ENHANCHING PERFORMANCE AND SECURITY IN HEALTHCARE 4.0 APPLICATION THROUGH BLOCKCHAIN TECHNOLOGY

BY

MD. SADIQUL ISLAM PAPPU
ID: 172-15-9769

MD. HASAN MOON
ID: 172-15-9768

This Report Presented in Partial Fulfillments of the Requirements for the Degree of Bachelor of Science in Computer Science and Engineering

Supervised By

Narayan Ranjan Chakraborty
Assistant Professor
Department of CSE
Daffodil International University

Co-Supervised By

Ahmed Al Marouf
Lecturer
Department of CSE
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY

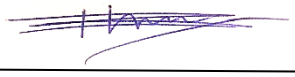
DHAKA, BANGLADESH

JUNE 2021

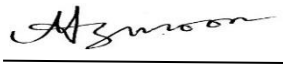
APPROVAL

This Project/internship titled **"Enhancing Performance and Security in Healthcare 4.0 Application through Blockchain Technology",** submitted by *Md. Sdiqul Islam Pappu*, *Hasan Moon*, ID No: *172-15-9769*,*172-15-9768* to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on *03-06-2021*.

BOARD OF EXAMINERS



Dr. Touhid Bhuiyan — **Chairman**
Professor and Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Nazmun Nessa Moon — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Aniruddha Rakshit — **Internal Examiner**
Senior Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Dr. Mohammad Shorif Uddin — **External Examiner**
Professor
Department of Computer Science and Engineering
Jahangirnagar University

DECLARATION

We hereby declare that, this project has been done by us under the supervision of **Narayan Ranjan Chakraborty, Assistant Professor, and Department of CSE** Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for award of any degree or diploma.

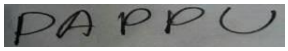
Supervised by:

Narayan Ranjan Chakraborty
Assistant Professor
Department of CSE
Daffodil International University

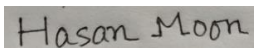
Co-Supervised by:

Ahmed Al Marouf
Lecturer
Department of CSE
Daffodil International University

Submitted by:



Md. Sadiqul Islam Pappu
ID: 172-15-9768
Department of CSE
Daffodil International University



Md. Hasan Moon
ID: 172-15-9768
Department of CSE
Daffodil International University

ACKNOWLEDGEMENT

First, we express our heartiest thanks and gratefulness to Almighty God for His Devine blessing that makes us possible to complete the final year project successfully.

We really grateful and wish our profound our indebtedness to **Narayan Ranjan Chakraborty, Assistant Professor**, Daffodil International University, Dhaka. Deep knowledge & keen interest of our supervisor in the field of "Blockchain" to carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts and correcting them all stage have made it possible to complete this project.

We would like to express our heartiest gratitude to Prof. Dr. Touhid Bhuiyan, Head, Department of CSE, for his kind help to finish our project and also other faculty member and the staff of CSE department of Daffodil International University.

We would like to thank our entire course mate in Daffodil International University, who participated in this discussion while completing the course work.

Finally, we must acknowledge with due respect the constant support and patients of our parents.

ABSTRACT

In this era of science, the medical healthcare system is considerably more basic. It is so much convoluted and exorbitant too. This can be lower by improving wellbeing records, medical coverage, refreshing wellbeing execution, and Blockchain innovation moreover. At first, blockchain was utilized to give cash trade records that were circulated and didn't depend on any incorporated position. Presently Blockchain innovation needs to enhance clinical records or medical care execution. Presently by utilizing Blockchain innovation, it can change the medical care information base, patient clinical record, medical clinic resources, and medication quality too. At this, we are confronting an exceptionally essential second for this we need some development. In such manner In this paper, we give blockchain-based proposition that have likewise improved medical services proficiency and security and have a decentralized record the executives framework to oversee EHRs applying blockchain innovation. Blockchain is transforming the current medical care rehearses that mean, later on, blockchain could be an innovation that saves the by and large clinical information of a patient's wellbeing and adds to customized and ensured medical care through the introduction of present day dependable medical care set up by the accompanying system. The momentous benefit of Blockchain is that it will eliminate the awareness of defiling information. Blockchain will overcome the difficulty of individual degree of disappointment for getting information. Blockchain will assist with eliminating the capacity of information hacking or harming and hardening in any utilization of information guaranteeing. In this topic, we catch up on both present and future improvement in the space of medical services execution and security by improving Blockchain innovation for instance. We also examined the principle use of Blockchain innovation and confronted the test as well. Finally, we audit the Objective, Motivation, and Expected result moreover.

TABLE OF CONTENTS

LIST OF TABLES

LIST OF FIGURES

CHAPTER 1
INTRODUCTION

1.1 Introduction

Medical healthcare has made up a mandatory part of our life. Clinical data, like solutions and past medical records, have likewise become another piece of patient determination and further procedures. At that point, it is important to protect the data electronically. Abrupt progression and selection of advanced wellbeing, the uprising of IoT, causes improved the nature of patients care through distant patient observing. For the security and execution of data in medical healthcare, we need to ensure the debasement of information security. In addition, awesome work is progressing on medical services and data innovation in a consolidated technique; on the other Blockchain innovation has as of late been given as a basic innovation. It is prepared to change the manner in which successive medical frameworks and organizations have been occupied with the healthcare area. These adjust are stimulus patients' treatment strategies than requiring cautious information handling. Further, they don't examine non-specialized perspectives that make wellbeing information reasonable. Our witticism is to make strides with unlimited admittance to patient information and get around an outsider to enter it without consent. They don't diagram some hidden standards of this framework as far as moral issues and receptiveness. Be that as it may, in the medical care field, three (3) components are required: protection, security, and interoperability. Also, they were not referenced to upgrade patients' wellbeing by pre-venting botches and expanding data access at existing Blockchain gave with shrewd resources and brilliant agreements to improve the Blockchain innovation. ((copy with green line) In a ton of examination has set up observationally that Blockchain innovation is commendable for treating information supplant in the medical services area, at present different security, protection, and control inconveniences that outbound medical care should settle. On the off chance that a section is taken out from a provider information base, the information can be for acceptable lost, however it was not told about it. There are a few quality difficulties that they are dealing with issue constantly, the protection,

security, and trade of clinical information between healthcare associations or exploration establishments.

In a Blockchain, information is allocated across the organization, and there is no individual degree of disappointment prompting a potential reinforcement component.) Blockchain and brilliant agreements can be productive to improve HER. They don't discuss non-specialized perspectives that make wellbeing information reasonable. Our aphorism is to make strides total admittance to patient's information, get around an outsider section it without authorization. Blockchain innovation is the major innovation of Bitcoin that in-vented by puzzling Satoshi Nakamoto in 2008. They don't diagram some hidden standards of this association as far as moral results and receptiveness. In another examination, they proposed one real way to deal with work with patient-driven admittance control is by coordinating patient acknowledgment. The creators were not referenced improving the security perspective on the patients by moderating errors and upgrading data access at present Blockchain gave with shrewd resources and keen agreements to upgrade this innovation. Numerous specialists have exhibited observationally that Blockchain innovation is commendable for tending to information trade in the medical services area. At present a few security, protection, and control issues that outbound keen urban communities should resolve. On the off chance that a record is eliminated from a supplier data set, the data can be 1 for each for all time lost, however, they didn't tell about this. There are different capacity challenges that they are dealing with issue ceaselessly, the protected, secure, and trade of clinical information between medical care associations or examination foundations. In a Blockchain, information is appointed across the organization, and there is no single mark of disappointment prompting an inert reinforcement system. In this paper, various clinical information security is intended for various medical services the board. The last answer for information security could and should possibly be Blockchain innovation. At first, Blockchain innovation makes strides in life against breakdown and information indication. We propose diminishing data expenses and necessities to trust in a cut-down number of outsider foundations. Presently numerous organizations and examination establishments dissect the clinical applications dependent on Blockchain innovation. We sum up some exploration to attempt in medical care information entrance dependent on

the Blockchain stockpiling stage, which offers patients to handle their information without beguiling security. We propose a decentralized record of the executive's framework utilizing Blockchain innovation. We additionally propose a property-based mark conspire with different specialists. The EHR frameworks predominantly the improvement in security consider a fundamental piece of the medical services framework as it gives a lot of usefulness to medical services. Our center is to give security, sealed across various stages. The prerequisite of protection safeguarding information accomplishment for clinical information investigation in the cutting edge advanced medical services framework proposes a safe administration engineering Blockchain innovation and savvy contracts. For this, we use to foster the engineering by recommending a plan through a grand survey of the excess design. The fundamental exhibition of this paper is the proposed dynamic assent the executives engineering that agglutinates to the above plan objective. Our objectives: 1) information security, 2) information protection, 3) access control, 4) legitimate assent. 5) Stop information hardening

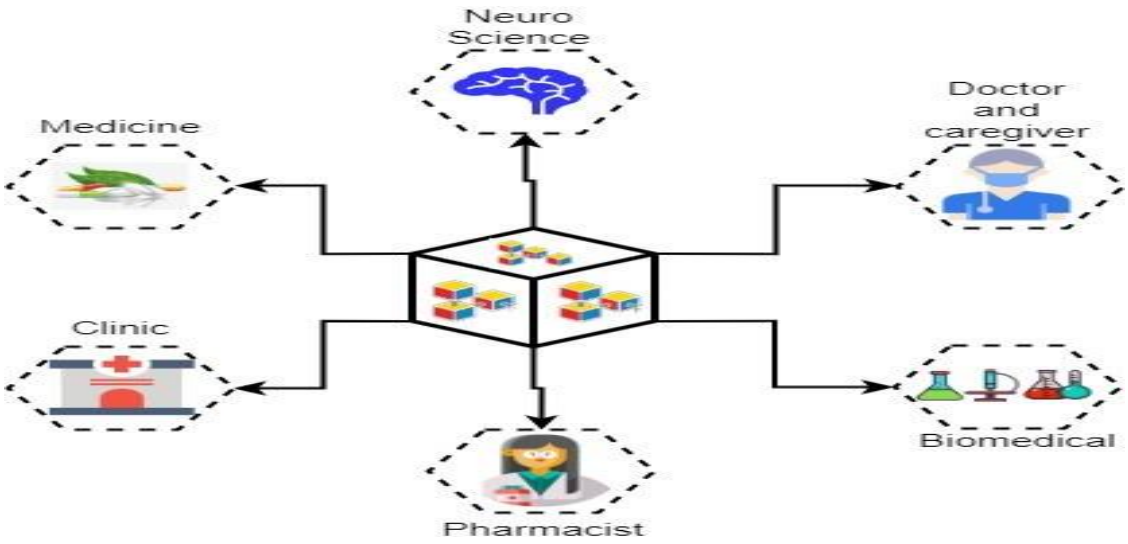


Fig. 1. Healthcare in Blockchain

1.2 Motivation

We admit to the hospital and give them our confidential and valuable information such as PII and PHI. We know that medical identity and information theft is one of the most dangerous and harmful to anyone. The attacker gets medical records that will be harmful to us. If any third parties get this personal data that's will occur a bad impact on personal life. Due to this inherent transparency and security, we want to secure our data with the help of blockchain technology. For this reason, we want to do this to secure our personal information and data. Overview of healthcare and Blockchain: The healthcare industry is a field that provides products and services for the treatment, preventive, rehabilitation, or palliative care of patients. Blockchain is a strategy for recording data that makes it hard to change, hack, or cheat a framework. A blockchain exchange requires an advanced record replicated and appropriated across the whole organization of PC frameworks in the blockchain.

1.3 Research Contribution

This report presents a healthcare security of a blockchain-based Healthcare system. Our healthcare security blockchain application allows healthcare system to create security for patient publishing them onto the blockchain platform like Ethereum with the help of our Healthcare System. Once the certificates are deployed on a public ledger onto Ethereum through smart contracts (blockchain chain code), they are permanent and immutable. It cannot be changed or modify by anyone. So, there is no need for a third-party or traditional centralized database server or extra maintenance cost.

1.4 Problem Definition

The most self-evident and exceptional advantage of blockchain is the way that it will eliminate the cognizance of ruining information. Blockchain will beat the issue of a solitary mark of a disappointment for getting information. Instead of a focal power, blockchain utilizes an agreement system that will join errors between hubs in a dispersed application. Notwithstanding, using innovation can be very difficult, however, we figure our examination will assist with eliminating the issue. We are living

in a particular world where innovation is becoming quicker. In the period of innovation, our clinical information is a higher priority than some other information. We know clinical information touchy. It very well may be made, duplicated, and changed by anybody quicker than any time in recent memory. We need to get our information blockchain will be the most ideal decision for us. We can share information all the more productively and securely with the assistance of blockchain. When a square is made then just individuals with the right key can make, adjust and transform it.

1.5 Research Question

The Research Question of our works are supposed to be answered by the following questions:

- What are the present flaws in the verification system?
- How these present flaws are eliminated using Blockchain Technology?
- How can these obstacles be tackled and what are the potential solutions?

1.6 Objectives

We are living in a particular world where innovation is becoming quicker. In the time of innovation, our clinical information is a higher priority than some other information. We know clinical information touchy. It tends to be made, replicated, and changed by anybody quicker than any time in recent memory. We want to secure our data blockchain will be the best choice for us. We can share data more efficiently and safely with the help of blockchain. Once a block is created then only people with the correct key can create, modify and change it.

1.7 Future Outcome

Computerized change in healthcare is a positive effect of healthcare innovation. Wearable wellness innovation, telemedicine, and AI-empowered clinical gadgets are solid instances of the advanced change in healthcare. Also, these are intended to alter the healthcare industry by lessening patient consideration, smooth out tasks and expenses, however all things being equal, it faces huge difficulties in network protection and patient information classification, invoicing and conveyance preparing, clinical stock chains, and medication trustworthiness. Blockchain innovation can't address these difficulties to the healthcare industry; it could set up a blockchain of clinical records. Blockchain is viewed as exceptionally secure, straightforward, and shielded from programmers because of its computerized encryption, as it is totally decentralized and furthermore assumes a huge part in moderate charge decrease. This survey paper looks at the capability of blockchain innovation to improve the security, classification, and convenience of medical services data, and after an itemized examination of current critical difficulties in the medical services area, we propose some improved utilization of blockchain in medical care areas. Recently endorsed and wearable wellness gadgets coordinate and screen wellbeing.

