

Blockchain Based Medical HealthCare System

Rohit Sharma¹ | Saurabh Gautam²

¹B. Tech Scholar, Department of IT, Maharaja Agrasen Institute of Technology, Delhi, India,

²Assistant Professor, Department of IT, Maharaja Agrasen Institute of Technology, Delhi, India,

To Cite this Article

Rohit Sharma and Saurabh Gautam, "Blockchain Based Medical HealthCare System", *International Journal for Modern Trends in Science and Technology*, 6(11): 147-152, 2020.

Article Info

Received on 26-October-2020, Revised on 18-November-2020, Accepted on 25-November-2020, Published on 27-November-2020.

ABSTRACT

Most of the world has switched to the online world today. Online networking and sharing of data have become a common aspect. With the increasing population in the online world and various sectors switching online, data breaches and security vulnerabilities have become quite common. Healthcare sector has been using old methods in securing patients data which has caused a big loss to the healthcare industry. To subside this issue, we have implemented a solution for this problem using blockchain in the healthcare sector. Blockchain technology is a technology built to provide a decentralized system. Patients can easily store their data and provide access only to those they want to provide access. Patients and doctors can easily access and share data without any security vulnerability. This project uses smart contracts and MERN stack technology in building web-based healthcare application.

This paper reviews the current EHR method and provide a better solution using the blockchain-based web application. This application further helps us in implementing a secured medical health-care record application.

KEYWORDS: Blockchain, decentralized, ledger, records, smart contracts

I. INTRODUCTION

Blockchain is now ready to explore and tackle the vulnerabilities of the healthcare system. Various data breach and security vulnerability are becoming common in the medical sector.[1] In 2019, 6.8 million user's data healthcare reports were hacked by a group in India according to the reports. The average breach of healthcare continues to grow and incurred a cost of \$7.12 million in the year 2019. Here, Blockchain overcomes the vulnerabilities of the old healthcare system by providing better ledger system and user verification. Introduced recently in the medical system, various organization have started researching more about the use cases of Blockchain in the healthcare system and thus providing better security.

Satoshi Nakamoto founded the cryptocurrency Bitcoin in 2008 which offered an attack-resistant system for recording data. Blockchain is a decentralized ledger which records the transaction by constructing immutable blocks linked together. Healthcare has been a traditional industry which has shown firmness against new and upcoming technologies.

Issues in healthcare (e.g. information security) have increased in the world in the last few years. Blockchain has solved the problem of current information distribution problems and provided better decentralization.

Research Future (MRFR) explains that blockchain technology in healthcare is expected to generate over 42 million in value and reach a compound annual growth rate of 71.8% by 2023. Such strong growth is induced by blockchain characteristics of decentralized ledger technology with more elevated

clarity, improved security and privacy, increased traceability, boosted performance and reduced costs.



Figure 1: Blockchain in healthcare

Blockchain is defined in a context-sensitive manner i.e. according to the usage. We have created a blockchain-based healthcare system as a web application using MERN stack, ganache and meta mask. It has used an MVC model to build doctors and patients schema. The application encrypts the secret to the blockchain application and stores the data of the patient on the IPFS server. To retrieve the data, the patient sends a secret then, a nonce is generated which is sent to the IPFS server to retrieve the data which is sent back to the node server. Our application will have data sharing option to share the data with among various doctors. Here, the key of the patient is encrypted so, that excessive data is not utilized. Patients will have the access and right to send the specific data to the doctor according to their will and thus, providing a decentralized application. Blockchain being decentralized provide efficient and secured measures for encrypting the data and storing the data.

With this application, there will be no data breach possible. Without any 3rd party interference, data ruptures or security vulnerabilities is nearly impossible. It creates a system that the patient can trust upon and provides other aspects as well. Healthcare has become online due to the COVID-19-crisis and to make it reliable and an efficient system, we need a technology to trust upon for our security and privacy. Blockchain helps us all and thus, helps in bringing security in the healthcare sector.

