Chapter

Blockchain-Based Medical Record Management with Biofeedback Information

Hui Li Wang, Shao-I Chu, Jiun-Han Yan, Yu-Jung Huang, I-Yueh Fang, Shu Ya Pan, Wei-Cheng Lin, Chao-Tien Hsu, Chih-Lung Hung, Tzung-Ching Lin and Te-Tsun Shen

Abstract

Blockchain is a new emerging technology of distributed databases, which guarantees the integrity, security and incorruptibility of data by means of the cryptography. Such features are suitable for secure and reliable data storage. This chapter investigates the blockchain-based architecture with applications to medical health record or biofeedback information management. This framework employs the smart contract to establish a medical record management system to ensure the privacy of patients. Moreover, the blockchain technique accelerates the medical record or information exchange such that the cost of human resource is significant reduced. All patients can manage their individual medical records and information easily in the different hospitals and clinics. They also have the privilege to deal with and authorize personal medical records in the proposed management framework.

Keywords: blockchain, medical record, security, privacy

1. Introduction

The conventional medical record systems face the complicated administration procedure for data processing to ensure patients' privacy, leading to the enormous waste of human resources. Such an architecture is obviously inefficient for the medical record exchange. Blockchain technique [1] has recently been adopted to secure medical data sharing and management. The cryptographic property in the blockchain networks guarantees the patients' privacy. Data integrity and incorruptibility protect medical data from being tampered. The blockchain can be viewed as a distributed database, which stores data in each network nodes to avoid the halting problem. It thus provides higher stability, consistency and attack-resistance. The problem of distributed denial-of-service attacks (DDOS) in the conventional centralized framework can be solved by the blockchain technique. Deployment of blockchain in the medical record system not only provides the reliable service but also speeds up the medical record exchange. Owing to decentralization, the ownership of the medical record is returned to the patients, allowing them to manage the medical record directly and take care of their own health.

Biofeedback is a technique that uses electrical sensors to measure human body functions such as blood pressure and heart rate. Biofeedback aims to help learn your body condition and how it works. You may have biofeedback training in clinics, medical centers and hospitals. These measurements or data about biofeedback are thus important for the future therapy. Such data storage or management is therefore required and may be integrated with the medical record system.

In this chapter, we investigate the blockchain-based medical record management systems in the literatures. The new medical record framework is thus proposed and implemented on an open-source platform, Ethereum. Note that Ethereum platform allows anyone to develop applications in blockchain networks. The Ethereum virtual machine (EVM) executes the smart contract on the virtual machine. With the aid of the smart contract, developers are able to put these codes on the blockchain. The codes will be automatically executed after the blockchain establishment. The medical record management system is developed by exploiting the smart contract. The aim of the level of health care will be achieved in the proposed architecture via the smart contracts.

2. Literatures surveys

Authors in [2] presented the MedRec system, a decentralized medical record management system based on blockchain technology. There are three types of Ethereum smart contracts to associate patients' medical data to allow third-party users to access the data. Yang *et al.* [3] further presented an attribute-based authentication mechanism on the MedRec system to enable the secure sharing of medical data. A high-level blockchain-based framework was designed in [4], where an identity-based authentication and key agreement protocol is applied to achieve user membership authentication. They also developed the MedShare [5] system to provide data provenance and control in cloud repositories among hospitals. Liang *et al.* [6] used the hyperledger fabric membership service and channel formation scheme to guarantee data privacy in a blockchain network for medical data sharing. The mobile application was also implemented to collect data from wearable devices for storage and sharing with healthcare providers. Patientory [7] is a peer-to-peer medical record data storage network. The software framework in [7] was presented to address the authentication, authorization, access control, data encryption interoperability enhancement and token management.

Authors in [8] proposed the MedChain system, where the timed-based smart contracts can interact with the various demands of health providers, patients and third parties. An incentive mechanism in [8] was also presented to leverage the degree of health providers about their efforts on maintaining medical records. In [9], an attribute-based signature scheme with multiple authorities was designed. There are multiple authorities without a centralized one to generate and deliver public/private keys of the patient, avoiding the escrow problem. Liu *et al*. [10] presented a healthcare insurance anti-fraud system based on blockchain. A hybrid architecture to facilitate access control of medical data was developed in [11]. A blockchain is used to manage identity and access control and acts as a tamper-proof log of access events. Hasavari *et al*. [12] introduced a combination of secure file transfer methods and blockchain techniques as a solution to record patient's emergency medical data such that ambulance crews can access and use it to provide high quality pre-hospital care.