1.8 Organization of Report

The remaining part of this report contains the following chapters:

- Chapter 2 states the Background of Blockchain technology, architecture, core components, and pillar of Blockchain,, and some related work of our project
- Chapter 3 represents the methodology including the proposed model design and different components of building this project.
- Chapter 4 demonstrates the Implementation & Evaluation of our work
- Chapter 6 presents the summary, conclusion, strengths and limitations, and future scope.

CHAPTER 2
BACKGROUND

2.1 Comparative Analysis and Summary

Tanwar et al. (2019) observationally researched the few answers for improving flow constraint in medical care framework utilizing Blockchain innovation are investigated including structures and instruments to gauge the exhibition of such frameworks for the entire world during the period 1970s to work now. The investigation is utilized an Access Control Policy Algorithm for improving information availability between medical services suppliers aiding the reenactment of conditions to execute the Hyperledger-based electronic medical care record sharing framework that uses the idea of a chain code. The result showed that it can change the interoperability of medical services information bases, giving expanded admittance to the patient clinical records, gadget following, remedy data set, and medical clinic resources. Siyal et al. (2019) observationally researched the current and most recent advancements in the field of medical care by carrying out Blockchain as a model for the entire world during the period 1970s to work now. The Study is acquired extensive consideration, with a rising interest in plenty of various applications, going from information the board, financial administrations, network safety, IoT, and food science to the medical care industry and cerebrum research. The result demonstrated is transforming the conventional medical services practices to a more solid method, as far as powerful finding and therapy through free from any danger information sharing. Rao et al. (2019) experimentally researched Blockchain fundamentally based guide information the executives, particularly, for EMR information dividing among help providers and for examination reads for the entire world during the period the 1970s to work now. The examination gives a novel opportunity to carry out a protected and solid EMR information on the board and sharing, framework exploitation. The result showed that the arranged paper will extensively downsize the turnaround for EMR sharing, improve the higher psychological interaction for clinical guide, and scale back the worth.

Beam et al. (2019) exactly examined in medical services, IoT gadgets can give constant tactile information from patients to be handled and dissected. Gathered IoT information is exposed to brought together calculation, preparing, and capacity. The investigation is by giving decentralized calculation and capacity to IoT information. Hence, the joining of IoT and blockchain advancements can turn into a sensible decision for the plan of decentralized IoT-based medical care frameworks. The result demonstrated methodologically given to show how key highlights of the IoT and blockchain can be utilized to help medical care administrations and biological systems. Agbo et al. (2019) observationally examined in a methodical survey of the continuous exploration in the use of Blockchain innovation in medical care and examination reads for the entire creation. The examination depends on the Preferred Reporting Items for Systematic Reviews and Meta-Analysis (PRISMA) rules and a methodical planning study measure, in which a very much planned hunt convention is utilized to look through four scientific data sets, to distinguish, separate and investigate every single important distribution. The result demonstrated diverse use cases for the utilization of Blockchain in medical services; be that as it may, there is an absence of satisfactory model executions and studies to portray the viability of these proposed use cases. Uddin et al.(2019) exactly explored level-based End-to-End engineering for consistent patient checking that has a Patient-Centric Agent (PCA) as its highlight for the entirely of humankind. The examination is based the Blockchain is altered for RPM with modifications that incorporate having the PCA select a Miner to diminish computational exertion, empowering the PCA to deal with various Blockchains for a similar patient, and the modification of each square with a prefix tree to limit energy utilization and consolidate secure exchange installments. The result showed Simulation results exhibit that security and protection can be upgraded in Remote Patient Monitoring with the PCA-based End to End engineering. Griggs et al. (2018) exactly researched using Blockchain-based brilliant agreements to work with secure examination and the board of clinical sensors for whole individuals. The investigation depends on the Ethereum convention, which made a framework where the sensors speak with a keen gadget that calls keen agreements and sets up accounts of all occasions on the Blockchain. The result demonstrated purpose numerous security weaknesses related to far-off tolerant checking and computerize the conveyance of warnings to all elaborate gatherings in a HIPAA agreeable way. Sadiku et al. (2018)

observationally researched innovation that is relied upon to upset numerous ventures, including medical services for the whole age. The investigation depends on innovation that permits members to move information continuously, without presenting the channels to burglary, imitation, and malevolence. The result demonstrated a short prologue to Blockchain and it examines a portion of its applications and advantages in the medical care industry.

2.2 Terminologies

There are basically two forms of blockchains. Which is a private and public blockchain. Although there are different variants like hybrid and consortium blockchains. Nodes have a package that works on peer-to-peer (P2P) network systems. Updated in a timely manner, the list of each transaction can be controlled by each node. In figure 2.1 shows the model of public, private and consortium blockchain.

Public:

Catalogs of these types of blockchains are visible to anyone connected to the Internet. This network allows you to review, add or subtract any blocks of transactions by allowing different devices.

Private:

Individual blockchain is a package of individuals with a specific entity authorized to verify or add blocks of transactions. Anyone else connected to this network can see.

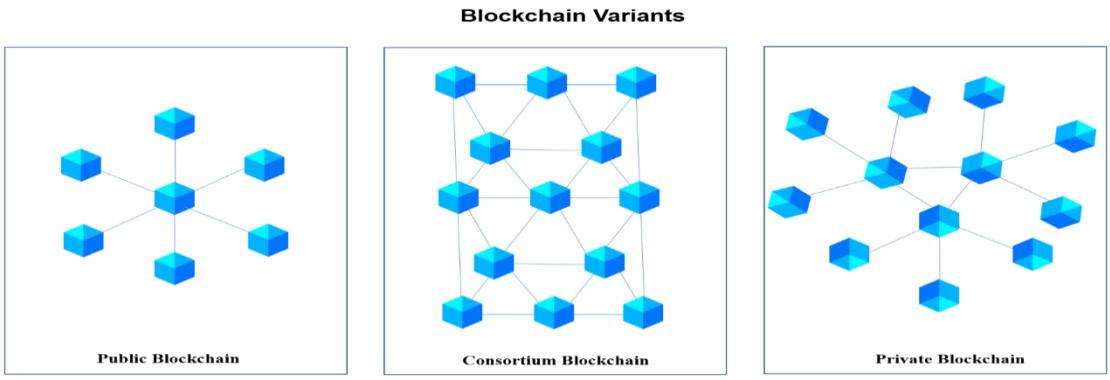


Figure 2.2: Public, Private & Consortium Blockchain Model

Consortium: This type of blockchain is used to add and verify transactions. It is often more effective collectively and individually. Control with pre-authorized nodes, anyone including the organization can use this BlockChain.

2.2.1 Pillars of Blockchain Platform

Nowadays, there are many public and private blockchain platforms available in the marketplace. For that, one has to choose a decent alternative based on one's spiritual obligation. This has to be appreciated based on the pillars of the blockchain platform as listed below:

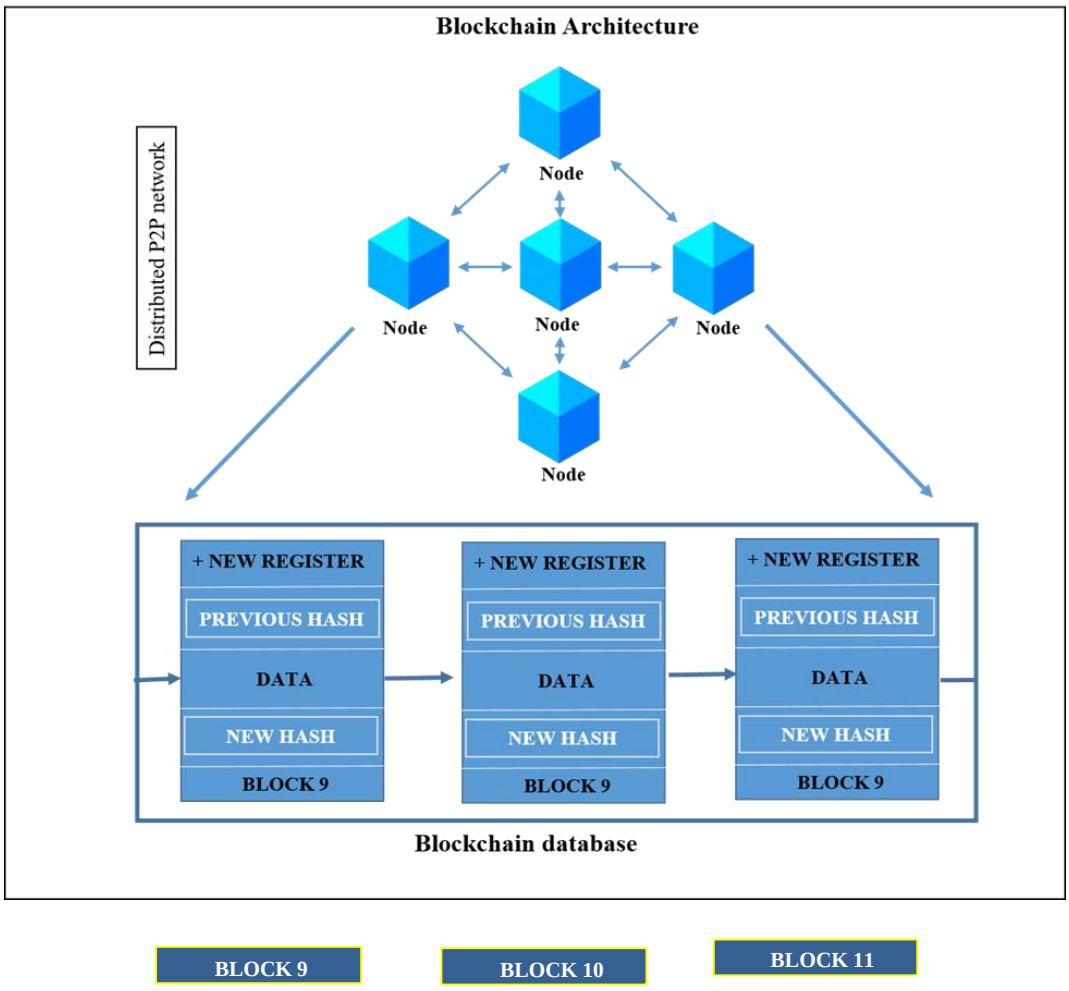
Decentralized network: One of the key architectural ethics of the blockchain platform is its decentralized mood. This implies that in a blockchain network the exchange is duplicated across all hubs in the organization and all hubs are associated. This blockchain platform is highly probable, as the transaction document is not likely to be corrupted because it has been copied to all nodes - and it is virtually impossible to interfere with all nodes in the network at any given time.

Platform security: Although blockchain platforms are decentralized to many users as part of a workflow scheme and involve several periods of time to conduct transactions, decentralized molds and multi-nodes have a higher level of security than any convinced record copy. Also, various blockchain platforms have a high degree of platform security such as sensing algorithms, unauthorized cryptocurrencies, use of cryptocurrencies for transactions, and smart contract opportunities to name a few.

Record immutability: The decentralized network of blockchain platforms across all nodes of the same network and the laser proves that the record kept in the account is sufficient to swap the record for any transaction to be executed only when all partners accept it there are limitations for. Correction of any record on the network changes the transaction to a new processing stage so that they can keep it as an exclusive entry.

2.2.2 Blockchain Architecture

Blockchain architecture includes node databases and networks. A blockchain database is split, fault-tolerant, only additions, and distributions are made. All record blocks are permanent. Users go to blocks but can't leave them. Each block is connected to each other by a chain and all of them have hash values. Each block arranges different types of displayed transactions. In addition, each block contains a timestamp specified fictitious time, a number for performing cryptographic activities. Blockchain networks initiate nodes that maintain the blockchain from peer to peer and distribution craze. Nodes are accessible, although uncovered supervision is prohibited.



igure 2.2.2: Architecture of Blockchain p2p Network

Figure 2.2.2 shows the point-to-point network architecture distributed by blockchain technology, as well as the architectural view of blocks, nodes, keys, and data. A blockchain database and network are decentralized and distributed. Building a block in a blockchain

network basically consists of three things: data, hash, and hash of the previous block. The data basically contains information related to the transaction. In the case of Bitcoin, the data is basically the details of where the transaction is from and where the transaction is from. The most important part of the block is the hash. It is completely unique. The hash value is created when creating a block. This is a kind of block identity. And the main thing is the previous one which needs to create a chain because a chain of blockchain blocks is connected to the new block hash to connect the hashes of the previous block to each other. When a block is found to be valid on a blockchain network, it is fixed in the blockchain database. Once a block is attached, it is difficult to change or modify. There are three generations of blockchain technology to support money, assets, and smart contract transactions. The first is Bitcoin cryptocurrency money transactions and the last generation is smart deals. The power of blockchain has been significantly enhanced by smart contracts that have led to its global acclaim.

2.2.3 Core Components of Blockchain

Node:

Node means users or computers that are connected to a blockchain network. It follows sensation rules and determines whether transactions are valid. Nodes can be any kind of device and data is stored there. Every node in an organization contains a duplicate of the whole blockchain, so every transaction is known. Essentially, a node resembles a gadget that contains a total duplicate of a blockchain transaction record.

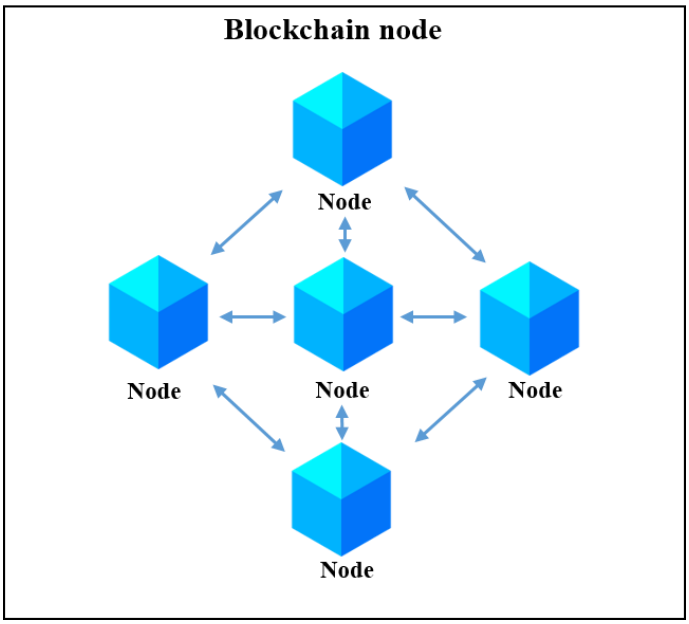


Figure 2.2.3: Nodes connection of Blockchain Network

In figure 2.2.3: there are 5 nodes, all nodes are connected with each other to run a Blockchain together.