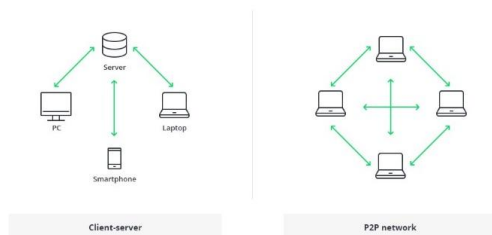


Figure 2: Block Chain P2P network

II. INTRODUCTION TO BLOCKCHAIN

During these times, technology has advanced to the next level. Most of the world has migrated to the online world. However, due to this recent migration, security vulnerabilities and privacy issues have increased a lot as well. To overcome this, the use of various security technologies has increased as well. Blockchain technology is one such technology that provides security and privacy to the users. Blockchain is a composition that stores blocks together in multiple databases, in a network through P2P network.

Blockchain makes information immutable to change, hack or inject. It is a ledger/chain of transaction that is spread across the various system. A new transaction is added to the chain and is also connected to the previous node. The ledger is handled by multiple people. It has transactions which are recorded with cryptographic sign known as a hash.

Blockchain starts when a transaction happens. The process is as follows: -

1. A transaction is requested by the user and is further, authenticated.
2. After that, Transactional block gets created.
3. It is, therefore, spread across various nodes.
4. Every transaction is then validated.
5. Nodes receive a reward for POW (proof of work), typically in cryptocurrency.
6. It gets added to the current chain.
7. The update gets distributed across the network.
8. Further, every node gets updated in the network.
9. Finally, the process gets completed.

Authentication

The blockchain is made in such a way that there is no central authority, however, it still needs authentication.

It is done by using keys, a string of data that verifies a user and give access to them. Every user has a public and private key that is visible to everyone. Both of these keys help in creating a secure digital signature using authentication and finally, unlocks the transaction the user wants to perform.

Proof of Work

Proof of Work allows the individuals who own the computers in the network to be able to add a block to the chain to solve a complex mathematical

problem [2]. Solving the issue is referred to as mining, and miners are typically paid for their cryptocurrency work.

Proof of stake

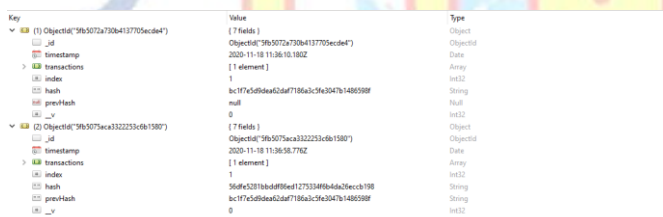
Blockchain network has adopted POS (Proof of stake) validation protocols, where a user has a stake in the blockchain. This reduces the computing power greatly because mining is not required.

III. Smart Contracts

A smart contract is a set of programs or a block of code that self-execute when certain conditions are met on the blockchain [3].

Smart contracts provide a lot of flexibility in developing and designing the solutions to various real-world problems without external involvement and help in making a decentralized system.

When the program is started, the contracts get executed automatically. Smart contracts are spread across all chains.



Key	Value	Type
(1) ObjectID("5f55072a730b4137705ecde4")	[7 fields]	Object
id	ObjectID("5f55072a730b4137705ecde4")	ObjectID
timestamp	2020-11-18 11:36:10.180Z	Date
transactions	[1 element]	Array
index	1	Int32
hash	bc17fcd9dea62daf786a3c5e304791485398f	String
preHash	null	Null
...	0	Int32
(2) ObjectID("5f55075aca3322353db15807")	[7 fields]	Object
id	ObjectID("5f55075aca3322353db15807")	ObjectID
timestamp	2020-11-18 11:36:58.776Z	Date
transactions	[1 element]	Array
index	1	Int32
hash	5d0ff6281ba0d096e1275334964da2fecb198	String
preHash	bc17fcd9dea62daf786a3c5e304791485398f	String
...	0	Int32

Figure 3: Blockchain using Node and MongoDB

IV. LITERATURE SURVEY

Blockchain has emerged in the past few years with various use cases. Fekih, Rim & Lahami in their paper on Blockchain, explained how EHR gets implemented using Blockchain [4]. EHR stands for electronic healthcare records. Most of the hospitals have switched on providing EHR to the patients. Due to this, data breaches and security vulnerabilities also increased as cited by A. Shahnaz, U. Qamar and A. Khalid in their paper on "Using blockchain in EHR"[5].

