# Application of Blockchain Technology in Patient-Centric Healthcare Systems

Subjects: Computer Science, Information Systems

Contributor: Ohud Aldamaeen , Waleed Rashideh , Waeal J. Obidallah

Healthcare data are considered sensitive and confidential, and storing these sensitive data in traditional (i.e., centralized) databases may expose risks, such as penetration or data leaks. Furthermore, patients may have incomplete health records since they visit various healthcare centers and leave their data scattered in different places. One solution to resolve these problems and permit patients to own their records is a decentralized personal health record (PHR); this can be achieved through decentralization and distribution systems, which are fundamental attributes of blockchain technology.

access control | blockchain technology | identity management | personal health records

## 1. Introduction

Healthcare systems currently face the dilemma of having to share medical data or electronic records with more stakeholders to serve many goals while also maintaining data integrity and protecting patient privacy. One common issue is the scattering of patient data in several places due to the fact that patients visit different healthcare providers. Moreover, reconducting procedures, such as X-ray and computed axial tomography scans, have drawbacks, such as loss of money and health dangers on top of a noncomplete health record. Furthermore, storing sensitive data in centralized databases may expose risks, such as penetration or data leaks. One solution to resolve the above problems and allow patients to own and control their records is a decentralized personal health record (PHR). According to Hau et al. [1], PHRs can be achieved through decentralization and distribution systems, which are fundamental attributes of blockchain technology. Blockchain technology stores the data and provides a copy of these data on all the connected nodes to continuously verify the validity of any transaction. A healthcare system based on blockchain offers a decentralized approach to storing and managing medical data without violating privacy. This method breaks the data silos of centralized, traditional health information systems. It enables patients to assemble and own their records without violating privacy [2]. Utilizing a consortium blockchain for PHRs helps patients have access to their complete health history at any time and from anywhere at first glance, and it helps physicians to know a patient's full medical history before issuing any prescriptions. In addition, a PHR allows for a unified source across numerous healthcare organizations after obtaining the patient's approval [3], thus reducing the cost paid by patients for a service (i.e., affordability) and saving time [4]. On the other hand, the disclosure of patient data through unauthorized access or data breaches remains a challenge as it is a threat to patient privacy. Moreover, according to Arndt [5], many legitimate healthcare providers earn profit from selling these data. Thus, patients must be aware of who has permission to view their data and the purposes for which it is used;

on top of this, patients should be the ones who benefit first from these data. Several laws and regulations have been enacted, such as the Health Insurance Portability and Accountability Act (HIPAA) [6] and the General Data Protection Regulation (GDPR) [7], to enable the application of guidelines and compliance in the healthcare industry on how to manage, process, and safeguard personal data; the recent attacks on the healthcare industry demonstrate that the sector's data security has challenges, as hackers find it an easy target [8].

# 2. Blockchain Technology

Recently, blockchain technology and its applications have gained significant attention from governments, organizations, and academics around the globe [9]. Blockchain was first presented through Bitcoin in 2008 by Nakamoto [10] and was created to keep track of financial transactions. Blockchain can be defined as a "cryptographic, distributed peer-to-peer ledger system which operates via a number of nodes, all jointly responsible for the maintenance of a database" [11].

Transactions in a blockchain are digitally signed to ensure their validity and correctness. Each block is cryptographically connected via a "chain" to the next block; this provides immutable storage and prevents fraudulent transactions. A node in a blockchain can be either a physical or a virtual machine with an IP address assigned to it [12]. Each user in the network has a public key, which is used as a reference, and a private key for cryptographically signing messages. All transactions stored in the network are replicated and synchronized on all existing nodes [13].

The blockchain is a distributed ledger technology designed to guarantee security, privacy, integrity, and traceability [14]. All transactions on the blockchain are verifiable and safe due to the existence of consensus algorithms that ensure standard agreement across all nodes in the current ledger state. Consensus algorithms guarantee that any new block added to the ledger is the sole version upon which all nodes agree [14].

