

Decentralized Access Control Model Based on Artificial Intelligence and Blockchain Technology to Enable Secure Interoperability for Healthcare

Mohammed Rashed*

Editorial office, Health Economics and Outcome Research, Brussels, Belgium

Corresponding Author*

Mohammed Rashed
Editorial office,
Health Economics and Outcome Research
Brussels, Belgium
E-mail: economics@journalinsight.org

Copyright: ©2022 Rashed, M. This is an open-access article distributed under the terms of the Creative Commons Attribution License, which permits unrestricted use, distribution, and reproduction in any medium, provided the original author and source are credited.

Received: 1 July, 2022, Manuscript No. HEOR-22-74486; **Editor Assigned:** 4 July, 2022, PreQC No. HEOR-22-74486 (PQ); **Reviewed:** 15 July, 2022, QC No. HEOR-22-74486 (Q); **Revised:** 22 July, 2022, Manuscript No. HEOR-22-74486(R); **Published:** 27 July, 2022, doi:10.37532/heor.22.8.7.1.

Abstract

The Internet of Things (IoT) and linking medical equipment are the main topics of study in the healthcare sector, one of the most significant businesses. The data generated by the healthcare sector is being studied by a very small number of academics. In this cutthroat environment, data are essential tools that may be used with Artificial Intelligence (AI) to advance sustainability. Patient health records, drug-related data, clinical trial data, data from different medical devices, etc. are all examples of healthcare data. The majority of data management procedures are laborious, error-prone, and manual. Even then, data sharing and collaboration between various healthcare companies are not trusted. Innovative uses of distributed ledger technology are being made in a variety of fields, including healthcare. This technology may be used to share information between various healthcare institutions, including hospitals, insurance providers, labs, pharmacies, etc. The immutability, transparency, provenance, and other characteristics of this technology, among others, can instill confidence and security in the healthcare industry. A decentralised access control approach is suggested in this study to allow for the safe interoperability of various healthcare organisations. The Ethereum blockchain is used to implement this approach. This link between patients, physicians, pharmacists, and insurance providers enables a reliable and secure data transfer. Maintaining a record of the transactions and preventing unauthorised alterations to medical information are the primary issues.

Keywords: Blockchain • Content identifier • Digitalization • Artificial intelligence

Introduction

The healthcare industry is one of society's most crucial foundations since it affects people's health and quality of life. This industry needs ground-breaking concepts that may improve the level of healthy living by offering answers to various health-related problems. As indicated, the healthcare industry creates a significant quantity of data that is used by many system stakeholders. Due to their extreme sensitivity, you must refrain from sharing this data over a public network. The sharing of patient data is essential because physicians in various places occasionally must reach a consensus or seek advice from a different specialist. This procedure should verify that entities interacting are receiving the most recent information. This trade must happen through a safe and verified procedure. The main issues with any interchange of health data are the security and privacy of the data. Furthermore, this industry is frequently plagued by serious interoperability issues. Such clinical data transfers call for extensive, reliable, and positive interactions between the parties. Security is still a concern due to the existing system's centralised structure. As a result, security may be offered

by blockchains, a young and developing technology. Blockchain technology has the potential to increase security by highlighting the shortcomings of current security measures [1-3]. There is no need for an intermediary in transactions or communication because of the decentralised nature of the point-to-point network. The transactions are independent of one another and stand alone. Security is still a concern due to the existing system's centralised structure. As a result, security may be offered by blockchains, a young and developing technology. Blockchain technology has the potential to increase security by highlighting the shortcomings of current security measures. There is no need for an intermediary in transactions or communication because of the decentralised nature of the point-to-point network [4]. The transactions are independent of one another and stand alone. The cutting-edge concept of cryptocurrencies is supported by the technology known as blockchains. Blockchains, a publicly distributed ledger system, is available to everyone. The chain's blocks are made up of data, the hash of the block before it, and a list of all the transactions [5]. The header and the transaction details make up its two components. The header contains the block's information. The block's "timestamp" records the date and time it was produced. The "difficulty level" controls how difficult it will be to mine a block. Merkle tree root is the hash of all transactions in the current block, and "NONCE" is the solution to the mathematical conundrum posed by the proof-of-work method.

Conclusion

Hospitals, laboratories, payers (i.e., insurance companies), and pharmaceutical companies all save medical data on patients in various ways under the traditional healthcare delivery models, but there is no standardisation in record keeping. The exchange of health records is now plagued by data disarray as a result of this. We describe a unique approach to managing medical records that makes use of smart contracts to offer accessibility, interoperability, and audibility. This system, which is intended to record flexibility and granularity, enables the sharing of insurance claims and medical information about patients by enabling them to exchange clinical expertise, offer suggestions, and distribute massive volumes of data more successfully while preserving higher levels of security and privacy protection. There is little question that the successful application of this technology in healthcare settings will open up new avenues for biomedical research advancement. The suggested solution's deployment on less expensive blockchains might be thought of as future work. The main obstacle to the application of this contemporary technology in medical facilities is a lack of expertise. More study is needed as blockchain applications are still in their infancy. However, medical organisations and authorities are accountable for it. Future growth in the usage of blockchain in healthcare is almost certain. This technical development will enhance its applications in healthcare since it helps to explain treatment outcomes and progress.

References

1. Zheng, Z., et al. "Blockchain challenges and opportunities: A survey." *Int J Web Grid Serv.* 14.4(2018): 352-375.
2. Hyla, T., & Pejas, J. "Long-term verification of signatures based on a blockchain." *Comput Electr Eng* 81(2020): 106523.
3. Kumar, G., et al. "Proof-of-work consensus approach in blockchain technology for cloud and fog computing using maximization-factorization statistics." *IEEE Internet Things J* 6.4(2019):6835-6842.
4. Thomason, J., et al. "Blockchain—powering and empowering the poor in developing countries." *In Transforming Clim Finance Green Invest Blockchains* (2018):137-152.
5. Clauson, K.A., et al. "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An exploration of challenges and opportunities in the health supply chain." *Blockchain Healthc Today* 1.1(2018).