Blockchain for Interoperability in Healthcare

Zay Soe
University of Computer Studies
Yangon, Myanmar
zaysoe@ucsy.edu.mm

Win Lelt Lelt Phyu
University of Computer Studies
Yangon, Myanmar
wllphyu@ucsy.edu.mm

Abstract— **Nowadays, most of the data is stored on the centralized cloud and needed to share data in secure ways for both private and public sectors. Data utilization is as important as data security in organizations. Many applications in Myanmar are currently supporting for Healthcare services but there are some issues to solve enthusiastically: (1) less of emphasize on data security and (2) Electronic Health Records (EHR) interoperability between healthcare providers and patients. The Blockchain technology is in its early stages of development with applications across various service sectors such as financial services, supply chains, automobile industry, Healthcare, etc. The application of Blockchain technology improves the standard of Service Providers and accessibility of information against privacy leaks and unauthorized changes. This article aims to offer the architecture of Blockchain for secure health data decentralization and transparency.**

Keywords—Blockchain, eHealth, Healthcare, EHR, Interoperability

I. INTRODUCTION

A blockchain is based on shared and distributed ledger of transactions and records. The blockchain infrastructure has no central authority. Today financial, businesses and healthcare applications are engaged with cloud and IoT security.

Ownership and the sharing of medical records is another contentious matter. Medical records can be in structure or unstructured form. The medical health record should be uniformity and readily accessible across various institutional partners, and the access to this information should be controlled by the patient [1, 2].

Sharing health data must be exchanged in a secure manner and with reliable infrastructure, as there are many risks associated with privacy, security, and interoperability. First, medical data is extremely privacy sensitive. Especially since so much health data is stored in the cloud. Therefore, the challenge of sensitive data exposure and leakage is increasing. Second, centralized architectures are widely used in current systems and security mechanisms. Therefore, it is difficult to effectively integrate interoperability between distributed healthcare systems. Additionally, the inability of users to access their private health data is also a major challenge [3].

Our motivation under this research is to provide greater transparency and accessibility of Patient Information, development of exchanging information between Health Facilities, Clinics and Laboratories, and patients with blockchain technology.

In this paper, an architecture of blockchain is implemented for Patient Data and sharing this information with cross-providers in healthcare. The system explores the blockchain and interoperability to improve healthcare services.

The subsequent sections of the paper are structured as follows: Section II Blockchain Architecture features and Types, Section III How to apply Blockchain with Big Data,

IoT and eHealth in Healthcare sectors, Data Security and Privacy, Section IV the Current Architectures of Healthcare Systems, challenges and the Proposed System. Finally, Section V wrap up the paper and outlines potential avenues for future research and exploration.

II. BLOCKCHAIN ARCHITECTURE FEATURES AND TYPES

As mentioned in introduction, the blockchain is openness, distributed ledger that can store transactions between two providers. A blockchain is a series of immutable and secured data blocks which has no single owner.

A private blockchain is permission based blockchain. It controls with access policy in the organization and has no chance of minor collision. In a private blockchain, the transaction cost and data redundancies are reduced. A public blockchain is permission-less blockchain. Anyone can join the P2P network and data access within the blockchain. It is decentralized and there is no central authority which monitor the network. In the public blockchain, data is secure as it uses cryptography and signature to store data in blockchain. The following features of the blockchain architecture are:

- Decentralization with Shared Ledger
- Immutability
- Transparency
- Consensus Mechanism
- Smart Contracts

III. RELATED WORK

This section will describe the different approaches for Healthcare and security with Big Data and Internet of Things (IOT) technologies.

A. Big Data in Healthcare

The utilization of big data in healthcare allows us to predict outbreaks, advance disease treatments, enhancements in quality of life, and prevent avoidable deaths. This information is directly sent to our doctor through a lot of wearable devices, as part of their diagnostic process. Increased data collection allows doctors to provide treatment recommendations based on data from other patients with similar symptoms, genetic factors, and behaviors [7, 8].

B. IoT in Healthcare

IoT-enabled smart healthcare systems primarily process patient information and personal outcomes. Thus, this data is highly susceptible to malicious attacks unless protected by advanced and robust security measures [11].

