Major Project Report

(7th Semester)

MédicoHistory

Submitted by:

Vageesh Sharma- 19103002 **Nitin Thwass – 19103082**

Mayur Khagta- 19103041 **Tejus Kaw – 19103104**

Mentors:

Dr. Trilok Chand **Dr. Sudesh Rani**

Department of Computer Science and Engineering

Punjab Engineering College (Deemed to be University), Chandigarh

August to December 2021

DECLARATION

We hereby declare that the project work entitled “MédicoHistory” is an authentic record of our own work, carried out at Punjab Engineering College (Deemed to be University), Chandigarh as per requirements of “Major Project” for the award of degree of B.Tech. Computer Science Engineering, Punjab Engineering College (Deemed to be University), Chandigarh under the guidance of Dr. Trilok Chand and Dr. Sudesh Rani. We further declare that the information has been collected from genuine & authentic sources and we have not submitted this project report to this or any other university for the award of diploma or degree of certificate examination.

Vageesh Sharma **Mayur Khagta**

Nitin Thwass **Tejus Kaw**

Date: 20/12/2021

ACKNOWLEDGEMENT

We would like to take this opportunity to thank our college Punjab Engineering College (Deemed to be University), Chandigarh and Department of Computer Science and Engineering for giving us an opportunity to work on this project. We are immensely grateful to our project mentor Dr. Trilok Chand and Dr. Sudesh Rani (Department of Computer Science and Engineering) whose continuous guidance, technical support and moral support at times of difficulty helped us to achieve milestones in the given time. They have been a great source of knowledge and without them, this project couldnot have been made.

We convey our deep sense of gratitude to all teaching and non-teaching staff for their constant encouragement, support, and selfless help throughout the project work. It is a great pleasure to acknowledge the help and suggestion, which we received from the Department of Computer Science and Engineering.

We wish to express our profound thanks to all those who helped us in gathering information about the project. Our families too have provided moral support and encouragement at several times.

Vageesh Sharma
Mayur Khagta
Nitin Thwass
Tejus Kaw

CERTIFICATE

This is to certify that the project entitled “MédicoHistory” by Vageesh Sharma, Mayur Khagta, Nitin Thwass and Tejus Kaw is an authentic record of the work carried out under the supervision of Dr. Trilok Chand and Dr. Sudesh Rani, Computer Science and Engineering Department, Punjab Engineering College (Deemed to be University), Chandigarh in the partial fulfilment of the requirements as a part of Major Project for the award of 02 credits in semester 7 of the degree of Bachelor of Technology in Computer Science and Engineering.

I certify that the above statement made by the students is correct to the best of my knowledge andbelief.

Dr. Trilok Chand **Dr. Sudesh Rani**

ABSTRACT

For a Doctor, it is very important to know the medical history of the patient , since it could be the case that the patient having symptoms now is similar to the past, and previous diagnosis might be wrong. So, it is very important for doctors to know whether the patient is allergic to one things which might be used in an operation. Such scenarios might occur in day to day life. It is very important for the treating doctor to properly document the management of a patient under his care.

Medical record keeping has evolved into a science of itself. This will be the only way for the doctor to prove that the treatment was carried out properly. Moreover, it will also be of immense help in the scientific evaluation and review of patient management issues. Medical records form an important part of the management of a patient. It is important for the doctors and medical establishments to properly maintain the records of patients for two important reasons. The first one is that it will help them in the scientific evaluation of their patient profile, helping in analyzing the treatment results, and to plan treatment protocols. It also helps in planning governmental strategies for future medical care. But of equal importance in the present setting is in the issue of alleged medical negligence. The legal system relies mainly on documentary evidence in a situation where medical negligence is alleged by the patient or the relatives. In an accusation of negligence, this is very often the most important evidence deciding on the sentencing or acquittal of the doctor. With the increasing use of medical insurance for treatment, the insurance companies also require proper record keeping to prove the patient's demand for medical expenses. Improper record keeping can result in declining medical claims. It is disheartening to note that inspite of knowing the importance of proper record keeping it is still in a nascent stage in India.

It is wise to remember that “Poor records mean poor defense, no records mean no defense”. Medical records include a variety of documentation of patient's history, clinical findings, diagnostic test results, preoperative care, operation notes, post operative care, and daily notes of

a patient's progress and medications. A properly obtained consent will go a long way in proving that the procedures were conducted with the concurrence of the patient. A properly written operative note can protect a surgeon in case of alleged negligence due to operative complications. It is important that the prescription for drugs should be legible with the name of the patient, date, and the signature of the doctor. An undated prescription can land a doctor in trouble if the patient misuses it.

There are also many records that are indirectly related to patient management such as accounts records, service records of the staff, and administrative records, which are also useful as evidences for litigation purposes. Medical recording needs the concerted effort of a number of people involved in patient care. The doctor is the prime person who has to oversee this process and is primarily responsible for history, physical examination, treatment plans, operative records, consent forms, medications used, referral papers, discharge records, and medical certificates. There should be proper recording of nursing care, laboratory data, reports of diagnostic evaluations, pharmacy records, and billing processes.

This means that the paramedical and nursing staff also should be trained in proper maintenance of patient records. The medical scene in India extends from smaller clinics to large hospitals. Medical record keeping is a specialized area in bigger teaching and corporate hospitals with separate medical records officers handling these issues. However, it is yet to develop into a proper process in the large number of smaller clinics and hospitals that cater to a large section of the people in India.

CONTENTS

Table of Figures

CHAPTER 1

INTRODUCTION

Confidentiality of Medical Records

Medical records can be used as a personal or impersonal document.

Personal document - This information is confidential and should not be released without the consent of the patient except in some specific situations.

Impersonal document – The record loses its identity as a personal document and patient permission is not required. These records could be used for research purposes. Confidentiality is an important component of the rights of the patient. The hospital is legally bound to maintain the confidentiality of the personal medical records. The patient can claim negligence against the hospital or the doctor for a breach of confidentiality. However, there are certain situations where it is legal for the authorities to give patient information.

The impersonal documents have been used for research purposes as the identity of the patient is not revealed. Though the identity of the patient is not revealed, the research team is privy to patient records and a cause of concern about the confidentiality of information. Historically, such research has been exempt from an ethics review and researchers have not been required to obtain informed consent from patients before using their records. Recently, a need has been felt to regulate the use of medical records in research, effectively restricting the manner in which this type of research is conducted. An ethics review is required for using the patient data. However this is not widely followed all over India.

Problems with existing electronic medical records (EMRs)

Most of us remember going to the doctors and seeing them pull out a dreary-looking folder with our name written on the front. If you had found yourself going to the doctors quite frequently, your folder will probably have been loaded with different pieces of paper making it look scarily full.

When I was young, I remember walking past this immense collection of files as I made my way to see the doctor and thinking two things.

How do they find my small file in such a huge amount of folders that all look the same?

What would happen if there was a fire or an accident where all these records got destroyed?

The second thought scared me a little. Would this mean that I would have to have all those horrible injections again because they weren‘t sure what I had already had and what I hadn‘t? Clearly, these kinds of thoughts had not escaped governments either. The advent of the personal computer saw governments around the world determined to create electronic medical records to replace all of our dusty old paper records.

The Failed Promise Of Universal Electronic Medical Records

In the early 2000s, tech experts everywhere were making incredibly optimistic predictions about how electronic medical records were set to save the healthcare industry enormous amounts of time and money.

RAND Corp predicted in 2005 that the adoption of EMRs “could eventually save more than $81 billion annually.” Just over a decade later and the promise of universal EMRs, and the savings they promised, have still failed to materialize.

But what were the reasons behind this? After all, any computerized record has to be better than the paper version, right?

There were a few fundamental reasons why the attempt to create universal electronic records failed.

System/Program Compatibility – The biggest problem in developing a universal electronic medical record is overcoming system compatibility issues.

Poor User Experience – Badly designed user interfaces and poor workflows have led to a deep sense of frustration among doctors. Whereas with a paper form, doctors could quickly jump to any relevant section, with a computerized form they are often forced to waste valuable time trying to skip through pages until they get to the one they want.

Data Entry is often time-consuming – A large numbers of doctors find data entry very laborious. This is one of the main negatives doctors cite when asked about their experience using EMRs.

Overcomplicated – Many EMR programs feature such things as alert alarms or reminders. While these are built-in to try to prevent doctors from overlooking important problems, they are considered an unwanted nuisance by many.

A universal solution for individual problems – Doctors also dislike EMRs because they often lack the necessary electronic health information or pages to input important data.

In the past, doctors could simply include a note or fax a report to the relevant department in a matter of seconds.

The chart above shows just how widespread dissatisfaction with EMRs has become. It is important not to underestimate the seriousness of this problem. A single oversight or mistake by a doctor could result in death.

It is for this reason that EMRs should decrease workload as well as make life easier for the doctors who rely on them.

Blockchain For Medical Records Security

So, how can blockchain ensure medical records security and succeed when other systems have already failed?