Main Data:

The types of transactions determine the main data. This is enough to convert two nodes into one network. However, money transfer or record transfer can be a good example of such data.

Hash Values:

Hash is the extraordinary worth of a square. The hashed message is called input and the capacity used to do this is called hash work and the yield is known as hash esteem. There are numerous approaches to hash a message, however, a cryptographic hash work should have some quality. The capacity needed for hashing is single-direction work. Each hash an incentive for yield should be one of a kind. Hash in a blockchain is utilized to address the present status of a blockchain. These are useful in demonstrating the respectability of the square. A slight change in the hash worth will change the entirety. In the event that the hash worth of the square remaining parts as before for quite a while frame, it will give the

client a more elevated level of dependability. This makes clients trustworthy to the blockchain exchange history.

Hash of the Previous Block:

A hash is excited and broadcast as soon as the transaction is completed. Marshall Tree is the most common algorithm for hash formation because it allows easy hash and easy de-hash options.

Hash of the Current Block:

Current hash blocks allude to the last hash that is put away in the square. The block has a specific size which is the reason there are limitations on the number of transactions.

Transaction:

The transaction is little squares in the framework. These generally incorporate the sender's location, the beneficiary, and worth. Visa claims are a great representation. The expansion of the past transaction and the client's public key produces the hash by the proprietor's moved computerized signature. Exchanges are then indecently declared. the transaction is arranged and left on every hub as a square. An autonomous confirmation measure is executed by every hub when new exchanges are relegated. Every one of them was stepped and killed with time blocks.

Block:

Blocks store information from a blockchain network. Their primary objective is to package sets of exchanges and duplicate them to all hubs in the organization. The excavators make blocks in the blockchain. To deliver a legitimate square, the most favored activity among all organizations is mining. Putting away exchange records in blockchain, hubs are making a few strides like confirming forthcoming exchanges, checking cryptographic seals, and enveloping them by blocks. The block title assumes a significant part as metadata to confirm the legitimacy of the square. The primary topics in the square metadata are appeared beneath:

The remainder of the block is steady with the exchange. It very well may be quite a few transactions stuck in a square contingent upon the decision of an excavator.

Block type:

1. Major branch blocks extend the current main blockchain which is the longest chain in a network.
2. The side branch blocks refer to a parent block without the longest chain.
3. The orphan blocks the certificate of a parent block who has no knowledge of node processing. From the diving concept, when low blocks are mined, side branch blocks cannot be considered as part of the main branch. Only when more blocks are mined have they considered parent blocks. However, a separate branch will be reorganized into the main branch.

P2P Network:

In light of the IP convention, blockchain is a shared (P2P) network working framework. It is smooth geography with decentralized hubs. In this organization, all hubs are similarly circulated and can get administrations on account of tactile calculations. Since (P2P) networks have no single attack or compression points, they have more protection. Permitted and unlicensed is a type of blockchain network. In blockchain without permission, anyone can join the network. There are restrictions on adding new members to the permission-based blockchain. Pre-verification of new members is mandatory for permission-based blockchains or private blockchains. In a blockchain structure, each and every hub in the organization stores an imitation of the blockchain. The decentralization of blockchain engineering is the sole credit to the P2P network it has assembled.

Miners

In blockchain, miners play an important role. They validate the newly added transaction and record the block on the blockchain public ledger. After successfully adding blocks to a blockchain ledger, they receive a reward as a gas fee that pays users what they actually want to add their block to their blockchain network.

Smart Contracts:

Because of the computerized nature of blockchain, it has become a worker with savvy contracts. A concurrence with Corporal World is an understanding between the gatherings that executes certain stipulation and the exchange of resources happens. To start the exchange of resources and meet the conditions approved by the machine, the shrewd agreement code encodes these highlights. Furthermore, for handling or approving authoritative exchanges, the blockchain stage can give computational substance where different gatherings are keen on the exchange, permitting the area to get an offer in the exchange for confirmation. Etherium is a model that permits clients to interface with brilliant agreements. Clients should pay a charge for setting up good assets, granting brilliant agreements, and authorizing exchanges in Etherium.

Private smart contract:

Supported blockchain in business is being lauded step by step. Concerning deals, there is a ton of emergency of partners which gives a higher speed of exchanges. Contrasted with a public blockchain, the acknowledgment of a private blockchain is less For the situation of a lower set number of hubs, the individual blockchain might be viable. The two kinds of sensations will go against the quantum cycle. An individual blockchain relies upon the requirements of the business. As per the demand, it utilizes the accompanying calculations: The proper climate to produce the business application given by IBM is HyperLearder Composer, HyperLeader Fabrics, HyperLeader Indy, and HyperLeader SideDB. Among them, presently the trendiest stage is HyperLearder the texture of the pieces of its improvement which are called individuals. Each partner declaration of the part association is endorsed by the power.

Public smart contract:

Unauthorized blockchain is an independent platform because there is no need to collaborate with its peer nodes. Each node in the system has permission to install smart contracts. However, the cost of legitimizing a public blockchain is very prudent, as members have to pay a nominal fee for spamming, executing and instant smart contracts. To create contractual terms, Bitcoin scripts have developed Bitcoin. Many applications use Etherium

to control money and create decentralized applications. Ethereum's environment developed a cryptocurrency known as Eth.

Mining Techniques:

Mining is a way to include transaction records in blockchain public ledgers so that every transaction is secured and every single user on the network can easily access this account. Blockchain technology has a lot of mining techniques. In Table 1, we see a comparison of different types of mining techniques.

TABLE 2.2.3.1: COMPARISON OF DIFFERENT MINING TECHNIQUES

MINING TECHNIQUES	RESOURCE	RANDOMNESS	EXAMPLES	MINERS REWARD
Proof of Work	High computation energy & power	NO	BITCOIN	YES
Proof of Stake	Assets or stake	Randomized selection of Blockchain	ETHEREUM	NO
Proof of Space	Huge Storage	NO	PERMACION	YES
Proof of Importance	Significance of Node	NO	NEM WALLET	YES
Measure of trust	Reliability	NO	NO	YES (TRUST)

In this Table 2.2.3.1 it represents the different mining Techniques of blockchain. All mining techniques are demonstrating bellow:

Proof-of-Work:

PoW is a blockchain network algorithm used to secure transactions and chain newly created blocks. Minerals have a competition to finalize the transaction and be rewarded in the PoW.

Proof of Stake:

The Wikipedia Forum is a POS con Camus algorithm launched in 2011 to address issues raised by POW. Reaching the minimum is the main goal of both of them. But the process of reaching their goal is different.

Proof of Space:

During mining, mining nodes need to have a higher level of storage capacity rather than a higher capacity. PoS has a number of theoretical and material implementation exemptions. However, the essential high level of memory is a major challenge, such as the calculation challenge of PoW.

Proof of Importance:

PoI is a type of mining technique that calculates the outcome of an individual node based on the volume of transactions and the balance of those nodes. It prioritizes the most significant nodes, including the hash count, and selects the nodes to form the next block.

Measure of Trust:

Loyalty is the most important issue for starting a block. Nodes are getting priority based on their behavior. Nodes of good behavior go after the protocol and receive rewards.

TABLE 2.2.3.2: BLOCKCHAIN PLATFORMS FOR RAPID PROTOTYPING

Name	Working Types	Cost Evaluation	Language Supported
Ethereum Blockchain	Public & Smart Contract based	Ether for the transaction and computational services	Python, Go, C++
Hyper ledger	Private & Public	Open-Source	Python
Multi-chain	Private & Permissioned	Free & Open-Source	Python, JS, PHP, Ruby, C#,
IBM Blockchain	Private or Permissioned	Limited & enterprise plan (free/paid)	Go, JS

From Table 2.2.3.2 it gives an idea of how different blockchain platforms and their popularity, activity, network type, pricing, and the languages they support for development purposes.

Ethereum:

Etherium is a common platform for both private and public blockchain. First, make smart deals in blockchain to execute business logic. It produces intelligent contracts and decentralized autonomous bodies. Ethereum will take over the world as a global computing system if the Bitcoin blockchain is investigated as a global payment network, moreover,

like Android, Etherium is an open-source (developed by Google) platform. It provides a basic framework that is very helpful for developers to create applications. Etherium and the developers maintain and improve the infrastructure.

Hyper ledger:

Considered an umbrella task of open-source blockchain and related instruments, Hyper ledger, dispatched in December 2015 by the Linux Foundation, has effectively gotten enormous advantages from IBM, Intel, and SAP Ariba that help blockchain-based appropriation pioneers.

Multi-chain:

Multichain technology is a policy that helps users create some private blockchain institutes that can be used by companies that perform financial transactions. Multichain provides us with a very simple API and a command-line embrogator. It is helpful for protection and chain placement.

2.3 Related work

A few specialists have been proposed as of late dependent on Blockchain and medical services applications. In this part, the creators will introduce some writing's audit of ongoing works: For featuring the medical care 4.0 application, Tanwar et al. [1] exactly examined the few answers for improving current restriction in medical services framework utilizing Blockchain innovation are investigated including structures and apparatuses to quantify the presence of such frameworks for the entire world during the period the 1970s to work now. The result demonstrated that it could change the interoperability of medical services information bases, giving expanded admittance to the patient clinical record, gadget following, and remedy data set, and emergency clinic resources. Incomparable exploration for medical services utilizing Blockchain innovation, Ekblaw et al. experimentally proposed MedRec: a novel, decentralized record the board framework to deal with EHRs, utilizing Blockchain innovation [2]. The result demonstrated that it gives patients an exhaustive, unchanging log and simple admittance to their clinical data across suppliers and treatment destinations, and furthermore, MedRec oversees verification,

classification, responsibility, and information sharing—vital contemplations when dealing with delicate data. On the other examination, Siyal et al. [3] researched the current and most recent improvements in the field of medical care by executing Blockchain as a model. Further, the creators showed are transforming conventional medical care practices to a more dependable method, as far as able conclusion and therapy through free from any danger information sharing. Once more, Ray et al. researched in medical services, IoT gadgets can give constant tangible information from patients to be prepared and examined. Gathered IoT information is exposed to concentrated calculation, preparation, and capacity [4]. The examination is by giving decentralized calculation and capacity to IoT information. In [5] introduced a deliberate survey of the continuous exploration in the utilization of Blockchain innovation in medical care and examination reads for the entire creation. The examination dependent on the Preferred Reporting Items for Systematic Reviews and MetaAnalysis (PRISMA) rules and an efficient planning study measure, in which an all-around planned pursuit convention used to look through four logical information bases, to recognize, separate, and dissect every single applicable distribution. Further exploration, Uddin et al. proposed level-based End-to-End engineering for consistent patient checking that has a Patient-Centric Agent (PCA) as it's the highlight for entire mankind [6]. The showed Simulation results exhibit that security and protection can be improved in Remote Patient Monitoring with the PCA-based End to End engineering. In another work [7], Griggs et al. used the Blockchain-based brilliant agreements to work with the security investigation and the board of clinical sensors for whole individuals. Besides, this occasion on the Blockchain. Also, they settled numerous security weaknesses related with far off tolerant observing and examination depends on the Ethereum convention, made a framework where the sensors speak with a brilliant gadget that calls shrewd agreements and sets up accounts of all computerize the conveyance of warnings to all elaborate gatherings in a HIPAA consistent way. Pavlo et al.[8] Data security guarantees clients have authority over admittance to individual data where information availability guarantees that admittance to data is wild it isn't unexpected to be separated among protection and openness, and medical services are a space to which they are especially important. Reti et al.[9] Most of the time, patients need care from various doctors and various organizations that ought to have the option to get to the clinical notes and wellbeing

records of different doctors rather than them. Institutional wellbeing records are not generally open to different associations and institutional or individual wellbeing records are not generally interrelated. These issues are notable in medical care, and there is a central issue in a therapy known as the mix of care. Peterson et al.[10] The most well-known utilization of Blockchain innovation was in cryptographic forms of money like Bitcoin. All the more as of late, they have been proposed as an approach to execute different sorts of decentralized applications. Blockchain innovation depends on the idea of a distributable area, which goes about as a data set containing data on the exchange history of those specialists included. It is continually checked by a gathering of representatives (chose by various approaches relying upon the application space). The aftereffects of each check are put away in a square and communicated to the organization. The squares are haphazardly added to the record, making a cryptographically connected chain. Endeavors to mess with squares or endeavors to change their request can be handily identified. Azaria et al.[11] Provide a proof-of-idea that utilizations blockchain as a go-between according to wellbeing data. This model, known as Medrec, brings "mining" to an organization of clinical scientists and medical services partners, and as an award for mining, it gathers and uncovers admittance to mysterious clinical information. The creators contend that to engage analysts while including patients and suppliers, a maintainable and secure distributed organization must be made by giving enormous information. The stage Medrec was just approved for clinical records and should be stretched out for more basic wellbeing data and complex circumstances. Vujičić and et. [12] Blockchain technology presents an outline of Bitcoin and Etherium. The creators de tin that data innovation finishing sanitizing and blockchain innovation data frameworks. They deciphered Bitcoin as a shared circulation network used to perform Bitcoin exchanges. They additionally investigated the Proof-of-Work Sens Camus calculation with the Mining Blockchain Concept. Etherium likewise isolates the blockchain.Wang et al. [13] Conducted an investigation zeroing in on keen registering and its application to blockchain innovation. They initially present savvy gets, their work structure, working frameworks, and other significant ideas related to them. The creators further examine how keen agreements can be utilized for new ideas of equal blockchain. They distinguish that the justification for utilizing shrewd agreements in the blockchain is because of the decentralization gave by

