Application of Blockchain in Healthcare

Conference Paper · March 2022

DOI: 10.1109/ICAITPR51569.2022.9844186

3 authors, including:

Akshet Patel
University College London
15 PUBLICATIONS **111** CITATIONS

SEE PROFILE

Application of Blockchain in Healthcare

Akruti Sinha
Department of Computer and Communication
Manipal University Jaipur
Jaipur, India
Email: akruti.sinha25@gmail.com

Akshet Patel
Department of Mechatronics
Manipal University Jaipur
Jaipur, India
ORCID: https://orcid.org/0000-0002-2884-3080

Mukta Jagdish
Department of Information Technology
Vardhaman College of Engineering(Autonomous)
Hyderabad, India
Email: mukta.jagdish13@gmail.com

2022 First International Conference on Artificial Intelligence Trends and Pattern Recognition (ICAITPR) | 978-1-6654-2521-6/22/$31.00 ©2022 IEEE | DOI: 10.1109/ICAITPR51569.2022.9844186

***Abstract*—**

Blockchain appears to be the way of the future in today's technological age. Blockchain technology has recently proven itself worthy of praise by facilitating cryptocurrency financial transactions. Despite being widely researched, there have recently been growing worries about the privacy and security of patient data because of the use of a centralized system to handle patient data. The General Data Protection Regulation (GDPR) grants the subject the right to know where and how his or her personal data is stored, as well as who is privy to it and to what extent. Blockchain has been shown in numerous studies to be capable of supporting the safe and secure recording of patient data in the health-care system. This paper summarizes recent research into how blockchain technology can be successfully implemented in the healthcare field. In our assessment of such publications, we discovered that the majority of blockchain applications are limited when only briefly examined. The products are only used by a small number of people. Perhaps this is due to the fact that healthcare blockchain applications have more demanding authentication, interoperability, and record sharing requirements. However, the quality of the products is constantly improving.

Keywords—blockchain, healthcare, security, privacy, IoT.

I. INTRODUCTION

Smart healthcare and biomedical breakthroughs have been extensively investigated in light of current technological improvements, with the purpose of enhancing treatment and healthy living. The advances, however, have put the healthcare system at the peril of a variety of security threats. There is a dearth of awareness and education of security issues in the healthcare arena, as [1] indicates. Blockchain sprang to prominence recently because of its ability to eliminate the requirement for a centralized authority or management, which was previously required for financial transactions. [2]

That is precisely how blockchain should be applied to address the security issues in smart healthcare. The architecture, process, and performance of health-care services can all be improved by blockchain. As a result, patients will have more trust in the system, and the sector will be less vulnerable to privacy issues.

The Internet of Things (IoT)'s superiority in the healthcare applications areas has been mentioned by both [2] and [3] and although developments are continuing to increase in the field of IoT, the privacy and security of the data is always a concern. This occurs due to the utilization by the stakeholders who often pursue their respective activities. [2] Since patient data is typically maintained on a server, or in a centralized application, potential threats have considerably increased.

Blockchain technology has the ability to secure data from misuse while also establishing a clear level of trust between patients and various stakeholders.

With the convergence of IoT and blockchain, it might thus simplify the diagnostic procedures and conveniently monitor the activities of patients. Regrettably, however, while the applications of how Blockchain can help increase data privacy, it has received relatively little attention to date.

What is unique about blockchain is that it operates through a time-stamped sequence of data entries that are not administered by any single entity or corporation but rather by a group of computers.

Cryptographic concepts, known as chains, are used to link the blocks together. First, a record of each transaction is created, which comprises the information about the people who initiated the transaction and is further authenticated using each person's digital signature. The verification process is conducted by computers linked to the network that operate independently.

Each block also contains a hash value, which is actually a code. This hash value serves as a function that identifies it and displays its position on the blockchain. The hash also verifies that the data in the block has not been changed since it was recorded. The block is attached to the end of the blockchain once it is finished.

By eliminating the need for intermediaries, blockchain technology will enable healthcare businesses to minimize operating expenses, avoid costly middleman management processes. In the sphere of healthcare, it appears that blockchain combined with IoT applications can have a significant influence.

II. LITERATURE REVIEW

The authors in [2] offer a framework that incorporates Internet of Things (IoT), Blockchain, and Machine Learning. This framework is used to discover anomalies in the behavior of a patient's health data. Patients must wear devices that record data like heart rate, calorie burn, breath strengthening, and sleep stage monitoring. According to [2], the IoT module intercepts, fetches, and monitors this data. The blockchain module utilized by the authors in [2] is particularly intriguing. The Blockchain Network is in charge of managing and processing the massive amounts of data supplied by patients.

