with complete control over their health records while ensuring that healthcare providers and insurers have access to accurate and up-to-date information.

In addition, the proposed solution can simplify the insurance settlement process, leading to faster and more transparent payments for patients. This is particularly important in the current healthcare landscape, where patients often face significant delays and frustrations in receiving insurance payments for their healthcare services.

Overall, the proposed solution has the potential to improve the efficiency, accuracy, and security of managing health records and insurance settlements, ultimately leading to a more patient-centric healthcare system. By reducing administrative overhead, improving data accuracy, and streamlining processes, blockchain technology can help to alleviate many of the challenges currently faced by the healthcare industry.

5.2 Future Scope

While the proposed solution provides a promising new approach to managing health records and insurance settlements, there is still significant room for further research and development in this field. Some of the potential areas for future development include:

Integration with wearable devices and Internet of Things (IoT) devices to collect and store health data automatically, providing patients with real-time access to their health information and enabling healthcare providers to make more informed decisions.

Development of a mobile application for patients to access their health records and receive insurance settlements, providing patients with greater convenience and flexibility in managing their healthcare.Integration with other blockchain-based healthcare systems to enable interoperability, ensuring that patients can seamlessly share their health information with healthcare providers and insurers across different platforms.Incorporation of artificial intelligence (AI) and machine learning (ML) algorithms to analyze patient data and provide personalized healthcare recommendations, enabling healthcare providers to deliver more targeted and effective treatments.

Further research into the ethical and legal implications of using blockchain technology in healthcare, ensuring that patients' rights and privacy are protected while still enabling the benefits of blockchain technology to be realized. In conclusion, the proposed blockchain-based solution for managing health records and insurance settlements provides a promising new approach to address many of the challenges currently faced by the healthcare industry. By leveraging the security, transparency, and decentralization of blockchain technology, the proposed system can provide patients with greater control over their health information while streamlining administrative processes for healthcare providers and insurers. With continued research and development, blockchain technology has the potential to revolutionize the healthcare industry and improve patient outcomes.

CHAPTER 6: REFERENCE

1. Reen, G.S., Mohandas, M. and Venkatesan, S., 2019, December. Decentralized patient centric e-Health record management system using blockchain and IPFS. In 2019 IEEE Conference on Information and Communication Technology (pp. 1-7). IEEE.

2. Mayer, A.H., da Costa, C.A. and Righi, R.D.R., 2020. Electronic health records in a Blockchain: A systematic review. Health informatics journal, 26(2), pp.1273-1288.

3. Vazirani, A.A., O'Donoghue, O., Brindley, D. and Meinert, E., 2020. Blockchain vehicles for efficient medical record management. NPJ digital medicine, 3(1), pp.1-5.

4. Azaria, A., Ekblaw, A., Vieira, T. and Lippman, A., 2016, August. Medrec: Using blockchain for medical data access and permission management. In 2016 2nd international conference on open and big data (OBD) (pp. 25-30). IEEE.

5. Vardhini, B., Dass, S.N., Sahana, R. and Chinnaiyan, R., 2021, January. A blockchain based electronic medical health records framework using smart contracts. In 2021 International Conference on Computer Communication and Informatics (ICCCI) (pp. 1-4). IEEE.

6. Tith, D., Lee, J.S., Suzuki, H., Wijesundara, W.M.A.B., Taira, N., Obi, T. and Ohyama, N., 2020. Application of blockchain to maintaining patient records in electronic health record for enhanced privacy, scalability, and availability. Healthcare informatics research, 26(1), pp.3- 12.

7. Boiani, F., 2018. Blockchain based electronic health record management for mass crisis scenarios: A feasibility study.

8. Fang, H.S.A., Tan, T.H., Tan, Y.F.C. and Tan, C.J.M., 2021. Blockchain personal health records: systematic review. Journal of medical Internet research, 23(4), p.e25094.

9. Wang, H.L., Chu, S.I., Yan, J.H., Huang, Y.J., Fang, I.Y., Pan, S.Y., Lin, W.C., Hsu, C.T., Hung, C.L., Lin, T.C. and Shen, T.T., 2020. Blockchain-based medical record management with biofeedback information. In Smart Biofeedback-Perspectives and Applications. IntechOpen.

10. Martínez, A., Molina, C. and Subauste, D., 2020, October. Electronic medical records management in health organizations using a technology architecture based on blockchain. In 2020 IEEE ANDESCON (pp. 1-6). IEEE.

11. Haleem, A., Javaid, M., Singh, R.P., Suman, R. and Rab, S., 2021. Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks, 2, pp.130-139.