their composed programming language code. Subsequent to presenting the fundamentals of brilliant agreements, the creator clarifies the various layers of blockchain that incorporate to keep the framework working. These levels are the information, organization, sense minimization, motivation, and agreement and application levels. The paper not just examines the engineering and design behind keen agreements yet, in addition, give bits of knowledge into their application and difficulties. Kuo et al.[14]Conducted a survey that examined the different utilizations of blockchain in the organic and medical services areas. Continuous admittance to information and eventually secure data is available to biomedical or medical care partners. The restrictions of blockchain innovation are location, deftness, speed, versatility, and the danger of malignant assaults, i.e., 51% assaults. The creators have recognized these limitations as basic for the medical care or biomedical area since they are being utilized to safeguard delicate clinical or clinical records. The answer for this issue was introduced by the creators to utilize VPN (Virtual Private Network) to guarantee delicate clinical information chain of stores, information encryption to guarantee confession booth and extreme assurance from malevolent assaults. Guo et al.[15] Proposed a quality-based mark plot with different specialists. Be that as it may, most examinations consider security insurance instead of essentially access control frameworks. Touchy information itself. Truth be told, shielding information protection from information security is simpler and more successful than access control frameworks. Bergman et al.[16] Wang and Jin et al. Planning profoundly unique consistency frameworks to improve patient information security has effectively been examined by joining new assent-related highlights into existing access control approaches in medical services frameworks. A portion of the key highlights considered are assent type (award/refusal/withdrawal), approved movement (read/compose/move), care, explicit information record, reason, setting, assent acceptor, assent guarantor, signature, creation The connection between time, extra room, legitimacy period, care and beneficiary issues. Of every one of these highlights, "setting" can be distinguished as a quality that must be given through powerful assent the executives. Also, an approval model has been proposed to merge medical services data from circulated information sources, where the two patients and parental figures can go about as agree suppliers solidify information.Liang et al.[17] Decentralized authorization the executives conventions, access control arrangements will be put away in the blockchain

and all Access-related exercises will be recorded in the blockchain for checking purposes and when new clinical records are made, the information will be transferred to the blockchain just with the assent of the patient. Unexpectedly, there are some blockchain-based assent the board arrangements proposed in the medical services area, the greater part of which just apply to assent the executives for essential use. Accordingly, these arrangements uncover the personality of patients by plan. Be that as it may, when getting information for auxiliary use, the arrangement ought to give a security ensured design to consistence the board. Bhaskaran et al.[18] likewise, for the assortment and confirmation of "No-your client (KYC)" information between banks, a twofold visually impaired, assent driven information sharing instrument is proposed to acquire the client's express agree to get to their own data. . Nonetheless, none of these arrangements consolidate the different highlights expected to make profoundly unique consistence frameworks for medical care. Additionally, these arrangements are not equipped for dealing with the assorted and dispersed nature of patient information remembered for medical care information organizations. Rolim et al.[19] The framework offers a structure where the framework measures information in information assortment and information appropriation steps. In this model, the sensors go about as gatherers that gather the information and store this information straightforwardly and send it to the framework for work. This data will be gotten to by clinical experts and sensors were proposed to be joined to the treatment hardware in this framework. Yue et al.[20] Has presented cloud-based patient-focused frameworks. This model has three levels: information assortment level, information the executives level, and information administration level. Heath depicted a blockchain-based admittance control administrator for information to expand the ease of use of the framework. The O-Blockchain framework was proposed as an entrance control chief for medical care data, including public blockchain. Ekblaw et al[21]. Proposed a model called "Medrec" that utilizations blockchain as the spine and looks for security answers for H n EHR frameworks. They attempted to share their model respectability, validness, perceptibility, and information through blockchain. The segments of their framework are the Registrar Contract (RC), Patient-Supplier Relationship Agreement (PPR), Short Agreement (SC), where the RC maps the members' distinguishing proof strings to their Etherium address, while the PRP framework gives an understanding between two hubs. By

storing and managing medical records, the SC searches participants 'history of medical records. Linn & Co, Alexander, Brodersen et al. [22] Top security, medical care blockchains should shield EHRs from forceful dangers to various pieces of the framework. For instance, man-in-the-center assaults can bargain access control of a framework. Peterson et al. (2016) propose different systems to set up and secure access control. Lynn and Cook (2016) proposed a biometric distinguishing proof framework for the endorsement of the gatherings. Brodersen et al. [23] Instructed with respect to confided in specialists, for example, banks and bosses gives the genuineness of an individual's character in the framework. For the significance of classification of exchanges in the blockchain, Brodersen et al. announced that exchanges should not be found in expert patients. To do this, Brodersen et al. recommend the execution of tokenization: an interaction by which just a reference to touchy data is unveiled to the general population, permitting crude, very much educated data to be kept hidden. Griggs et al.[24] A private blockchain dependent on the Ethereum convention has been received just to work with the free from any and all harm utilization of treatment sensors and furthermore to wipe out dangers related with far off quiet observing frameworks. Their blockchain is continuous far off observing that permits doctors to distantly follow their patients' medical care status and keep a protected, secure, and modern history. Chen et al. [25] has proposed an incorporated blockchain and distributed storage based design for overseeing and sharing patient clinical information. The proposed plan can be utilized for free from any danger stockpiling and trade of individual patient clinical information. This is remarkable in the idea of the proposed approach, as it gives patients full access and command over their own clinical information, subsequently disposing of any outer outsider inclusion.Jiang et al. [26] dye has made a special blockchain-based stage for trading medical services data. Works principally on close-to-home medical care-related information and electronic clinical records with an assortment of information, including the prerequisites for the edge stage Malleus HealthCare Data Sharing and the use of blockchains between various sources. To check the good prerequisites of both validness and protection, they join the stage with on-chain and off-chain confirmation measures. Kaur et al. [27] talk about medical services information as a significant asset and along these lines, there is a dire need to protect such information successfully, including safe techniques. Information in medical care is

exceptionally different, which has demonstrated to be a test for analysts. Along these lines, it must be survived. . They imagined that if blockchain innovation and cloud conditions were utilized together, this issue could be survived. They proposed a blockchain-based stage that could undoubtedly, precisely store and oversee tremendous medical care information and furthermore give security of putting away information. Presently, all medical care information is put away on concentrated workers. Xia et al. [28] recommend that the secrecy of treatment data is right around the main concern since it jeopardizes the patient's condition. On the off chance that this infringement happens, it contrarily influences all patients, partners, and excavators. To keep away from such a circumstance, the creators propose blockchain-based designs to ensure information self-rule utilizing cloud conditions. The proposed structure just permits confirmed clients or accomplices to get to any framework. Clients' activities can be checked by the proposed blockchain-based system. The sharing of patient information is confirmed by embracing cryptographic procedures. The framework is a go-between between clients and delicate medical services information. Their proposed framework utilized a lightweight blockchain that guaranteed quick exchanges and precise productivity.Dubovitskaya et al. [29] recommend that medical care data is exceptionally delicate and basic and that occasionally wellbeing data should be divided between various investors for their particular purposes. To accomplish the referenced issue, they proposed blockchain-based wellbeing the board, which guarantees trust, responsibility, and straightforwardness in wellbeing data. A system has been made in light of malignant growth patients. The model of the construction guarantees insurance, security and diminishes turnaround time for sharing medical care information. The proposed framework incorporates membership administration data sets for clinical information stockpiling, hubs, and different application programming interfaces (APIs).Omar et al. [30] accept that digital aggressors have an exceptional premium in medical services information since it creates colossal measures of income. The creator recommends that decentralized property could make medical services somewhat more secure. In this way, they have executed it by proposing a medical services information executive's framework utilizing blockchain innovation since it upholds responsibility and uprightness. Namelessness is guaranteed by ensuring patient information in different cryptographic strategies. The creators' proposed conventions have various substances and

jobs. The information sender layer assumes a significant part, it gets all the treatment-related information of the client and scrambles and saves it utilizing cryptographic techniques. The concept of blockchain technology was first published in a white paper published by Nakamoto et al, [31] which revises every one of the difficulties looked by cryptographic forms of money. The creator proposed an innovation with the goal that the exchange could be finished securely. In light of these enormous turns of events, different areas all throughout the planet have picked blockchain innovation over other existing advancements for secure information sharing and trust, responsibility, validness, honesty, and character recognizable proof. To incorporate advancement in the medical services industry, they proposed a framework for dealing with all medical care information utilizing blockchain innovation. Their proposed framework had the important verification, classification, and responsibility to share the essential data. High et al. [32] proposed a novel strategy for getting to patient data that couldn't be conveyed yet could be securely put away on a wearable gadget utilizing a blockchain. Patient data will be put away utilizing encoded private keys and public keys. The private key must be decoded by the patient's biometric signature. Genuine patient records must be gotten to in a crisis utilizing a mix of public and private keys. The creators propose an engineering that guarantees decentralization. Li et al. [33] bring up that medical services has become a fundamental spot in the existences of people, which incorporates putting away information at a more significant level. It profoundly affects an individual's life. Whatever it is, this information can be successfully changed or taken by assailants which results in misdiagnosis and a great deal of adversity as far as income. Consequently, the creators proposed a blockchain-based information stockpiling system that ensures strong information stockpiling and, also, secures clients utilizing blockchain models. This structure guarantees client assurance utilizing cryptographic estimations. Along these lines, they carried out this framework on a stage called Etherium. It gives successful and productive execution results. Uddin et al. [34] proposed a blockchain-based structure for far off patients in the medical care framework. In their design, they consider that every understanding has a wearable gadget (sensor) that is utilized to get wellbeing data. Subsequent to preprocessing from the framework, the data is put away in the blockchain. The proposed project utilizes mineral frameworks to make blocks. The proposed mining framework varies from the idea of

bitcoin-based mining. Partaking in the framework to produce the hash worth of the current square of numerous diggers in the bitcoin framework. Be that as it may, in the proposed framework, just a single excavator does likewise work. This choice of reasonable minerals is made by the patient's representative dependent on specific boundaries. From the above conversation, a few specialists have effectively been tended to different examination dependent on medical services applications utilizing various innovations. By in regards to this examination, the creators present an approach to give information security to the medical care climate productively. Likewise, the creators additionally feature the presentation estimation of medical services dependent on Blockchain innovation appropriately.

2.4 Scope of the Problem

The last half of the 20th century and the principal long periods of the twenty-first century saw some gigantic disclosures and revelations that changed our reality until the end of time. Be it a PC, the web, and now the new detecting blockchain. Blockchain innovation has arisen as another popular expression on the planet. Some even allude to it as the new or "next web". The extent of blockchain innovation in medical services is tremendous. This is upheld by a report that expresses that worldwide blockchain advancement innovation in medical services.

With a worth of about. 34.47 million, income will increment to income 15.59 million out of 2024. Besides, CAGR development will be around 70.45% between 2018-2024. The insights look encouraging however there are key reasons why blockchain is so significant for medical care.

2.5 Challenge

Information security is a significant test in conveying medical services frameworks for patient-focused exploration, market examination, clinical exploration, medical services information mining, and that's only the tip of the iceberg. Overseeing the enormous scope of information and safeguarding patients 'protection has for quite some time been a test for scientists. Conversely, blockchain innovation has lightened a portion of the issues by

giving a safe and disseminated stage. Unfortunately, in existing medical care the board situation experience the ill effects of information control, deferred correspondence, and solid collaboration in information assortment, stockpiling, and circulation. This part talks about the recent concerns of protection identified with medical services and the current and impending guidelines in this area. This section incorporates an outline of the design, existing issues, and future freedoms for blockchain innovation to effectively deal with the privacy and the board of current and future clinical records. This section likewise presents various blockchain arrangements that help medical care, huge information, and future examination scope in the blockchain.

CHAPTER 3
RESEARCH METHODOLOGY

3.1 Methodology

The proposed methodology utilizes Blockchain technology through the functionality of some systems. All transactions recorded and verified on the Blockchain cannot be modified, hacked, or deleted. The principle motivation behind both present and future improvement in the field of medical care execution and security by improving Blockchain innovation as a model. We additionally examine the principle utilization of Blockchain innovation and confronted the test too. For developing this, we utilized the Solidity language for smart contract implementation on the ethereum platform. We also used the web3.js ethereum library, Remix IDE, Solidity language. In the front-end, we have used the React.JS, JavaScript library for building user interfaces. It ensures faster rendering and interactive single-page web applications and allows users to easily interact with the smart contract.

3.2 Blockchain Healthcare Requirements

3.2.1 Solidity Language

Solidity Language is a term made by Ethereum and dispatched in 2014. Savvy It is an undeniable level, OOP language for keen agreement composing and advancement and it upholds numerous libraries and heritages. Solidity is powered by C ++, JavaScript, Python and intended for EVM targeting.

EVM means Ethereum Virtual Machine.

The main advantage of Solid for creating smart contracts in Ethereum blockchain:

Effective: Consistency is used for smart contracts. It is used for most money-related needs (such as auctions, crowdfunding, or wallets with multi-signature features). However, we can create other decentralized applications such as voting, land registration, healthcare, and more.

Flexible: We can use a remix IDE to write smart contracts or download a command-line compiler to a PC. Both options are free to create, compile and deploy.
Improving: Silent language updates are constantly being introduced, such as new features or bug fixes.

3.2.2 Remix IDE

Remix IDE is a browser-based open-source ide. It has an expeditious advancement cycle and has a superb number of plugins with built-in graphical user interface. The remix ide is used for the development of smart contracts as well as an immersive platform for learning the Ethereum Blockchain. It is a development tool that uses a plugin-based architecture. It has also massive module features like various solidity compiler, EVM version, web.3 environments, metamask wallet support, debugger, and one-click deployment tool. Remix is a robust browser-based open-source tool that assists you to write, debug and deploy smart contracts directly from the browser.

3.1.3 Web3.js Library

Web 3.JS is a storehouse of libraries that permits you to speak with neighborhood or distant workers of Ethereum hubs through HTTP, IPC, or WebSocket. It is likewise an assortment of modules that fuse the usefulness of the etherium environment. Then again, we've distinguished Athyrium as the JavaScript API.

- **WEB3-SHH**
- **WEB3-ETH**
- **WEB3-BZZ**
- **WEB3-UTILS**

Benefits of Web 3.0 Technology

- Transparency
- Fewer Middlemen
- Privacy-preserving and interoperability protocols

- Data Ownership & Sharing Ability
- Decentralized Identity
- Trust Verification
- Decentralized infrastructure and application platforms

Web 3.0 is the new age of the Internet, where all applications become smarter, more close to home and more decentralized, and safer. The experience of utilizing the Internet will change impressively as new establishments and stages come on the web. The current web is an astounding asset and it enables us to do viable things. However, we additionally need to give a lot of information to our mediators who are not legitimate about their training. Web 3.0 tries to change this and make a more open and straightforward Internet.