Unfortunately, the majority of smart devices and sensors used in the smart healthcare field have limited resource capacity and are characterized by low processing and memory capabilities. Therefore, it is difficult to integrate comprehensive security protocols into these devices. [12, 13].

Furthermore, these devices are mobile and connect to public network in nature. This vulnerability is further exacerbated by the variety of environments in which these devices are deployed, including hospitals, homes, and offices. With the exponential growth of interconnected IoT devices, building dynamic and robust security mechanisms can be a daunting endeavor [14, 15].

For example, a patient's health development record is confidential and needs protection to prevent the spread of the information to unauthorized groups [16].

C. The Application of Blockchain in eGovernment

The Blockchain can be utilized in eGovernment Systems. Some country tries to improve the government services with Blockchain Technology such as China. The domain where Blockchain technology finds application in government services has advantages for data quality, services, exchanging information between government organizations. In 2016, the Chinese government published a white paper on the development and application of blockchain technology in China. This white paper has a typical discussion with the core technology of blockchain applications, standardizing technology development and using blockchain in various sectors of China [16].

In the Proposed system section, the discussion focused on providing Electronic-Health (eHealth) using Blockchain technology. Another issue for healthcare sector is patients' medical records, sensitive information and data ownership. The next discussion is a set of related problems that covers Data Security and Privacy.

D. Decentralised Protection of Personal Data

Blockchain technology has three contributors: users, companies / organizations that provide services, and blockchain. Blockchain includes two categories of transactions: access transactions and data transactions. These transaction types facilitate access control management, data storage, and data retrieval processes. The subscriber accepts the permission configuration, which is a data policy, and registers with the blockchain network. Users can use digital signatures or shared keys with public and private keys by accessing the data in the blockchain [15].

IV. BLOCKCHAIN BASED HEALTHCARE SYSTEM

A. The Architecture of current Healthcare Systems

In healthcare system, there are private health facilities use the Enterprise Resource Architecture and Hospital Management Information System and privately store their data. Under health facilities, it includes clinics, hospitals and health departments. On the other hand, the public government health facilities separate data storage and handling data management. The cloud-based applications in healthcare uses separate data storage and diverse architecture for recording patient information and medical records.

The "Fig. 1" shows the current healthcare systems, patients and sharing information. There are three cloud-based data storage. The current healthcare systems provide centralized data management and analysis techniques in their own ways. The main issue of healthcare sector is how to identify patient and how to retrieve the patient information and medical records between healthcare providers. In Myanmar,

the Ministry of Health and Sports is trying to solve this issue with Master Patient Index (MPI). MPI is the unique identifier value for individual patients. Another challenges we face related with the current systems are as follows:

1) *Data Security for medical and sensitive information*
2) *Data Sharing between trusted organizations*
3) *Digital Identity Signature for Patients*

In the next section, the proposed system describes the architecture to address the aforementioned issues and challenges using Blockchain technology.
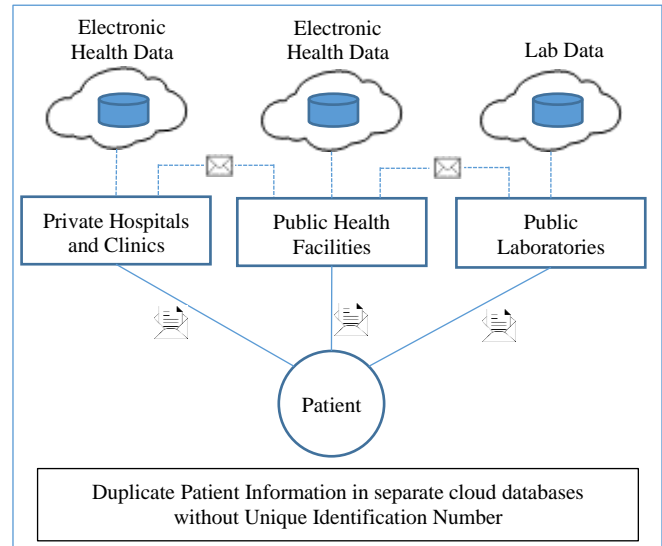

Fig. 1. Architecture of the Current Healthcare Systems

B. The Proposed System

Electronic Health and medical records and data sources are very complex and diverse in facility areas, such as clinics, hospitals and laboratories. Besides, private and public healthcare facilities have different data capture formats and own privacy.