Nakamoto first invented the blockchain application in terms of transactions between various users without any central authority [6]. Now, with an increase in the use of online resources Interoperability has also increased in EHR. Various techniques are in the testing phase to improve the current health-care sector. Blockchain technology has also improved the health-care sector and is coming up with other

methods as well to provide better services to the users.

Interoperability problem present in EHR proposed problems to the users. Data can be easily transferred between various parties posing problems to patient privacy. Linn [7] proposed a better alternative using Blockchain technology in EHR without causing any excessive data usage. He proposed using blockchain as an access-control manager to health-records. He put forward his ideas based on three main features, data privacy, security and scalability. His idea was to store the indexes in the blockchain and save the data. He wanted to make sure that the data is secured so, the encrypted link had a user unique id, timestamp and link to a health-care record. He used the same idea of blockchain in bitcoin. Storing all the records in encrypted form would lead to excessive usage of bandwidth and loss of data. To have a better and efficient application the transaction contained data that was used frequently. The records were stored in another database that stored images and records etc, in encrypted and digitally-signed format with each document linked to the patient unique id. Whenever a new user signed up a digital record was created in data-lake with the pointer to patient-id.

In the current EHR, the data is being kept in the local databases of health care providers. This becomes a problem when the patient needs to access their data and sharing the data between two health care providers. Because of these disadvantages in using traditional relational databases for storing patient medical records, there is a need to shift to the new technology. We used blockchain technology for the implementation of the patient medical record management application. Blockchain technology offers many advantages like security, interoperability, etc. In the next chapter, we elucidate how blockchain technology is used for storing medical records and its implementation using various frameworks and tools.

V. METHODOLOGY

The application has been developed using MERN stack and using ganache and solidity language. MERN stack includes MongoDB, Express.js, React.js and Node.js. Blockchain code has been written in solidity and JavaScript.

The project saves patient records on the blockchain. The blockchain basically stores the access key in it and the records are stored in the

MongoDB server. There will be two participants doctor and patient.

- The doctor signs up by providing the name and email and password.
- Patient signs up by providing email, password and role.
- Patient uploads files and provides a secret to encrypt the file, the file will be uploaded to MongoDB and secret is stored in Blockchain.
- The patient provides access to a particular doctor.
- Once a doctor is given access by the patient, he will be able to see the all the documents.

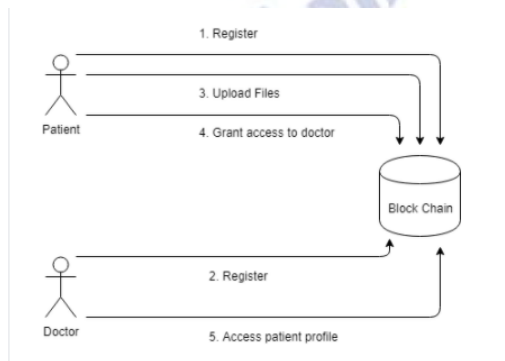


Figure 4: DFD for patient and Doctor

- The project is divided into 5 components basically:

1. We used SDLC (Software development lifecycle) to develop this project. The model used the iterative model for developing this project. Iterative model is a method of implementation of the software development life cycle which concentrates on the iterative implementation of all the steps until the final system is complete.
2. In the backend, we used Rest Apis for the project. We used MongoDB in the backend for storing users and jwt (JSON-web-token) authentication and verification of patients and doctors. The backend is completely independent and doesn't rely on the frontend.
3. The libraries We used in the backend include mongoose, jwt, object-code and various others. We used the MVC model for constructing Rest APIs. We used passport.js library as well for authentication in Sign in and Signup.