3.3 Proposed Model and Design

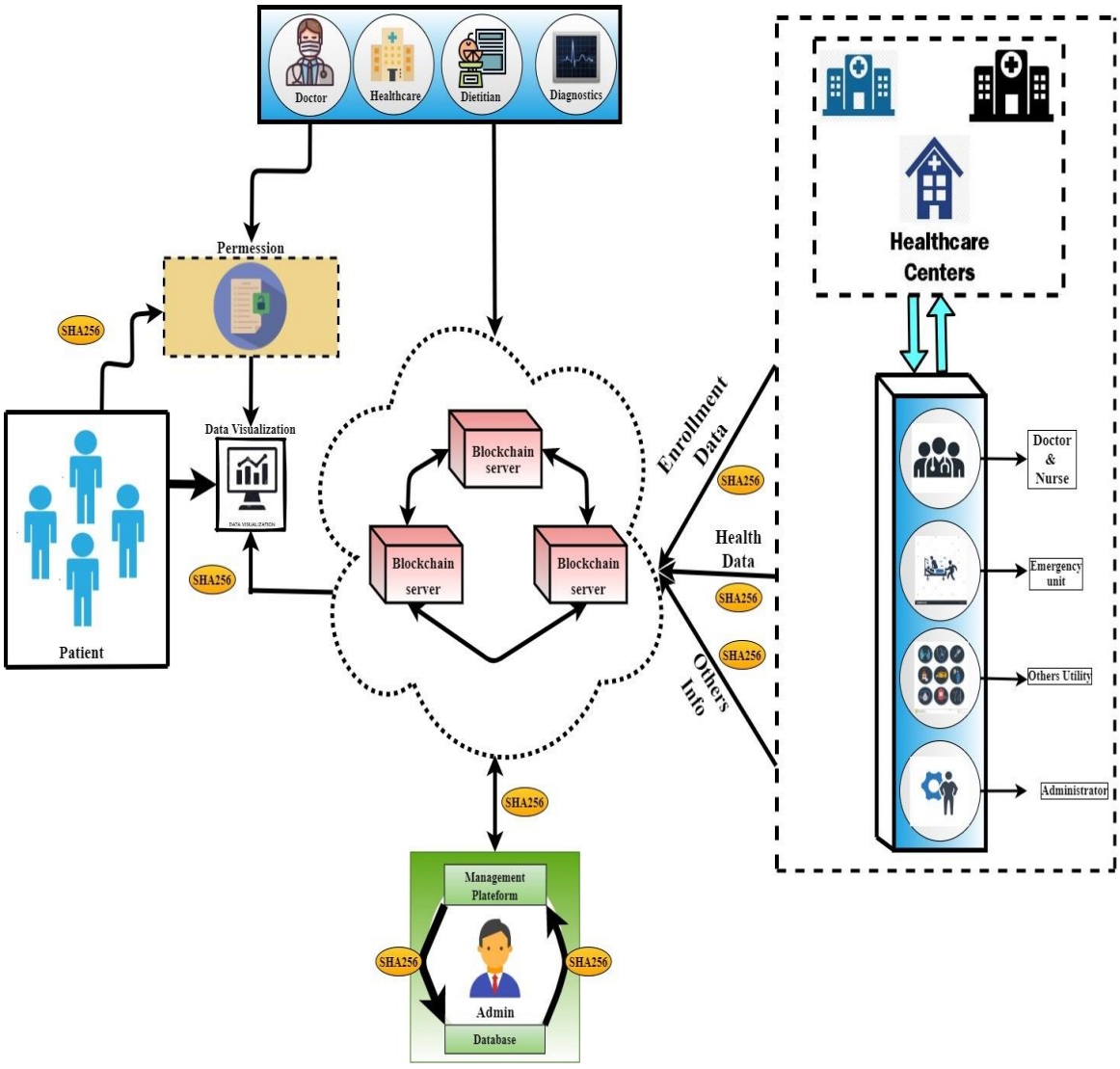


Fig: 3.3 Proposed Model and Design

This section will discuss our proposed model where we talk about data add, visualizations, delete, permissions, and talk about data safety. Our main goal of the proposed model is securing hospital data. When we admit a hospital, we all know that we give them our

valuable information such as national id card(NID), credit card, and personal information, which is too much more important than any other data. With this security in mind, we introduce hospital management to new, more secure technologies, more reliable, and easier to share and access data based on Blockchain than any previous security. In the proposed system, a common symmetric key and private key empower the EHR to be conveyed to different members in the blockchain network. A common symmetric key and private key empower the EHR to be dispersed to different members in the blockchain network in the proposed a system. They can also share data, display data with this method. Our system workflow is reliable and straightforward to use. At the point when a patient goes to our medical care place through this work process, their data will be submitted to the blockchain worker. From there, the hospital management or admin will access the data via sha256 encryption and save it in the database. They will see live updates on how much a patient's hospital is spending in some places through our Blockchain's distributed ledger. When they are admitted to the hospital corresponding to their ID, they will be connected to a blockchain. When they go to another hospital or diagnostic center, a Dietician, Gym trainer, and Public Health advisor can share their data with those entities with permission.

• Data Encryption: Health data encryption happens when data is encoded and changed over to indiscernible content to make the data open without unscrambling keys. Encryption secures patient wellbeing data when it is sent starting with one client then onto the next.

•Decryption: Decryption is accepting an encoded or scrambled content or other data and changing over it back into text so you or the PC can peruse and comprehend. This term can be utilized to depict a technique for physically scrambling information or any decoded information utilizing the right code or keys.

•Hashing: A cryptographic hash (sometimes' Digest known as) is a kind of text or data files' signature '. SHA-256 for a text almost unique 256-bit (32-byte) to create the signature. See below for source code. A SHA- 256 hash can only enter a message.

Distributed storage network and patient data and management

As health providers move toward the reconciliation of innovative data innovation (IT), they are progressively becoming ward on the accessibility of electronic wellbeing records. Odd current data innovation (IT) can change manual paper records with the possibility to decrease medical care costs and improve patient wellbeing and results, zeroing in on existing stockpiling arrangements oversaw separately by every medical services supplier to guarantee information security, accessibility, and excess. Through electronic wellbeing records, at present made enormous scope upkeep inside an association, patient wellbeing data can be effectively shared through standard electronic exchanges with different elements inside the wellbeing data trade organization. Such public organizations may incorporate patients through wandering facilities, sub-concentrated consideration conditions, different emergency clinics just as contributors, and surprisingly however the Patient Healthcare Records (PHR) interface.

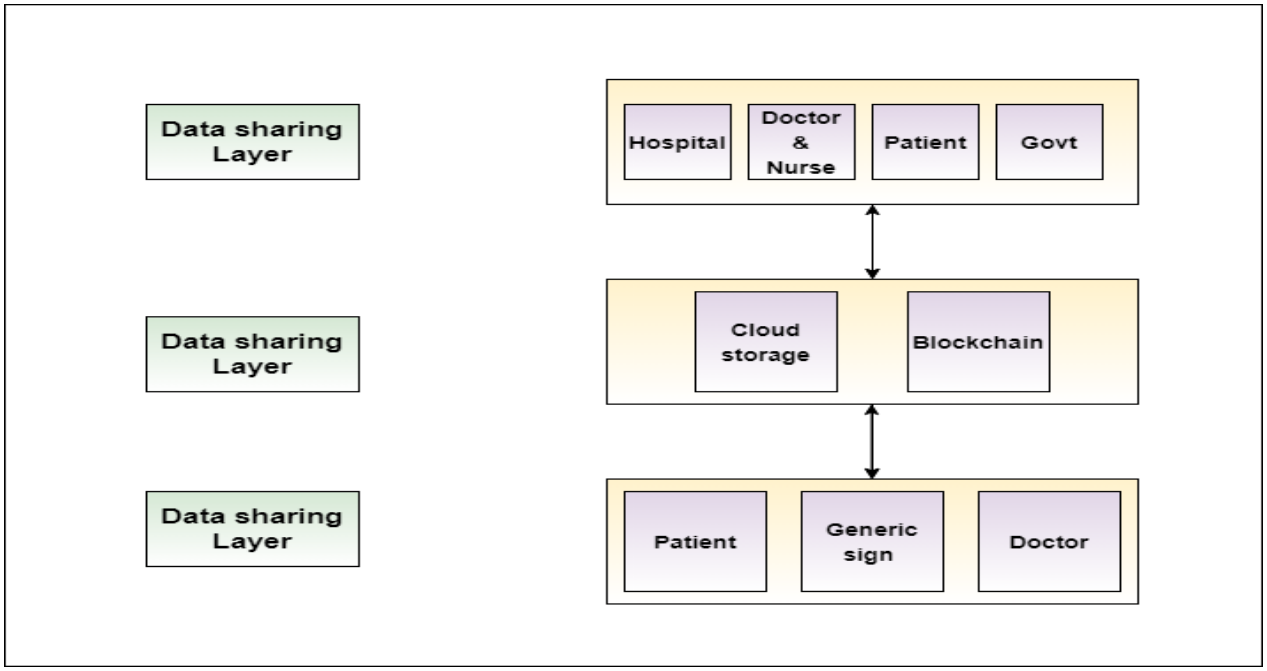


Fig: 3.3.1 Distributed storage network and patient data and management

Share data Different Entities

- Dietician: Dietitian (or dietitian) dietitian subject matter expert; that is control of human sustenance and diet. A dietitian changes their patient's nourishment dependent on their treatment conditions and individual necessities. Dietitians are checked by authorized medical care experts to analyze, analyze and treat healthful issues.

- Gym trainer: Gym trainers help and instruct people as they exercise. They can have practical experience in at least one field, not restricted to high-impact exercise, weight lifting, Pilates, yoga, and moving. They can direct gathering classes, give one-on-one preparation to customers, or join both.

- Public Health advisor: Although broadly defined, a public health counselor is a person who provides support and advice on matters related to the improvement of public health activities. General wellbeing specialists can uphold a wide scope of offices and associations, including public, philanthropic, and private organizations.

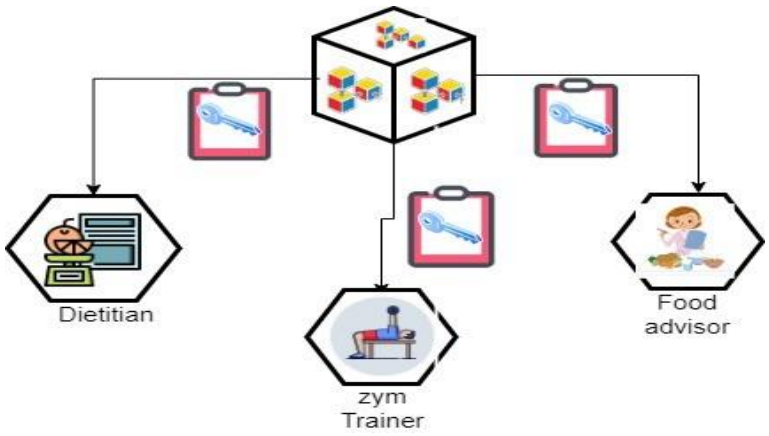


Fig: 3.3.2 Share data Different Entities

Improve DOS and DDos attack

With the help of Blockchain, we can prevent and mitigate Dos and DDoS attacks. Blockchain is a decentralized system with multiple nodes. Conducting DNS in Blockchain will ensure that attacks are crippling, not centering on a centralized source. To successfully bring down DNS in a blockchain, hackers need to simultaneously access multiple nodes, making the attack more difficult, time-consuming, and costly to carry out.

A decentralized network of servers that can send bandwidth quickly to other servers in the face of attacks. The infected server can withstand the DDos attack by absorbing the extra traffic using the extra bandwidth.

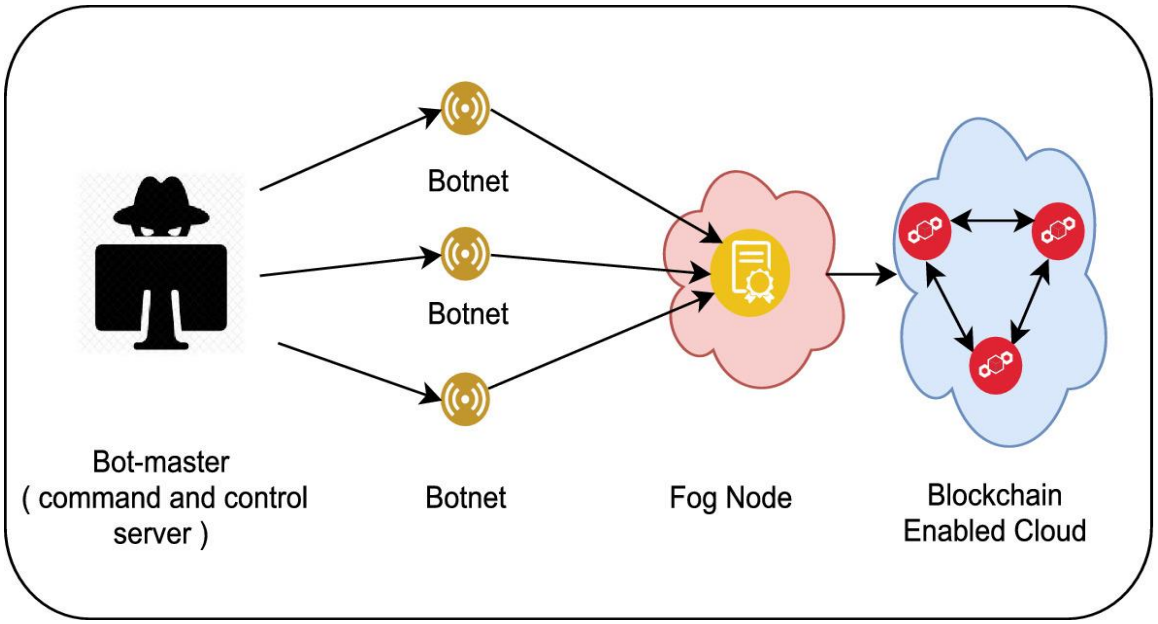


Fig: 3.3.3 Improve DOS and DDos attack

3.4 Implementation Requirements

3.4.1 Cipher

The Avanzer blockchain execution stage is known as Cipher. It is a platform agonistic arrangement that can drive any sort of hidden blockchain innovation. The code goes about as mindware for government organizations and controllers in various regions, fortifying four blockchain DPS portfolios. The critical spaces of Cipher's blockchain-based arrangements are the progress to advanced government and monetary control and oversight. As the world moves towards decentralization, the up and coming age of blockchain technocrats will make strides as a degree of code empowering to guarantee that they keep on performing admirably.

