

Privacy and Security of Blockchain in Healthcare

Subjects: **Computer Science, Cybernetics**

Contributor: Hamed Taherdoost

Blockchain offers a cutting-edge solution for storing medical data, carrying out medical transactions, and establishing trust for medical data integration and exchange in a decentralized open healthcare network setting. While blockchain in healthcare has garnered considerable attention, privacy and security concerns remain at the center of the debate when adopting blockchain for information exchange in healthcare.

blockchain technology

security and privacy

medical industry

1. Introduction

In recent years, there has been an increase in the use of blockchain across a variety of industries, including healthcare ^{[1][2][3]}. This is not unexpected given that blockchain is an immutable, transparent, and decentralized distributed database ^[4] that may be used to create a trustworthy value chain. The digitization of the healthcare business is leading to the creation of medical information systems. While healthcare is a vital aspect of an individual's life, so are its associated data, which aid in the diagnosis of sickness and support future actions. In the past, information was written and recorded on media that may be easily altered and destroyed ^{[5][6]}. These systems need to possess the capacity to communicate data safely and efficiently ^[7]. Also, they need to enable increased anonymity, privacy, and access control for each user. If there is little or no security, privacy, and trust, people will be reticent to share their sensitive information, or they may delay obtaining treatment ^[8]. Data protection becomes necessary. Consequently, blockchain technology, a developing technology that claims to safeguard data leaks and data from vulnerabilities, has come to light ^[9].

Due to its distributed nature, blockchain technology might alter this dependency. It offers the capacity to overcome failure and assaults in a distributive and unchanging manner. Moreover, it gives a record of the data's ownership and legitimacy ^[10]. Hence, blockchain is increasingly seen as a general-purpose technology with applications in a variety of sectors and use cases, including healthcare, insurance, supply-chain management, contract administration, dispute resolution, and identity management ^[11]. Blockchain is characterized by its special characteristics of transparency, traceability, reliability, and decentralization. Hence, blockchain may be able to solve security, confidentiality, and interoperability problems. Blockchain enables parties who lack confidence to conduct a wide range of network transactions. A distributed network of devices' data may be recorded and stored in a blockchain ^[12].

The application of blockchain in healthcare has the potential to transform the storage and sharing of patient data, making the processes safer and more efficient. Concerns exist, however, about the security and privacy of blockchain in healthcare, especially with the safeguarding of sensitive patient data.

Blockchain

Blockchain was popularized by Bitcoin's success ^[13] and may be used to conduct secure and trustworthy transactions over an untrusted network without depending on a centralized third party. Based on the rights granted to network nodes, three kinds of blockchain systems exist:

- Private blockchain: Access control governs how the private blockchain network functions, requiring authorization or an invitation before users may join.
- Public ledger system: The public blockchain is accessible to anybody at any moment who wishes to participate as a basic node or a miner for economic benefits.
- Blockchain consortium: The consortium blockchain, which hovers between public and private blockchains, is referred to as "semi-private". It is given to a collection of authorized organizations that are often used in enterprises to advance business.

Blockchain's fundamental elements serve as an example of its structural underpinnings. Decentralization, first and foremost, is a key feature; data are stored and verified throughout a network of nodes, doing away with the necessity for a central point of control ^[14]. Additionally, data integrity is ensured by cryptographic hashing since each block contains a cryptographic hash of the preceding one, making it very difficult to tamper with the data ^[15]. Proof-of-work and proof-of-stake consensus processes make it easier to add additional blocks, while smart contracts automate and enforce contracts directly ^[16]. Blockchain is a trustworthy source of truth due to the immutability of the ledger and its dependence on public key cryptography, which guarantees the security and transparency of transactions ^[17].