Securing medical records with blockchain would allow for the first viable universal electronic medical records. I‘m aware that many people will remember reading the same kind of statement back in the early 2000s, but this time there is a difference.[1]

Up until now, conventional electronic medical records databases were not able to offer the all-important medical records security that would allow them to have physical access control anywhere, anytime, and on any system. Overcoming compatibility issues between different software applications was just one of the problems.

The next question became who would store these records and ultimately be responsible for them should there be a data breach that demanded some accountability.

Fortune recently published an article that stated "Hackers Don't Want Your Credit Card. They Want Your Medical Records."

The article quoted Roy Schoenberg, CEO of American Well Corp, as saying that "when considering online privacy and data security our chief concerns are often financial records, credit card numbers, and bank account details. But it might be surprising to learn how little value those actually hold to hackers: anywhere from ten cents to a couple of dollars". However,"medical records can sell for up to $30 each."

Medical records security is too much of a risk

The statement above shows just how much is at stake when it comes to our medical records. Health companies risk massive financial losses should they not adequately protect our data. In 2017, there were 477 separate breaches that resulted in 5.6 million patient records being compromised.

In some cases, cyber attackers demanded ransoms to be paid as part of a ransomware attack, while the failure to report a breach within 60-days led to other organizations receiving hefty fines.

It is for this reason that healthcare providers are so reluctant to try out new systems or to allow other healthcare providers access to their records.

Electronic health record systems blockchain solution

Advantages

The solution is to use blockchain for medical records security, but many physicians are left wondering – how can blockchain keep medical records secure.

Blockchain technology would prevent the majority of the 477 separate breaches that took place in the last years from ever happening. Any attack that exploited the single point of failure weakness of the traditional client-server model has would be useless against a blockchain database.

Since blockchain technology relies on a distributed network there is no one point of failure. This means that it is not possible for hackers to simply find an electronic health record security flaw and then gain access to the data in this way.

Should a hacker target any one node on the blockchain network and attempt to make an unauthorized change then the other nodes will prevent it from happening.

As each participant on the network has a complete copy of the entire blockchain ledger, they are able to independently verify any new block being added and identify any attempt to alter any previous block.

Blockchains are designed to be unalterable once written unless the change has the support of 51% of the network. This makes them excellent for storing patient medical records as it means any data in the record cannot be tampered with.

As every new data block that is added would also contain details of the doctor who added it, blockchain EMRs would offer full accountability for the data that they contain.

In the case of incorrect diagnoses, for example, patients could be confident that there is no way that records could be altered should the doctor or healthcare provider wish to deny accountability.

Universal Access

The fact that it is possible to encrypt data stored on a blockchain means that it is possible to keep sensitive patient data on these distributed networks without the risk of unauthorized access. Creating a non-centralized EMR blockchain would mean that it is possible for any authorized healthcare provider to access patient information.

Since no one healthcare provider would be liable for any data breach when using such a database, there need not be any resistance to making records universally available. As long as a provider has software that is compatible with the data to the blockchain then they will be able to access it.

All that would be required is for a patient to authorize access to their protected health information, possible through a secure blockchain-based ID verification solution like Sovrin. After this, the doctor would have full access to their records and would, therefore, be able to treat the patient.

Aside from allowing lifesaving care by emergency services to be improved, such universal access to personal health information also promises to save healthcare providers huge sums of money from lower administration costs relating to the upkeep and transfer of records as well as from reduced liability from data breaches, etc.

Summary of potential advantages to blockchain EMR

- Universal Access
- Real-Time Up-To-Date records
- Reduced Costs
- Better Security
- Automation through the use of Smart Contracts
- Health insurance portability

Health care organizations no longer need to keep large amounts of records on theirsystem

All these points provide an answer to the question How can blockchain keep medical records secure?

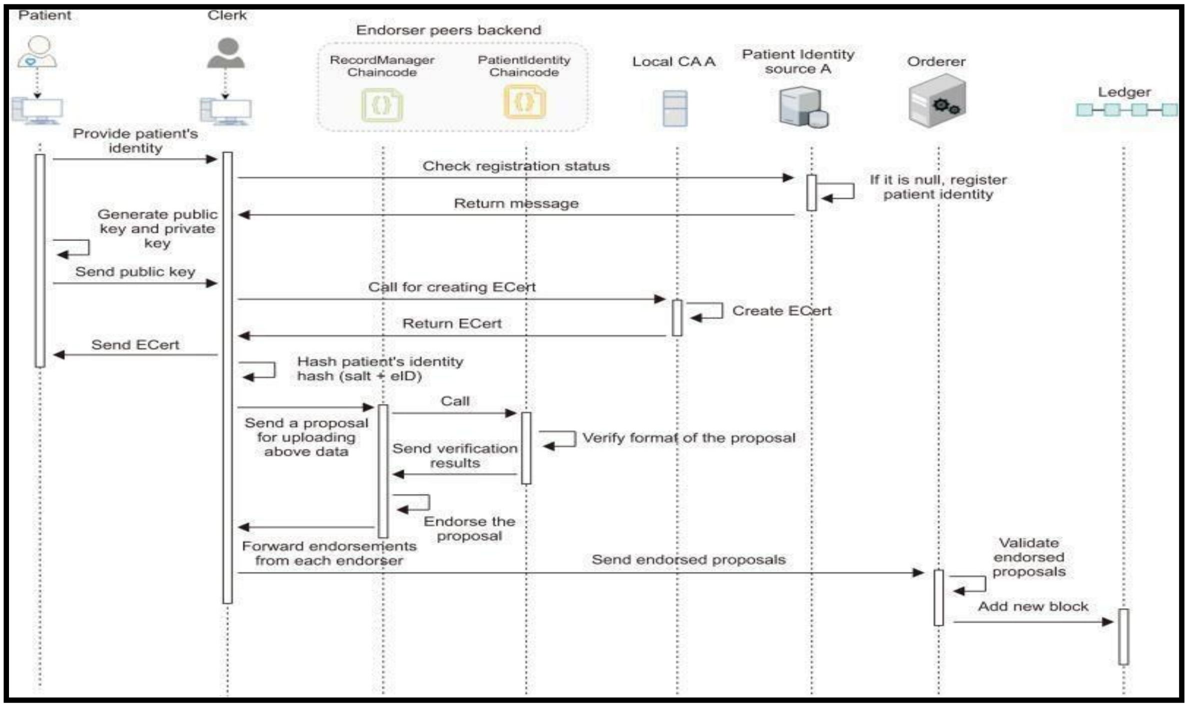

Patient
Clerk
Endorser peers backend
RecordManager Chaincode
PatientIdentity Chaincode
Local CA A
Patient Identity source A
Orderer
Ledger
Provide patient's identity
Check registration status
If it is null, register patient identity
Return message
Generate public key and private key
Send public key
Call for creating ECert
Create ECert
Return ECert
Send ECert
Hash patient's identity hash (salt + eID)
Call
Send a proposal for uploading above data
Verify format of the proposal
Send verification results
Endorse the proposal
Forward endorsements from each endorser
Send endorsed proposals
Validate endorsed proposals
Add new block

Figure 1Activity Diagram of Health Chain using Blockchain

CHAPTER 2

BACKGROUND

Problem Description

There are various projects already using the blockchain to implement the storing of data and retrieving it but can that be really used directly in the real world?

No.

We cannot use this model in day to day life roles because with the advantage of its secureness, their is a disadvantage of blockchain technology i.e. it is slow.

In this research project, our aim is to make this technology fast so that no matter what this technology can be used in other places as well with a better speed.

Slow Blockchain

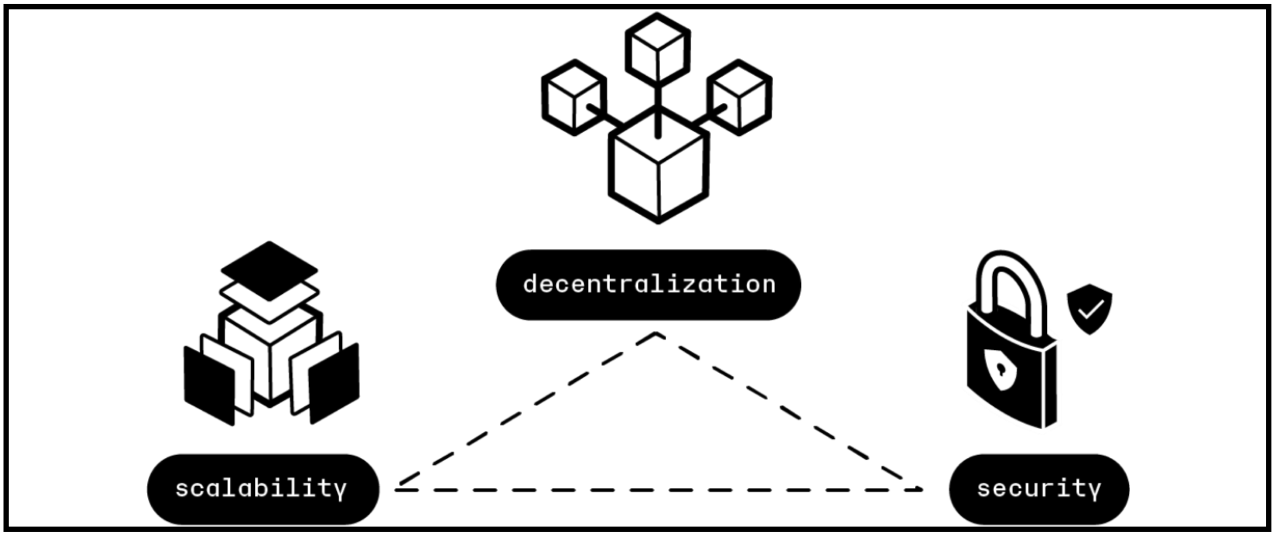


Figure 2 Blockchain Trilemma

Security. Decentralization. Scalability. Three of cryptocurrency's pillars that all seem to constantly strive to co-exist but struggle to live in harmony.

