Healthcare information exchange using blockchain technology

A. Murugan, Tushar Chechare, B. Muruganantham, S. Ganesh Kumar
Department of Computer Science and Engineering, Faculty of Engineering and Technology,
SRM Institute of Science and Technology, Chennai, India

Article Info	ABSTRACT
	Current trend in health-care industry is to shift its data on the cloud, to increase availability of Electronic Health Records (EHR) e.g. Patient's medical history in real time, which will allow sharing of EHR with ease. However, this conventional cloud-based data sharing environment has data security and privacy issues. This paper proposes a distributed solution based on blockchain technology for trusted Health Information Exchange (HIE). In addition to exchange of EHR between patient and doctor, the proposed system is also used in other aspects of healthcare such as improving the insurance claim and making data available for research organizations. Medical data is very sensitive, in both social as well as legal aspects, so permissioned block-chain such as Hyperledger Fabric is used to retain the necessary privacy required in the proposed system. As, this is highly permissioned network where the owner of the network i.e. patient holds all the access rights, so in case of emergency situations the proposed system has a Backup Access System which will allow healthcare professionals to access partial EHR and this backup access is provided by using wearable IOT device.

Corresponding Author:

A. Murugan,
Department of Computer Science and Engineering,
Faculty of Engineering and Technology,
SRM Institute of Science and Technology,
Chennai, India.
Email: muruganaabap@gmail.com

1. INTRODUCTION
a. Motivation

User's in today's world expect seamless and instantaneous flow of data and many industries have already adopted and some are beginning to adopt necessary technologies to provide their user's with required information quickly and in a secured manner. Unfortunately, the healthcare industry has lagged behind to meet its users' expectations. Conventional systems are many times vulnerable to attacks, slow and have very little role for the patient [1]. The health data which is stored in conventional system are very difficult to share due to varying standards and data formats i.e. current healthcare ecosystem is ill-suited for the instantaneous needs of modern user. The primary objective of HIE system is to transmit health information on the far side geographical and institutional boundaries to supply a good and secure delivery mechanism [2]. We need to consider few factors with respect to this sharing mechanism.

a. Maintaining privacy in user data is very important and failure to this will result in implications related to financial as well as legal sectors.
b. In traditional data sharing system, it requires centralized source of data which increases the risk of data security and it also requires single trusted central authority.

In this centralised system, failure of central-storage will risk the storage of medical records of various patients. As data for each patient from various sources such as wearables, physicians, lab reports are increasing, HIE are under pressure to scale the infrastructure and support variety of data sources [3].

b.   Problem statement

Currently, in the traditional system Electronic Medical Record EMR's are stored in the centralized cloud-based database in which medical records remain largely un portable. Centralization increases security risks and requires trust in single authority. Regardless of controlled access and de-identification, centralized databases cannot guarantee integrity and data security. The disadvantages of current system are vital and thus cannot be ignored, which makes it necessary to develop a new solution for sharing EMR's which is more secured, reliable and should be able to handle all the data privacy, data redundancy and other security related issues related to Healthcare Information Exchange System.

c.   Use of blockchain in HIE system

In Healthcare Information Exchange System, various Healthcare entities like Doctor, Pharmacist, Medical Lab incharge and insurance company may have to submit transactions which may result in change in contents of the Electronic Medical Records (EMR) [4]. These EMR's are critical and highly sensitive patient's medical information which needs to secured. It requires that the participants performing transactions should be known and trusted by other participants [5]. Centralization does not guarantee integrity and data security so; this paper proposes a distributed solution to implements a HIE System to share EMR's between various entities present in the healthcare using Blockchain. Blockchain is a distributed ledger which is used for making logs and storing every transaction block in distributed ledger [2] i.e. whenever a participant performs a transaction on EMR's it will be recorded in the ledger. Blockchain depends on previously known cryptographic methods which will allow every node in the network to participate in the interaction (e.g. store information, exchange of information, and view that information), without having prior trust between the participants of the network. There is no central authority in a blockchain system instead, transaction blocks are recorded and distributed to all the peers in the network [6]. So, all participants in the network will know every interaction with blockchain and requires it to be verified before adding to the blockchain, which will enable trust-less interaction between the peers in the network [7]. The block once added to the blockchain can neither be deleted nor updated i.e. it is immutable.