Personal Health Care (PHC) as well as the External Record Management (ERM) Blockchain, were the two vital blockchain networks that are employed by the authors in [2]. The PHC collects data from the patients' wearable devices and is thus maintained by the patients themselves. This information can be used to determine how the patient is affected by the disease and to prescribe medications accordingly. However, because all this information is being

housed in a third-party cloud database, there are certain privacy concerns. According to the authors, this database is governed by the blockchain network.

The External Record Management Blockchain stores the data generated when patients visit their doctors.

Finally, the Machine Learning Module was used by the authors of [2]. The module examines the data gathered by the patient wearable devices and detects any irregularities. When an aberration is detected, the module sends an alert to the concerned doctor, who can then take any appropriate action based on the information and the irregularity.

The authors in [3] propose a modification to the traditional Blockchain architecture in order to protect patients' privacy. The authors of [3] commenced by reducing data redundancy by clustering the miners. As a result, all miners are not involved in the consensus procedure. Another advantage of this is that it reduces the size of transactions.

In contrast to [2], the authors of [3] store the hash of a patient's healthcare data rather than the original data. This appears to be a promising solution for ensuring data security. The authors of [3] have put in a lot of effort to address and resolve the privacy concerns. They collect and manage data in the location closest to the patient.

To protect the patients' privacy, they are given a pseudonym, as well. [3]'s system model is made up of several components. In contrast to [2], patients need not wear any device to capture their data like blood pressure, and heart rate; but nevertheless, sensors are attached to the patient's body.

There is a central server that uses the Internet of Things Module to manage and store the patient's data [11]. The IoT module is in charge of a variety of tasks, such as receiving and storing data from sensors and smartphones.

The IoT module also performs major operations such as hashing and other cryptographic operational activities. This hash of the data is then sent to the central blockchain network.

The authors of [3] propose storing hash and user data in separate entities. Because there are different transaction structures, policy management is simplified. In comparison to [2], the operation of this architecture [3] is rather complex. The first step is to collect data from sensors obtained through smartphone usage. The data is classified by the PDA and sent to the Internet of Things Module known as the IoT Healthcare Manager.

The IoT module then decrypts the encrypted data and stores it in the database. After computing the hash of the data, the module encrypts it using asymmetric cryptographic data. This encrypted data is then sent as a transaction to the blockchain network's cluster miner.

The commendable feature of [3]'s developed framework is that if the patient's responsible doctor desires to access the data, they can request a transaction that includes the patient's ID.

The miners usually check the patient's data policies. If the policies are validated, the data and its location are encrypted using the public key of the responsible doctor and sent to the doctor [9]. After receiving the response, the doctor can obtain the hash of the patient's data and decrypt it with a private key.

Finally, a message containing the hash of the patient's data is sent to the IoT module [10]. It is decrypted and the hash value is computed by this module. When a valid hash value is obtained, the patient's data is returned.

While this process appears to be time-consuming and necessitates extensive knowledge of cryptography, it ensures that patients' privacy is not jeopardized. The data is completely secure.

The authors of [1] are focused on using blockchain to achieve smart healthcare in smart cities. While no framework is proposed, the authors do an excellent work of distinguishing and summarizing how blockchain can be useful in the healthcare sector.

According to [1] a startling number of people are unaware of the privacy risks associated with their data. According to [5] 60 percent of mobile health users are unaware of the security risks associated with storing medical data on their smartphones. This raises concerns about the use of smartphones in [3].

The authors of [5] conduct an interesting survey on the use of mobile healthcare applications to provide services to patients. While the overwhelming majority, 90 percent of those polled, have embraced technology, there have been a select few, 10%, who have yet to trust technology and transition to using mobile healthcare applications.

People who use these medical monitoring applications believe that Blockchain technology allows them to secure their money during medical transactions [12].

The robust encryption of data that blockchain technology is capable of providing increases user trust in it. The technology can keep sensitive information secure by making it visible only to authorized users in the system. [1]

The authors of [3] have yet to implement the architectural design and conduct analysis in order to evaluate the proposed architecture's performance.

Despite the complex architecture, the proposed system in [2] is such that it can be considered as a possible implementation in society, with the potential to significantly influence existing privacy and security concerns while also providing effective and precise healthcare.