3. Proposed Ethereum-based framework for medical record management

Instead of using the traditional centralized databases, the Ethereum-based blockchain is applied to our designed system framework of medical record management to ensure the security of data. The medical records are stored within individual nodes in the blockchain networks by utilizing the smart contracts. The automatic smart contracts for the administration procedure are also designed with an aim to reducing the waste of human resource and speeding up the medical process.

The presented medical record management system is essentially rooted in the Ethereum-based blockchain architecture. The management framework is developed and established based on the relationship among the smart contracts. The proposed architecture is modified from the framework in [2]. The whole system is viewed as a private blockchain network, where all medical records are stored to guarantee data security, privacy and integrity. Innovatively combined with the data exchange mechanism in [13], the user identity is directly recognized by the system and the corresponding privilege is authorized to ensure data integrity in the blockchain networks.

3.1 Blockchain-based medical record management system

Figure 1 illustrates the proposed medical record management system with smart contracts. There are three types of smart contracts, including registrar contract, patient-provider relationship contract and summary contract.

3.1.1 Registrar contract (RC)

Similar to [2], this contract maps member identification strings to the Ethereum address identity. All the registered members are divided into two groups, patients and medical personnel. Each identity has different access rights for the proposed system.

Authorized privilege of patients:

a) Review their own medical records. b) Authorize their own medical records.

Authorized privilege of the medical personnel:

a) Create/modify the authorized medical records. b) Review the authorized medical records. Notice that different kinds of the medical personnel has different authorized or restricted rights.

3.1.2 Patient-provider relationship contract (PPR)

Each PPR smart contract is a medical certificate. The PPR smart contract is utilized to record the current situation of medical records, details of diagnosis and the access permission of different summary contracts. Sometimes other relevant PPR diagnostic address information will also be included. All summary smart contracts must be licensed by the owner of the PPR contract to access the PPR smart contract.

As shown in **Figure 2**, the medical personnel will be allowed to modify or read only based on the access right in the summary contracts after getting the permits. Moreover, the administration system can track the current diagnosis by the assistance of the PPR contract.

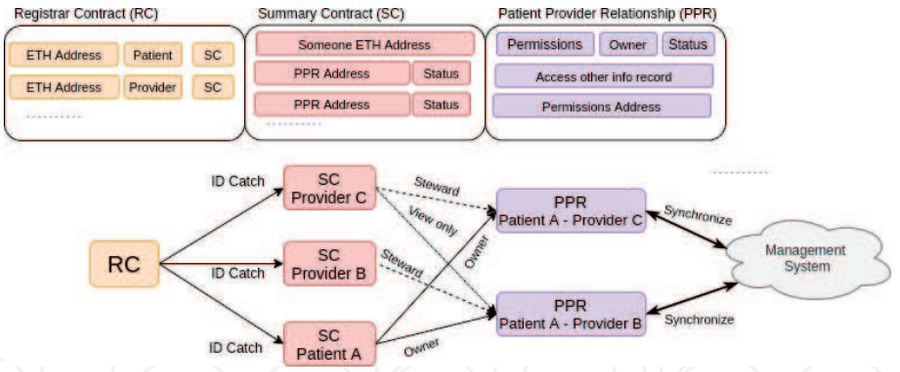

Figure 1.
Proposed smart contract-based medical management system.