In a blockchain based HIE, the patient has the ownership of the medical records, in contradiction to traditional architecture, where a central authority controls accesses and distributes data across network [8]. In this system medical record access is permitted to only limited healthcare entities (people or organizations). Data shared across the blockchain network enables near real time updates across all healthcare entities. Distributed ledger allows secure access to patient data [9]. Data redundancy is reduced as the same copy of data is available to all peers in network. Privacy and confidentiality in blockchain network is maintained by restricting few nodes to access data.

d.   Hyperledger fabric to support private data

The proposed system requires that some information to be private to some participants and should not be seen by other participants in the network, for e.g. the research organizations and insurance companies need not to know all the transactions in the network [10]. The other permissioned blockchain network requires that all participants should have same view of the distributed-ledger, which makes it difficult to support private data for various different participants whereas Hyper-ledger fabric provides a way to keep certain data/transactions confidential among a subset of members in network [11].

e.   Objectives of HIE system

Secure, immutable and decentralized EHR database with patient owing her / his own health data

Easy to share selective or all EHRs as consented by the patient

Full medical history of a patient at one single point

Easy verification of medical prescription

Redacted EHRs for research purposes

Increased transparency

No insurance fraud

2.   TECHNOLOGICAL DETAILS

Basic concept of hyperledger fabric

Fabric network is distributed permission based which requires its users to sign-up before using it. Using Hyperledger modelling and access control languages, permissioning on the network is controlled [12]. It is implementation of DIL (Distributed Ledger Technology) which provides Enterprise ready network scalability, security, performance and confidentiality in flexible blockchain architecture [13]. Like other blockchain's Fabric also has ledger which uses smart contract which is called as chaincode. Hyperledger

Fabric blockchain has configurable and modular architecture which enables optimization, innovation and versatility for different industrial use-cases [14].

Unlike other distributed ledger platform Hyperledger fabric allows smart contract to be written in various general purpose languages such as Go, Node.js and Java rather than using Domain-Specific Languages (DSL). Unlike other permission-less network, Fabric is fully permissioned platform; it means that, all the participants in the network are known to each other, rather than anonymous and therefore fully untrusted. Hyperledger Fabric allows new architecture called as execute-order-validate for transactions in the network [15]. This architecture overcomes various challenges faced by the order – execute - model like resiliency, flexibility, scalability, performance and confidentiality by separating the transaction flow into three steps: 1. Execute a transaction and check its correctness, 2. Order transactions using consensus protocol, 3. Before committing transactions to the ledger validate them against an application-specific endorsement policy. Hyperledger Fabric provides multi-layer permissions which allows owner of data to control which part of data is accessed [16].

2.1. Functionalities of Hyperledger Fabric
2.1.1. Identity management
Hyperledger Fabric enables permissioned network by providing membership identity services [17]. This service is responsible for managing user ID's and also authenticates all network participants.

2.1.2. Privacy and confidentiality
It allows competing businesses and a group that needs their transactions to be confidential and private to coexist on one network. Members of the network use private channel to maintain confidentiality and privacy in transactions [18]. A member who doesn't have access to the private channel won't be able to see channel information, transactions on that channel and members of it.

2.1.3. Chaincode functionality
Chaincode which is also called as smart contract manages business logic agreed by all the participants in the network [19]. It is basically a program written in programming languages such as Go, Java and node.js. This program runs on Docker container which is secured and isolated from other peer processes

2.1.4. Modular design
Hyperledger Fabric provides functional choice to network designers by implementing modular architecture [20]. It allows particular algorithms encryption, ordering and identity to be plugged into any fabric network. This results in universal architecture for blockchain which can be adopted by any public or industry domain with the guarantee that the network will be inter-operable across regulatory, market and geographical boundaries [21].

2.2. Hyperledger composer
Hyperledger Composer is a set of collaboration tools for building blockchain business networks that makes it simple and fast for business owners and developers to create smart contracts and blockchain applications to solve business problems. It supports existing Hyperledger fabric blockchain runtime and infrastructure, which support pluggable conscious protocol which ensures that transactions are validated according to the policy designed by participants of the business network.

3. SYSTEM DESIGN
3.1. System overview
The Figure 1 shows a system overview of personal healthcare information exchange system. It consist of following entities which included, namely patient, emergency contact, hospitals, insurance company, research organization, doctor, pharmacist and the patients private blockchain network.

3.2. HIE System Entities
3.1.1. Patient/user
Patient/User is the owner of the network and has complete control over his personal health data. Patient is responsible for revoking, granting and denying data access to the other peers in the network such as doctors, hospitals, insurance companies and research organizations [21]. While taking medical treatment from doctor's patient can share his Electronic Health Records with the doctor by granting read access rights and when treatment is completed patient can revoke access rights from doctor to decline further access to HER. Similarly, patient can grant, deny or revoke access to other peers connected in the network such as, research organizations, insurance companies. Besides this, the patient can record some personal information like daily health routine, allergies or any other related data which will in improving medical treatment.