12. Mukherji, A. and Ganguli, N., 2020, October. Efficient and scalable electronic health record management using permissioned blockchain technology. In 2020 4th International Conference on Electronics, Materials Engineering & Nano-Technology (IEMENTech) (pp. 1- 6). IEEE.

13. Pawar, P., Parolia, N., Shinde, S., Edoh, T.O. and Singh, M., 2022. eHealthChain—a blockchain-based personal health information management system. Annals of Telecommunications, 77(1), pp.33-45.

14. Sangeetha, R., Harshini, B., Shanmugapriya, A. and Rajagopal, T., 2019. Electronic health record system using blockchain. Int Res J Multidiscip Technovation, 1(2), pp.57-61.

15. Shahnaz, A., Qamar, U. and Khalid, A., 2019. Using blockchain for electronic health records. IEEE Access, 7, pp.147782-147795.

16. Zhuang, Y., Sheets, L.R., Chen, Y.W., Shae, Z.Y., Tsai, J.J. and Shyu, C.R., 2020. A patient-centric health information exchange framework using blockchain technology. IEEE journal of biomedical and health informatics, 24(8), pp.2169-2176.

17. Harshini, V.M., Danai, S., Usha, H.R. and Kounte, M.R., 2019, April. Health record management through blockchain technology. In 2019 3rd International Conference on Trends in Electronics and Informatics (ICOEI) (pp. 1411-1415). IEEE.

18. Assan, A., Ali, M.I., Ahammed, R., Khan, M.M., Alsufyani, N. and Alsufyani, A., 2021. Secured insurance framework using blockchain and smart contract. *Scientific Programming*, *2021*, pp.1-11.

19. Akande, A., 2018. Disruptive power of blockchain on the insurance industry. *Master's Thesis, Universiti of Tartu, Institute of Computer Science, Tartu*.

20. Shetty, A., Shetty, A.D., Pai, R.Y., Rao, R.R., Bhandary, R., Shetty, J., Nayak, S., Keerthi Dinesh, T. and Dsouza, K.J., 2022. Block chain application in insurance services: A systematic review of the evidence. *SAGE Open*, *12*(1), p.21582440221079877.

21. Chen, C.L., Deng, Y.Y., Tsaur, W.J., Li, C.T., Lee, C.C. and Wu, C.M., 2021. A traceable online insurance claims system based on blockchain and smart contract technology. *Sustainability*, *13*(16), p.9386.

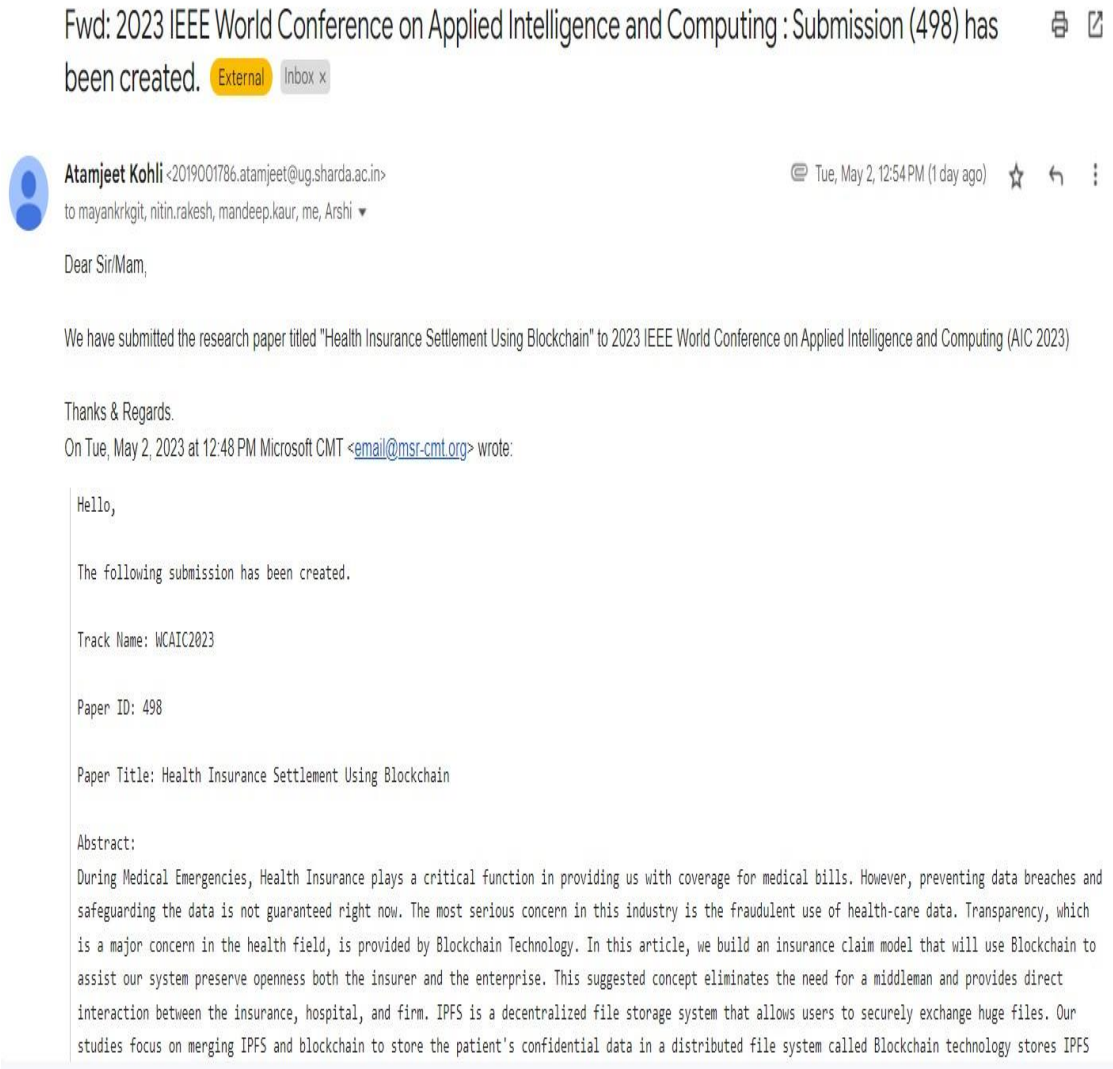
22. Kuckreja, J., Nigde, P. and Patil, P., 2021. Health Insurance Claim Using Blockchain. *International Research Journal of Engineering and Technology*, *8*(5), pp.2406-2409.