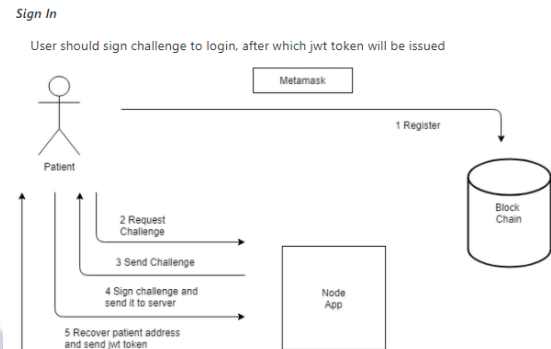


Figure 5: Sign in DFD

4. In the front-end, we used React.js. We developed various components in frontend like signup, sign in, dashboard, doctor-dashboard etc. The main aim is to provide a better user-friendly environment and to make the application less complex.
5. For blockchain integration, we used solidity for making contracts and JavaScript. We used vanilla JavaScript for developing the blockchain using class-based architecture. The blockchain is integrated into the backend in Node.js.
6. Testing is also being done in the project using ganache and unit testing environment.

```

10  "author": "",
11  "license": "ISC",
12  "dependencies": {
13    "bcryptjs": "^2.4.3",
14    "body-parser": "^1.19.0",
15    "concurrently": "^5.3.0",
16    "cors": "^2.8.5",
17    "express": "^4.17.1",
18    "is-empty": "^1.2.0",
19    "jsonwebtoken": "^8.5.1",
20    "mongoose": "^5.10.14",
21    "morgan": "^1.10.0",
22    "nodemon": "^2.0.6",
23    "passport": "^0.4.1",
24    "passport-jwt": "^4.0.0",
25    "validator": "^13.1.17",
26    "web3": "^1.3.0"
27  }
28

```

Figure 6: Libraries Used

About the application:

- The patient sign in using email, name and password and role. The patient then, provides access to the doctors for the access to the documents.
- Patient has to upload documents with a secret, and that transaction is stored in the blockchain.

- The documents get encrypted and gets stored in the database and can only be accessed if, the user has the correct secret and access rights. The doctor is able to access the documents only when patient provides the rights.

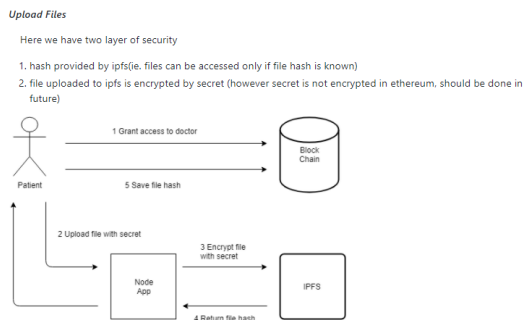


Figure 7: Upload Data DFD

The schema of the doctor contains various attributes:

- Name of doctor
- Email id
- User id
- Patients access



Figure 8: Doctor Document

The schema of patient contains these attributes:

- Name of patient
- Email id
- User id
- Doctors given access right

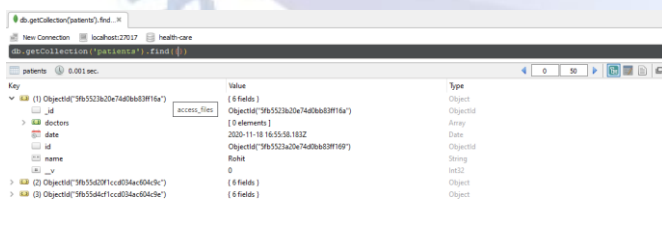


Figure 9: Patient Document

VI. RESULT

The old EHR system poses various vulnerabilities. The single central authority causes various security problems and leads to the data breach. Our application focuses on providing a better user interface and better security to the users. Blockchain helps in making a better-secured application without any third-party

interference. We have used MERN stack and ganache and smart contracts in our system.