The blockchain trilemma, as coined by **Vitalik Buterin** himself, refers to this idea and it's leading to some interesting ways that projects and networks are looking to solve the problem once and for all. But what exactly is the blockchain trilemma, and why isn't there an easy solution? Let's get into it!

The Three fighting factors

You know how you can’t balance a social life, work, and sleep easily? The blockchain trilemma is similar. It’s the belief held across the cryptocurrency community that truly decentralized networks need to choose between security and scalability. Let’s have a quick look at them before we dive in.

What is decentralization?

Decentralization talks about how control is shifted from one central entity, company, or government and is split across smaller groups to govern something. In blockchain, decentralization gives power to people across the world to govern using their computer (nodes) rather than having a central control of the network live with one person or party.

What is security on the blockchain?

Blockchain is inherently secure, but is not entirely immune to hacking. If a hacker is able to secure control of more than half of the network (51%), they are able to alter a blockchain and manipulate transactions to steal from the network. In blockchain, the more nodes, the more security.

What is scalability?

Scalability in blockchain is the same as in business – it refers to how much a network can grow in the future while maintaining the same sort of transaction speed and output.

Scalability and decentralization tag-teaming up tends to compromise security, while security restricts changes that allow the decentralized network to scale. Why? Well, basically because decentralized networks take a bit of work to operate and it makes scaling a little difficult.

Decentralization is basically the backbone of blockchain and cryptocurrency. It means there is no central authority or entity driving the project and eliminates the need for third parties to allow industries to operate. For example, in traditional finance, we’ve got banks. They’re centralized and act as a party that sits in the middle between you and your money. This is generally accepted because banks take responsibility to offer a way for us to store and send money safely – we expect money to go where we send it and in exchange for security we give some control of our money.

With blockchain, decentralized networks hand the keys to the individual, with direct access to their money.

It does this by making use of community control and relies on blockchain technology rather than the corporation. Blockchain, by means of a set of self-executing rules, offers an alternative to a middleman approach. The network keeps its security because each transaction needs to be validated by more than half of the network's nodes (and remember: the more nodes that are part of the network, the more the blockchain becomes decentralized, enhancing the security that the network offers.

This is great because no one is in control, but it comes with a bit of a tricky drawback: because of the sheer weight of information processed to maintain the shared system, transaction times can be slow, and the system is harder to scale.

Blockchain scalability is arguably the holy grail and bottleneck of the cryptocurrency world and mainly refers to transaction speed. At the moment, the transaction time of crypto doesn't compare to other payment methods. However, crypto communities are working within different theories on how best to overcome this hurdle, and in this piece, we dive deep into the promising developments that might finally get us to near-instant transaction speed[2].

But first let's dive into the basics of what transaction speed is before we look into different scalability solutions to speed things up.

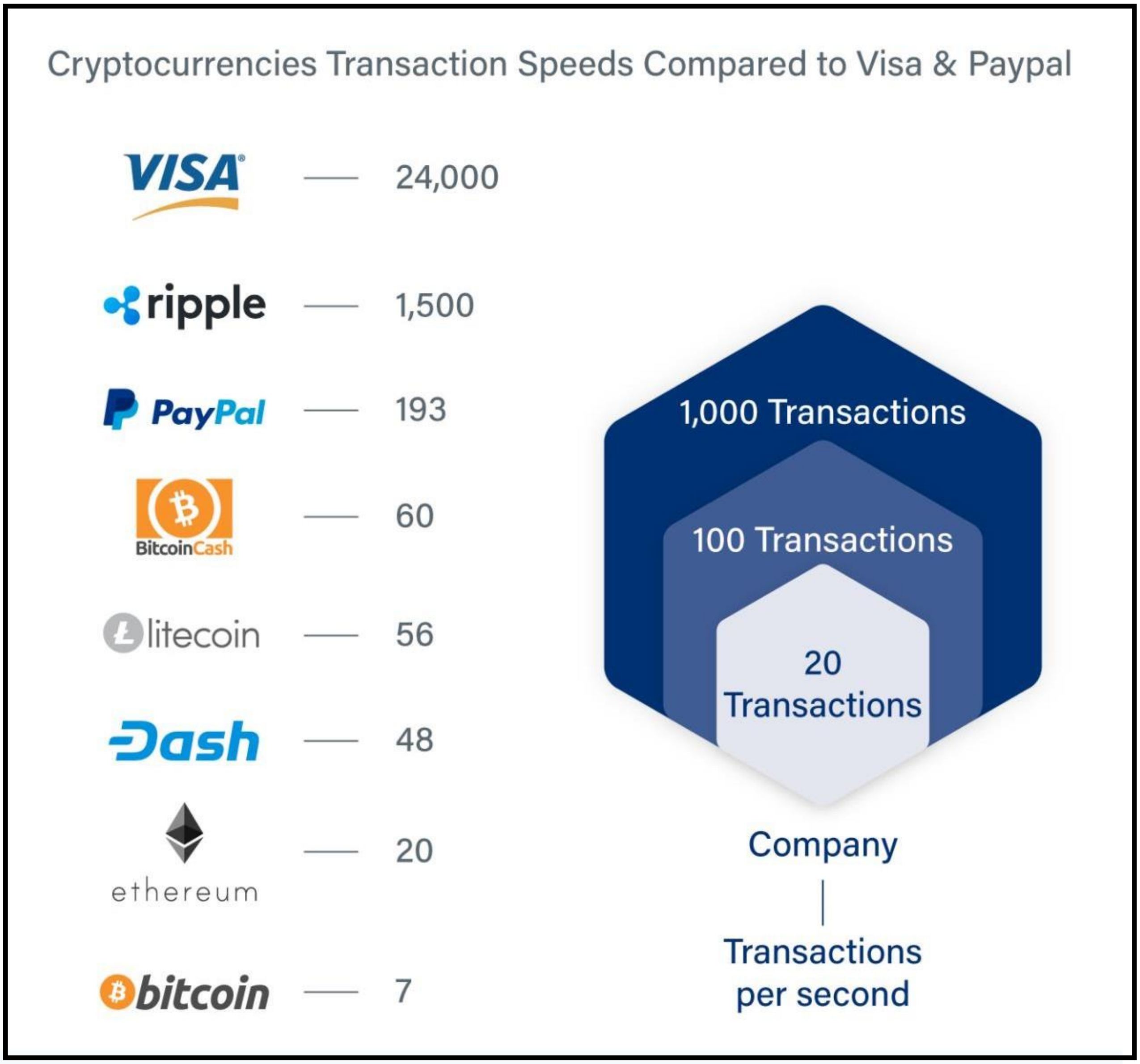


Figure 3 Transaction Speed of CryptoCurrencies vs VISA and Paypal

The Bottlenecks - Throughput, Finality, and Confirmation Time

How is transaction per second related to processing speed? What exactly does it mean when people ask if cryptocurrency is scalable? To answer those, we need first to understand the concept of throughput, finality, and confirmation time.

Consider this story:

"'You are waiting for a bus at a bus station to go home. The bus arrives at a 10 minute interval,

and it takes 60 minutes for the bus to arrive at your destination. The route is popular, and there is always a long queue of people waiting for the bus.

Two minutes have passed, and the bus has arrived, but there are too many people ahead of you in the queue and the bus is filled. You now need to wait for another 10 minutes before you can begin your journey home.'"