3.1.2. Doctor/practitioner

Patient/User can appoint a healthcare professional such as doctor to give medical treatment or to perform some medical tests and give them access to his EHR's. When more than one doctor are involved in providing treatment to patient the doctor may request patient to give permission to other doctor / doctors to access patients medical records. The doctors can read previous blocks containing medical records and can add new block in the blockchain with current medical record after getting permission from the patient.

3.1.3. Health insurance company

Patient can allow Health Insurance Company to access their Electronic Health Records [22]. Insurance company in return can suggest a better insurance policy by analysing patients HER's. In addition to this the insurers will have a trusted source of healthcare data based on which they make better decisions [23].

3.1.4. Research organizations

Research organizations can request access for patient's medical history for medical research purposes. Patient's medical history will helps research organizations in improving health services, development of more effective diagnostics and treatments, insights into cause of diseases and identification of public health risks [23].
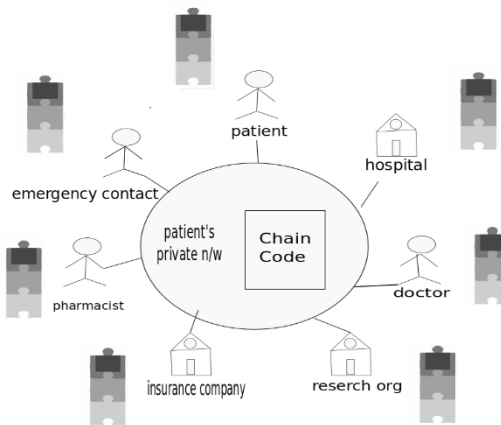

Figure 1. HIE system using blockchain

3.3. HIE system participants and permissions

Table 1 show the Health Information Exchange system participants and permissions.

Table 1. HIE system participants and permissions

SR. No.	Participant	Permissions
1	Practitioner / Doctor	- Request Read or Write permission on EHRs - Request Read or write permission for other practitioners to access HER - Read HER
2	Patient / User	- Give permission to Practitioner or doctor to read or write HER - Revocation of read or write permission from practitioner or doctors - Permit emergency contact to read or grant permission
3	Research organization	- Read permissioned EHRs
4	Insurance Company	- Read permissioned EHRs

3.4. Goals

The main goal of this proposed system is to provide a way to store and share the health information in more secured and effective manner [24]. The patient's EHR must be consistent, available when needed and only patient should control the terms of its access. The secondary goal is to share the EHR in such a way that its structure and the meaning must be easily understandable to improve data utilization which will result in good patient care.

3.5. Backup access system

The proposed system is to be implemented using Hyperledger fabric which is highly permissioned blockchain where all the access rights of EMRs are with owner of the network i.e. Patient. However, in the case of an emergency and with the patient unable to give access his medical records, there must be an ability to view certain information in order to provide the best possible care. So in the proposed system a backup access system is provided in order to gain partial access to patient's Electronic Medical Records. This can be done using wearable IOT device [25]. The medical representatives can scan IOT device in case of emergency situation to gain access to critical healthcare information like blood group, allergies, age, and critical decease information. This would enable doctors to provide the best care possible to a patient in an emergency situation.

4.   CONCLUSION

This work proposes aBlockchain enabled Healthcare Information Exchange system which will provide solution to various challenges such as integrity, data interoperability and Integration of blockchain in HIE will allow access to historic and authentic healthcare data. In addition to this the proposed system is also used in other aspects of healthcare such as improving the insurance claim and making data available for research organizations.