# 3. Application of Blockchain Technology in Patient-Centric Healthcare Systems

## 3.1. Access Control and Data Ownership

Electronic health records (EHRs) and PHRs allow physicians and healthcare providers to access and review their patients' health histories electronically. Various studies have been pursued to allow patients to control, own, and share their data. Zhuang et al. [15] proposed a system with two models based on a private Ethereum network to allow patients to own their data. First, there is a linkage model on the healthcare center's side that links EHRs to the blockchain to create a touchpoint for patient visits. Second, there is the request model, where patients provide permission for a clinic's physician and then add them to the authorized list. A patient also has the option to reveal what information the physician can view and can choose the data they wish to reveal. However, the system has scalability constraints. Zaabar et al. [16] developed a system to manage patient data from reports or IoT devices; the solution is based on Hyperledger Fabric and Composer. The solution focuses on collecting data from IoT

devices to monitor a patient's vital signs, allowing the physician make the right decision at the right time. The patient has complete control of their EHR, and the physician must request permission to view it. Similarly, Pawar et al. [17] proposed a blockchain-based personal health information management system that allows users to have complete control over their data and the sharing of their data from their medical IoT devices. The system focuses on an adapter component that collects data from the backend of a wearable health device and sends it to the blockchain for storage rather than a provider's cloud storage. Another work, by Balistri et al. [18], proposed a high-level architectural solution for collecting and sharing health data while assuring immutability and data privacy. Following GDPR compliance, each patient has the right to be forgotten in terms of their data. Another solution for cross-institution and medical data sharing with highly secure data sharing was proposed by Tang et al. [19]. The system is built on the Ethereum framework and has two sorts of access based on incentives to allow patients to benefit from sharing their data. Non-incentive access is normal access provided to a physician, who can then view a patient's record. The incentive model is for researchers or marketing companies using these data for non-medical purposes. Uddin et al. [20] designed architecture for EHRs to ensure secure and private communication across various stakeholders utilizing Hyperledger Fabric. The proposed solution gives a patient access control over their record. The solution provides a general overview of how patients will manage their reports and how blockchain will be utilized. However, a deeper look is needed to address the real requirements for stakeholders and what kind of permissions and restrictions they must have. Another work, by Antwi et al. [21], designed and implemented scenarios based on a Hyperledger Fabric consortium after determining the general requirements for EHRs. The scholars present experiments and illustrate how the system complies with the GDPR, achieving security, privacy, and confidentiality by storing all data on-chain and providing access control. Considering the user's perspective, Meier et al. [22] developed three principles that should be considered when developing solution-based PHRs. First, the data structure should be unified in order to be easily integrated into the existing ecosystem. Second, the implementation should have a safe, reliable, and traceable infrastructure to prevent unauthorized access; finally, it should have an easy-to-use access control mechanism. The scholars continued their work by developing an operational prototype based on a private blockchain and a Hyperledger Fabric framework. The scholars recommended considering these principles in future works and utilizing consortium blockchain and stakeholder engagement. Other studies engaged stakeholders to understand their needs.

From another angle, in the traditional emergency system, patients cannot provide access permission to emergency personnel to access their PHR. In some cases, a patient may transfer their record from healthcare centers where no medical record belongs. Few studies have been conducted to overcome this issue. Rajput et al. [23] proposed a simple framework for a patient emergency access control system that defines permission access rules through Hyperledger Fabric. Patients can determine access to their data in emergency conditions by setting an authorization access control policy for their data through a developed smart contract. Thus, in an emergency, the medical staff does not need to contact a patient's relatives or wait for a third party to approve access to their data. In contrast, the patient determines and defines an access control policy for their data by enabling an emergency physician to access their data for a limited time to ensure patient privacy.

Based on the storage of off-chain data in a decentralized file system, in [24] a healthcare data sharing system was proposed to overcome the performance and scalability issues of centralized databases. The study mainly focused

on the performance analysis of a network considered for an emergency case of a patient, since traditional and off-chain-based cloud databases need to be much faster and scalable. The scholars proposed a blockchain-based architecture containing three types of smart contracts: registry contracts for system protection from malicious users, data contracts for records storage, and permission contracts for access permission. The experiment showed better results compared to a traditional approach. However, the mechanism for how emergency conditions will be performed was not clarified in the architecture or even described.