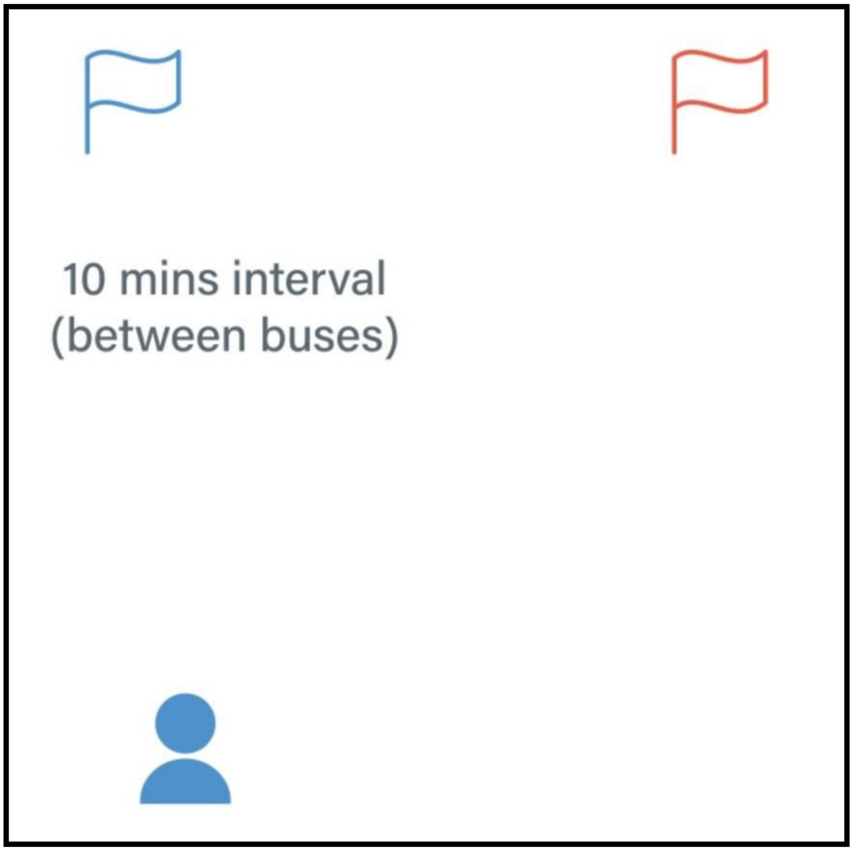
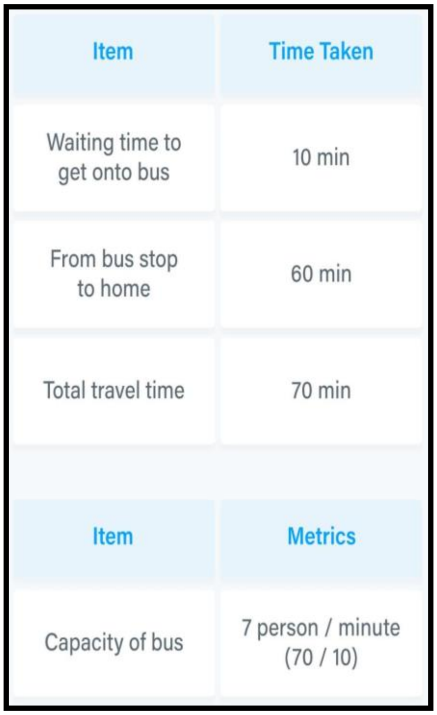


Figure 4 Throughput Example

The journey can be summarised like this:



Item	Time Taken
Waiting time to get onto bus	10 min
From bus stop to home	60 min
Total travel time	70 min

Item	Metrics
Capacity of bus	7 person / minute (70 / 10)

Figure 5 Summary of Journey

Using the concepts demonstrated above in the context of throughput, finality, andconfirmation:

Capacity of bus (7 person/minute) = throughput

Travel time from the bus stop to home (60 min) = finality

Waiting to get on the bus (10 min) = average first block waiting time

Total travel time (70 min) = Confirmation timeIt should be noted that:

Measuring throughput (tps) is not enough – we must also consider confirmation time. Simply put, a protocol that can process up to 100,000 tps is great, but if it has a two day confirmation time, that is not sufficient for daily life usage.

When there is network congestion, throughput won't decrease (since the bus can still carry seven passengers per minute), but the confirmation time will deteriorate because of the longer average first block waiting time.

Finality is a fixed waiting time. We need to wait for the "6 blocks confirmation" to ensure that the block is not reversible. The average first block waiting time varies depending on the situation.

The Blockchain Scalability Trilemma

The blockchain scalability trilemma is one of the greatest hurdles for cryptocurrencies. It states that you can only achieve two out of either decentralisation, scalability, or security simultaneously, but never all three. Therefore trade-offs are inevitable. The trilemma was originally coined by Vitalik Buterin, the founder of Ethereum (ETH), who invented the name regarding the scalability of blockchain technology.[3]

However, we would like readers to remember that the scalability trilemma is only an observation instead of a formal mathematical proof. Despite how difficult it is, an algorithm may exist that can solve the trilemma unless someone has proven that it is impossible. We will cover some recent directions on how people in the space are attempting in later sections of thisarticle series.

Decentralisation

Decentralisation refers to the degree of diversification in ownership, influence and value on a blockchain. Cryptocurrencies are generally ‘decentralised since no single party can govern the whole network. However, decentralisation is a spectrum rather than a binary ‘yes or no’, as we see different levels of decentralisation in various projects like Bitcoin, Ethereum, Ripple, EOS, etc.

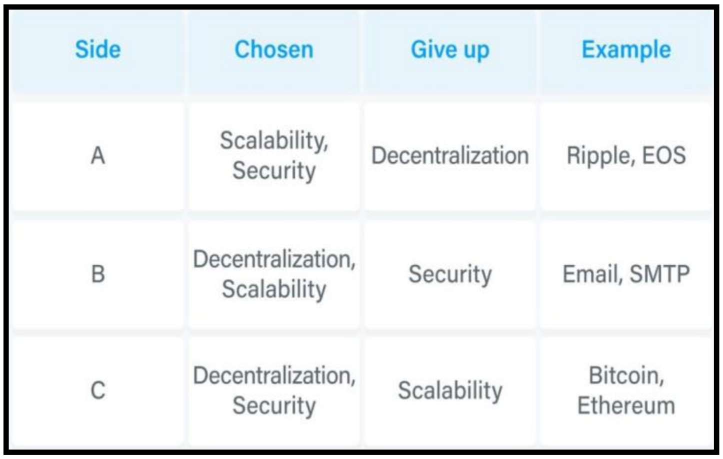
Security

Security is the level of defensibility blockchain has against attacks from external sources and the resistance of the system to tampering. There are many attack vectors in a blockchain system, including double-spending, sybil, DDoS, and 51% attacks. In general, more freedom (i.e. free entrance/exit of the network) results in higher decentralisation but lower security since it is hard to verify the identity of the new participants where they can be owned by a single malicious entity or collude together to cause harm to the network.

Scalability

Scalability determines the network's capacity, including the number of nodes in the network, the number of transactions that the network can process, how fast the network can process and so on. The term scalability is sometimes confusing because Bitcoin's blockchain is scalable upon new participants joining the network. The PoW system will automatically adjust the difficulty, and the network can tolerate any number of nodes that exist in the network.

The common saying that "Bitcoin is not scalable" is mainly focused on its throughput, i.e. it can only handle seven transactions per second (tps) which is not enough for real-life usage (when compared to VISA, which can reportedly reach 24,000 tps). The finality speed is also another-issue as people won't wait for 60 minutes to confirm that a purchase of a coffee is valid.



Side	Chosen	Give up	Example
A	Scalability, Security	Decentralization	Ripple, EOS
B	Decentralization, Scalability	Security	Email, SMTP
C	Decentralization, Security	Scalability	Bitcoin, Ethereum

Figure 6 Three Sides of BlockChain Trilemma

CHAPTER 3

PROPOSED WORK

Architecture

Analogy

After getting to know about blockchain trilemma , we know that if we try to increase the scalability of our blockchain then it will lead to less secure transactions or no decentralization. Our Aim is to get all three at a same time.

Our idea has an analogy with the Operating system.

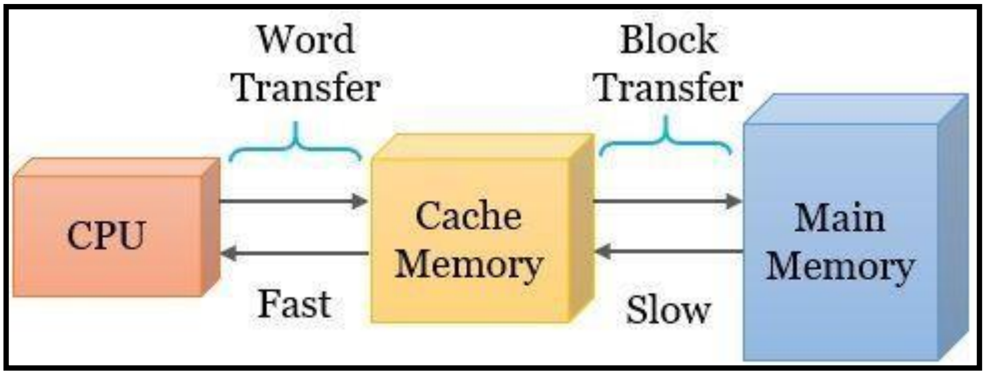


Figure 7 Concept of Virtual Memory in OS

Here we see that since there is a speed gap between the CPU and main memory, we use cache to make the system overall fast thus matching with the CPU. Using the same analogy, here we are CPU and main memory is Blockchain and in between we can use cache and Database.