3.4.2 Chainlink

As per ChainlLink's official site, "ChainLink networks give dependable sealed information sources and yields for complex shrewd agreements in any blockchain." This stage gives a sound and constant start to finish issue. Steel guarantees information uprightness and utilizations similar reasonable calculations utilizing blockchain on their foundation. Likewise, the steel gives your brilliant arrangement every one of the data sources and yields you need to accomplish your latent capacity.

3.4.3 Hash Value

Hash esteem is a numeric worth of a specific length that exceptionally distinguishes the information. Hash esteems address a lot more modest number qualities as bigger measures of information, so they are utilized with advanced marks. You can sign hash esteem more productively than marking a bigger worth. Overseen hash classes can either hash a variety of bytes or an over saw stream object. The accompanying model uses the SHA1 hash calculation to make a hash an incentive for a string. Model The Unicode coding class utilizes the SHA256 class to change a string over to a variety of hashed bytes. The hash worth will at that point be shown on the reassuring. The information can measure up to the hash worth to decide its genuineness. Normally, information is hashed at specific occasions and the hash esteem is some way or another secured. Sometime later, the information can be hashed again and contrasted with the ensured esteem. On the off chance that the hash esteems match, the information isn't changed. On the off chance that the qualities don't coordinate, the information is undermined. For this framework to work, the ensured hash should be encoded or hidden from every corrupt gathering.

3.4.4 SHA 256

SHA-256 is one of the replacement hash elements of SHA-1 (all things considered known as SHA-2) and it is perhaps the most remarkable hash capacities. The SHA-256 code is not any more unpredictable than SHA-1 and has not been undermined at this point. This makes it a decent accomplice work for 256-bit key AS. It is characterized in the NIST (National Institute of Standards and Technology) standard 'FAC 1804'. NIST likewise gives a few trial vectors to confirm the legitimacy of execution.

3.4.5 Firefox Browser

Mozilla Incorporated and the Mozilla Foundation created Firefox, a cross-platform internet browser. It was first invented in 2002 utilizing free programming parts from Microsoft Windows, Apple WebKit, and Mozilla Firefox. It was then ported to Linux, macOS, iOS, and Android, where it is presently the working framework's default program. The program is likewise a significant piece of Firefox OS, as it goes about as a stage for online applications. Firefox may permit you to use your time and get more out of your program by using Google applications like Gmail, Google Play, and Google Assistant. Firefox bends over backward to protect your information and security on the web. Firefox permits you to customize your visual experience to assess how your inclinations and riding propensities line up with basic security measures. Firefox assists you with completing things and be protected online with highlights like secret phrase check, dark mode, and the Google address bar.

3.4.6 Metamask

The main features of the metamask wallet given below:.

● MetaMask is available at browser extension in chrome, Microsoft edge, Firefox and also available in the mobile application store. It provides you with a secure login, key vault, token wallet, and also balance transfer access— it supports you with everything need to manage digital assets.

● It also provides the most manageable yet most reliable, secured and easiest getaway to connect with the Blockchain-based applications.

● It provides passwords and key, so only you have entrance to your accounts and personal data. Just choose what to share and what to keep private.

3.4.7 Ropsten Test Network

The Ropsten test network is a POW (proof-of-work) test net for the Ethereum platform.To acquire ETH on Ropsten, anyone can willing to mine on the network.The Ethereum blockchain has a few test-nets like kovan,rinkeby, and goerli test net. The Ropsten test-net

supports blockchain developments to test their work in a convenient setting but without the need for real ETH like ethereum main-net. Moreover, this offers

the ability to perform transactions without facing any significant gas fees or risking main-net 2KEY. It’s is an exact copy of the real main-net Network, and it allows anyone to engage without requiring real ETH tokens.

CHAPTER 4
IMPLEMENTATION & EVALUTION

4.1 Implementation

In the present age we are advancing in the modernity of science, one of the technologies of the present age is blockchain. We are trying to bring our current 'hospital management' under the blockchain and we have been able to accomplish something through this research.

4.2 Experimental Results and Analysis

Tools and Technology used in Blockchain Healthcare:

- Blockchain Framework: Ethereum
- Language for implementing smart contracts: Solidity
- IDE for deploying smart contracts: Remix IDE
- Ethereum wallet: Metamask
- Blockchain Network: Ropsten Test Network
- Web Technology: Web 3.0
- Web 3.0 Module: Web3.JS library, web.th

Set and Get patient and output:

Fig 4.2.1 shows the set and Get patients output where we can input our data and it also shows output data.

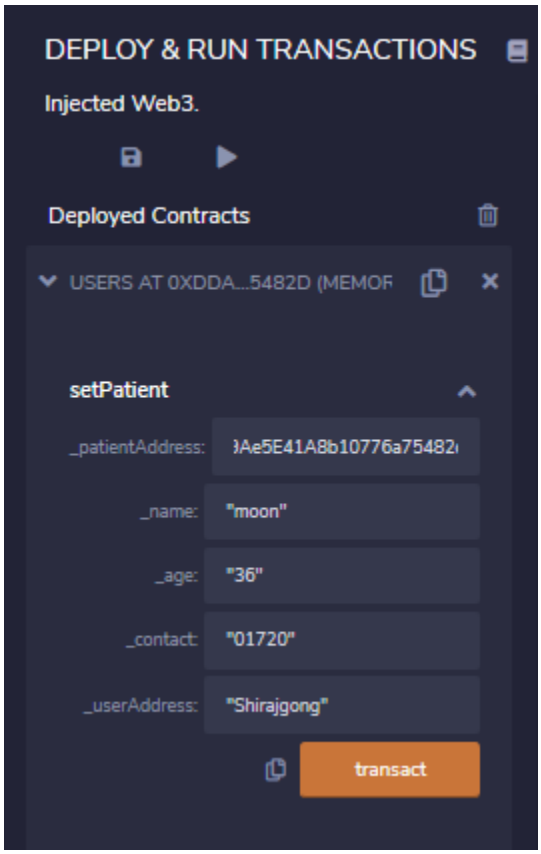


Fig: Set Patient 1

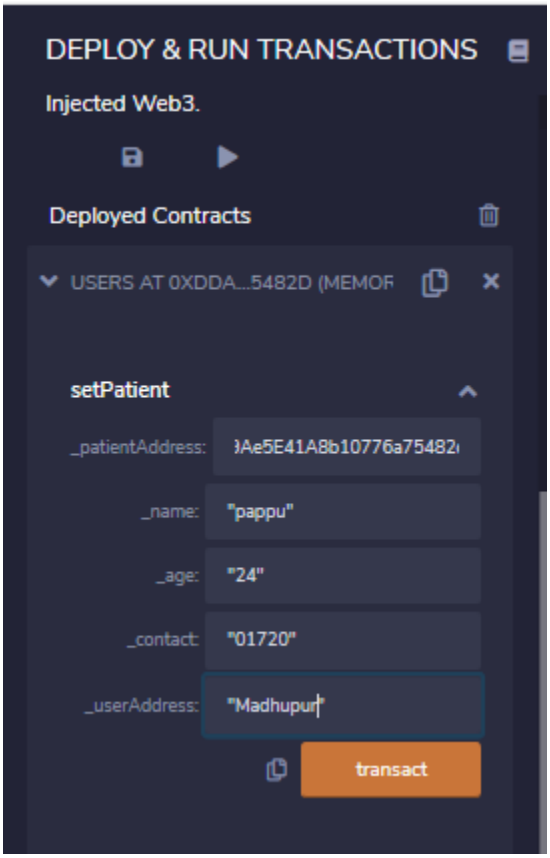


Fig: Set Patient 2

Fig: Patient Output 1

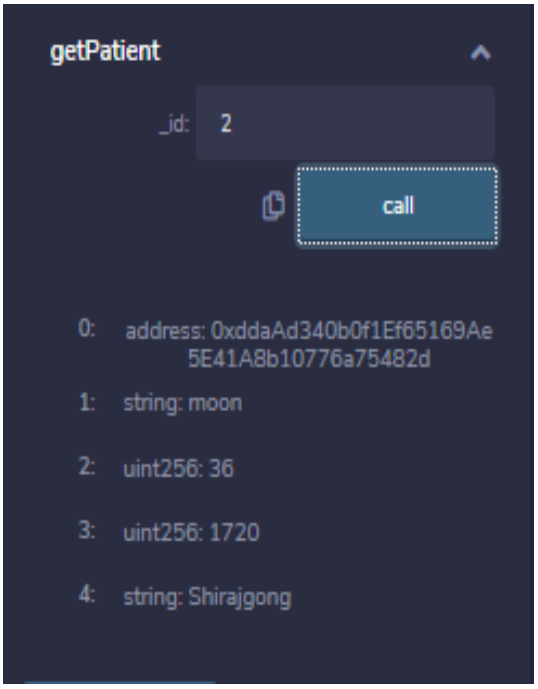


Fig: Patient Output 2

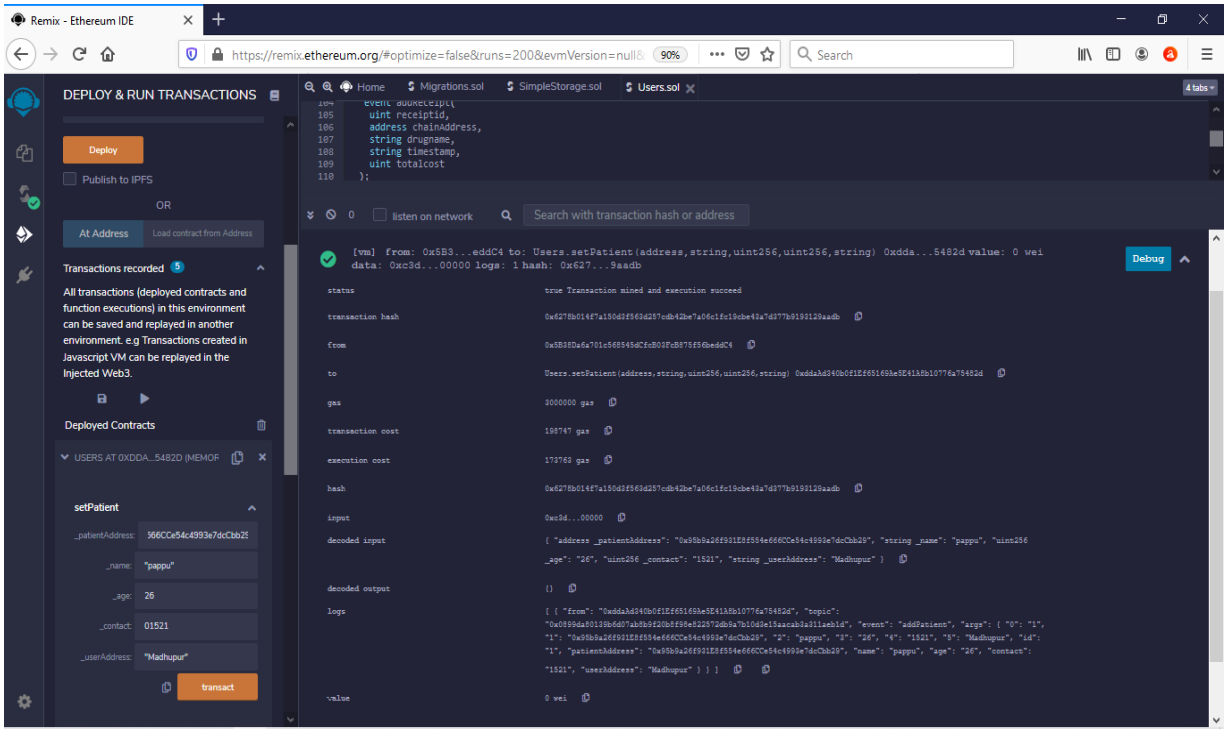


Fig 4.2.1: set & Get Patient input and Output

Set prescription input & output:

Fig 4.2.2 shows the prescription input and output in this section we set patients prescription after compiling it can shows out result.

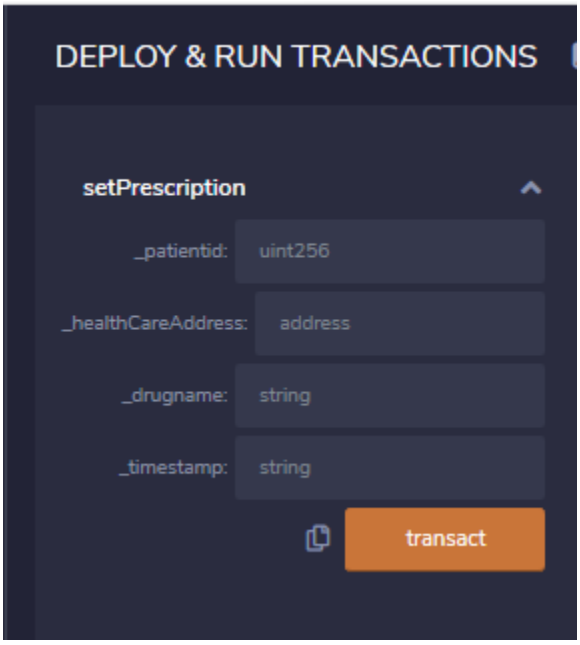


Fig: Set Prscription

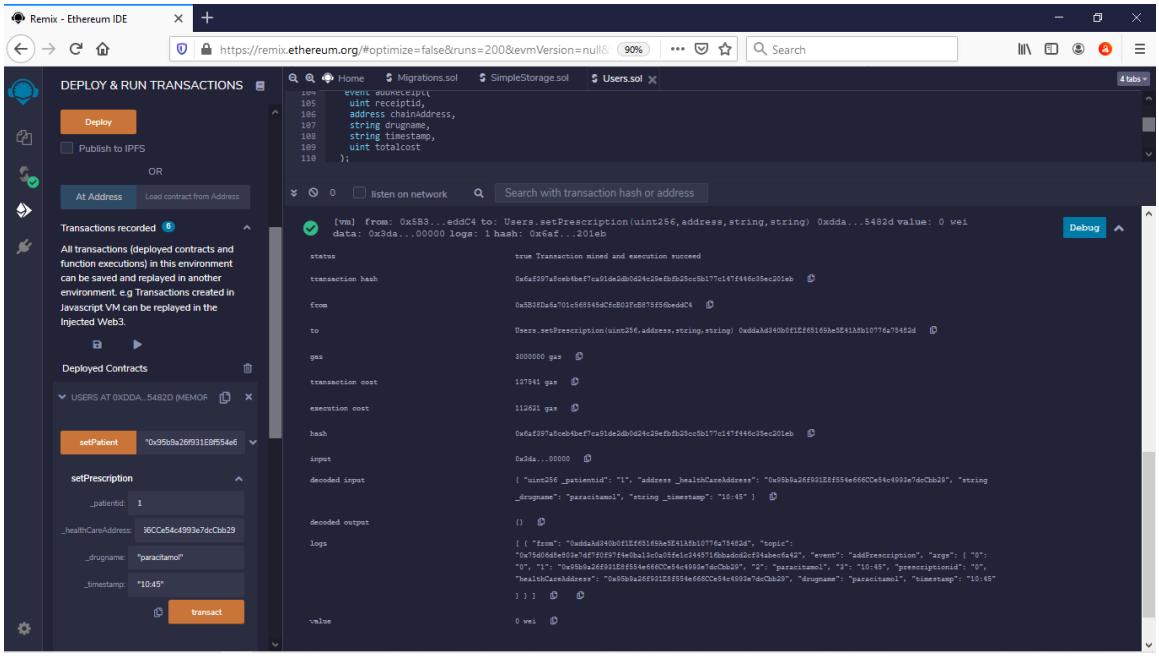


Fig 4.2.2: set prescription input and output

Set Recipt input and output:

Fig 4.2.3: shows the Set recipt input and output in this section we can set recit input and get output.