23. FICCI & PWC, 2020, August. Revamping India's health insurance sector with blockchain and smart contracts. In *Virtual health insurance conference*.

24. Sravan, N.P.V., Baruah, P.K. and Mudigonda, S.S., 2018. Use of blockchain technology in integrating heath insurance company and hospital. *Int J Sci Eng Res*, *9*(10), pp.1664-1669.

ANNEXURE 1

Research paper submission details (8th sem)



Fwd: 2023 IEEE World Conference on Applied Intelligence and Computing : Submission (498) has been created. External Inbox ×

Atamjeet Kohli <2019001786.atamjeet@ug.sharda.ac.in> Tue, May 2, 12:54 PM (1 day ago)

to mayankrkgit, nitin.rakesh, mandeep.kaur, me, Arshi

Dear Sir/Mam,

We have submitted the research paper titled "Health Insurance Settlement Using Blockchain" to 2023 IEEE World Conference on Applied Intelligence and Computing (AIC 2023)

Thanks & Regards.

On Tue, May 2, 2023 at 12:48 PM Microsoft CMT <email@msr-cmt.org> wrote:

Hello,

The following submission has been created.

Track Name: WCAIC2023

Paper ID: 498

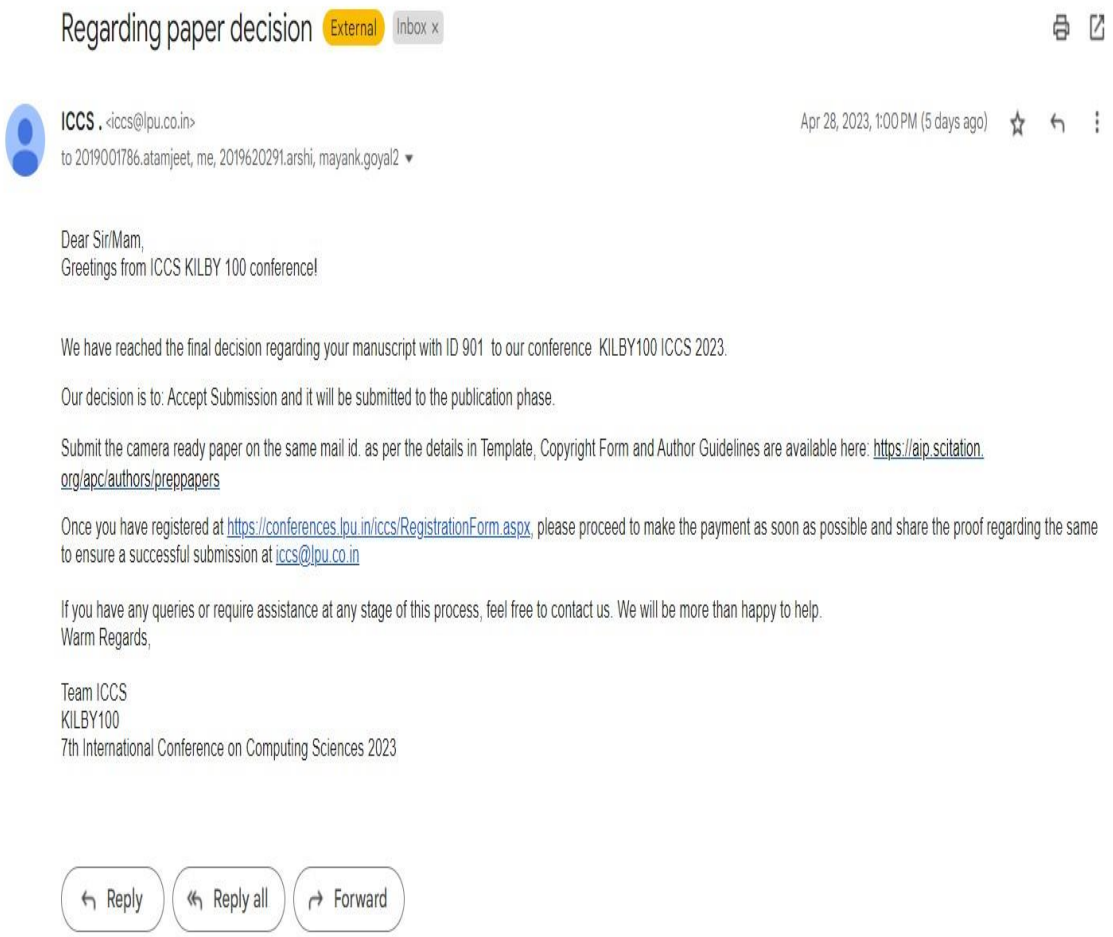
Paper Title: Health Insurance Settlement Using Blockchain

Abstract:

During Medical Emergencies, Health Insurance plays a critical function in providing us with coverage for medical bills. However, preventing data breaches and safeguarding the data is not guaranteed right now. The most serious concern in this industry is the fraudulent use of health-care data. Transparency, which is a major concern in the health field, is provided by Blockchain Technology. In this article, we build an insurance claim model that will use Blockchain to assist our system preserve openness both the insurer and the enterprise. This suggested concept eliminates the need for a middleman and provides direct interaction between the insurance, hospital, and firm. IPFS is a decentralized file storage system that allows users to securely exchange huge files. Our studies focus on merging IPFS and blockchain to store the patient's confidential data in a distributed file system called Blockchain technology stores IPFS

ANNEXURE 2

7th semester outcome details



Regarding paper decision External Inbox x

ICCS , <iccs@lpu.co.in> Apr 28, 2023, 1:00 PM (5 days ago)

to 2019001786.atamjeet, me, 2019620291.arshi, mayank.goyal2

Dear Sir/Mam,
Greetings from ICCS KILBY 100 conference!

We have reached the final decision regarding your manuscript with ID 901 to our conference KILBY100 ICCS 2023.

Our decision is to: Accept Submission and it will be submitted to the publication phase.

Submit the camera ready paper on the same mail id. as per the details in Template, Copyright Form and Author Guidelines are available here: https://aip.scitation.org/apc/authors/preppapers

Once you have registered at https://conferences.lpu.in/iccs/RegistrationForm.aspx, please proceed to make the payment as soon as possible and share the proof regarding the same to ensure a successful submission at iccs@lpu.co.in