## 3.2. Health Records and Patient Incentives

The incentive mechanism encourages patients to contribute their medical data for research, marketing, or other benefits and to receive incentives such as cryptocurrency. This mechanism is distinct from the blockchain system's incentive itself. According to Stafford and Treiblmaier [25], an incentive mechanism is valuable for patients since they are empowered to monetize their private data through EMR applications. Gan et al. [26] presented a solution for patients to benefit from their data by obtaining a reward for sharing it with any third party; the proposed implementation method used a private blockchain network and the Ethereum framework. Another study was conducted by Mohammed Yakubu and Chen [27] to allow DNA donors to profit from shared genomic data in addition to having access control on a private blockchain. This solution is driven by the profits that organizations receive from selling these data, while donors receive nothing. Faber et al. [28] proposed a general architecture system for patient identity, data management, and access control. In addition to empowering patients to be the owners of their data, it allows patients to monetize the sharing of their data with businesses. A patient can receive a reward in two ways: first, the patient can take the initiative to share their data; second, they can respond to requests by confirming their permission to share. The patient only receives a reward once when sharing their data, and they cannot receive a reward when sharing multiple times, unless there is an update to their data.

## 3.3. Health Records and Stakeholder Engagement

The stakeholders' engagement should be considered when they are targeted as users. Beinke et al. [29] conducted interviews to collect requirements for EHRs based on blockchain. Thirty-four requirements were identified, both from previous studies and from stakeholders, and a five-tier architecture-based blockchain was designed as a future guide for EHRs based on decentralized systems. Nevertheless, the scholars did not specify which framework these requirements and prototypes should be applied to. A survey on blockchain as a solution for managing health information was conducted by Hau et al. [1]. Patients and physicians were targeted to understand their attitudes regarding managing patient data. The patients showed a positive impression toward applying this technology to enhance their lives, as compared to the physicians, who showed a negative impression. As the research employed a quantitative method, the scholars called for more research utilizing another method, such as interviews, to better understand the real needs and to obtain more explanations. Another interview-based study was conducted by Stafford and Treiblmaier [25] with stakeholders to obtain their views on the potential for blockchain to provide access and control to EMRs. The healthcare providers did not appear enthusiastic about EHRs because they are not financially viable and because they treat patients as clients. Moreover, there is a lack of awareness of blockchain and its potential in healthcare. The study does not reflect the industry's current

situation, and its findings cannot be generalized. In addition, the study recommends future research to focus on understanding the current limitations and problems of user satisfaction with existing healthcare applications and the possibility of replacing them with blockchain applications.

## References


1. Hau, Y.S.; Lee, J.M.; Park, J.; Chang, M.C. Attitudes toward blockchain technology in managing medical information: Survey study. J. Med. Internet Res. 2019, 21, e15870.
2. Chen, Y.; Ding, S.; Xu, Z.; Zheng, H.; Yang, S. Blockchain-Based Medical Records Secure Storage and Medical Service Framework. J. Med. Syst. 2018, 43, 5.
3. Li, C.; Dong, M.; Li, J.; Xu, G.; Chen, X.; Ota, K. Healthchain: Secure EMRs Management and Trading in Distributed Healthcare Service System. IEEE Internet Things J. 2020, 8, 7192–7202.
4. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. Neural Comput. Appl. 2021, 34, 11475–11490.
5. Arndt, R.Z. How Third Parties Harvest Health Data from Providers, Payers and Pharmacies. Modern Healthcare. 2018. Available online: http://search.ebscohost.com/login.aspx?direct=true&db=cin20&AN=129027739&site=ehost-live&scope=site (accessed on 1 October 2020).
6. Office of the Federal Register. Health Insurance Portability and Accountability Act of 1996. Public Law 104-191. 110; U.S. Government Printing Office: Washington, DC, USA, 1996; pp. 1936–2103.
7. Viorescu, R. 2018 Reform of Eu Data Protection Rules. Eur. J. Law Public Adm. 2017, 4, 27–39.
8. Argaw, S.T.; Bempong, N.E.; Eshaya-Chauvin, B.; Flahault, A. The state of research on cyberattacks against hospitals and available best practice recommendations: A scoping review. BMC Med. Inform. Decis. Mak. 2019, 19, 10.
9. Zhu, Q.; Loke, S.W.; Trujillo-rasua, R.; Jiang, F.; Xiang, Y.; Trujillo-Rasua, R. 20 Applications of Distributed Ledger Technologies to the Internet of Things: A Survey. ACM Comput. Surv. 2019, 52, 1–34.
10. Nakamoto, S. Bitcoin: A Peer-to-Peer Electronic Cash System. 2008. Available online: www.bitcoin.org (accessed on 29 January 2022).
11. Despotou, G.; Evans, J.; Nash, W.; Eavis, A.; Robbins, T.; Arvanitis, T.N. Evaluation of patient perception towards dynamic health data sharing using blockchain based digital consent with the

Dovetail digital consent application: A cross sectional exploratory study. Digit. Health 2020, 6, 2055207620924949.