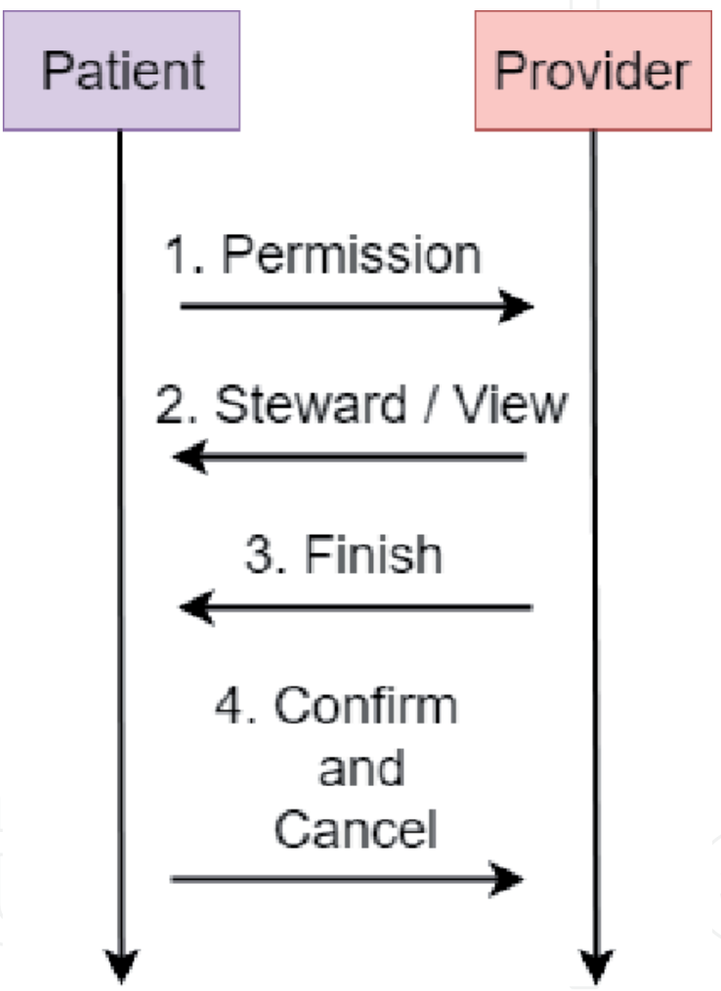

Figure 2.
Authorization procedure of getting medical record permission.

3.1.3 Summary contract (SC)

This contract holds a list of references to PPRs, locating patients' medical record history. The patient-oriented medical record classification structure in the proposed system is designed. Each record is viewed as an PPR smart contract. The proposed medical record structure is shown in **Figure 3.**

3.2 Private blockchain network

The deployment of the private blockchain network is illustrated in **Figure 4**, which is applied for the level of care. The main private blockchain network is plotted

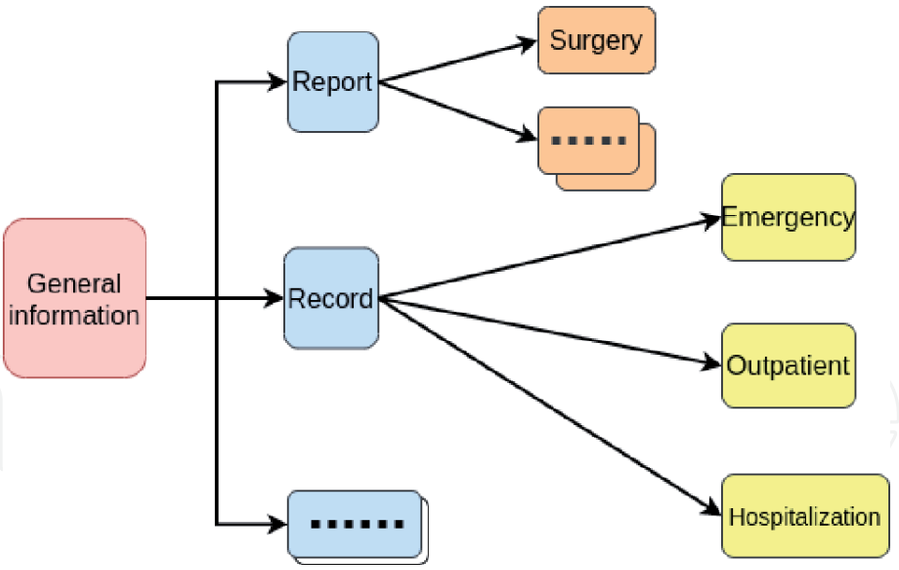

Figure 3.
Proposed personal medical record.