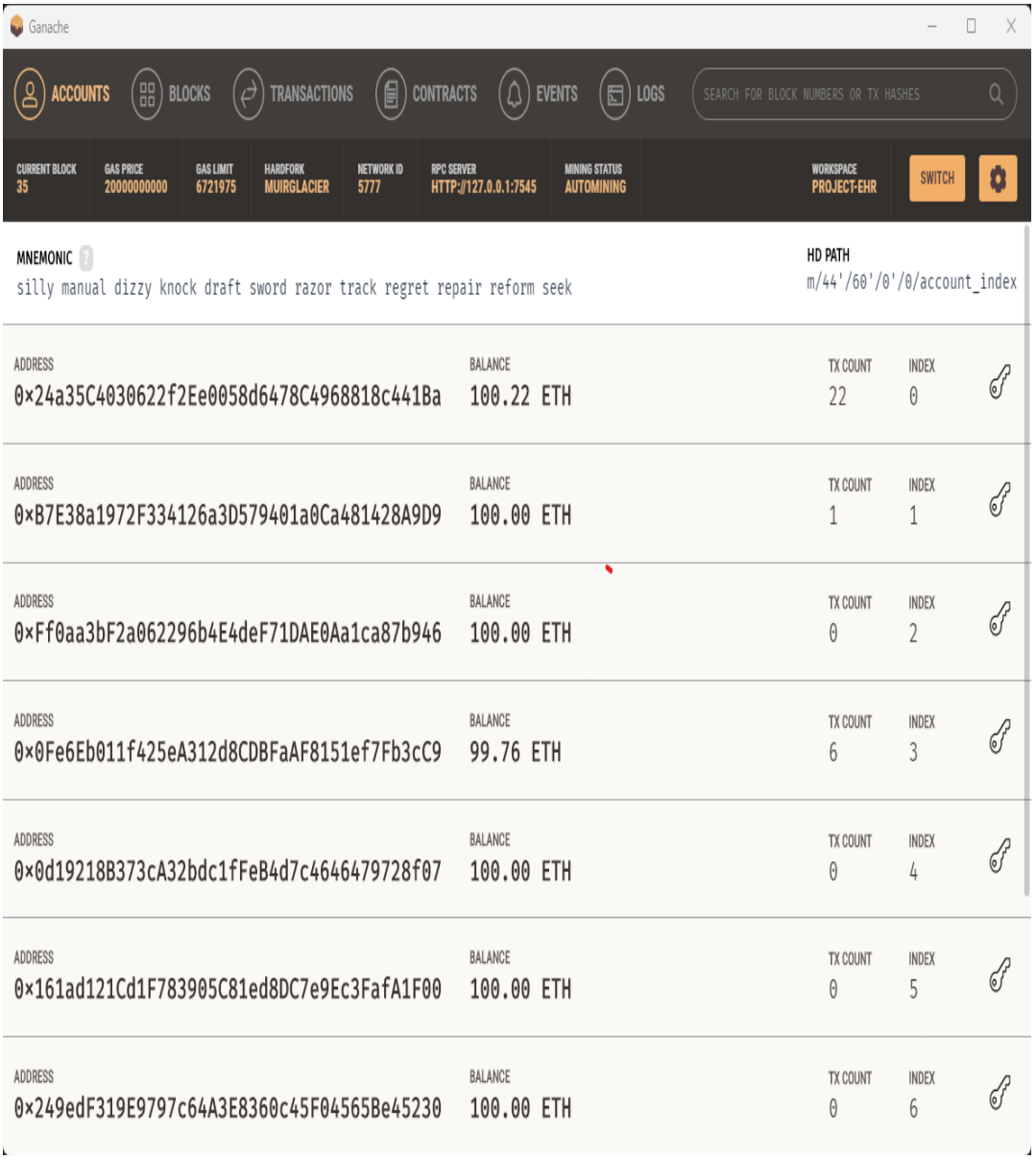
If you have any queries or require assistance at any stage of this process, feel free to contact us. We will be more than happy to help.
Warm Regards,