12. Thwin, T.T.; Vasupongayya, S. Blockchain-Based Access Control Model to Preserve Privacy for Personal Health Record Systems. Secur. Commun. Netw. 2019, 2019, 8315614.
13. Christidis, K.; Devetsikiotis, M. Blockchains and Smart Contracts for the Internet of Things. IEEE Access 2016, 4, 2292–2303.
14. Daraghmi, E.Y.; Daraghmi, Y.A.; Yuan, S.M. MedChain: A design of blockchain-based system for medical records access and permissions management. IEEE Access 2019, 7, 164595–164613.
15. Zhuang, Y.; Sheets, L.R.; Chen, Y.W.; Shae, Z.Y.; Tsai, J.J.P.; Shyu, C.R. A patient-centric health information exchange framework using blockchain technology. IEEE J. Biomed. Health Inform. 2020, 24, 2169–2176.
16. Zaabar, B.; Cheikhrouhou, O.; Jamil, F.; Ammi, M.; Abid, M. HealthBlock: A secure blockchain-based healthcare data management system. Comput. Netw. 2021, 200, 108500.
17. Pawar, P.; Parolia, N.; Shinde, S.; Edoh, T.O.; Singh, M. eHealthChain—A blockchain-based personal health information management system. Ann. Telecommun. Telecommun. 2021, 77, 33–45.
18. Balistri, E.; Casellato, F.; Giannelli, C.; Stefanelli, C. BlockHealth: Blockchain-based secure and peer-to-peer health information sharing with data protection and right to be forgotten. ICT Express 2021, 7, 308–315.
19. Tang, X.; Guo, C.; Choo, K.-K.R.; Liu, Y.; Li, L. A secure and trustworthy medical record sharing scheme based on searchable encryption and blockchain. Comput. Netw. 2021, 200, 108540.
20. Uddin, M.; Memon, M.S.; Memon, I.; Ali, I.; Memon, J.; Abdelhaq, M.; Alsaqour, R. Hyperledger fabric blockchain: Secure and efficient solution for electronic health records. Comput. Mater. Contin. 2021, 68, 2377–2397.
21. Antwi, M.; Adnane, A.; Ahmad, F.; Hussain, R.; Rehman, M.H.U.; Kerrache, C.A. The case of HyperLedger Fabric as a blockchain solution for healthcare applications. Blockchain Res. Appl. 2021, 2, 100012.
22. Meier, P.; Beinke, J.H.; Fitte, C.; Brinke, J.S.T.; Teuteberg, F. Generating design knowledge for blockchain-based access control to personal health records. Inf. Syst. E-Bus. Manag. 2021, 19, 13–41.
23. Rajput, A.R.; Li, Q.; Ahvanooey, M.T. A blockchain-based secret-data sharing framework for personal health records in emergency condition. Healthcare 2021, 9, 206.
24. Shuaib, K.; Abdella, J.; Sallabi, F.; Serhani, M.A. Secure decentralized electronic health records sharing system based on blockchains. J. King Saud Univ.-Comput. Inf. Sci. 2021, 34, 5045–5058.

25. Stafford, T.F.; Treiblmaier, H. Characteristics of a Blockchain Ecosystem for Secure and Sharable Electronic Medical Records. IEEE Trans. Eng. Manag. 2020, 67, 1340–1362.
26. Gan, C.; Saini, A.; Zhu, Q.; Xiang, Y.; Zhang, Z. Blockchain-based access control scheme with incentive mechanism for eHealth systems: Patient as supervisor. Multimed. Tools Appl. 2021, 80, 30605–30621.
27. Yakubu, A.M.; Chen, Y.P.P. A blockchain-based application for genomic access and variant discovery using smart contracts and homomorphic encryption. Futur. Gener. Comput. Syst. 2022, 137, 234–247.
28. Faber, B.; Michelet, G.C.; Weidmann, N.; Mukkamala, R.R.; Vatrapu, R. BPDIMS: A Blockchain-based Personal Data and Identity Management System. In Proceedings of the 52nd Hawaii International Conference on System Sciences, Maui, HI, USA, 8–11 January 2019; Volume 6, pp. 6855–6864.
29. Beinke, J.H.; Fitte, C.; Teuteberg, F. Towards a stakeholder-oriented blockchain-based architecture for electronic health records: Design science research study. J. Med. Internet Res. 2019, 21, e13585.