Security in Healthcare

The security of healthcare data is achieved in several ways. Several studies have managed this by using administrative, physical, and technological concepts. To better safeguard the secure and safe patient data included in digital health information, these standards are made up of a variety of security methods that are used by healthcare organizations ^{[18][19]}. Patient data access is restricted using security protocols to protect it from unauthorized individuals. Operational controls may be used to do this inside a covered entity ^[20].

By securely storing and exchanging sensitive patient data, blockchain technology has the potential to transform the healthcare sector ^{[21][22]}. Data security is crucial in the healthcare sector because it protects sensitive patient data including medical histories, medications, and test results. Any compromise of this information might have negative effects on patients.

Blockchain technology appeals to healthcare businesses because it offers a safe, decentralized method of data sharing and keeping. Blockchain is simply a digital ledger that securely and impenetrably records transactions [13]. The information is kept in blocks, and each block is connected to the one before it in a chain, hence the term “blockchain”.

Privacy in Healthcare

Many issues in healthcare have been identified as possible candidates for blockchain technology solutions, including enhancing the security and privacy of patient data [22]. Since medical records include sensitive information that needs to be kept private, privacy is a crucial issue in the healthcare industry. Patients may suffer as a result of unauthorized access to such data, and healthcare professionals may face legal repercussions.

Blockchain technology offers certain advantages that make it a desirable choice for boosting healthcare privacy. It is a decentralized and distributed ledger, which means that data are spread among several network nodes. As a result, there is less chance of a centralized point of failure or attack target. Second, blockchain technology enables the development of smart contracts that can automate data sharing and enforce privacy laws [21]. The ability to encrypt and pseudonymize data stored on a blockchain allows for the protection of personal information while still enabling authorized parties to access the essential data.

Blockchain technology has the potential to enhance patient privacy, but some issues need to be resolved. The interoperability of various blockchain platforms is one of the biggest issues since healthcare providers may be utilizing dissimilar systems that cannot connect [23].

The use of zero-knowledge proofs on the blockchain offers a novel way to validate information without revealing the underlying data, thus enhancing data secrecy [24]. The idea of off-chain data storage is crucial for very sensitive data, guaranteeing that crucial information is kept outside the blockchain with just a reference (cryptographic hash) recorded there, reducing the danger of data disclosure [25]. Blockchain adds a further degree of anonymity by identifying transactions with cryptographic addresses rather than real-world identities, working in combination with various privacy-enhancing technologies. This pseudonymity increases patient confidentiality by making it less likely that private information will be connected to particular blockchain transactions [26]. Blockchain improves transparency and accountability in healthcare data management by automating consent management and data access rights. This not only assures regulatory adherence but also offers an auditable record of data treatment [27].

In conclusion, by offering a decentralized and secure platform for storing and exchanging patient data, blockchain technology can potentially improve healthcare privacy. Before blockchain technology is extensively used in healthcare settings, several issues need to be resolved.

Data Interoperability and Standards in Healthcare Blockchain

The key technological hurdle in using blockchain technology in the healthcare industry is interoperability [28]. The seamless interchange of healthcare data is made more difficult by the diverse character of healthcare systems,

each of which uses different electronic health record (EHR) systems and medical equipment with their own specific data formats and standards. It takes careful planning and data translation to integrate these many systems into a blockchain network. This difficulty is exacerbated by legacy systems that are inherently incompatible with blockchain technology [29].

Several possibilities and solutions exist to overcome these interoperability issues and realize the full potential of blockchain in healthcare. The creation of standardized data models and standards for healthcare data inside blockchain networks is one viable route. To provide a common language for data across various systems, these standards include standardized data formats for patient records, prescription information, test findings, and more [30].

Middleware, which permits connection between existing systems and blockchain networks, is another essential element [31]. These solutions make data translation and transmission between formats simple. Building consensus on data standards is also crucial. Collaboration between healthcare organizations, regulators, and technology providers is essential to develop these standards and lay the foundation for efficient data exchange and interoperability [32].