Team ICCS
KILBY100
7th International Conference on Computing Sciences 2023

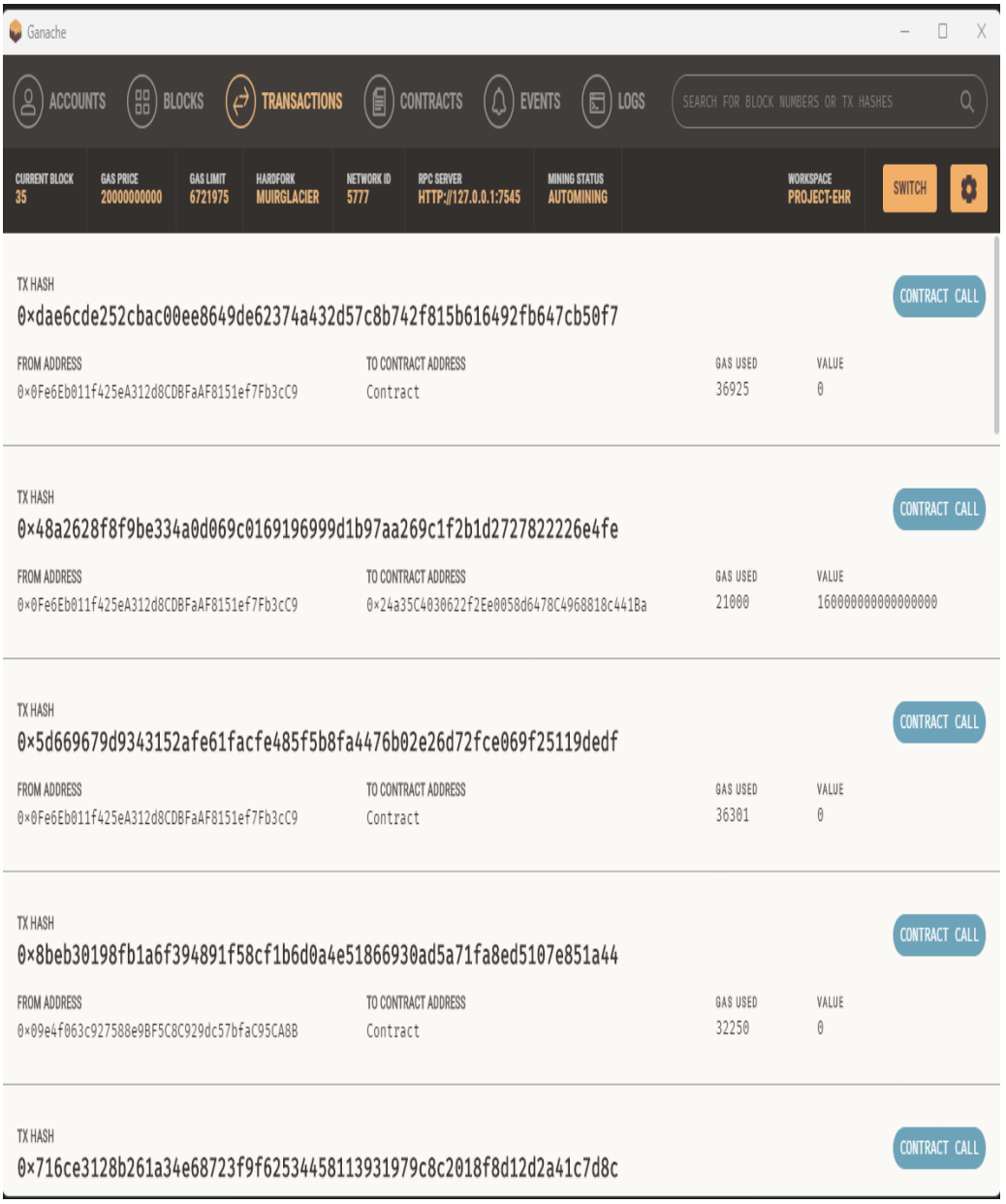