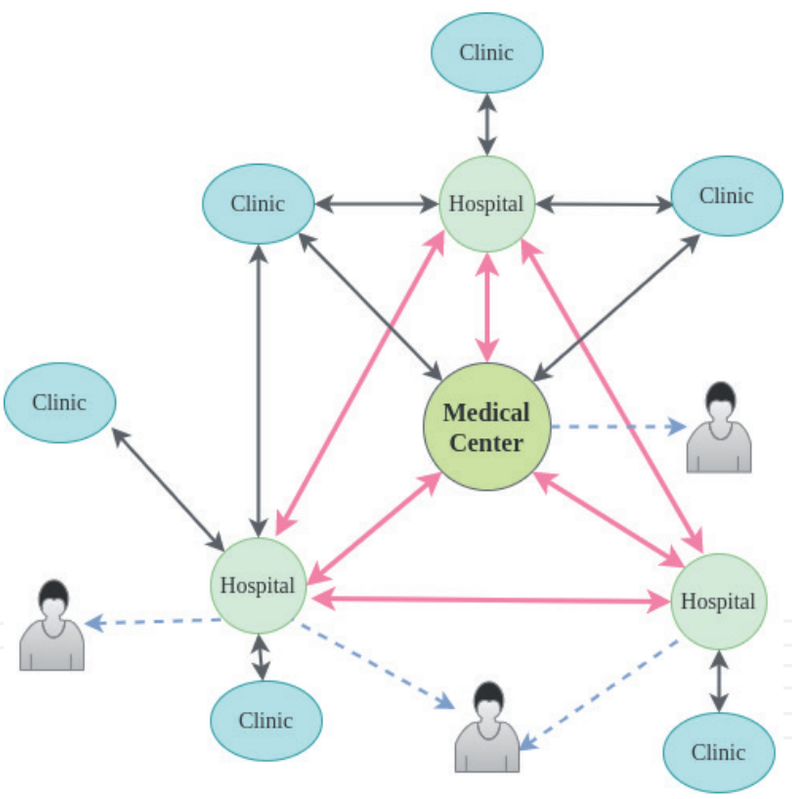

Figure 4.
Deployment of private blockchain.

by the solid lines. The critical network devices are maintained by the medical centers or hospitals, and the distributed databases among them must be synchronized. The clinics only need to synchronize with the nearby blockchain network nodes to ensure their database stay latest and correct.

Dotted lines stand for the data requests to the blockchain network from patients whom made inquiry for medical record. In this case, the main blockchain network nodes (e.g. the medical center or hospital) are responsible to deal with the requests since their network equipments are capable of handling the heavy network traffic due to plenty of requests. As a primary node in blockchain network, the synchronization speed and correctness should be guaranteed.

3.3 System workflow

How the proposed management system works is presented in **Figure 5**.

3.3.1 New entry

The medical personnel uploads the diagnosis to provider B Node.

3.3.2 External process and outside process

The external management system detects the updates from the blockchain databases, automatically validates the latest data and notifies the patients of the new updates.

3.3.3 Update nodes

The blockchain network automatically synchronizes all nodes and offers the latest information to the patient node.

3.3.4 Notification from provider B

The patient will be notified by the information about who updated the medical record and then checks these updates.

3.4 Limitations

With the blockchain-based technique for distributed databases, the additional network facilities and storage devices for network nodes are required to stabilize the whole system. However, it helps save human resource, reduce human errors and accelerate administration process.