III. APPLICATION OF BLOCKCHAIN IN HEALTHCARE

Healthcare systems can be greatly improved with the introduction of Blockchain technology [13]. Without the explicit requirement for a centralized system, blockchain can thus be used to eliminate or at least minimize risks to security and medical data privacy. Because blockchain is a new concept, research on how to import any information from outside a blockchain distributed ledger has yet to be completed [4].

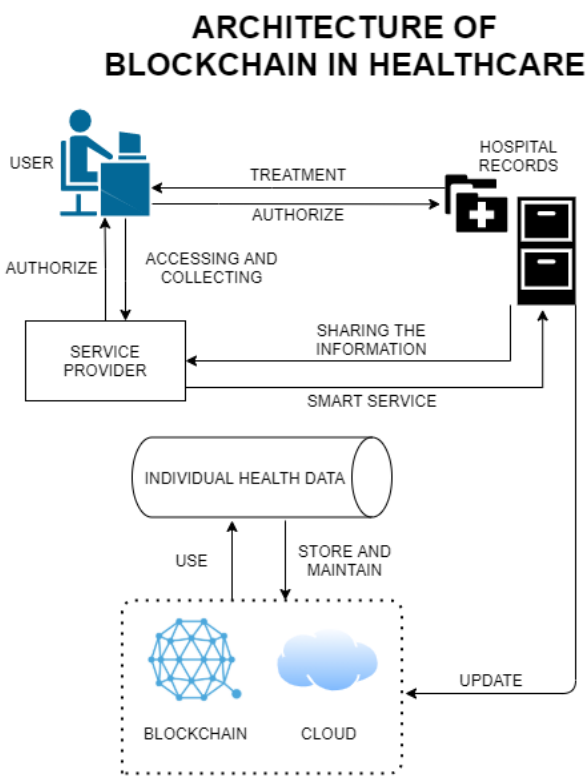

Fig.1: Architecture of Blockchain in Healthcare

Fig.1 depicts the architecture of Blockchain in Healthcare where in the hash of the previous block is stored in the current block so that it becomes nearly impossible to tamper with the data since one change will alter the hash of all the proceeding blocks. Following the laudable solution of financial transaction security, blockchain is now being considered as the solution to all privacy issues in the field of healthcare [14]. The healthcare industry has seen an increase in the hazard to data integrity, which means that not only is data accessed by third parties, but it is also altered. Integration of Blockchain and Internet of Things.

The authors of [7] suggest an intriguing framework that combines the Internet of Things model with Blockchain Technology. The proposed framework consists of five separate sections: a blockchain-to-device interface, a chain code execution interface, a membership service provider (MSP), a peers node, and an ordering node.

The data from the IoT model is received via the API gateway [16]. When the data is received, the gateway triggers the chain code configured in each blockchain peer by broadcasting a transaction proposal to the peers.[7]

A. Integration of Blockchain and Machine Learning

Recently, there has been an increase in the use of machine learning models and blockchain technology to address privacy concerns in the healthcare sector. Some of these proposed architectures disseminate the gathered data to several divergent nodes, and then machine learning models are applied. Finally, they are assembled after the local application.[1]

Unfortunately, these models are not completely secure because the use of a centralized server increases security risks. This shortcoming, however, is addressed by using a decentralized server, as stated in [1].Blockchain guarantees that the system is protected and authentic, which only satisfies the requirements of Machine Learning models to provide efficient findings. As the authors of [6] suggest, combining these two technologies complements each other and has the potential to produce accurate and reliable results in terms of security.

The authors of [6] do an excellent job of providing an overview of machine learning and blockchain network integration. According to [6], the certificates issued by the Certificate Authority in the blockchain network provide users with a unique identity, adding an additional layer of security. This certificate will contain the user's digital signature and will be submitted to the blockchain.

The authors of [6] explain the advantages of digital signatures. Here are a few examples:

i. The signature ensures that users have legal access to the ledger, which contains transaction details.

ii. Most importantly, it verifies the identity of the user who is seeking the transaction.

Many people have criticized the idea of combining blockchain and machine learning [15]. Nonetheless, proponents of the concept claim that this integration will effectively address privacy concerns.