Reply Reply all Forward

ANNEXURE 3

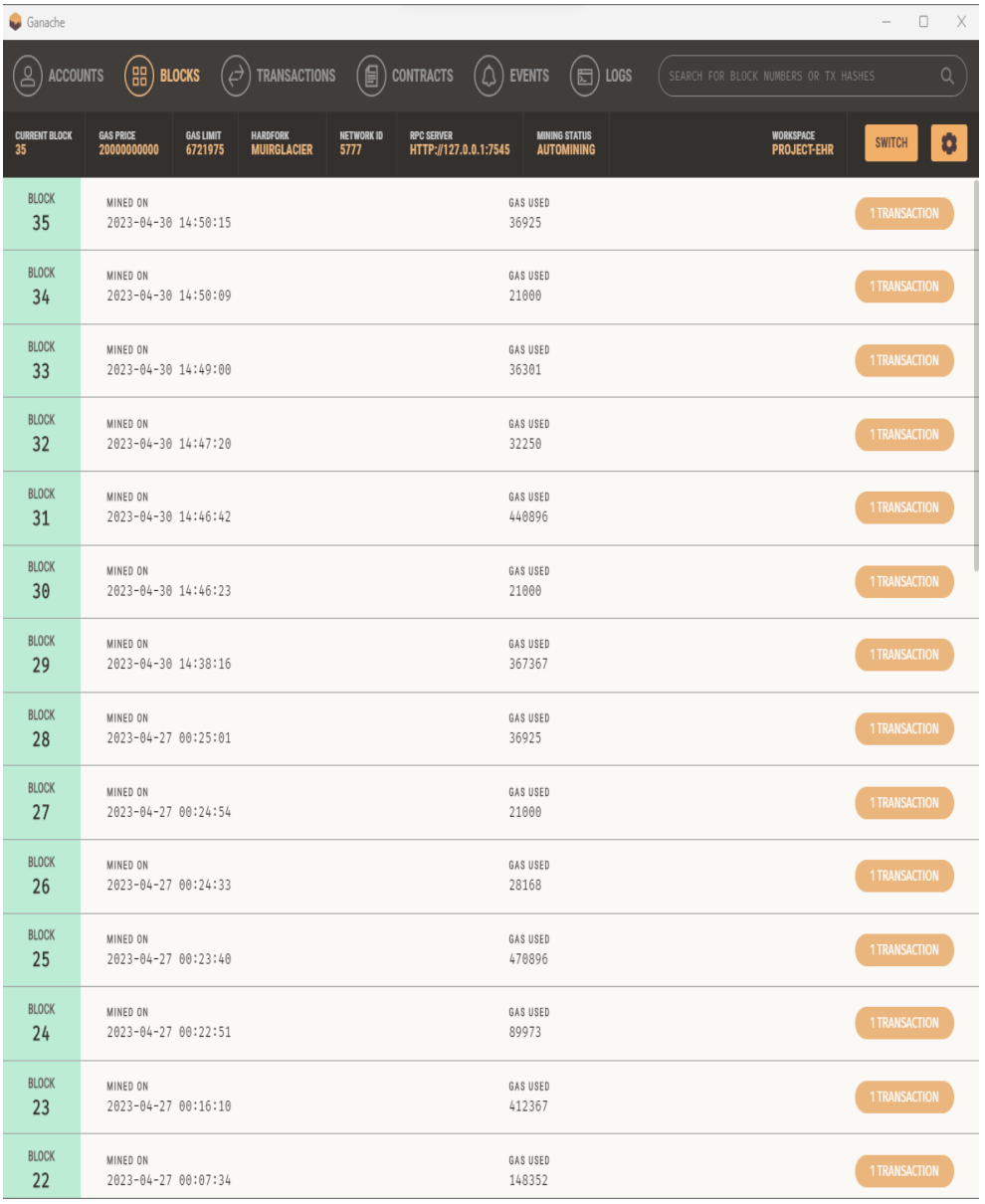
Record list of the parties present on the blockchain.

