Blockchain based Electronic Health Record Maintenance System

Mr. Jaskirat Singh Bhatia[1*], Dr. M. Prakash[2]
[1,2] Department of Computer Science and Engineering
SRM Institute of Science and Technology
Kattankulathur, Kancheepuram, Tamilnadu, India.
[1]jaskiratsingh_so@srmuniv.edu.in, +1 (226)-507-2637
[2]prakashm2@srmist.edu.in, ORCID : 0000-0001-8008-4424, +91-9894664948
*Corresponding author

Abstract – The biggest concern in this era is trust; No one is willing to trust anyone. The latest trend in development of trust is the Blockchain technology and we now bring it into the medical branch. EHRs (Electronic Health Records) are the basis of storing the health records for the patients on the computer, but they have a major disadvantage, that is they are not decentralized plus the patients don't trust them and they can be modified or deleted by an authorized person or a hacker which makes them quite unreliable. The base for this research paper is to give all the power to the patient by implementing the EHRs System on blockchain. By this we make the records unmodifiable undeletable and decentralized so that we can develop a sense of trust with the patient. To increase the security, we have also used public and private keys of the Doctor / Patient to encrypt and digitally sign the EHR saved on the blockchain. The advantage of this is that no middle man can decode what the EHR is and the doctors signature binds the EHR to the doctor which in-turn if is dis-honest in his analysis of the patient, can be blamed for.

Keywords – Blockchain, Encryption, Private Keys, Health care, Privacy, Decentralizing.

I. INTRODUCTION

With the rapid development in technology, new inventions keep on developing and we must exploit the new technologies to do well for the world. The Blockchain technology [1] focuses on a distributed ledger, hence decentralising the data. The advantage of this is that if one of the ledgers is corrupted or hacked, we do not lose any data as rest of the ledgers support the uncorrupted data. Blockchain also encrypts the next block of the chain with its predecessor, making the data unmodifiable; the pro of this is that insurance companies would trust on the patient more as all his records would be original and showing transparency with the insurance companies [2, 3]. As the Health Record will be accessible by the patient unlike the existing system where the hospitals and the doctors access the records for the patient and each hospital has a separate record, hence providing a common record of the patient for any hospital.

II. ELECTRONIC HEALTH RECORD

It stands for Electronic Health Record. It is the collection of the details of the patient in a digital format which are stored electronically. These records can be shared across various health care settings.

EHRs include a range of data which includes demographics, medication, medical history, allergies, immunization status, Radiology images and personal statistics like age, weight, lab test results and billing information.

The EHR has the ability to generate the complete record of any clinical patient encounter - as well as supporting the other care-related activities directly or indirectly via interface which includes evidence-based, quality management, out- comes reporting and decision support.

The EHR was invented so that all the medical history of the patient could be looked upon at, at a glance. It stores all the details of the patient from start to the end [4, 5]. Generally, each hospital has its own EHR for the patient that is if the patient went to multiple hospitals he would have multiple EHRs.

III. BLOCKCHAIN

A blockchain consists of a ton of records called blocks where every block uses the previous block's cryptographic hash to link with it. A block usually contains the cryptographic hash of the previous block, a timestamp and some transaction data.