The use of blockchain-based identity management solutions may improve data security and interoperability [33]. These systems provide a safe basis for data transmission by discretely handling patient identities and access rights. The integration process is also made easier by systems that can map and translate data from diverse sources into a uniform format for blockchain [34]. Planning, data transformation, standards consensus, middleware solutions, cooperation, and identity management are just a few of the strategies shown in **Figure 1** for overcoming interoperability issues in healthcare blockchain integration.

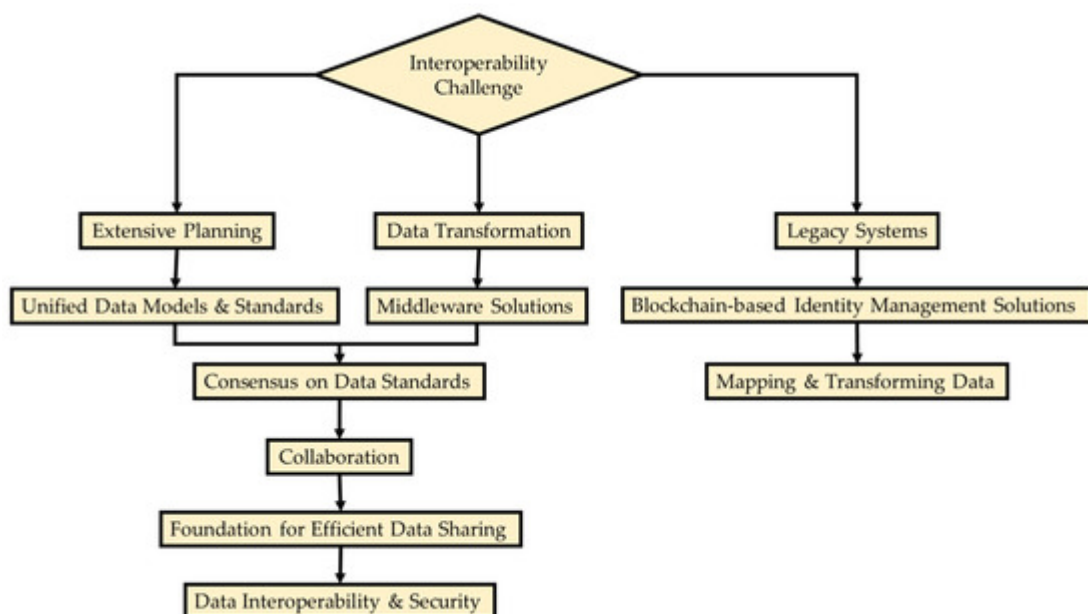


Figure 1. Blockchain in healthcare: interoperability challenges and solutions.

2. Privacy and Security of Blockchain in Healthcare

A new paradigm for exchanging medical picture data through a decentralized network is made possible by the use of blockchain and federated learning in the research by Kumar et al. [35]. The InterPlanetary File System-based infrastructure that has been developed for off-chain storage of health data enables the healthcare system to remain extremely secure, scalable, and resilient while still preserving patient privacy. The findings show that transmitting data to the blockchain has an influence mostly on execution time and computing effort, which is reasonable given the privacy and security that the architecture and encryption offer [36][37][38][39][40].

Several studies [41][42][43][44][45][46] suggested solutions that put the patient in control of approving and denying access rights, which make it simple for healthcare practitioners and organizations to adhere to privacy laws. The suggested solutions also provide safe payment procedures, enabling both individuals and hospitals to dependably pay for diagnostic and storage services.

The suggested techniques can withstand a variety of assaults, including impersonation, collusion, and man-in-the-middle attacks, according to a security analysis and extensive experimentation. The findings also show that the suggested solutions have strong anti-attack capabilities, balanced storage space allocation, and high-security encryption performance, all of which enhance the storage and transmission of health privacy data both within and outside the healthcare system.