The following are the most distinctive features that ensure the safety and privacy of data records: The following are the most distinctive features that ensure the safety and privacy of data records:

a. When machine learning models are trained with actual data, it opens the door to increased efficiency and accuracy. As a result, the additional cost is reduced.

b. Because the results are stored in blockchain and governed by machine learning models, this integrated model can predict outbreaks. This speeds up the process of the doctor issuing the correct prescription.

c. Each user who has been authenticated will receive a copy of the ledger [17]. This increases the user's trust and ensures that the data is only acquired by the parties to whom he grants access.

Several other models, such as Natural Language Processing, can also be used to provide accurate and precise prescriptions. Machine Learning models can recommend methods and medications based on the symptoms displayed by the patient.

Among these observations are numerous others that demonstrate how well blockchain technology can integrate with machine learning models to produce more reliable results [18].

The authors of [6] have taken care not to overlook the challenges. They state that the main challenge is that once a transaction takes place, it cannot be changed, and because there is always risk of human error, this issue must be addressed.

IV. CHALLENGES BY THE INTEGRATION OF BLOCKCHAIN

Healthcare is one of the most prominent application areas for blockchain technology because of its decentralized and distributed technology. The application of blockchain in the field of healthcare, however, faces numerous challenges

and obstacles, as with any other application. These issues must be investigated and resolved prior to the sector's actual adoption of technology.

A. High Costs of Development

As [8] suggests, the application of blockchain in the healthcare industry may take some time due to the high costs involved. The total implementation cost, as well as the operating costs, are extremely high, posing a significant challenge to the global adoption of this technology. As a result, it is critical that unnecessary costs be eliminated, and total costs be minimized when constructing such systems.

B. Issue with Smart Contracts

Both [1] and [8] authors demonstrated how a Smart Contract is an essential component of blockchain-based applications. Smart Contracts are computer-based digital programs that serve as a type of agreement between various parties. The authors of [8] propose that during the implementation of blockchain in the healthcare sector, the patient and other network stakeholders agree to a deal to accept the terms in order to develop the requirements in the smart contract. As a result, the process is more reliable. The authors of [1] have made it perfectly clear that the public may require some time to fully trust the process of smart contracts because users are being asked to trust a completely virtual process. In the event of a coding error, the system is bound to throw an error that cannot be resolved unless a technician with the necessary knowledge is present on-site. [8]

CONCLUSION

There have been numerous technological advancements, and with them, we must also improve the healthcare sector, which is currently dealing with a major issue of security and privacy concerns. The current centralized approach used in the healthcare sector exacerbates these flaws. Blockchain technology appears to be a promising solution for addressing the shortcomings, as well as many others.

While the works we've looked at have created commendable blockchain solutions that introduce blockchain technology into the healthcare business, there are still a lot of roadblocks to overcome. They make use of smart contracts, which allow for personalized care without violating clinical guidelines. The blockchain will ensure that data cannot be tampered with. It will successfully disseminate a large amount of data while maintaining privacy. Blockchain technology, when combined with IoT and Machine Learning models, has the potential to significantly improve efficiency. Using a decentralized approach through use of Blockchain Technology aids in guaranteeing data integrity and security.

REFERENCES

[1] J. Qiu, X. Liang, S. Shetty and D. Bowden, "Towards Secure and Smart Healthcare in Smart Cities Using Blockchain," 2018 IEEE International Smart Cities Conference (ISC2), 2018, pp. 1-4, doi: 10.1109/ISC2.2018.8656914.

[2] S. Chakraborty, S. Aich and H. Kim, "A Secure Healthcare System Design Framework using Blockchain Technology," 2019 21st International Conference on Advanced Communication Technology (ICACT), 2019, pp. 260-264, doi: 10.23919/ICACT.2019.8701983.

[3] K. M. Hossein, M. E. Esmaeili, T. Dargahi and A. khonsari, "Blockchain-Based Privacy-Preserving Healthcare Architecture," 2019 IEEE Canadian Conference of Electrical and Computer Engineering (CCECE), 2019, pp. 1-4, doi: 10.1109/CCECE.2019.8861857.

[4] P. Ndayizigamiye and S. Dube, "Potential Adoption of Blockchain Technology to Enhance Transparency and Accountability in the Public Healthcare System in South Africa," 2019 International Multidisciplinary Information Technology and Engineering Conference (IMITEC), 2019, pp. 1-5, doi: 10.1109/IMITEC45504.2019.9015920.