In the research secure sensitive patient information is provided, and interoperability between healthcare providers is achieved using blockchain technology without impacting data ownership. In "Fig. 2", there are 3 stakeholders, Health Facilities (private/public hospital and clinics), Laboratories and Patients. Health facilities include private and public hospital, clinics and departments. We consider Decentralized data logs, protect individuals' identities and data, and quick transfers.

- Data Access Layer is responsible for maintaining the Electronic Health Data with separated cloud databases. This is the clear of ownership for records. Each database system has own EHR formats.

- Blockchain Network Layer is a distributed transaction ledger in P2P network. The node (Patient, Health Facility) is needed to register to enter the blockchain network via Proof-of-Work. When the patient visits to a health facility, the confirmed transaction signed by the patient is broadcasted to all of the nodes in the blockchain network. Each node will verify and then the transaction node is added to the blockchain network.

- Applications with API Layer is cross-exchange information Electronic Health Records with the links

in the blockchain between trusted organizations. To exchange information the API and some metadata will be provided in the blocks of the blockchain network.
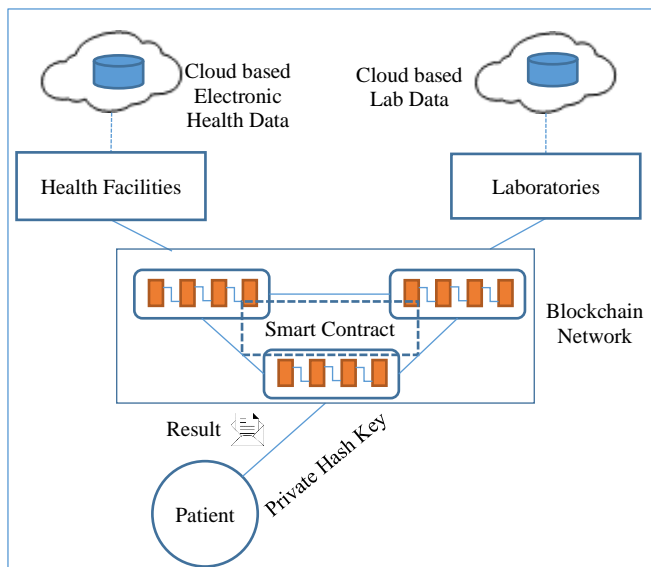

Fig. 2. Our proposed architecture with Blockchain

Distributed block ledger includes Patient Identity (the digital signature of patient), Facility and Result, Test Date, hash value, etc. are stored on a Blockchain. The related medical records are recorded in separate facilities' cloud. A Patient must be registered in Blockchain network before clinical trials. The patient's metadata transactions are kept in blockchain on every visit to health facility and laboratory. Healthcare providers interoperates by passing secure Blockchain Virtual Machine. Result is verified by users of HER networks and it is digitally signed agreements between patients and healthcare providers which relies on a consensus mechanism.

The system is proposed with blockchain technology for interoperability and patient's signed contracts. In the context of a consensus mechanism, the computationally intensive and energy-consuming proof of work is implemented by the involvement of a trusted organization. and patients who must sign the transaction block as valid. For scalability concerns, the blockchain is kept as the distributed ledger.
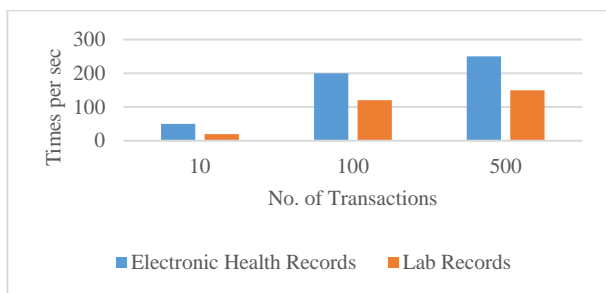

Fig. 3. Comparison of throughput among EHR and Lab Records

C. Discussion and Evaluation

Using the proposed system, there are some benefits to the eHealth environment. Firstly, this system solves the data ownership issue between patients and separate healthcare providers. The healthcare providers can manage their own data. Secondly, the patients can retrieve their medical health records with digital signature. The metadata blockchain supports secure interoperability between healthcare providers. Finally, this system solves the cost of blockchain consensus mechanism with patients' digital signature.