REFERENCES

[1]   X. Zhang, "Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR),"*2018 IEEE International Conference on Communications (ICC)*, 2018.
[2]   R. J.Krawiec, *et al*., "Blockchain: Opportunities for health care," 2016.
      Available: https://www2.deloitte.com/us/en/pages/public-sector/articles/blockchain-opportunities-for-health-care.html.
[3]   X. Liang,*et al*., "Integrating blockchain for data sharing and collaboration in mobile healthcare applications,"*2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, 2017.
[4]   C. Esposito,*et al*., "Blockchain: A Panacea for Healthcare Cloud-Based Data Security and Privacy?" *IEEE Cloud Computing*,vol. 5, pp. 31-37, 2018.
[5]   Whitepaper,"Medicalchain," 2018. Available: https://medicalchain.com/en/whitepaper/
[6]   "Hyperledger Fabric - Introduction," Available: https://medium.com/coinmonks/hyperledger-fabric-introduction-2282e955ca6e.
[7]   "Hyperledger Fabric A Blockchain Platform for the Enterprise," Available: https://hyperledger-fabric.readthedocs.io/en/release-1.2/
[8]   F.Benhamouda,*et al*., "Supporting Private Data on Hyperledger Fabric with Secure Multiparty Computation,"*2018 IEEE International Conference on Cloud Engineering*, 2018.
[9]   "Hyperledger Fabric Functionalities," Available: https://hyperledger-fabric.readthedocs.io/en/release-1.2/functionalities.html.
[10] White Paper, "Blockchain for Healthcare," 2018.
      Available: https://www.ehidc.org/sites/default/files/resources/files/blockchain-for-healthcare-341.pdf.
[11] L. Mertz, "(Block) Chain Reaction: A Blockchain Revolution Sweeps into Health Care, Offering the Possibility for a Much-Needed Data Solution," *IEEE Pulse*,vol. 9, pp. 4-7, 2018.
[12] K. Peterson, *et al*., "A Blockchain-Based Approach to Health Information Exchange Networks,"Available: https://www.healthit.gov/sites/default/files/12-55-blockchain-based-approach-final.pdf.
[13] A. Murugan, Tushar Chechare, B. Muriganantham, S. Ganesh Kumar, Healthcare Information Exchange (HIE) Using Hyperledger Fabric Blockchain",Volume 11 | 05-Special Issue, Pages: 1420-1424.
[14] AlevtinaDubovitskaya, [1,2] Zhigang Xu, [3] Samuel Ryu, [4] Michael Schumacher, and Fusheng Wang, [5] Secure and Trustable Electronic Medical Records Sharing using Blockchain, AMIA AnnuSymp Proc. 2017; 2017: 650–659.
[15] Ariel Ekblaw , Asaph Azaria , John D. Halamka, , Andrew Lippman,A Case Study for Blockchain in Healthcare: "MedRec" prototype for electronic health records and medical research data, White Paper, Augut 2016.
[16] Office of the National Coordinator for Health Information Technology. (2015). Version 1.0. "Connecting Health and Care for the Nation: A shared nationwide interoperability roadmap." [Online] Available: https://www.healthit.gov/sites/default/files/hie-interoperability/nationwide-interoperabilityroadmap-final-version-1.0.pdf
[17] "About the Epidemic." U.S. Department of Health & Human Services. [Online] Available: http://www.hhs.gov/opioids/about-the-epidemic/. Accessed Aug. 4, 2016.
[18] "Research We Support." Patient-Centered Outcomes Research Institute (pcori). [Online] Available: http://www.pcori.org/research-results/research-we-support. Accessed Aug. 4, 2016.
[19] "Precision Medicine Initiative Cohort Program." National Institutes of Health. [Online] Available: https://www.nih.gov/precision-medicine-initiative-cohort-program. Accessed Aug. 4, 2016.

[20] "Fact Sheet: President Obama's Precision Medicine Initiative." The White House Briefing Room. Jan. 30, 2015. [Online] Available: https://www.whitehouse.gov/the-press-office/2015/01/30/fact-sheetpresident-obama-s-precision-medicine-initiative.

[21] Forrest P. Blockchain and non financial services use cases.
Linkedin. 2016. https://www.linkedin.com/pulse/blockchain-non-financial-services-use-cases-paul-forrest.
Accessed May 28, 2017.Google Scholar

[22] Tapscott D, Tapscott A. The impact of the blockchain goes beyond financial services.Harvard BusinessReview. 2016. https://hbr.org/2016/05/the-impact-of-the-blockchain-goes-beyond-financial-services.
Accessed January 25, 2017.Google Scholar

[23] Popper N. Business giants to announce creation of a computing system based on Ethereum.The New York Times. 2017. https://www.nytimes.com/2017/02/27/business/dealbook/ethereum-alliance-business-banking-security.html. Accessed March 1, 2017.Google Scholar

[24] Belinky M, Rennick E, Veitch A. The Fintech 2.0 Paper: rebooting financial services.Santander InnoVentures. 2015. http://santanderinnoventures.com/wp-content/uploads/2015/06/The-Fintech-2-0-Paper.pdf.
Accessed March 1, 2017.Google Scholar

[25] Mettler M. Blockchain technology in healthcare: the revolution starts here.IEEE 18th International Conference on e-Health Networking, September 14–16, Piscataway, NJ: IEEE, 2016.
http://ieeexplore.ieee.org/stamp/stamp.jsp?arnumber=7749510. Accessed March 3, 2017