In the Internet of Medical Things (IoMT) situations, the suggested solutions make use of customized smart contracts and modified attribute-based cryptographic primitives to ensure safe search, privacy preservation, and individualized access control. One of the constraints of sensor nodes in the Internet of Things (IoT) devices is space, hence the method in some of the research has been space-optimized [47].

The aforementioned studies demonstrate the promise of blockchain and cryptography technologies for safe, private, and effective access control and healthcare data exchange. The suggested methods are appropriate for IoMT applications because they have competitive computation and communication costs while meeting anticipated security requirements. The outcomes show that these technologies are practical and efficient in resolving long-standing privacy and security problems in the healthcare sector. **Figure 2** shows the papers' implications for healthcare privacy and security.

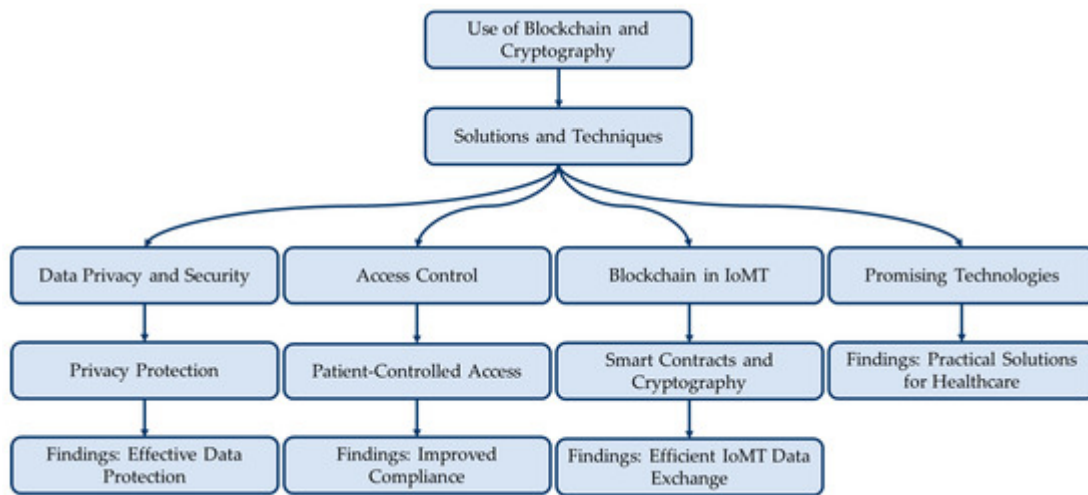


Figure 2. Privacy and security in healthcare with blockchain and cryptography.

Healthcare-related blockchain applications for security and privacy

The safety and privacy of patient information are major issues in the healthcare sector. To safeguard patients' rights and prevent data breaches, electronic health records (EHRs) need to be secure and private since they include sensitive and private information about patients. Blockchain technology is one use that may enhance EHR security and privacy. EHR systems built on blockchain technology may provide a safe and unhackable platform for exchanging and storing patient data. The decentralized nature of the blockchain can prevent data breaches and guarantee data integrity, while the use of smart contracts and cryptocurrency payments can guarantee that only authorized users have access to the data. Patient-controlled access is another example in which patients may decide who has access to their data and give or remove that access as necessary. By enabling patients to give or cancel access to their data at any moment and guaranteeing that it is only available to authorized parties, access control utilizing blockchain technology may also enhance data privacy. Neither of them demonstrates the utilization of smart contracts.

Strong security and privacy safeguards are also needed for PHR administration and sharing. PHRs, which include medical histories, test findings, and diagnoses, contain sensitive information about individuals' health. The privacy of patients can be secured, and only authorized people can access the data with the help of blockchain-assisted data sharing. The exchange of EHRs can also protect privacy, and the security and privacy of healthcare data can be increased by using privacy-preserving K-nearest neighbors (K-NN) training for IoT data [48][49]. Healthcare blockchain privacy may provide safe and unhackable platforms for storing and exchanging medical data, protecting the confidentiality and integrity of the information. Authentication and permission for healthcare data on the blockchain can further increase data security and privacy, ensuring that only authorized individuals have access to the data.