Inserting Data to Blockchain

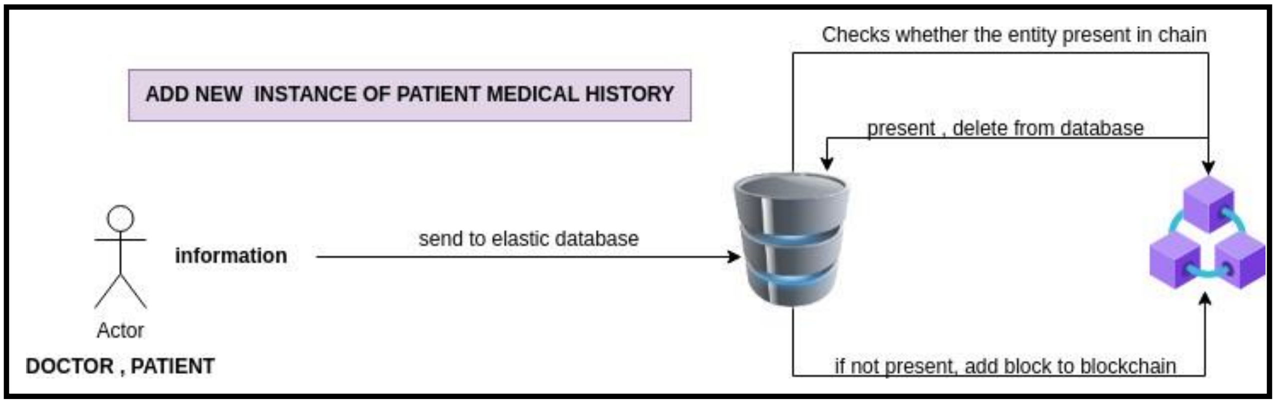

Checks whether the entity present in chain
ADD NEW INSTANCE OF PATIENT MEDICAL HISTORY
present , delete from database
information
send to elastic database
Actor
DOCTOR , PATIENT
if not present, add block to blockchain

Figure 8 Data Insertion Architecture

Here we can see that if a user wants to add the info to blockchain, we can first send it to elastic search and then the elastic search queries the blockchain, check whether the same data is already present in the blockchain or not , if not , then we can add it to blockchain at the backend. But for the front user, task is already done no matter, the task is still in progress in backend.

Fetching of Data from Blockchain

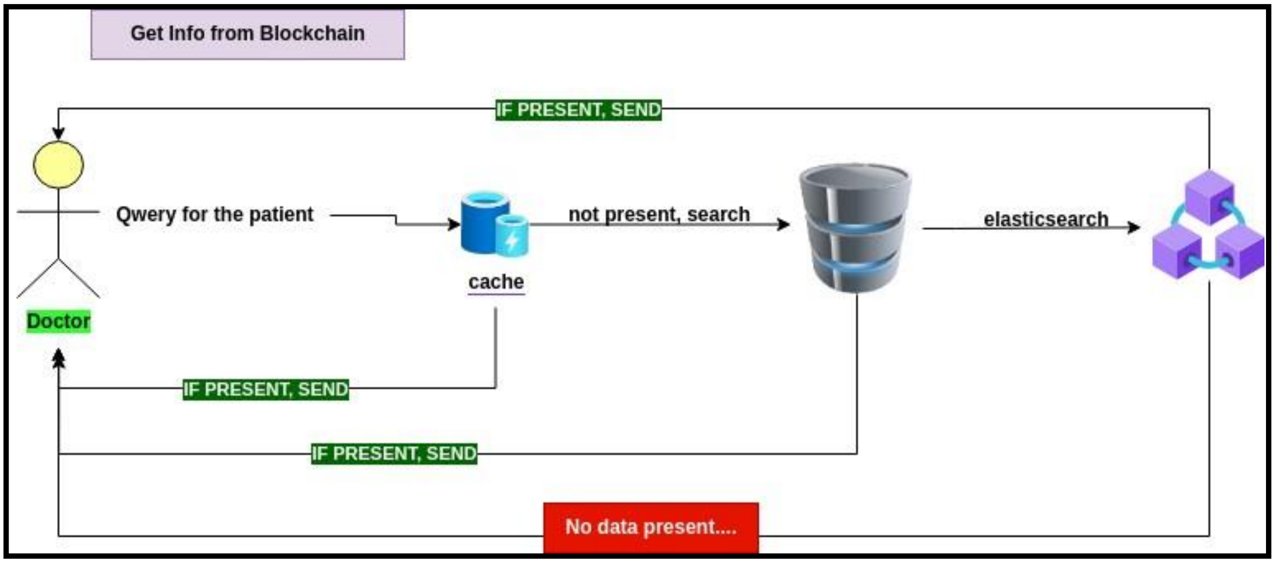


Figure 9 Data Fetching Architecture

In querying the data for history of a patient, we can first check the data in cache, if it is present, we can give it to the user, otherwise check in database means the this data is yet to be added in blockchain, we can give the data to the user and at last,if the data is not present in the database also , we can search the data in blockchain with the help of some query finder since finding the data in blockchain with a for loop can be a lot of time taking task.

So here we are going to take the help of elastic search which can retrieve the data from the blockchain as well as from the database very fast.

Blockchain Merkle Tree

What is Merkle Tree ?

Merkle tree is a fundamental part of blockchain technology. It is a mathematical data structure composed of hashes of different blocks of data, and which serves as a summary of all the transactions in a block. It also allows for efficient and secure verification of content in a large body of data. It also helps to verify the consistency and content of the data. Both Bitcoin and Ethereum use Merkle Trees structure.

A hash tree, also known as a Merkle tree, is a tree in which each leaf node is labeled with the cryptographic hash of a data block, and each non-leaf node is labeled with the cryptographic hash of its child nodes' labels. The majority of hash tree implementations are binary (each node has two child nodes), but they can also have many more child nodes.

But what actually is the Merkle tree in Blockchain, and how it is used in Blockchain? So, if you want to know the answer to all these questions, then you are in the right place.

Merkle trees, also known as Binary hash trees, are a prevalent sort of data structure in computer science.

In bitcoin and other cryptocurrencies, they're used to encrypt blockchain data more efficiently and securely.

It's a mathematical data structure made up of hashes of various data blocks that summarize all the transactions in a block.

It also enables quick and secure content verification across big datasets and verifies the consistency and content of the data.

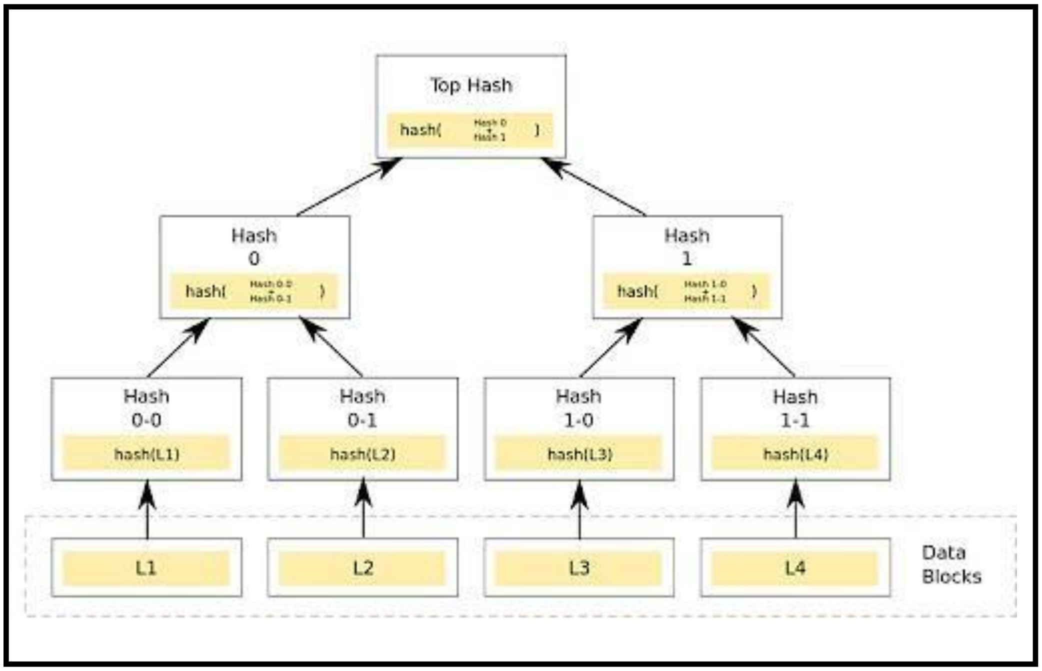


Figure 10 Merkel Tree

What Is a Merkle Root?

A Merkle root is a simple mathematical method for confirming the facts on a Merkletree. They're used in cryptocurrency to ensure that data blocks sent through a peer-to-peer network are whole, undamaged, and unaltered.