Our application helps in various aspects:

1. Easy User interface and better security.
2. No central authority and better user experience.
3. Protection from hackers and various other services like the sign in, signup and login.
4. Using the latest technologies like MERN stack in developing and maintaining the application.
5. Data verification and having extra protection layer in maintaining the application.

Using NoSQL databases to provide horizontal scaling i.e. sharding to the application.

Figure 10: Sign up

Figure 11: Sign in

VII. CONCLUSION

In this paper, we tried to build an application that provides better user experience and security to users. We have explained the methodology and the results obtained in this project. We have used Rest APIs and NoSQL database in this project. It includes blockchain that adds security to the application. The application follows the SDLC model and provided exposure to various technologies. MERN stack technology helped this application to become scalable on later on stages. Currently, the application is using simple web-based architecture but on later stages, it can be upgraded with various functionality and better security as well. With other use cases as well, this application can be used in other sectors and along with more added capabilities.

REFERENCES

- [1] <https://www.csoononline.com/article/3541148/the-biggest-data-breaches-in-india.html#:~:text=Hackers%20steal%20healthcare%20records%20of%206.8%20million%20Indian%20citizens&text=Details%3A%20Enterprise%20security%20firm%20FireEye,Chinese%20hacker%20group%20called%20Fallensky519>.
- [2] <https://www.euromoney.com/learning/blockchain-explained/how-transactions-get-into-the-blockchain>.
- [3] Mohanta, Bhabendu Kumar, Debasish Jena, and Soumyashree S Pand (2018), "An Overview of Smart Contract and Use cases in Blockchain Technology." Institute of Electrical and Electronics Engineers, 9th ICCNT, 12–20
- [4] Fekih, Rim & Lahami, Mariam. (2020). Application of Blockchain Technology in Healthcare: A Comprehensive Study.
- [5] A. Shahnaz, U. Qamar and A. Khalid, "Using Blockchain for Electronic Health Records," in *IEEE Access*, vol. 7, pp. 147782-147795, 2019, doi: 10.1109/ACCESS.2019.2946373.
- [6] Nakamoto, Satoshi (2009), "Bitcoin: A peer-to-peer electronic cash system."
- [7] Linn, L. A. (2016), "Blockchain for health data and its potential use in health it and health care related research." ONC/NIST Use of Blockchain for Healthcare and Research Workshop, Gaithersburg, MD, USA: ONC/NIST.
- [8] Priefer, Dennis & Kneisel, Peter & Strüber, Daniel. (2017). Iterative Model-Driven Development of Software Extensions for Web Content Management Systems. 10.1007/978-3-319-61482-3_9.
- [9] Brancaccio P, Maffulli N, Buonauro R, Limongelli FM. (2008) Serum enzyme monitoring in sports medicine. *Clin Sports Med*; 27(1): 1-18, vii.
- [10] Tom Joseph, Seymour, Dean Frantsvog, and Tod Graeber (2014), "Electronic Health Records (EHR)." American Journal of Health Sciences, Research Gate.
- [11] Marko Vidrih (2018), "What Is a Block in the Blockchain?". URL <https://medium.com/datadriveninvestor/what-is-a-block-in-the-blockchain-c7a420270373>
- [12] Mohanta, Bhabendu Kumar, Debasish Jena, and Soumyashree S Pand (2018), "An Overview of Smart Contract and Use cases in Blockchain Technology." Institute of Electrical and Electronics Engineers, 9th ICCNT, 12–20.
- [13] Niya, Sina Rafati, Florian Shupfer, Thomas Bocek, and Burkhard Stiller (2018), "Setting up Flexible and Light Weight Trading Contracts with Enhanced User Privacy Using Smart Contracts." IEEE/IFIP Network Operations and Management Symposium, Institute of Electrical and Electronics Engineers, 1–2.
- [14] Pinyaphat, Tasatanattakool and Techapanupreed Chian (2018), "Blockchain: Challenges and applications." In International Conference on Information Networking, Institute of Electrical and Electronics Engineers, 473–475.