The blockchain's privacy and security problems in the healthcare industry

Healthcare has severe privacy and security problems. Security and privacy are crucial problems in healthcare because of the sensitivity of medical data and the potential damage that unauthorized access or data breaches might bring to people or organizations. By offering a decentralized and secure platform for data exchange and storage, blockchain technology provides a remedy. Secure search and individualized access control are made possible by cryptographic primitives, while access control and data privacy are guaranteed by smart contracts.

By simulation and experimental research, several suggested solutions have been verified and analyzed, proving the viability, effectiveness, and security of these systems. Several studies have shown that blockchain-based systems may retain competitive computing and communication costs while meeting anticipated security requirements. Other approaches, such as modified attribute-based cryptographic primitives and certificateless public-key encryption technology, have also proven successful in preserving privacy and enabling individualized access control in healthcare settings. However, healthcare practitioners and organizations need to carefully assess these solutions to make sure they adhere to privacy laws and are practical and scalable in real-world contexts.

The potential for blockchain security and privacy in the medical industry

In the coming years, it is anticipated that the healthcare sector will continue to prioritize enhancing security and privacy. Blockchain technology is being used more often as a method to safeguard healthcare data. User privacy is protected via a smart medical cloud platform where data may be utilized but not borrowed. To improve data security and privacy, one approach is the integration of new technologies like blockchain, federated learning, and edge computing. For instance, federated learning may enable collaborative data analysis without disclosing sensitive information, while blockchain technology can be utilized to provide secure access control and avoid data manipulation. Also, by processing data near its origin rather than sending it to a centralized place, edge computing may help lower the risk of data breaches.

Another possibility is implementing tougher rules and guidelines to guarantee private health information safety. It is more crucial than ever to protect health data from unwanted access and breaches as the volume of data grows. Regulations that attempt to safeguard the privacy and security of personal health information include the General Data Protection Regulation and the Health Insurance Portability and Accountability Act. Such laws and standards will probably keep being created and implemented to guarantee the security of health data in the future.

References

1. McGhin, T.; Choo, K.-K.R.; Liu, C.Z.; He, D. Blockchain in healthcare applications: Research challenges and opportunities. *J. Netw. Comput. Appl.* 2019, 135, 62–75.
2. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* 2018, 5, 31–37.