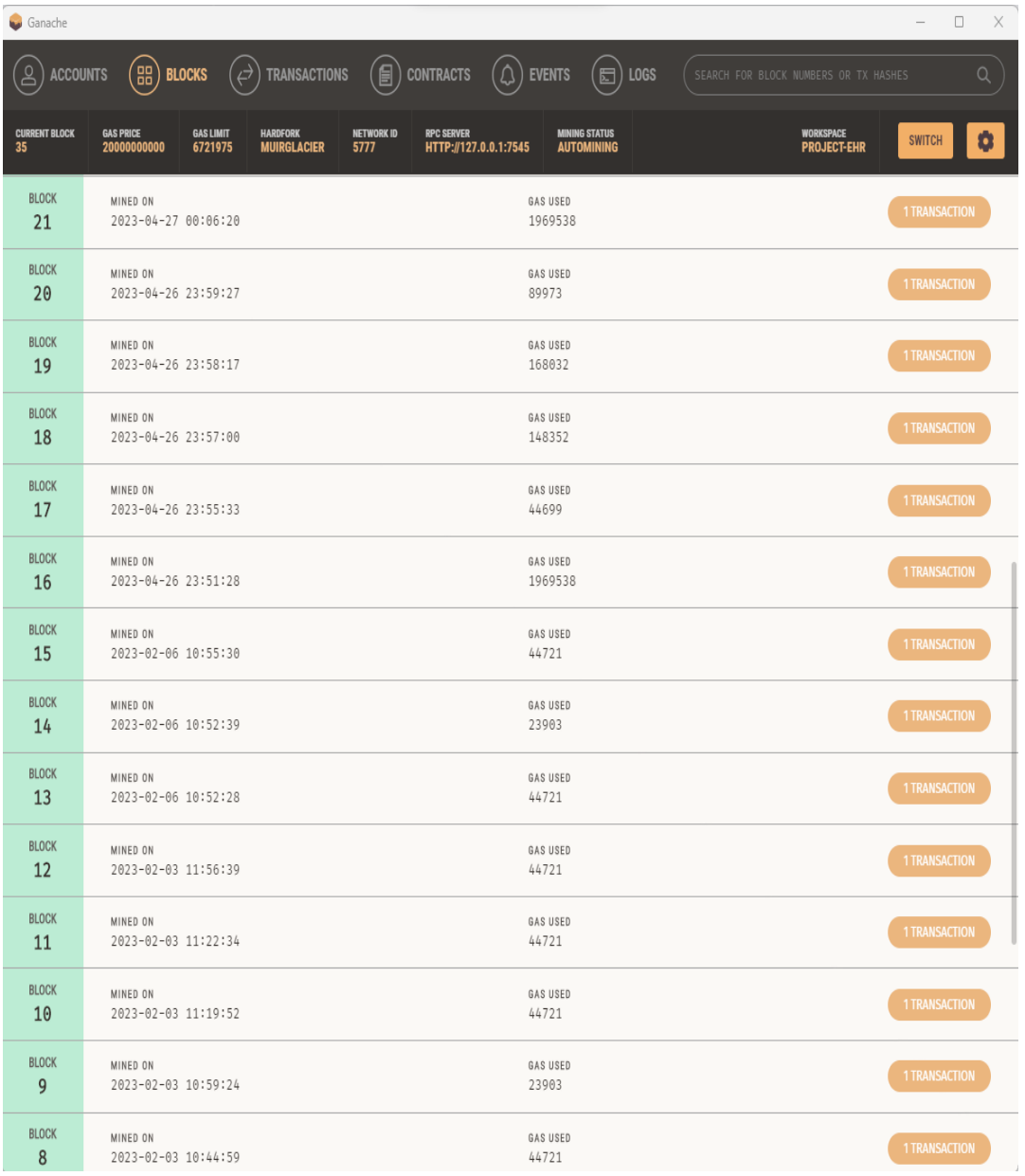


Transaction that took place on the blockchain.



Blocks present on the Blockchain.




Ganache
ACCOUNTS
BLOCKS
TRANSACTIONS
CONTRACTS
EVENTS
LOGS
SEARCH FOR BLOCK NUMBERS OR TX HASHES
CURRENT BLOCK 35
GAS PRICE 20000000000
GAS LIMIT 6721975
HARDFORK MUIRGLACIER
NETWORK ID 5777
RPC SERVER HTTP://127.0.0.1:7545
MINING STATUS AUTOMINING
WORKSPACE PROJECT-EHR
SWITCH
BLOCK 21 MINED ON 2023-04-27 00:06:20 GAS USED 1969538 1 TRANSACTION
BLOCK 20 MINED ON 2023-04-26 23:59:27 GAS USED 89973 1 TRANSACTION
BLOCK 19 MINED ON 2023-04-26 23:58:17 GAS USED 168032 1 TRANSACTION
BLOCK 18 MINED ON 2023-04-26 23:57:00 GAS USED 148352 1 TRANSACTION
BLOCK 17 MINED ON 2023-04-26 23:55:33 GAS USED 44699 1 TRANSACTION
BLOCK 16 MINED ON 2023-04-26 23:51:28 GAS USED 1969538 1 TRANSACTION
BLOCK 15 MINED ON 2023-02-06 10:55:30 GAS USED 44721 1 TRANSACTION
BLOCK 14 MINED ON 2023-02-06 10:52:39 GAS USED 23903 1 TRANSACTION
BLOCK 13 MINED ON 2023-02-06 10:52:28 GAS USED 44721 1 TRANSACTION
BLOCK 12 MINED ON 2023-02-03 11:56:39 GAS USED 44721 1 TRANSACTION
BLOCK 11 MINED ON 2023-02-03 11:22:34 GAS USED 44721 1 TRANSACTION
BLOCK 10 MINED ON 2023-02-03 11:19:52 GAS USED 44721 1 TRANSACTION
