IIETA International Information and Engineering Technology Association
Advancing the World of Information and Engineering

Revue d'Intelligence Artificielle
Vol. 33, No. 1, February, 2019, pp. 45-48
Journal homepage: http://iieta.org/journals/ria

Avoiding Interoperability and Delay in Healthcare Monitoring System Using Block Chain Technology

Vejendla Lakshman Narayana*, Arepalli Peda Gopi, Kosaraju Chaitanya

Vignan's Nirula Institute of Technology and Science for Women, Peda Palakaluru, Guntur 522005, Andhra Pradesh, India

Corresponding Author Email: lakshmanv58@gmail.com

https://doi.org/10.18280/ria.330108

Received: 10 October 2018
Accepted: 25 January 2019

Keywords:
block chain technology, health care monitering, interoperability

ABSTRACT

Blockchain is using in every aspect now because of its distributed ledger which is immutable. It provides the information to the users directly without any third party involvement. It mediates the transactions directly between the interacting parties securely. It also eliminates the friction and also the cost of current intermediaries. It is now using in healthcare system to provide the interoperability, security, decentralization and other. EMR is presently using in healthcare which has some issues. The issues in healthcare are patient cannot access the data of his/her own health information. So by this healthcare has issues like interoperability and delay in communication and some other. These issues can be solved by using the Blockchain in healthcare. By this Blockchain provide security by giving the patients to access their own data rather than provider.

1. INTRODUCTION

Blockchain is a platform which supports the trustless and the secure transactions between the interacting parties. It offers decentralization and immutability and consensus. Smart contracts are enchanters the Blockchain technologies. It provides code to control the exchanges or redistributions of digital assets between two parties or more according to their rules which are established previously between them.

Smart contracts store the data objects and define operations on data which is enabling in the development of DApps which is used to interact with Blockchain and provide countless services to the application users. We construct the contracts to contain metadata about the record ownership, permissions and data integrity [1].

The healthcare system which was present was not given the permissions management to the patients on their own health information. It also has many issues like no security and not having access permissions for patient and also retrieval of patients data from EMR [2].

By using Blockchain rather than EMR in healthcare we can solve the issues in it. EMR is a medical record that stores the patients data which can be helpful for the patients in their health checkups. There are some issues with EMR like it has only the provider permission. It does not have the patients access permission. So there is no security for the patient information. The other issue is at the retrieval time where the data cannot be retrieved after the completion of the retrieval time [3].

To deal with interoperability, security, retrieving and other issues we use MRecord instead of EMR. MRecord is using the Blockchain which is able to solve all the issues with EMR [4].

In this MRecord patient gets the access permission without the mediators involvement. By this patient can feel that hi/her data is safe. Here MRecord uses the username and password as key login to get the patient information. By this retrieval can also be done at any time [5].

2. RELATED WORK

2.1 Healthcare issues

MRecord restores process by giving access permissions and reviewing their medical history to patients and also provides an easy mechanism for data sharing across different medical organizations [6]. Patients can authorize a new doctor to review their record and obtain a second opinion or grant viewership rights to the guardian they trust.

Healthcare researches today struggling with fragmented and soiled data, delayed communications and desparate workflow tools. On the other hand provides feel reluctant to exchange data due to the opinion that patients information cannot be safe by sharing and also have financial effects by sharing. The main issues are interoperability, not providing the patient access permissions on their own healthcare information and retrieval of data beyond the time period [7].

2.2 Blockchain dealing with health system

Patients has their data in many hospitals or authorities due to number of check-ups done in different hospitals in their life time. So there are challenges of information exchange between the provider and organizations [8]. Due to this challenge health records are not present as united.

MRecord contains the data ownership and also viewership permissions. Smart contract is used here with the support of Blockchain technology which allows to track the state transitions and also to automate [9]. In ethereum Blockchain we have smart contracts and by using this we give login, viewer perrmissions and also data retrieval instructions for the patients. In this MRecord providers can add records of patients and patients share their information according to

their usage.

When the record is adding the patients get a notification of accepting or rejecting. So that patient can check it and decide whether can accept it or reject. MRecord prioritizes the patient and provider relationship by providing backup called reference for checking the updates in medical information [10]. We use public key cryptography for id verification of the patient.