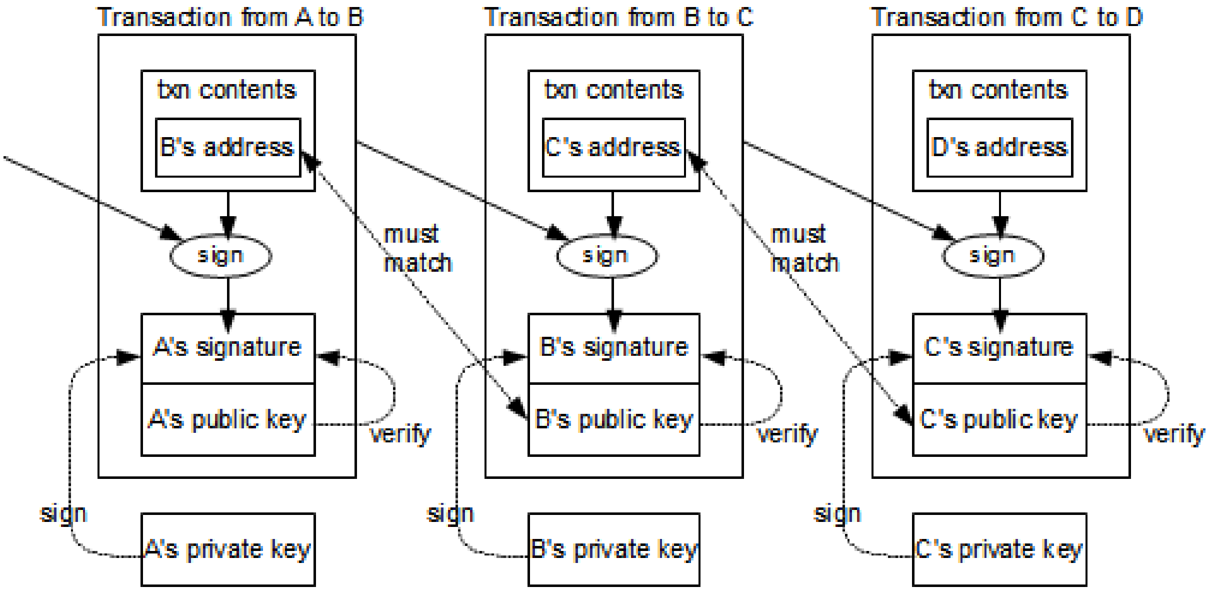
It works on a peer to peer basis, which means that two or more PC's are inter-connected together and they share resources without going through any kind of separate server computer [6].

1) *Transactions:*

An electronic coin is named as a gathering of computerized marks. Every holder, when he needs to exchange the coin to the following individual, carefully signs the prior exchange with the open ey of the later holder, adding all these as far as possible of the coin. The chain of proprietorship can be effectively confirmed by the representative which should be possible by just checking the marks appended in the exchange which is shown in fig.1.

2) *Proof of Work:*

The verification of work is utilized to make sense of if the square has really being mined or not. It involves an esteem which when hashed with a hashing calculation, the hash starts with a required least number of zeros. The middle work required is the time required to mine a specific square which is the exponentials of the quantity of zeros compulsory and can be confirmed by executing a solitary hash. When the measure of CPU control which should be a great deal has been used to influence it to fulfill the required confirmation of-work, at that point the substance of the square can't be changed without playing out that very work once more. As the squares which arrive later are attached onto it, the work done to change the square would consolidate re-trying all the work (or mining) obstructs it which aggregates to be a great deal.



3) *Evidence of work:*
It is additionally in charge of the blockchain to just proceed in the first or unmodified chain. The choice of which chain to choose s made by the longest chain; as that will be the chain with the most extreme verification of work used in it. On the off chance that most of the hubs in the chain are straightforward hubs, the valid chain will become the most quickly and will be certainly quicker than any contending chains. To refresh a past square, a programmer would have to mine the square he is assaulting alongside all squares which are after it and after that connect with and outperform crafted by all the legit hubs considering the way that the legitimate hubs become all around quickly; the likelihood of which is by zero.

4) *Transparency and Privacy:*
As Blockchain uses Public-Private Key cryptography, each user has his own pair of keys. When a transaction is made, the user can share his public key and make his transaction visible to the person with whom he shared his key. If the user wishes privacy, he can choose to keep his public key anonymous and all the other people will notice that a transaction took place. Hence giving the user full power for his transparency or privacy.

IV. BLOCKCHAIN BASED EHRMS

Each User and Doctor / hospital will have its own set of Public – Private keys [7].