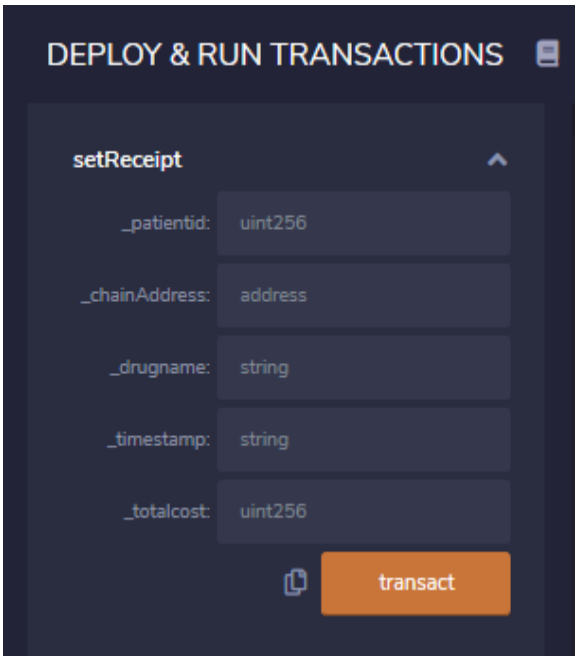


Fig: Sset Receipt

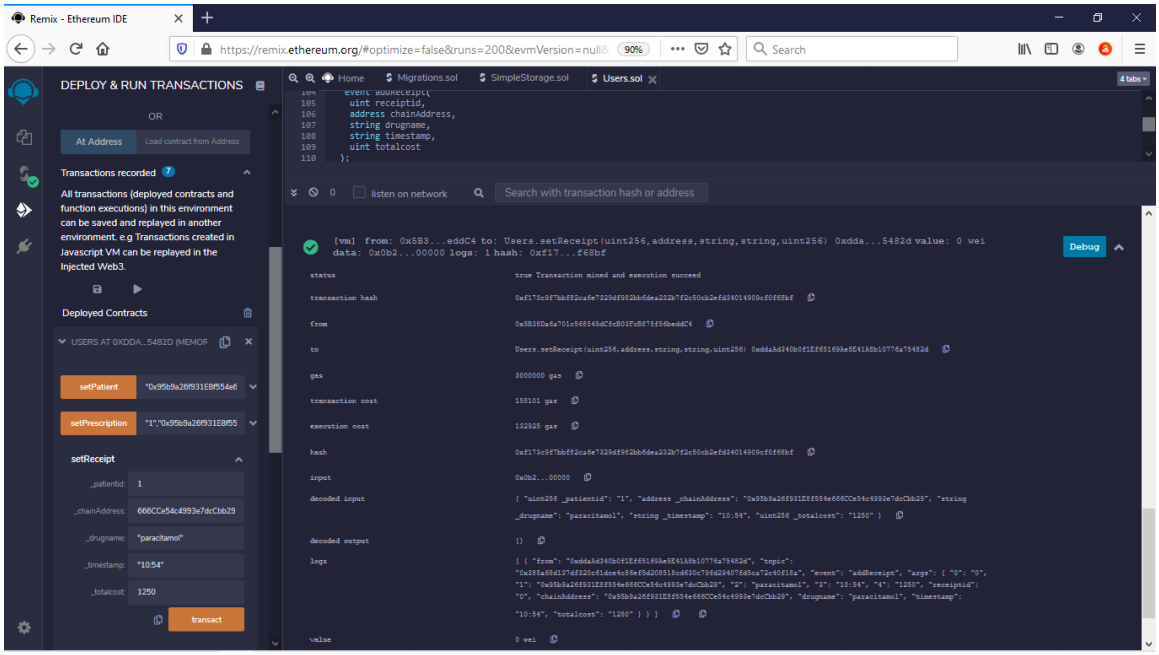


Fig 4.2.3 set recipt input and output

Set record input and output:

Fig 4.2.4 shows the set record input and output in this section we set patient records and when we press thr getbuttonit shows required pateint recipt.

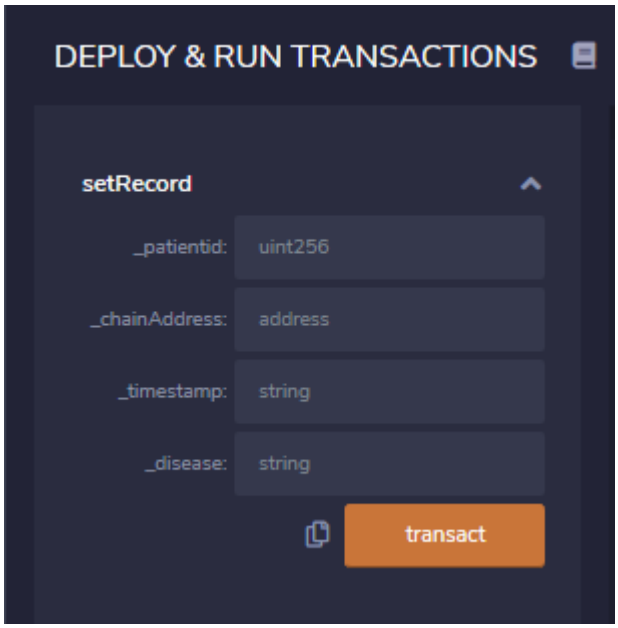


Fig:Set Record

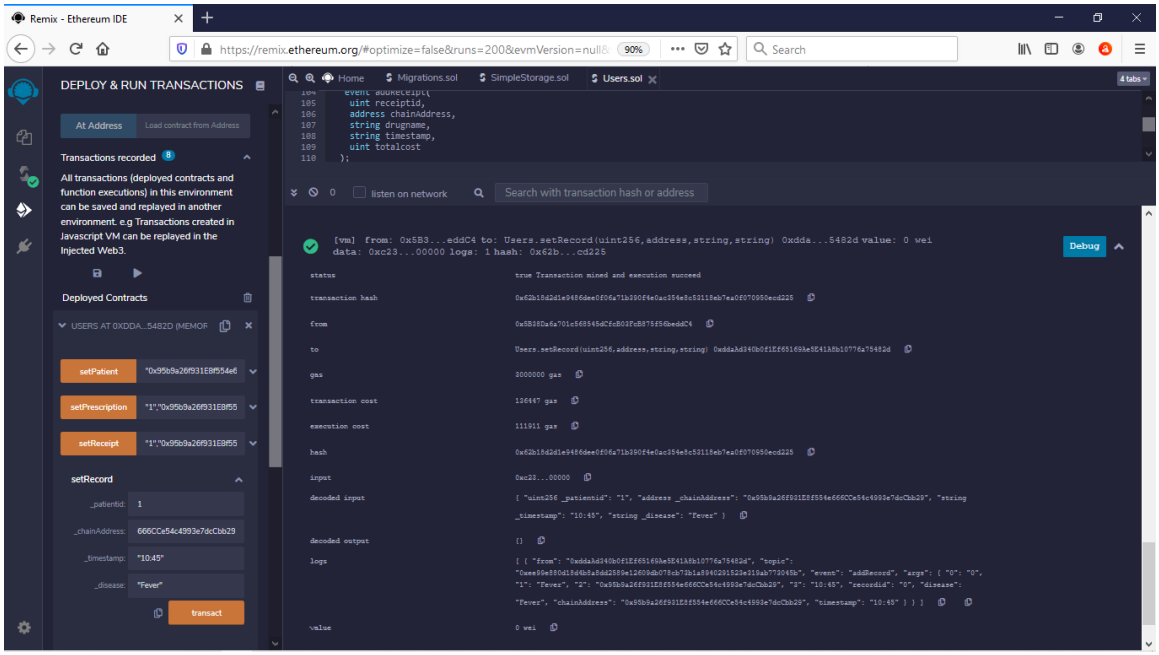


Fig 4.2.4 set record input and output

Initial and final output:

Fig 4.2.5 Shows the Initial and Final output in this section we want to show that our initial and Final output, initial output means when we just run our code and final output means when we complile our code and deploy it in Remix ID it shows the result.

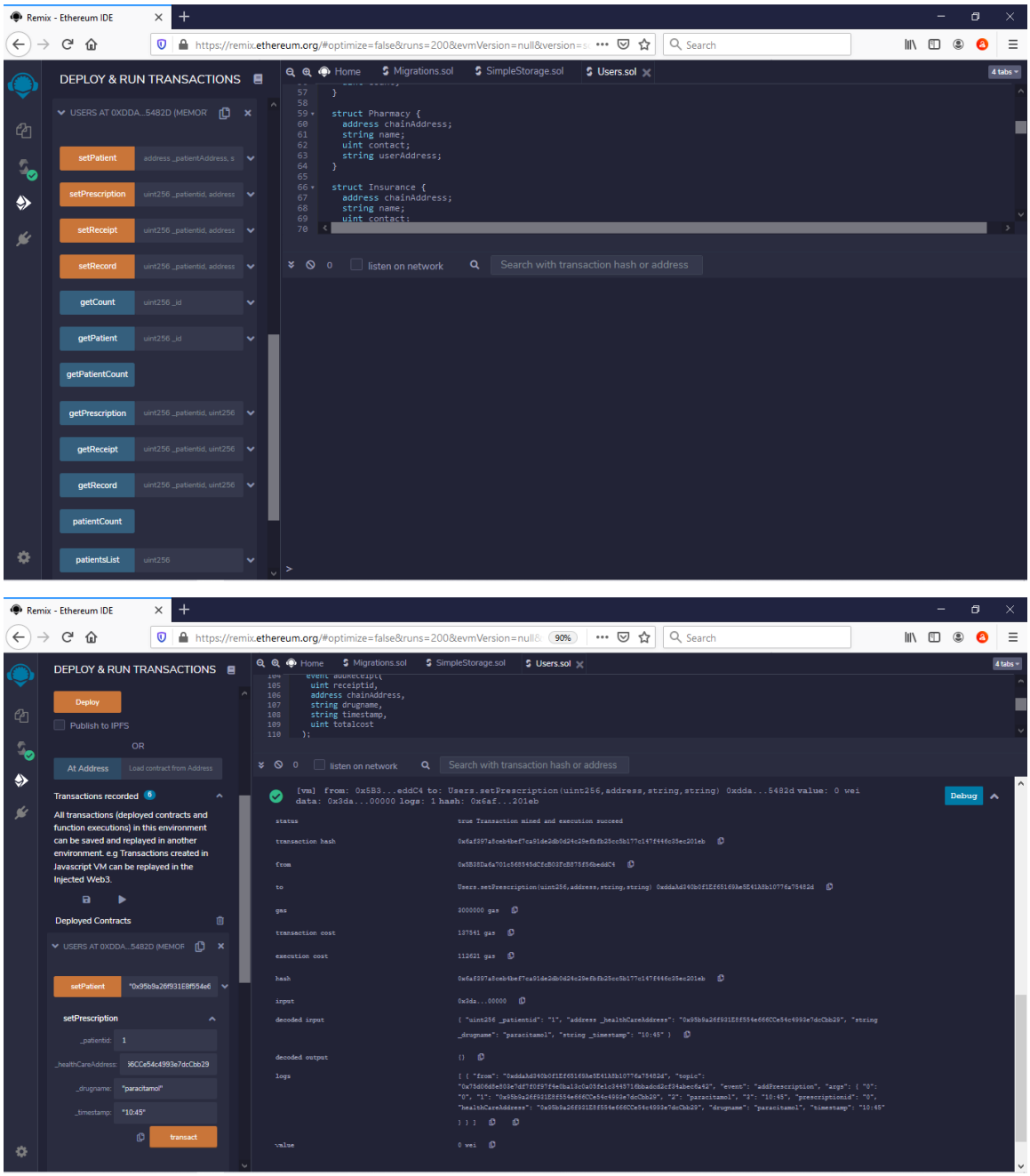


Fig 4.2.5 Initial and Final output

4.3 Discussion

In our research we want to combine blockchain and hospital management system. Our motto is to take steps unrestricted access to patient data and get around a third party not to enter it without permission. However, there are a few things we need to deal on in healthcare if we look very closely, but three of them are vital: privacy, security, and interoperability. Additionally, we highlighted how to use blockchain technology to improve patient efficiency by minimizing errors and increasing access to information on blockchains using smart resources and smart contracts. A record can be permanently altered if it is eliminated from a provider database, but from our model blockchain technological standpoint, it is impossible to erase someone's data. The safe, secure, and interchange of clinical data across healthcare organizations or research institutes is one several interoperability difficulties they face on a regular basis. In many researches has demonstrated empirically that blockchain technology is potential for resolving data interchange in the healthcare area, outbound hospitals must currently overcome various security, privacy, and control issues.

CHAPTER 5
IMPACT ON SOCIETY, ENVIRONMENT AND SUSTAINABILITY

5.1 Impact on Society

Blockchain lets you search for counterfeit drugs: With the use of blockchain technology, healthcare and drugs can be freed from counterfeit drugs. This enables for the detection of all counterfeit pharmaceuticals as well as the identification of the source of the counterfeiting.