3. BACKGROUND WORK

3.1 Healthcare

Electronic Medical Records are using in healthcare to store the patient records. We are now facing a problem in healthcare that is a patient cannot access his own health information and also not sure about security for his health information.

3.2 Blockchain

Work on Blockchain mainly started for the security purpose which was firstly used in the bitcoins transactions. It is a distributed system which is used for storing and recording the transaction records [11].

In this Blockchain we may not have any central authority and the transaction records are stored and distributed across all network participants [12]. Blockchain truly satisfies sharing the repositories with multiple parties, to trust the transactions as valid by parties, intermediaries are not trusted, more security measures are needed.

Here we have to consider two things mainly they are firstly to verify and authenticate information and another is to transfer value. In verification Blockchain technology checks and verify the login details with stored details and if it was valid then it gives the access to login. In transaction values the technology used is cryptocurrencies [13].

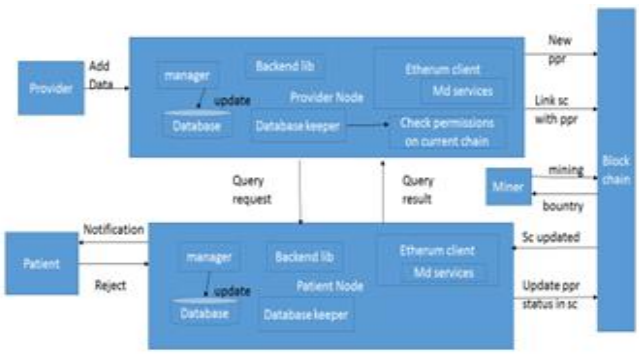

Figure 1. Blockchain system design

Platforms such as ethereum can provide the ability to create the decentralized applications on the top of Blockchain architecture which will be lead the Blockchain protocol for both permission and permissionless Blockchain development [14]. Blockchain provides the health information which is standardized by providing a layer called transaction layer which helps all the stakeholders to meet securely. According to the layer which is mentioned above is used to store two types of data or information. First type is on-chain and the another is off-chain.

In On-chain data can be directly stored on Blockchain. In this on-chain standardized data-fields has the needed information in text form. In Off-chain data with links stored in Blockchain that act as pointers to information stored in separate, traditional database. The summarized data-fields in this contains the expansive medical details and abstract data types.

There are advantages and also disadvantages for both On-chain and Off-chain. The advantages of the On-chain are data can visible immediately and are taken by the organization which are connected in Blockchain. On-chain disadvantages are constraints present in the type and size of the data which is going to be stored. The advantages of Off-chain are the disadvantages in On-chain. For Off-chain disadvantages are data cannot be visible immediately and also not taken by organization which are connected in Blockchain and also want to access for each healthcare organizations source system for each record.

Once a standardized healthcare information is established then the specific data fields can be created in smart contract to employs rules for processing and storing information on Blockchain. Each time when the patient enters username and password the health organization ass it to smart contract for checking whether valid information has been entered or not. Hacker also feels the difficulty for hacking every single key of patients. So there is less damage.

All healthcare organizations connected to Blockchain maintain their own updated copy of healthcare ledger. If any update is required then it should have 51% of network participants approval to change each and Blockchain copy should be updated to make a throwback for each and every change. These features improve the security of patient information and also helps to reduce the malicious activities. In future this Blockchain creates many rare opportunities like reducing the complexities and avoiding the trustless collaborations and create a secured and make data unchangeable without the permission from patients.

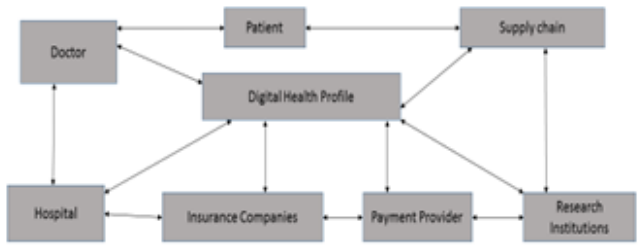

Figure 2. Blockchain supply chain in healthcare

3.3 MRecord using Blockchain on healthcare issues

Patients and providers may face significant hurdles in initiating data retrieval and sharing due to economic incentives that encourage “health information blocking”. When we are going to design a new system we have to take care of each and every issue of the patient. By this we can make patient to use our new system. By having trust of our new system patients feel secured for their data which was provided and also confident on using the new system.