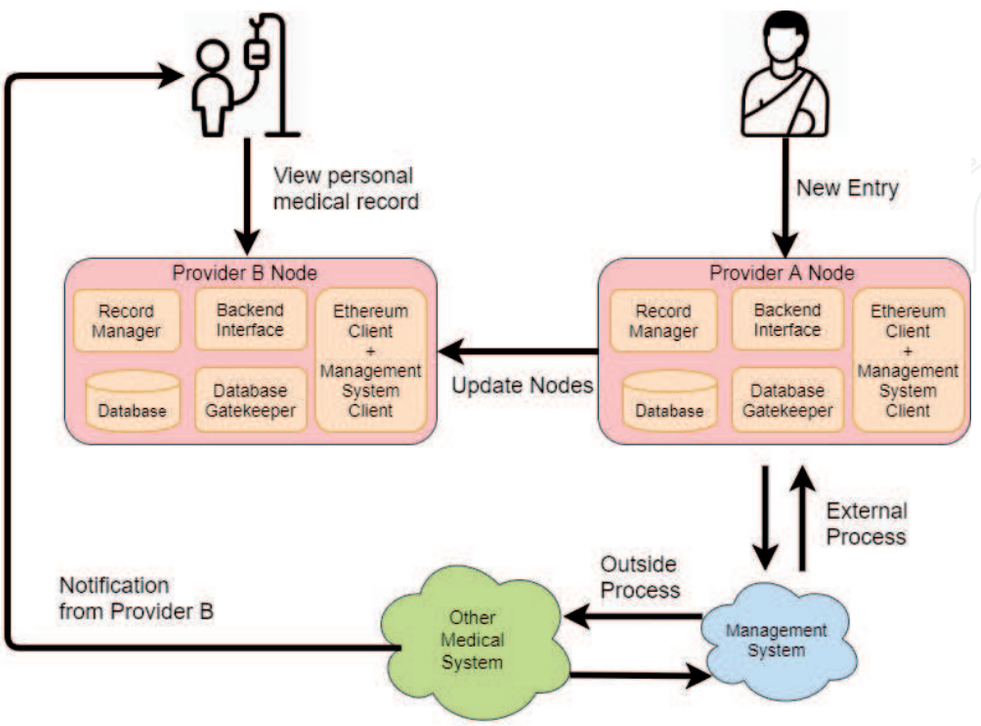

Figure 5.
System workflow.

DOI: http://dx.doi.org/10.5772/intechopen.94370

Research work	**MedRec [2]**	**MedRec++ [3]**	**BBDS [4]**	**MeDShare [5]**	**Liang *et al.* [6]**	**Patientory [7]**	**BSPP [14]**	**Proposed**
Identity management	v	v	v	v	v	v	v	v
Data authenticity	v	v	v	v	v	v	v	v
Data encryption	—	v	—	—	—	v	v	v
Blockchain type	Public	Public	Consortium	Consortium	Consortium	Consortium	Hybrid	Public
Smart contract	v	v	—	v	—	v	—	v
Data storage	Off-chain	Off-chain	Cloud	Cloud	Off-chain	Off-chain	Off-chain	Cloud

Table 1.
Comparison with frameworks.

Properties	MedChain [8]	MedRec [2]	MeDShare [5]	Amofa *et al.* [15]	Ancile [16]	FHIRChain [17]	Proposed
Access control	v	v	v	v	v	v	v
Privacy preservation	v	v	v	v	v	v	v
Healthcare legislation	v	v	v	v	v	v	v
Smart contracts	v	v	v	v	v	v	v
Timed-based smart contracts	v	—	—	v	—	—	v
Notification based smart contract	v	v	—	—	v	v	v

Table 2.
Comparison with other frameworks.

3.5 Comparison with other frameworks

Table 1 compares the proposed medical record management framework with the existing architectures based on blockchain techniques. Security metrics (identification, data authenticity, data encryption), architecture metrics (blockchain type, data storage) and functionality metrics (smart contract) are all taken into consideration.

Table 2 also surveys the existing systems. The proposed framework verifies legitimate users before performing the registration process, check the identity to ensure that personal information is only given to authorized users.

4. Conclusions

This chapter investigated the blockchain-based and patient-oriented medical record system with the smart contract on EVM. In the future, the drug pedigree may be included into the blockchain. The drug traceability is thus carried out for efficient management and control.

Acknowledgements

This work was supported by Intelligent Medical Center of E-DA Healthcare Group under Grants EDAH-AI-107-010.

Author details

Hui Li Wang[1], Shao-I Chu[2*], Jiun-Han Yan[2], Yu-Jung Huang[3], I-Yueh Fang[1], Shu Ya Pan[1], Wei-Cheng Lin[4], Chao-Tien Hsu[5], Chih-Lung Hung[6], Tzung-Ching Lin[6] and Te-Tsun Shen[7]

1 Medical Record Section, E-DA Hospital, Kaohsiung, Taiwan

2 Department of Electronic Engineering, National Kaohsiung University of Science and Technology, Kaohsiung, Taiwan

3 Department of Electronic Engineering, I-Shou University, Kaohsiung, Taiwan

4 Medical Research Department, E-DA Hospital, Kaohsiung, Taiwan

5 Department of Pathology, E-DA Hospital, Kaohsiung, Taiwan

6 Administrative Center, E-DA Hospital, Kaohsiung, Taiwan

7 E-DA Healthcare Group Executive Committee, Kaohsiung, Taiwan

*Address all correspondence to: erwinchu@nkust.edu.tw

References

[1] H. Jin, Y. Luo, P. Li and J. Mathew, "A Review of Secure and Privacy-Preserving Medical Data Sharing," in IEEE Access, vol. 7, pp. 61656-61669, 2019, doi: 10.1109/ACCESS.2019.2916503.