They play a very crucial role in the computation required to keep cryptocurrencies like bitcoin and ether running.

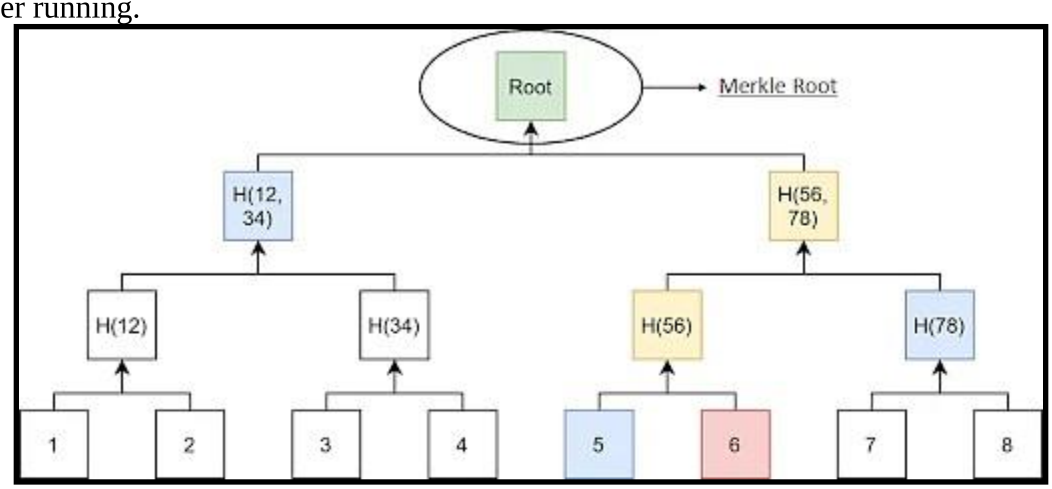


Figure 11 Merkle Root

Cryptographic Hash Functions

A hash function maps any type of arbitrary data of any length to a fixed-size output. It is commonly used in cryptography since it is a cryptographic function.

They are efficient and are well-known for one property: they are irreversible. It's a one- way function that's only meant to work in one direction.

Some of the Hash families available are Message Direct (MD), Secure Hash Function (SHF), and RIPE Message Direct (RIPEMD).

Now, take an example, if you use the SHA256 hash algorithm [6]and pass 101Blockchains asinput, you will get the following output

fbffd63a60374a31aa9811cbc80b577e23925a5874e86a17f712bab874f33ac9

In conclusion, these are the following key properties of the hash function:

- Deterministic
- Pre-Image Resistant
- Computationally Efficient
- Cannot be Reversed Engineered
- Collision Resistant

Working of Merkle Trees

A Merkle tree totals all transactions in a block and generates a digital fingerprint of the entire set of operations, allowing the user to verify whether it includes a transaction in the block.

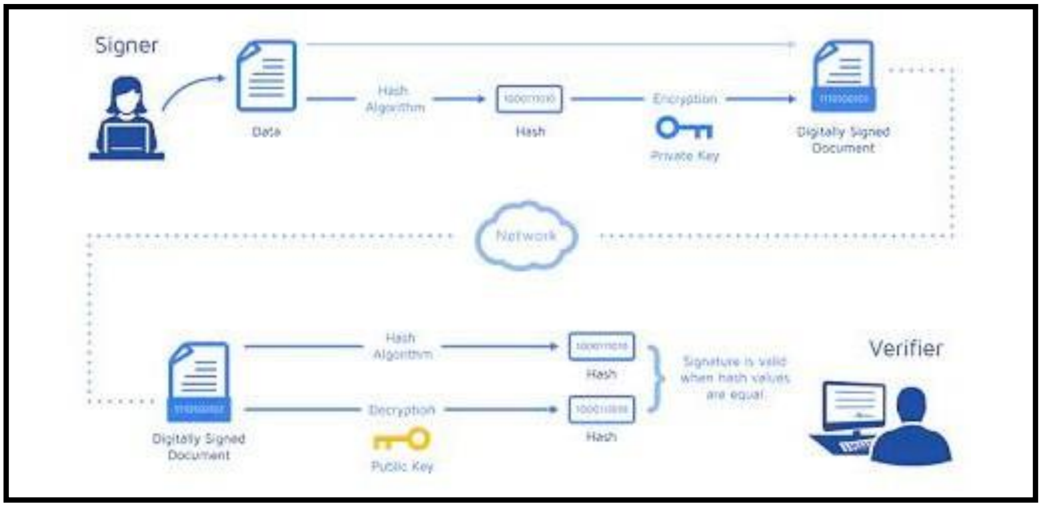


Figure 12 Working Architecture of Merkle Tree

Merkle trees are made by hashing pairs of nodes repeatedly until only one hash remains; this hash is known as the Merkle Root or the Root Hash.

They're built from the bottom, using Transaction IDs, which are hashes of individual transactions.

Each non-leaf node is a hash of its previous hash, and every leaf node is a hash of transactional data.

Now, look at a little example of a Merkle Tree in Blockchain to help you understand the concept. Consider the following scenario: A, B, C, and D are four transactions, all executed on the same block. Each transaction is then hashed, leaving you with:

Hash A

Hash B

Hash C

Hash D

The hashes are paired together, resulting in:

Hash AB

and

Hash CD

And therefore, your Merkle Root is formed by combining these two hashes: Hash ABCD.

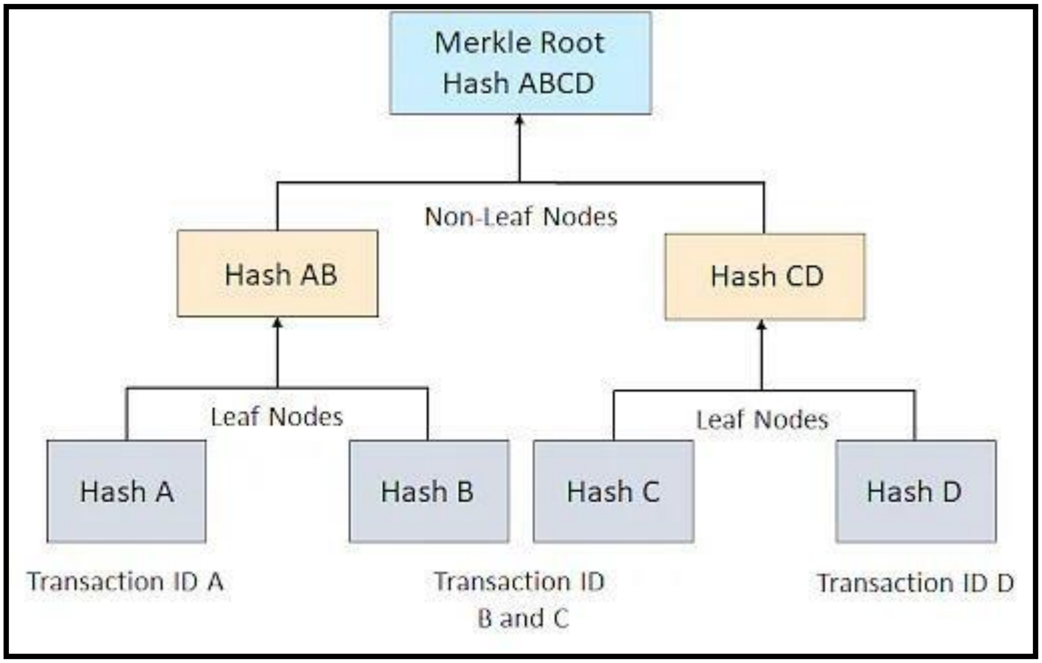


Figure 13 Binary Merkle Tree

In reality, a Merkle Tree is much more complicated (especially when each transaction ID is 64 characters long). Still, this example helps you have a good overview of how the algorithms work and why they are so effective.[5]

Benefits of Merkle Tree in Blockchain

- Merkle trees provide four significant advantages -
- Validate the data's integrity: It can be used to validate the data's integrity effectively.
- Takes little disk space: Compared to other data structures, the Merkle tree takes up very little disk space.
- Tiny information across networks: Merkle trees can be broken down into small pieces of data for verification.
- Efficient Verification: The data format is efficient, and verifying the data's integrity takes only a few moments.

Why Is It Essential to Blockchain?

Think of a blockchain without Merkle Trees to get a sense of how vital they are for blockchain technology. Let's have one of Bitcoin because its use of Merkle Trees is essential for the cryptocurrency and easier to grasp.

If Bitcoin didn't include Merkle Trees, per se, every node on the network would have to retain a complete copy of every single Bitcoin transaction ever made. One can imagine how much information that would be.

Any authentication request on Bitcoin would require an enormous amount of data to be transferred over the network: therefore, you'll need to validate the data on your own.

To confirm that there were no modifications, a computer used for validation would need a lot of computing power to compare ledgers.[4]

Merkle Trees are a solution to this issue. They hash records in accounting, thereby separating the proof of data from the data itself.