To identify the health risks by the data stored of the patient and to provide various new treatments by taking the analysis from providers and patients and also by some surveys we can identify the risks which are going to be occurred in the future. Through this collection we can implement the new system

without any risks. In this paper Blockchain structure is applied on EMRs. Blockchain uses the public key cryptography which may create add-only, unchangeable and time-based chain of content.

The chain contains nodes which represents the participants in the process of storing records in the chain. The information which is updated is send to all nodes so there is no need of any malicious acts. MRecord Blockchain implementation tells mainly about the issues likedata which was not stored in only one place, slow in accessing the patients information, interoperability and some other.

Via smart contracts on an Ethereum Blockchain, we log patient-provider relationships that associate a medical record with viewing permissions and data retrieval instructions (essentially data pointers) for execution on external databases. By using the cryptography keys in the Blockchain data integrity is maintained. The new information once added to the nodes are shared by the patients and the providers.

Automatically the notifications send to all the participating people in the chain. So they can easily verify the information before adding. MRecord provides references to the patients and the providers which helps them to modify history if there is any need to update. We handle the confirmation of identities through public keys. We employ DNS-like implementation that maps an already existing and widely accepted form of ID (e.g. name, or social security number) to the person's Ethereum address.

A syncing algorithm handles data exchange "off-chain" between a patient database and a provider database, after referencing the Blockchain to confirm permissions via our database authentication server. To navigate the potentially large amount of record representations, our system structures them on the Blockchain by implementing three types of contracts.

3.3.1 Registrar Contracts (RC)

In this the contract is used to identify the patient's identity by comparing it with the Ethereum address. Here strings are used rather direct use of public keys which allow us to use the already present data. Verification process can be given to particular institutions only.

3.3.2 Provider-Patient relationship contract (PPR)

Provider-Patient Relationship Contract is present in system in two separate nodes in which one node is used to store and manage medical records for second. PPR deals with data pointers and also its related permissions of accessing that which identifies provider records. Every pointer of information has its own query string which is executed based on the database provided by provider and returns patient information subset. Queries and the related information are taken by the provider and make the changes when there is needed.

3.3.3 Smart Contract (SC)

This contract holds the references which locates the medical history of the patient. The references which are given by the PPR are held by this contract. This Smart Contract is given to the patients which can have references which are populated with. Providers, on the other hand, are likely to have references to patients they serve and third-parties with whom their patients have authorized data sharing. Provider can join again multiple times with the Blockchain by downloading the latest Blockchain network. If there are nodes in the network participation then the Blockchain log cannot be maintained. In this contract we have the notifications or status updates which is used to recognize whether the connection is new or already established. The data which is missing can come back by the nodes present in summary contract. In this smart contract we perform the operations by mainly using Backend Library, Ethereum Client, Database Gatekeeper and EMR manager.

4. BENIFITS AND DRAWBACKS OF USING BLOCKCHAIN IN HEALTHCARE

4.1 Benefits

1. A database is consisting of bits and bytes which are not enough to store the patients records securely where Blockchain can make it.
2. The patients records which are placed in database are stored in the physical memory of a particular system. So, anyone who has access to that system could corrupt the data within. While in Blockchain we may not have these type of problems.
3. With Blockchain, there is no need for a mediator or central administrator. All the patients have control on their own health information.
4. Blockchain provides a quick access and also secure data sharing if needed.
5. Blockchain, offers security, scalability for health information of the patients.
6. The Blockchain concept in healthcare is innovative and ground-breaking. But, it was not a complete solution forsolving the issues in data management.
7. Blockchain is a type of a distributed ledger, all nodes in the network share a copy of the documentation. The data on a Blockchain ledger is easily accessible for everyone to view. If any in history, everyone in the network can see the change and the updated record. Therefore, all information about patient information is available to everyone.
8. Blockchain is better than any other record-keeping system like databases in the case of security. The shared documentation of transactions can only be updated and/or modified with consensus on a Blockchain network. The information can be edited only when the majority accepts to edit. When a transaction is approved, it is encrypted and connected with the previous one. Therefore, no single person or organization has the potential to alter a record. Blockchain is decentralized, and so, no one has the right to update records by themselves.
9. Blockchain can handle the risk of mistakes, which are making records of patients much more efficient and faster. As there is only one ledger, organizations connected with Blockchain don't have to maintain multiple records. And, when everyone has access to the same information without any need of intermediaries patients can access them.
10. Auditability is present in Blockchain to see and check the authenticity of patient's information as they are stored for their complete life in Blockchain.