[2] A. Azaria, A. Ekblaw, T. Vieira and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," 2016 2nd International Conference on Open and Big Data (OBD), Vienna, 2016, pp. 25-30, doi: 10.1109/OBD.2016.11.

[3] H. Yang and B. Yang, "A blockchain-based approach to the secure sharing of healthcare data", Proc. Norwegian Inf. Secur. Conf., pp. 1-12, 2017.

[4] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa and X. Zhang, "BBDS: Blockchain-based data sharing for electronic medical records in cloud environments", Information, vol. 8, no. 2, pp. 44, 2017.

[5] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain", IEEE Access, vol. 5, pp. 14757-14767, 2017.

[6] X. Liang, J. Zhao, S. Shetty, J. Liu and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications", Proc. IEEE 28th Annu. Int. Symp. Pers. Indoor Mobile Radio Commun. (PIMRC), pp. 1-5, Oct. 2017.

[7] C. McFarlane, M. Beer, J. Brown and N. Prendergast, Patientory: A Healthcare Peer-to-Peer EMR Storage Network v1, Addison, TX, USA:Entrust, 2017.

[8] E. Daraghmi, Y. Daraghmi and S. Yuan, "MedChain: A Design of Blockchain-Based System for Medical Records Access and Permissions Management," in IEEE Access, vol. 7, pp. 164595-164613, 2019, doi: 10.1109/ACCESS.2019.2952942.

[9] R. Guo, H. Shi, Q. Zhao and D. Zheng, "Secure Attribute-Based Signature Scheme With Multiple Authorities for Blockchain in Electronic Health Records Systems," in IEEE Access, vol. 6, pp. 11676-11686, 2018, doi: 10.1109/ACCESS.2018.2801266.

[10] W. Liu, Q. Yu, Z. Li, Z. Li, Y. Su and J. Zhou, "A Blockchain-Based System for Anti-Fraud of Healthcare Insurance," 2019 IEEE 5th International Conference on Computer and Communications (ICCC), Chengdu, China, 2019, pp. 1264-1268, doi: 10.1109/ICCC47050.2019.9064274.

[11] S. Hasavari and Y. T. Song, "A Secure and Scalable Data Source for Emergency Medical Care using Blockchain Technology," 2019 IEEE 17th International Conference on Software Engineering Research, Management and Applications (SERA), Honolulu, HI, USA, 2019, pp. 71-75, doi: 10.1109/SERA.2019.8886792.

[12] H. Guo, W. Li, M. Nejad and C. Shen, "Access Control for Electronic Health Records with Hybrid Blockchain-Edge Architecture," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, 2019, pp. 44-51, doi: 10.1109/Blockchain.2019.00015.

[13] N. Nchinda and A. Cameron, "MedRec: A Network for Personal Information Distribution", International Conference on Computing, Networking and Communications (ICNC), pp. 637-641, 2019.

[14] A. Zhang and X. Lin, "Towards secure and privacy-preserving data sharing in e-health systems via

consortium blockchain", J. Med. Syst., vol. 42, no. 8, pp. 140, 2018.

[15] S. Amofa, E. B. Sifah, K. O.-B. O. Agyekum, S. Abla, Q. Xia, J. C. Gee, et al., "A blockchain-based architecture framework for secure sharing of personal health data", Proc. IEEE 20th Int. Conf. e-Health Netw. Appl. Services (Healthcom), pp. 1-6, Sep. 2018.

[16] G. G. Dagher, J. Mohler, M. Milojkovic and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology", Sustain. Cities Soc., vol. 39, pp. 283-297, May 2018.

[17] P. Zhang, J. White, D. C. Schmidt, G. Lenz and S. T. Rosenbloom, "FHIRChain: Applying blockchain to securely and scalably share clinical data", Comput. Struct. Biotechnol. J., vol. 16, pp. 267-278, Jul. 2018.