Proving that giving tiny amounts of information across the network is all that is required for a transaction to be valid.

Furthermore, it enables you to demonstrate that both ledger variations are identical in terms of nominal computer power and network bandwidth.

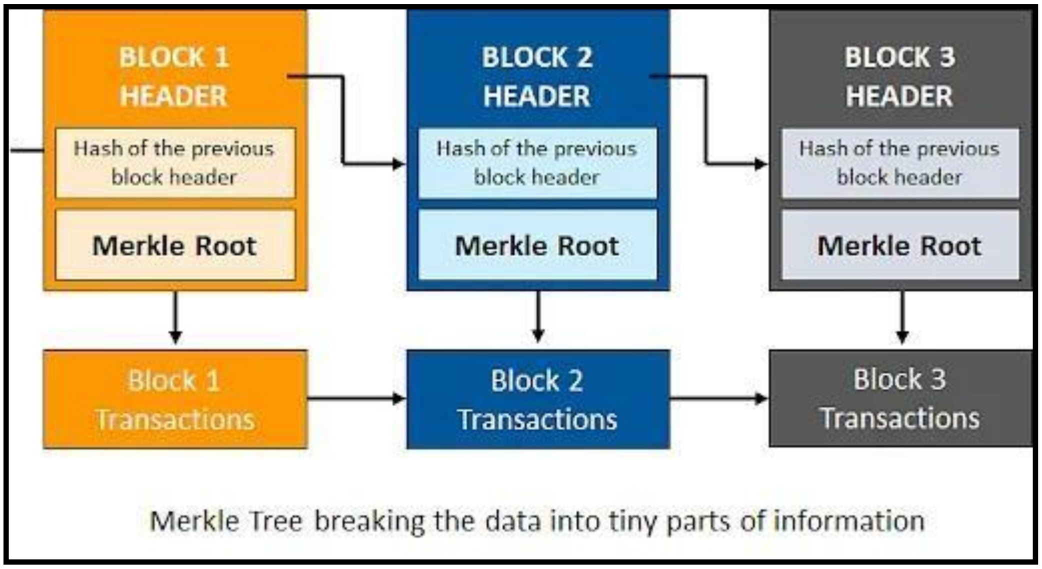

BLOCK 1 HEADER
Hash of the previous block header
Merkle Root
BLOCK 2 HEADER
Hash of the previous block header
Merkle Root
BLOCK 3 HEADER
Hash of the previous block header
Merkle Root
Block 1 Transactions
Block 2 Transactions
Block 3 Transactions
Merkle Tree breaking the data into tiny parts of information

Figure 14 Merkle Tree with Blockchain

Elastic Search with Blockchain

In one of the links in stackoverflow , there was one answer which gives the best answer to this question.

We can use the property of blockchain i.e. immutability. We can store whole blockchain inside the database and keep in sync the database and blockchain all the time.

Apply the elastic search on the database, if we finds out some result from the query, we have to check that transaction hash of the data with the blockchain so that we know that the data we are giving is right.

Yes, there are many defects in this idea as well like what if the data inside the database is not in sync with blockchain. That we have to implement some kind of technique so that we can apply the elastic search i.e. threading search inside the blockchain since we know that blockchain is too big and applying single thread search will take a lot of time to query.

CHAPTER 4

IMPLEMENTATION & DETAILS

Work Done

Backend

MongoDB

Mongo database is implemented with all the models and routes implemented like:

Models

doctor.js =>Doctor model is implemented which stores the name, password to login and walletAddress as well.

healthhistory.js => Health history model is implemented which takes in account the date, patient , doctor , transactionID, symptoms , diagnosis and medicine.

patient.js =>Patient models is implemented which takes in account the date of birth of patient, wallet Address to uniquely identify the patient as well as the name of the patient.

Routes

addDoctor.js => In this route , one can register new doctor to the system and add it in both blockchain as well as database.

addMedicalRecord.js => In this route, one can add medical record of a patient in the database and there is one assert that the data can only be added by the doctor attending the patient. After adding it to database, in the backend server, it continuously check the database and mine a block with the database.

addPatientAPI.js =>It could be the case that the doctor is attending to the patient who is not already present inside the system. Facing this situation, Doctor has the power of adding new patient to the blockchain as well as database.

SmartContract

In this we added a contract in /contract/Heathrecord.sol in which all the code on which the blockchain server is implemented.This code is deployed over the ganache as well and it works well on all the tests.

Frontend

ReactJS

There are few pages which have already been implemented like getData.js , addHistory.js and authentication.js .