4.2 Drawbacks

1. As Blockchain is a new technology many large corporations are struggling to integrate it into their core systems.

2. Blockchain is high in cost which makes difficulty for user.

3. Although it can handle data like IDs and certificates, large data like CT scans will be difficult to store in Blockchain.

4. Blockchain databases are stored on all network nodes, the issue of storage surfaces. With the increasing number of records of patients, which makes size of the database expand. To avoid this the speed of Ethereum Blockchain is increasing by 55 GB/year.

5. Patient information is on a public block chain which is encrypted and anonymous, but lies in the hands of all nodes in the network. So, this proves that block chain is not 100 percent secure, unfortunately.

5. CONCLUSION

By this technology, MRecord shows how decentralization principles is applicable to largescale information management in an EMR. It also provides a new approach for maintaining the records. It also provides the feasibility of the system and to gain the patient and providers interest. We are committed to the principles of open source software and want to make our framework available as a platform for further development.

REFERENCES

[1] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). MedRec: Using blockchain for medical data access and permission management. 2016 2nd International Conference on Open and Big Data (OBD). IEEE, Vienna, Austria. https://doi.org/10.1109/OBD.2016.11

[2] Tian, H.B., He, J.J., Ding, Y. (2019). Medical data management on the blockchain with privacy. Journal of Medical Systems, 43: 26.

[3] Zyskind, G., Nathan, O., Pentland, A.S. (2015). Decentralizing privacy: Using blockchain to protect personal data. 2015 IEEE Security and Privacy Workshops (SPW), pp. 180–184. https://doi.org/10.1186/s13635-016-0051-2

[4] Wood, G. (2014). Ethereum: A secure decentralized generalized transaction ledger. Ethereum Project Yellow Paper. https://doi.org/10.1504/IJNDC.2018.093625

[5] https://www.marutitech.com/Blockchain-benefits/

[6] https://hitconsultant.net/2018/01/29/Blockchain-technology-in-healthcare-benefits/

[7] Gopi, A.P., Babu, E.S., Raju, C.N. (2015). Designing an Adversarial model against reactive and proactive routing protocols in MANETS: A comparative performance study. International Journal of Electrical & Computer Engineering, 5: 5. https://doi.org/10.1504/IJASM.2015.068610

[8] Ashok Kumar, S. (2015). An empirical critique of On-Demand routing protocols against rushing attack in MANET. International Journal of Electrical and Computer Engineering, 5.5. https://doi.org/10.1504/IJACT.2012.045589

[9] Bikku, T., Gopi, A.P., Prasanna, R.L. (2019). Swarming the high-dimensional datasets using ensemble classification algorithm. First International Conference on Artificial Intelligence and Cognitive Computing. Springer, Singapore.

[10] Vejendla, L.N., Bharathi, C.R. (2016). Secured key production and circulation in mobile ad hoc networks using identity based cryptography. International Conference on Engineering and Technology, 1: 202-206. https://doi.org/10.1504/IJICT.2016.079963

[11] Vejendla, L.N., Gopi, A.P., Kumar, N.A. (2018). Different techniques for hiding the text information using text steganography techniques: A survey. Ingénierie des Systèmes d'Information, 23(6): 115-125. https://doi.org/10.3166/isi.23.6.115-125

[12] Gopi, A.P., Vejendla, L.N., Kumar, N.A. (2018). Dynamic load balancing for client server assignment in distributed system using genetical gorithm. Ingénierie des Systèmes d'Information, 23(6): 87-98. https://doi.org/10.3166/isi.23.6.87-98

[13] Vejendla, L.N., Gopi, A.P. (2017). Visual cryptography for gray scale images with enhanced security mechanisms. Traitement du Signal, 34(3-4): 197-208. https://doi.org/10.3166/ts.34.197-208

[14] Gopi, A.P., Vejendla, L.N. (2017). Protected strength approach for image steganography. Traitement du Signal, 34(3-4): 175-181. https://doi.org/10.3166/ts.34.175-181