A general transaction is of the form: To – From – Amount

Our transaction will be of the form: User– Doctor / hospital– EHR block - EHR number (self-incremental)

Each block is owned by the user and encrypted with the private key of the user

User is the User ID

The doctor / hospital is the doctor / hospital ID where the user went for a check-up

The EHR block is the block which contains the EHR by the Doctor / Hospital and is signed by the private key of the doctor / hospital, encrypted with the public key of the user and then inserted into the blockchain.

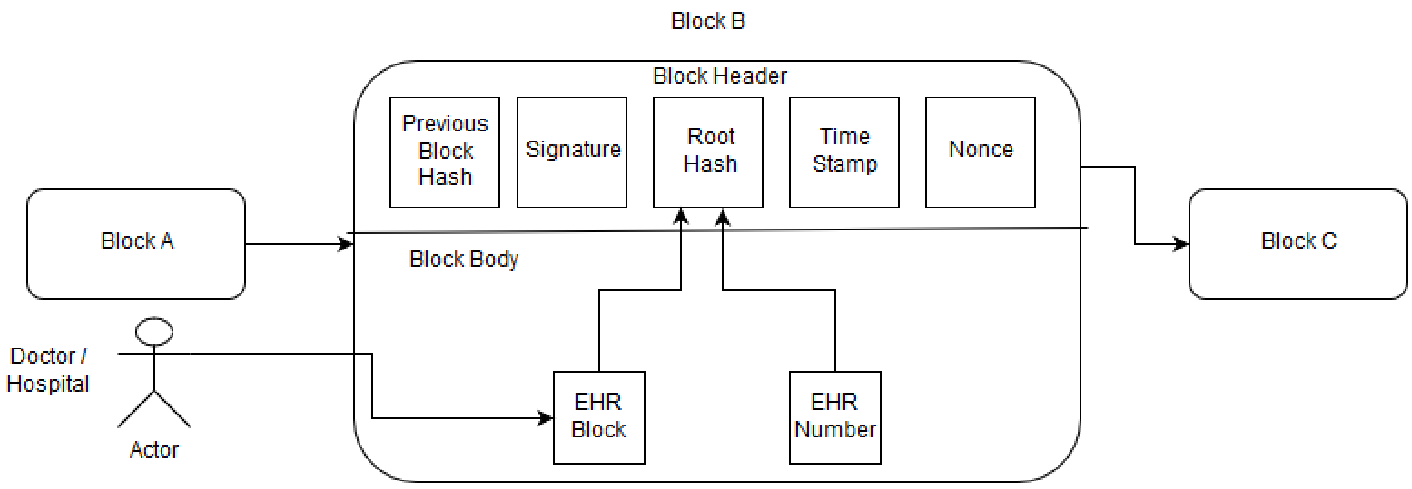
Self-incremental means that each block in the Blockchain will be given a number starting from 0 and the successive block will be plus 1 of the previous block [8].

The EHR-block is encrypted by the private key of the doctor so that its originality is preserved. And there is a proof about which Doctor wrote that EHR.

When the user wishes to access his records, all the EHRs corresponding to each EHR number will be displayed. (fig.2)

V. APPLICATIONS

There are a lot of cases of forging a medical record. With the EHRs implemented on a blockchain, there is no chance of forging, hence companies can depend on our medical records to be official records. For example, Alice bought a fake medical record and with the help of that, she got a medical leave. But with our technology, getting a fake record or modifying the original record would not be possible, hence Alice would



not be able to get a leave until and unless she was actually sick.

Medicines are sold illegally without a proper prescription and sometimes with a forged prescription. Again, with our technology, forging a prescription will be impossible, thus removing this problem too.

Insurance companies offer a better package with you if you show them transparency. In our model, all the records are broadcasted publicly, there will be 100% transparency with the companies and hence a better package for the user [9, 10].