[5] Ribitzky, Ron, James St Clair, David I. Houlding, Chrissa T. McFarlane, Brian Ahier, Michael Gould, Heather L. Flannery, Erik Pupo, and Kevin A. Clauson. "Pragmatic, Interdisciplinary Perspectives on Blockchain and Distributed Ledger Technology: Paving the Future for Healthcare." Blockchain in Healthcare Today (2018).

[6] S. Vyas, M. Gupta and R. Yadav, "Converging Blockchain and Machine Learning for Healthcare," 2019 Amity International Conference on Artificial Intelligence (AICAI), 2019, pp. 709-711, doi: 10.1109/AICAI.2019.8701230.

[7] A. Bhawiyuga, A. Wardhana, K. Amron and A. P. Kirana, "Platform for Integrating Internet of Things Based Smart Healthcare System and Blockchain Network," 2019 6th NAFOSTED Conference on Information and Computer Science (NICS), 2019, pp. 55-60, doi: 10.1109/NICS48868.2019.9023797.

[8] T. Kumar, V. Ramani, I. Ahmad, A. Braeken, E. Harjula and M. Ylianttila, "Blockchain Utilization in Healthcare: Key Requirements and Challenges," 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), 2018, pp. 1-7, doi: 10.1109/HealthCom.2018.8531136.

[9] S. Jan *et al.*, "A framework for systematic classification of assets for security testing," *Comput. Mater. Contin.*, vol. 66, no. 1, pp. 631–645, 2021, doi: 10.32604/cmc.2020.012831.

[10] P. Randhawa, V. Shanthagiri, and A. Kumar, "Violent activity recognition by E-textile sensors based on machine learning methods," *J. Intell. Fuzzy Syst.*, vol. 39, no. 6, pp. 8115–8123, 2020, doi: 10.3233/JIFS-189133.

[11] B. C. Apostolopoulos and G. Halikias, "Towards the Facilitation of Project Change Risks : An IT Service Management Perspective," vol. III, no. Vi, pp. 1–12, 2014.

[12] M. Yamin and G. Tsaramirsis, "Cloud Economy & Its Implications for Saudi Arabia Yamin & Tsaramirsis," 2011.

[13] S. Warda Asher, S. Jan, G. Tsaramirsis, F. Qudus Khan, A. Khalil, and M. Obaidullah, "Reverse Engineering of Mobile Banking Applications," *Comput. Syst. Sci. Eng.*, vol. 38, no. 3, pp. 265–278, 2021, doi: 10.32604/csse.2021.016787.

[14] P. Randhawa, V. Shanthagiri, A. Kumar, and V. Yadav, "Human activity detection using machine learning methods from wearable sensors," *Sens. Rev.*, vol. 40, no. 5, pp. 591–603, 2020, doi: 10.1108/SR-02-2020-0027.

[15] I. Poernomo, G. Tsaramirsis, and V. Zuna, "A methodology for requirements analysis at CIM level," *CEUR Workshop Proc.*, vol. 376, 2008.

[16] P. Randhawa, V. Shanthagiri, R. Mour, and A. Kumar, "Design and Development of Smart-Jacket for Posture Detection," *2018 Int. Conf. Smart Comput. Electron. Enterp. ICSCEE 2018*, pp. 1–5, 2018, doi: 10.1109/ICSCEE.2018.8538384.

[17] G. Tsaramirsis, S. Al-Jammoor, and S. M. Buhari, "Proposing a new hybrid controlled loop," *Int. J. Softw. Eng. its Appl.*, vol. 8, no. 3, pp. 203–210, 2014, doi: 10.14257/ijseia.2014.8.3.18.

[18] P. Randhawa, V. Shanthagiri, and A. Kumar, "A review on applied machine learning in wearable technology and its applications," *Proc. Int. Conf. Intell. Sustain. Syst. ICISS 2017*, no. July, pp. 347–354, 2018, doi: 10.1109/ISS1.2017.8389428.

[19] P. Randhawa and V. Shanthagiri, "Concept of Operations to System Design and Development-An Integrated System for Aircraft Mission Feasibility Analysis Using STK Engine, Matlab and Labview," *Int. J. Instrum. Control Syst.*, vol. 5, no. 4, pp. 01–12, 2015, doi: 10.5121/ijics.2015.5401.

[20] I. Poernomo and G. Tsaramirsis, "Prototype generation from ontology charts," *Proc. - Int. Conf. Inf. Technol. New Gener. ITNG 2008*, pp. 1177–1178, 2008, doi: 10.1109/ITNG.2008.239