BLOCK 9 MINED ON 2023-02-03 10:59:24 GAS USED 23903 1 TRANSACTION
BLOCK 8 MINED ON 2023-02-03 10:44:59 GAS USED 44721 1 TRANSACTION


BLOCK 7
MINED ON 2023-02-03 10:40:39
GAS USED 709799
1 TRANSACTION
BLOCK 6
MINED ON 2023-02-03 10:37:37
GAS USED 709799
1 TRANSACTION
BLOCK 5
MINED ON 2023-02-03 10:37:20
GAS USED 709799
1 TRANSACTION
BLOCK 4
MINED ON 2023-02-03 10:36:18
GAS USED 44721
1 TRANSACTION
BLOCK 3
MINED ON 2023-02-03 10:34:33
GAS USED 44721
1 TRANSACTION
BLOCK 2
MINED ON 2023-02-03 10:25:29
GAS USED 709799
1 TRANSACTION
BLOCK 1
MINED ON 2023-02-03 10:25:09
GAS USED 709799
1 TRANSACTION
BLOCK 0
MINED ON 2023-02-03 09:45:36
GAS USED 0
NO TRANSACTIONS

change

ORIGINALITY REPORT

8%	4%	2%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Sharda University Student Paper	2%
2	Submitted to National Institute of Technology, Sri Nagar Jammu & Kashmir Student Paper	1%
3	Submitted to University of Newcastle upon Tyne Student Paper	1%
4	mail.easychair.org Internet Source	<1%
5	Submitted to Somaiya Vidyavihar Student Paper	<1%
6	link.springer.com Internet Source	<1%
7	vocal.media Internet Source	<1%
8	"Decentralised Internet of Things", Springer Science and Business Media LLC, 2020 Publication	<1%