VI. RESULTS AND DISCUSSIONS

We successfully implemented a blockchain based EHRs on Python. There was a login / sign-up portal to login / create more doctors or users. On creation of another User or Doctor, an instance of a class was created and it was assigned the respective public and private key along with all the other basic information of the User / Doctor. If the user wanted to enter an EHR, he would first have to go to a doctor, then the doctor will sign the EHR with his private key to authenticate it; then the user will use his public key to encrypt the EHR. After that, the user will go on to add the EHR onto the blockchain.

Our application was successfully tested on the first and second application where the EHR cannot be forged which means all the EHRs on the blockchain are original and unmodified. We also tested the proof of work in our blockchain, hence making the records stored in the blockchain undeletable. This application can be extended to various other applications such as the third application stated above which is to show transparency with insurance or any other company. Another benefit could be to detect a fraud doctor; this can be achieved by having a group of professional doctors which authenticate the EHRs if the user wants them to be authenticated. In the authentication, the professional doctors hired will check why the respective medicine or test was given to the patient (the reason must be entered by the doctor who signs the EHR). If the reason given does not correspond with the test, the doctor can be sued for giving fake prescriptions

And as the Doctor sins the EHR himself, he has no reason to deny that he did not give an unrequired or false prescription. More discussions can be made on the searching system. The current algorithm uses the user-ID or the EHR number to search for a record. Research can be done to implement a query system in a blockchain hence also increasing the speed of the search made.

VII. CONCLUSION

Aiming to a trustworthy system for storing EHRs, A blockchain can be used as it meets all the requirements of the structure of a record; moreover, it also offers immutability and anonymity of the information. There is a need for this type of system as an EHR can be easily forged and people can use it to get free treatment, medicine or even use it to fake their medical holidays. Another problem is that different hospitals have different EHR for the same patient.

Our paper addresses this problem by implementing it on a third party blockchain eliminating the issue regarding trust, forgery and modification. And as a third party will have all the records, the patient can use these records for all the hospitals ensuring the same EHR is used everywhere.

REFERENCES

[1] Rui Guo, Huixian Shi, Qinglan Zhao, and

Dong Zhengi, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems", IEEE Access (Special Section on Research Challenges and Opportunities in Security and Privacy of Blockchain Technologies), pp. 11676-11686, 2018.

[2] Qi Liu, Kenli Li, "Decentration Transaction Method Based on Blockchain Technology", International Conference on Intelligent Transportation, Big Data & Smart City (ICITBS), pp. 416-419, 2018.

[3] Mingjun Dai, Shengli Zhang, Hui Wang and Shi Jin, "A Low Storage Room Requirement Framework for Distributed Ledger in Blockchain", IEEE Access, pp. 22970-22975, 2018.

[4] Mertz L, "(Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution", IEEE Pulse, vol. 9, no. 3, pp. 4-7, 2018.

[5] Matthias Mettler, "Blockchain technology in healthcare: The revolution starts here", IEEE 18th International Conference on e-Health Networking, Applications and Services (Healthcom), 2016.

[6] Florian Wessling and Volker Gruhn, "Engineering Software Architectures of Blockchain-Oriented Applications", IEEE International Conference on Software Architecture Companion, pp. 45-46, 2018.

[7] Huawei Zhao, Peidong Bai, Yun Peng and Ruzhi Xu, "Efficient key management scheme for health blockchain", CAAI Transactions on Intelligence Technology, vol. 3, no. 2, pp. 114-118, 2018.

[8] Kraff, D, "Difficulty control for blockchain-based consensus systems", Journal of Peer-to-Peer Networking and Applications, vol. 9, no. 2, pp. 397–413, 2016.

[9] Junichi Kishigami, Shigeru Fujimura, Hiroki Watanabe, Atsushi Nakadaira and Akihiko Akutsu, "The Blockchain-Based Digital Content Distribution System", IEEE Fifth International Conference on Big Data and Cloud Computing (BDCloud), pp. 187-190, 2015.

Zyskind G, Nathan O, Pentland A.S, "Decentralizing privacy: using blockchain to protect personal data", IEEE Security and Privacy Workshops, San Jose, CA, pp. 180-184, 2015