Examine drug ingredients: The blockchain enables pharmaceutical companies to keep track of all substances used in their products. This guarantees that all of the components are in compliance with the treatment standard.

Treatment methods: The use of blockchain technology for research reasons might be beneficial. Researchers may efficiently examine the effects of a particular medication on a significant fraction of the patient population and set a standard for different diseases that will play a significant role in illness prevention thanks to lawful access to patient data.

This sort of research yields important results that enhance the treatment of a subset of patients.

Single patient identification: Patient record discrepancies and duplications are not uncommon in healthcare. Furthermore, the various schemas of different EHRs complicate the work by introducing additional methods to modify even the most basic data.

The full data set, including the blockchain, has been converted to a ledger, though. When searching for addresses, you'll come across a variety of addresses and keys; nonetheless, they'll all present a single patient who will assist you quickly identify the data.

5.2 Ethical Aspect

In our research we have strong ethical aspect because there is no scope violation. We know blockchain is the most secure platfrom on this day. We know that three things are more important in hospital management system: privacy, security, and interoperability. We assure that our proposed mode much safer and more acceptable from any other proposed

model. We are very much concern about our patient data and information cause we all know in this technology era data is more valuable thing any other things.

5.3 Sustainability plan

Our proposed model is more sustainable from compare existing model. In future if the new technology is come our model easily combine with those models from any other technology. We all know that blockchain technology too much updated technology from any other technology for that reason we can easily told that our model and blockchain technology is more efficient from any other technology.

5.4 Impact on Environment

I think in blockchain there are no impact on environment. Our proposed blockchain model also don not have any impact on environment. Blockchain basically have no impact on environment according to the study and definition.

CHAPTER 6
SUMMARY, CONCLUSION AND FUTURE WORK

6.1 Summary

The HealthCare industry is a field that provides products and services for the treatment, preventive, rehabilitation or palliative care of patients. Blockchain is a method of recording information that makes it difficult to modify, hack, or cheat a system. Blockchain technology more efficient from any other technology. A Blockchain transaction requires a digital account copied and distributed across the entire network of computer systems in the Blockchain. In this view if someone wants to temper data its look so hard because if one block is change, he needs to update all over the chain. One chain is connected to other chain. For this view we want to combine hospital management system with blockchain technology. We are partially done with our project and we will work on it in the future.

6.2 Conclusion

Nowadays, in spite of recent improvements in information technology, few health organizations provide data integration within units. An architecture proposed for health information management and secure data exchange. In our proposal, all information is owned by patients. Our primary aim of the suggested model is secure the data of the hospital. Our system work is straightforward to use and reliable. The proposed architecture is impossible to consider on technical and ethical issues. In this theme, we have talked about how latest blockchain technology can be effective in the healthcare department and how it used for EHRs (electronic health records). Our offered structure is a combination of ensure record storage with the access rules for those records. It creates a system that is easy for users to use and understand. In addition, the model suggests amounts to enable the system to deal with data storage problems while enabling the off-chain storage process. The role-based access system is also favorable as treatment records are only available to trusted and concerned individuals. For the future, we design to apply the payment option in the existing model. In this decentralized system working in blockchain, we need to consider some of it in order to decide how much it will cost to consult a patient's physician.

We need to disable some of the policies and regulations that abide by with the policies of the healthcare department.

6.2 Strengths and Limitations

The Strengths of our work are as follows:

- Why blockchain protection? Blockchain provides a secure way to manage records.
  Public Health: With the help of blockchain technology, regulatory agencies can produce take part stream of information on named patients.
- Managed Consent: Patients may particularly allow one to access their treatment data.
- Simplified Claims Processing: Blockchain technology can change composite medical charging processes by ridding of the legitimacy and continuity of working for many third-party organizations.
- Patient-generated data: Patients will be capable to easily can make upload and securely update their updated medical data without breaking any kind of previous records.

Limitations of our work are as follows:

- The current project inevitably set up on a huge scale and people need to be educated about its benefits.
- Privacy is another challenge for regulatory space due to privacy concerns.
- Trust: When calculated for each transaction, our current system still cannot detect false bills / prescriptions if issued by a credible source.

6.3 Future scope

- By cross-checking every receipt within the product serial range with mapping and listing we are able to make sure that the matter of false bills ne'er arises, notwithstanding uploaded by legitimate chemists.
- Biometric and IDs is coupled to health chains for non-stop exchange and storage of non-public info and information.
- End-to-end encoding and ability of health information publically and personal health establishments.

• Uninterrupted claims for health edges and refunds on to bank accounts with ID and health chain information

• Personalized AI help to every subject supported his or her case history. Consult supported would like predictions and treatment info.

• A slew of corking solutions is developed. Just in case of emergency, Answer} is to recover the history of the previous biometric-based treatment just in case of an accident of the victim exploitation the sole fingerprint. Etc.

A blockchain-based attention system is that they would like of the hour. Attention could be a necessity, not a luxury that ought to be for everybody, everyplace with simplicity.

References

[1] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “Continuous patient monitoring with a patient centric agent: A block architecture,” IEEE Access, vol. 6, pp. 32 700–32 726, 2018.

[2] M. A. Uddin, A. Stranieri, I. Gondal, and V. Balasubramanian, “A patient agent to manage blockchains for remote patient monitoring,” Studies in health technology and informatics, vol. 254, pp. 105–115, 2018.

[3] S. Tanwar, K. Parekh, and R. Evans, “Blockchain-based electronic healthcare record system for healthcare 4.0 applications,” Journal of Information Security and Applications, vol. 50, p. 102407, 2020.

[4] A. Ekblaw, A. Azaria, J. D. Halamka, and A. Lippman, “A case study for blockchain in healthcare: “medrec” prototype for electronic health records and medical research data,” in Proceedings of IEEE open & big data conference, vol. 13, 2016, p. 13.

[5] A. A. Siyal, A. Z. Junejo, M. Zawish, K. Ahmed, A. Khalil, and G. Soursou, “Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives,” Cryptography, vol. 3, no. 1, p. 3, 2019.

[6] P. P. Ray, D. Dash, K. Salah, and N. Kumar, “Blockchain for iot-based healthcare: Background, consensus, platforms, and use cases,” IEEE Systems Journal, 2020.

[7] C. C. Agbo, Q. H. Mahmoud, and J. M. Eklund, “Blockchain technology in healthcare: a systematic review,” in Healthcare, vol. 7, no. 2. Multidisciplinary Digital Publishing Institute, 2019, p. 56.

[8] K. N. Griggs, O. Ossipova, C. P. Kohlios, A. N. Baccarini, E. A. Howson, and T. Hayajneh, “Healthcare blockchain system using smart contracts for secure automated remote patient monitoring,” Journal of medical systems, vol. 42, no. 7, p. 130, 2018.

[9] P. A. Pavlou, “State of the information privacy literature: Where are we now and where should we go?” MIS quarterly, pp. 977–988, 2011.

[10] S. R. Reti, H. J. Feldman, S. E. Ross, and C. Safran, “Improving personal health records for patient-centered care,” Journal of the American Medical Informatics Association, vol. 17, no. 2, pp. 192–195, 2010.

[11] K. Peterson, R. Deeduvanu, P. Kanjamala, and K. Boles, “A blockchainbased approach to health information exchange networks,” in Proc. NIST Workshop Blockchain Healthcare, vol. 1, no. 1, 2016, pp. 1–10.

[12] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, “Medrec: Using blockchain for medical data access and permission management,” in 2016 2nd International Conference on Open and Big Data (OBD). IEEE, 2016, pp. 25–30.

[13] D. Vujicˇ c, D. Jagodi ´ c, and S. Rani ´ c, “Blockchain technology, bitcoin, ´ and ethereum: A brief overview,” in 2018 17th international symposium infoteh-jahorina (infoteh). IEEE, 2018, pp. 1–6.

[14] S. Wang, Y. Yuan, X. Wang, J. Li, R. Qin, and F.-Y. Wang, “An overview of smart contract: architecture, applications, and future trends,” in 2018 IEEE Intelligent Vehicles Symposium (IV). IEEE, 2018, pp. 108–113.

[15] R. Guo, H. Shi, Q. Zhao, and D. Zheng, "Secure attribute-based signature scheme with multiple authorities for blockchain in electronic health records systems," IEEE access, vol. 6, pp. 11 676–11 686, 2018.

[16] J. Bergmann, O. J. Bott, D. P. Pretschner, and R. Haux, "An e-consent based shared ehr system architecture for integrated healthcare networks," International journal of medical informatics, vol. 76, no. 2-3, pp. 130– 136, 2007.

[17] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC). IEEE, 2017, pp. 1–5.

[18] K. Bhaskaran, P. Ilfrich, D. Liffman, C. Vecchiola, P. Jayachandran, A. Kumar, F. Lim, K. Nandakumar, Z. Qin, V. Ramakrishna et al., "Double-blind consent-driven data sharing on blockchain," in 2018 IEEE International Conference on Cloud Engineering (IC2E). IEEE, 2018, pp. 385–391.

[19] C. O. Rolim, F. L. Koch, C. B. Westphall, J. Werner, A. Fracalossi, and G. S. Salvador, "A cloud computing solution for patient's data collection in health care institutions," in 2010 Second International Conference on eHealth, Telemedicine, and Social Medicine. IEEE, 2010, pp. 95–99.

[20] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control," Journal of medical systems, vol. 40, no. 10, pp. 1–8, 2016.

[21] C. Brodersen, B. Kalis, C. Leong, E. Mitchell, E. Pupo, A. Truscott, and L. Accenture, "Blockchain: Securing a new health interoperability experience," Accenture LLP, pp. 1–11, 2016.

[22] Y. Chen, S. Ding, Z. Xu, H. Zheng, and S. Yang, "Blockchain-based medical records secure storage and medical service framework," Journal of medical systems, vol. 43, no. 1, pp. 1–9, 2019.

[23] S. Jiang, J. Cao, H. Wu, Y. Yang, M. Ma, and J. He, "Blochie: a blockchain-based platform for healthcare information exchange," in 2018 ieee international conference on smart computing (smart comp). IEEE, 2018, pp. 49–56.

[24] C. Esposito, A. De Santis, G. Tortora, H. Chang, and K.-K. R. Choo, "Blockchain: A panacea for healthcare cloud-based data security and privacy?" IEEE Cloud Computing, vol. 5, no. 1, pp. 31–37, 2018.

[25] A. R. Rajput, Q. Li, and M. T. Ahvanooey, "A blockchain-based secret-data sharing framework for personal health records in emergency condition," in Healthcare, vol. 9, no. 2. Multidisciplinary Digital Publishing Institute, 2021, p. 206.

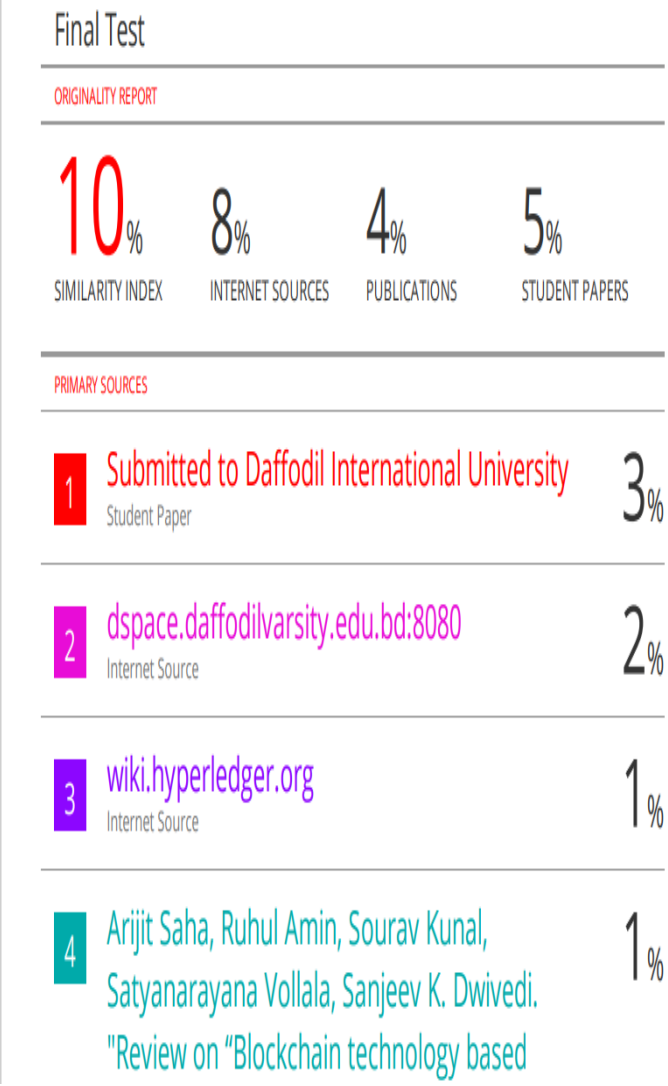
[26] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," inAMIA annual symposium proceedings, vol. 2017. American Medical Informatics Association, 2017, p. 650.

[27] A. Al Omar, M. S. Rahman, A. Basu, and S. Kiyomoto, "Medibchain: A blockchain based privacy preserving platform for healthcare data," in International conference on security, privacy and anonymity in computation, communication and storage. Springer, 2017, pp. 534– 543.

[28] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system. bitcoin. org," URL: https://bitcoin. org/bitcoin. pdf (accessed: 24.02. 2020), 2008.

[29] D. R. High, B. W. Wilkinson, T. Mattingly, R. Cantrell, V. J. J. O'Brien, B. G. McHale, J. Jurich et al., "Obtaining a medical record stored on a blockchain from a wearable device," Jun. 14 2018, us Patent App. 15/840,589.

[30] K. Fan, S. Wang, Y. Ren, H. Li, and Y. Yang, "Medblock: Efficient and secure medical data sharing via blockchain," Journal of medical systems, vol. 42, no. 8, pp. 1–11, 2018.



Final Test

ORIGINALITY REPORT

10%	8%	4%	5%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	3%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	2%
3	wiki.hyperledger.org Internet Source	1%
4	Arijit Saha, Ruhul Amin, Sourav Kunal, Satyanarayana Vollala, Sanjeev K. Dwivedi. "Review on "Blockchain technology based	1%