V. DISTRIBUTED CONCLUSION

The Blockchain offers huge opportunities for developing applications and research in many sectors. This technology supports distributed ledger and the public Peer-to-Peer network, cost effective using smart contract and sharing secure transactions and exchanging medical data. The patients and providers can access the health information. During this study, sample electronic Health records and lab results are tested on blockchain network in "Fig. 3". In the next study, load and performance testing is important for blockchain-based systems because of large amounts of records. This system can be adopted with the Blockchain data management for scalability and interoperability between healthcare providers for future Smart Healthcare systems.

[1] L. Marchesi, M. Marchesi, R. Tonelli, "A Blockchain Architecture for Industrial Applications," DMI, University of Cagliari, Italy, pp. 1–6, April 2020.

[2] M. Z. A. Bhuiyan, A. Zaman, T. Wang, G. Wang, H. Tao, M. M. Hassan, "Blockchain and Big Data to Transform the Healthcare," ICDPA: International Conference on Data Processing and Applications, pp. 62–68, May 2018.

[3] N. Tariq, A. Qamar, M. Asim, F. A. Khan, "Blockchain and Smart Healthcare Security: A Survey," The 6th International Workshop on Cyber Security and Digital Investigation (CSDI), Elsevier: August 2020, Leuven, Belgium.

[4] [Online]. Available: https://blockgeeks.com/guides/understand-blockchain-business-models/

[5] M. Liyanage, "Blockchain in Healthcare," University of College Dublin, Ireland, pp. 1–44, August 2020 [Tech Talk at University of Kelaniya].

[6] [Online]. Available: Research challenges and opportunities in blockchain and cryptocurrencies - Mahmoud - 2019 - Internet Technology Letters - Wiley Online Library

[7] M. Bhuiyan, G. Wang, W. Tian, M. Rahman, and J. Wu, "Content-Centric Event-Insensitive Big Data Reduction in Internet of Things," IEEE Globecom 2017, Singapore, December 4-8, 2017

[8] J. Son, J. Park, H. Oh, M. Bhuiyan, J. Hur, and K. Kang, "Privacy-Preserving Electrocardiogram Monitoring for Intelligent Arrhythmia Detection," Sensors 2017, 17(6):1-22, 1360, doi:10.3390/s17061360

[9] Z. Maamar, E. Kajan, M. Asim, T. Baker Shamsa, "Open challenges in vetting the internet-of-things, Internet Technology Letters," August 2019, e129.

[10] N. Tariq, M. Asim, Z. Maamar, M. Z. Farooqi, N. Faci, T. Baker, "A mobile code-driven trust mechanism for detecting internal attacks in sensor node-powered iot, Journal of Parallel and Distributed Computing," 2019, pp. 198–206.

[11] N. Abbas, M. Asim, N. Tariq, T. Baker, S. Abbas, "A Mechanism for Securing IoT-enabled Applications at the Fog Layer," Journal of Sensor and Actuator Networks, January 2019.

[12] N. Tariq, M. Asim, F. Al-Obeidat, M. Z. Farooqi, T. Baker, M. Hammoudeh, I. Ghafir, "The Security of Big Data in Fog-Enabled IoT Applications Including Blockchain: A Survey", April 2019.

[13] N. Tariq, M. Asim, F. A. Khan, "Securing scada-based critical infrastructures: Challenges and open issues," 2019, pp. 612–617.

[14] F. A. Khan, N. A. H. Haldar, A. Ali, M. Iftikhar, T. A. Zia, A. Y. Zomaya, "A continuous change detection mechanism to identify anomalies in ecg signals for wban-based healthcare environments," IEEE Access 5 (2017) 13531–13544.

[15] E. Karafiloski, A. Mishev, "Blockchain Solutions for Big Data Challenges," IEEE EUROCON 2017, 6-8 July 2017, OHRID, R. MACEDONIA

[16] H. Hou, "The Application of Blockchain Technology in E-government in China," School of Information Management, Sun Yat-sen University, Guangzhou, China.