CHAPTER 5

RESULTS

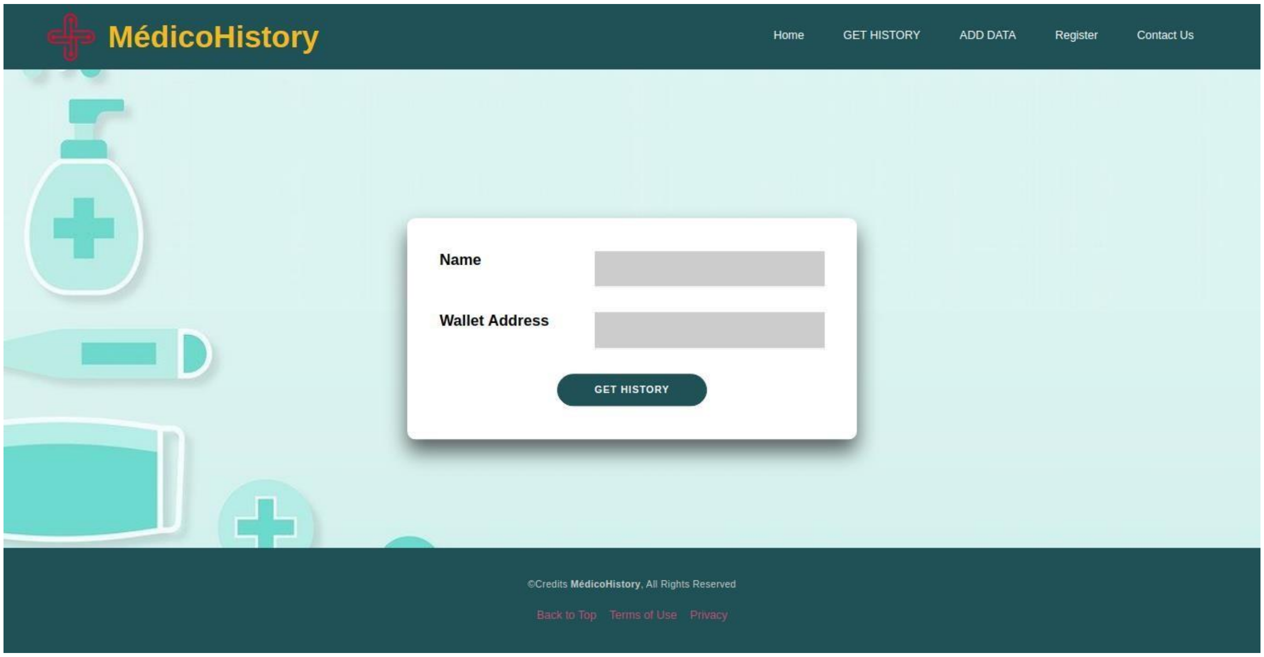


Figure 15 Get Data History from Blockchain

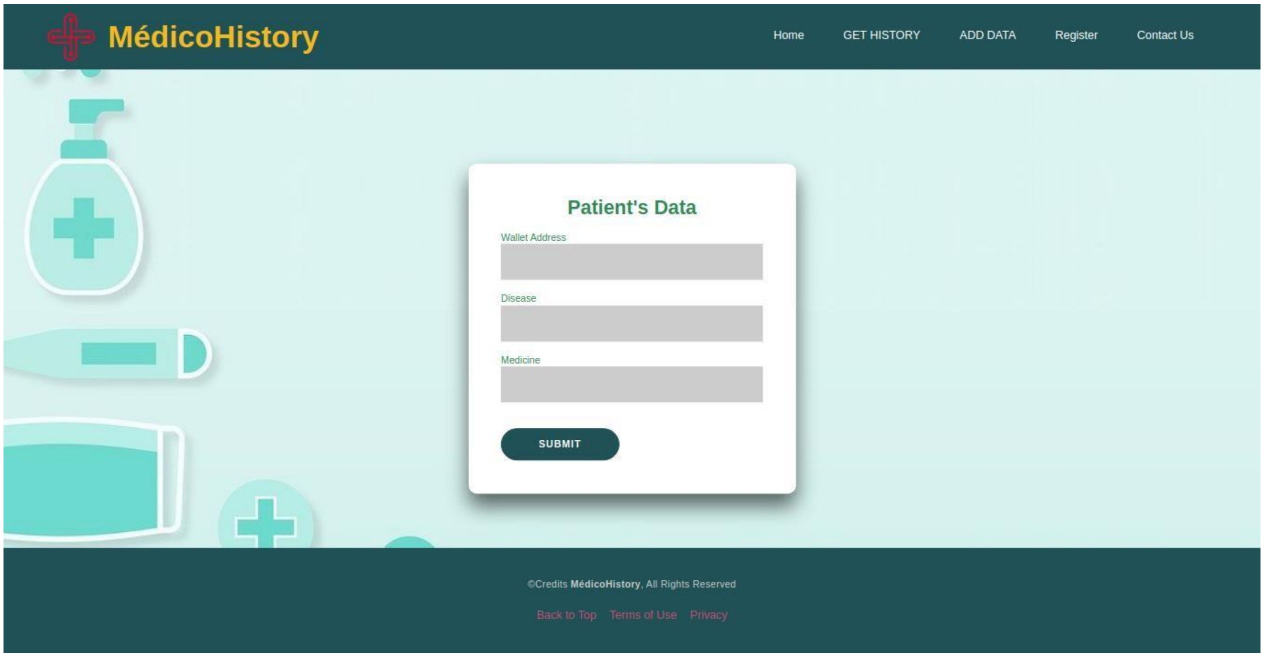
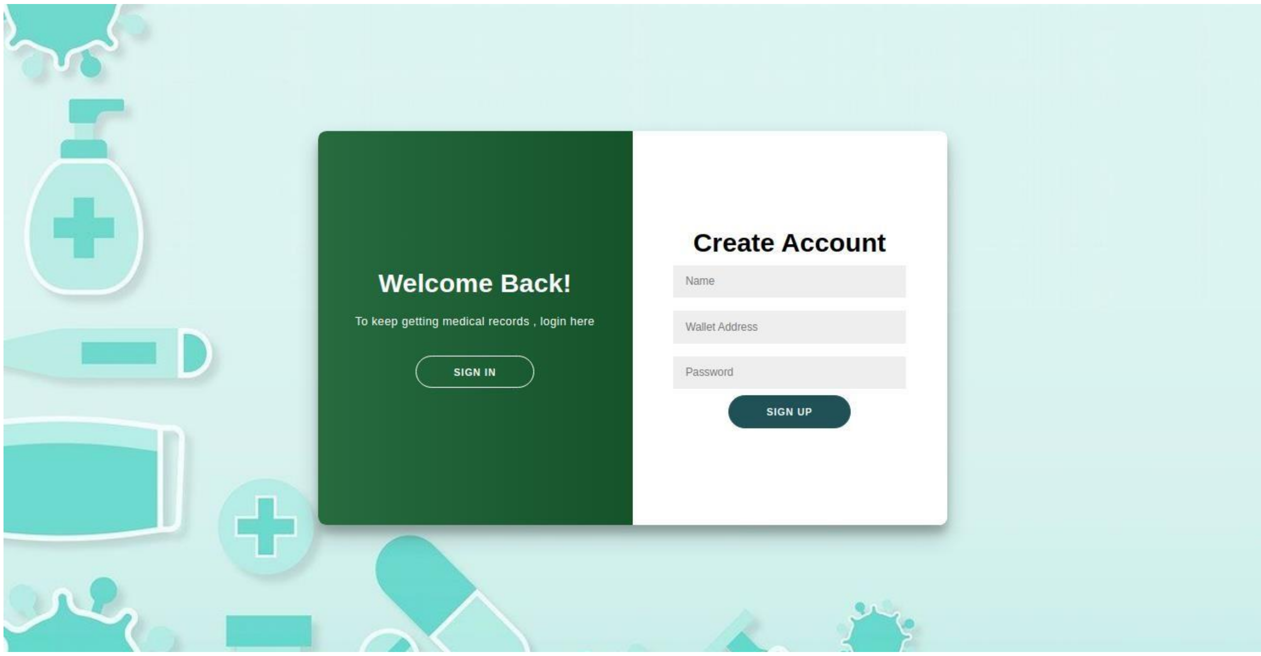


Figure 16 Add Data to Blockchain

SIGN IN & CREATE ACCOUNT PAGE WITHMETAMASK OR AUTHENTICATION

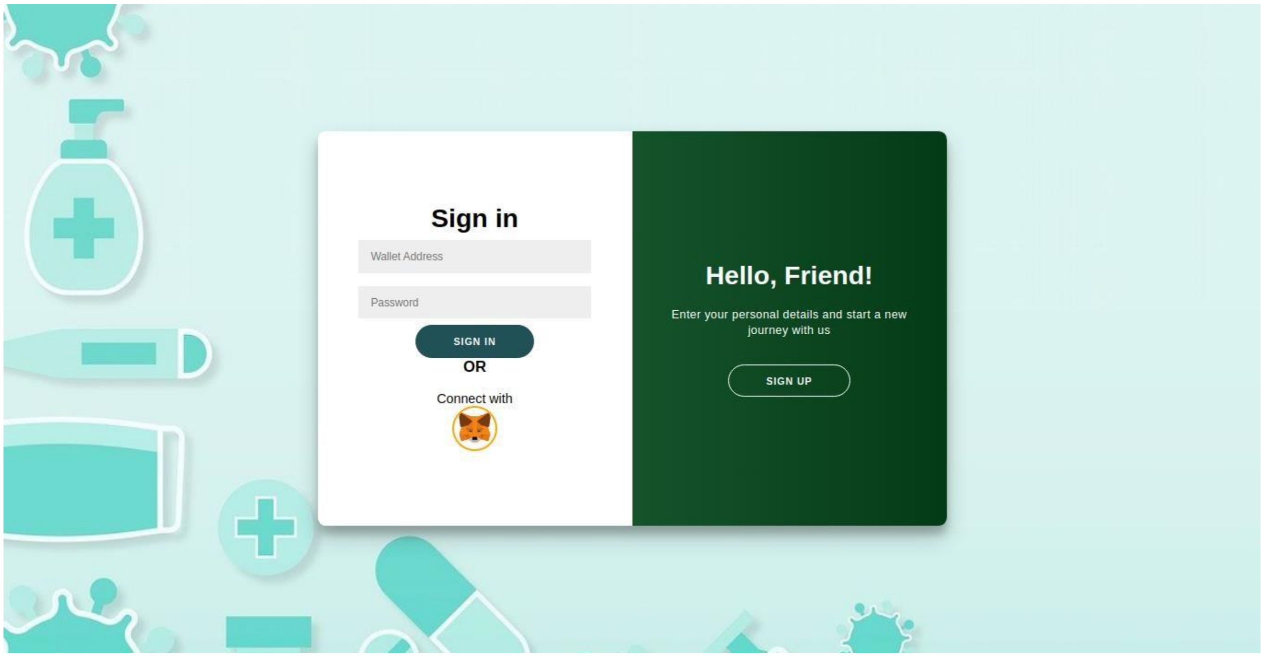


Welcome Back!

To keep getting medical records , login here

Create Account

Figure 17 Sign up Page



Sign in

Hello, Friend!

Enter your personal details and start a new journey with us

Figure 18 Sign In Page

CHAPTER 6

CONCLUSION & FUTURE SCOPE

- Other than this, we are making the overall system less secure, here comes the role of blockchain trilemma.

- So we need to make the use of crypto in the database so that the security concerns are not there.

- Implementing the Elastic search for both databases as well as for blockchain.

- Use the same concept in other places of Decentralised apps as well.

- Make the overall process more secure with a separate channel for adding the data to the database and from there to the blockchain using crypto methods.

CHAPTER 7

REFERENCES

1. Casalino, L.; Gillies, R.R.; Shortell, S.M.; Schmittdiel, J.A.; Bodenheimer, T.; Robinson, J.C.; Rundall, T.; Oswald, N.; Schauffler, H.; Wang, M.C. External incentives, information technology, and organized processes to improve health care quality for patients with chronic diseases. J. Am. Med. Assoc. 2003, 289, 434–441. [CrossRef] [PubMed]
2. DOC (U.S. Department of Commerce). The Emerging Digital Economy II: Appendices; U.S. Department of Commerce: Washington, DC, USA, 1999.
3. Heart, T.; Ben-Assuli, O.; Shabtai, I. A Review of PHR, EMR and EHR Integration: A More Personalized Healthcare and Public Health Policy. Health Policy Technol. 2017, 6, 20–25. [CrossRef]
4. Zhu, L.; Wu, Y.; Gai, K.; Choo, K.K.R. Controllable and trustworthy blockchain-based cloud data management. Future Gener. Comput. Syst. 2019, 91, 527–535. [CrossRef]
5. Siyal, A.A.; Aisha, Z.J.; Muhammad, Z.; Kainat, A.; Aiman, K.; Georgia, S. Applications of blockchain technology in medicine and healthcare: Challenges and future perspectives. Cryptography 2019, 3, 3. [CrossRef]
6. Dai, M.; Zhang, S.; Wang, H.; Jin, S. A low storage room requirement framework for distributed ledger in blockchain. IEEE Access 2018, 6, 22970–22975. [CrossRef]