3. Epiphaniou, G.; Daly, H.; Al-Khateeb, H. Blockchain and healthcare. In *Blockchain and Clinical Trial: Securing Patient Data*; Springer: Cham, Switzerland, 2019; pp. 1–29.
4. Ahram, T.; Sargolzaei, A.; Sargolzaei, S.; Daniels, J.; Amaba, B. Blockchain technology innovations. In *Proceedings of the 2017 IEEE Technology & Engineering Management Conference (TEMSCON)*, Santa Clara, CA, USA, 8–10 June 2017; pp. 137–141.
5. Kuo, T.-T.; Zavaleta Rojas, H.; Ohno-Machado, L. Comparison of blockchain platforms: A systematic review and healthcare examples. *J. Am. Med. Inform. Assoc.* 2019, 26, 462–478.
6. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* 2018, 10, 470.
7. Khan, F.A.; Gumaei, A.; Derhab, A.; Hussain, A. A novel two-stage deep learning model for efficient network intrusion detection. *IEEE Access* 2019, 7, 30373–30385.
8. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In *Proceedings of the 2017 IEEE 28th Annual International Symposium on Personal, Indoor, and Mobile Radio Communications (PIMRC)*, Montreal, QC, Canada, 8–13 October 2017; pp. 1–5.
9. Yaqoob, S.; Khan, M.M.; Talib, R.; Butt, A.D.; Saleem, S.; Arif, F.; Nadeem, A. Use of blockchain in healthcare: A systematic literature review. *Int. J. Adv. Comput. Sci. Appl.* 2019, 10, 644–653.
10. Khalid, U.; Asim, M.; Baker, T.; Hung, P.C.; Tariq, M.A.; Rafferty, L. A decentralized lightweight blockchain-based authentication mechanism for IoT systems. *Clust. Comput.* 2020, 23, 2067–2087.
11. Burniske, C.; Vaughn, E.; Cahana, A.; Shelton, J. *How Blockchain Technology Can Enhance Electronic Health Record Operability*; Ark Invest: New York, NY, USA, 2016.
12. Taherdoost, H. Blockchain-Based Internet of Medical Things. *Appl. Sci.* 2023, 13, 1287.
13. Nakamoto, S. Bitcoin: A peer-to-peer electronic cash system. *Decentralized Bus. Rev.* 2008, 21260.
14. Sultan, A.; Mushtaq, M.A.; Abubakar, M. IOT security issues via blockchain: A review paper. In *ICBCT 2019: Proceedings of the 2019 International Conference on Blockchain Technology*; ACM: New York, NY, USA, 2019; pp. 60–65.
15. Anwar, M.R.; Apriani, D.; Adianita, I.R. Hash Algorithm In Verification Of Certificate Data Integrity And Security. *Aptisi Trans. Technopreneurship (ATT)* 2021, 3, 181–188.
16. Busayatananphon, C.; Boonchieng, E. Financial technology DeFi protocol: A review. In *Proceedings of the 2022 Joint International Conference on Digital Arts, Media and Technology with ECTI Northern Section Conference on Electrical, Electronics, Computer and*

Telecommunications Engineering (ECTI DAMT & NCON), Chiang Rai, Thailand, 26–28 January 2022; pp. 267–272.

17. Javaid, M.; Haleem, A.; Singh, R.P.; Suman, R.; Khan, S. A review of Blockchain Technology applications for financial services. *BenchCouncil Trans. Benchmarks Stand. Eval.* 2022, 2, 100073.
18. Mohanasundaram, S.; Ramirez-Asis, E.; Quispe-Talla, A.; Bhatt, M.W.; Shabaz, M. Experimental replacement of hops by mango in beer: Production and comparison of total phenolics, flavonoids, minerals, carbohydrates, proteins and toxic substances. *Int. J. Syst. Assur. Eng. Manag.* 2022, 13, 132–145.
19. Sriram, G. Edge computing vs. Cloud computing: An overview of big data challenges and opportunities for large enterprises. *Int. Res. J. Mod. Eng. Technol. Sci.* 2022, 4, 1331–1337.
20. Hassan, N.H.; Ismail, Z. A conceptual model for investigating factors influencing information security culture in healthcare environment. *Procedia-Soc. Behav. Sci.* 2012, 65, 1007–1012.
21. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In *Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD)*, Vienna, Austria, 22–24 August 2016; pp. 25–30.
22. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* 2017, 24, 1211–1220.
23. 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.
24. Gabay, D.; Akkaya, K.; Cebe, M. Privacy-preserving authentication scheme for connected electric vehicles using blockchain and zero knowledge proofs. *IEEE Trans. Veh. Technol.* 2020, 69, 5760–5772.
25. Miyachi, K.; Mackey, T.K. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. *Inf. Process. Manag.* 2021, 58, 102535.
26. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. *ACM Comput. Surv. (CSUR)* 2019, 52, 1–34.
27. Liu, W.; Zhu, S.; Mundie, T.; Krieger, U. Advanced block-chain architecture for e-health systems. In *Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom)*, Dalian, China, 12–15 October 2017; pp. 1–6.
28. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain technology use cases in healthcare. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41.

29. Appelbaum, D.; Cohen, E.; Kinory, E.; Stein Smith, S. Impediments to blockchain adoption. *J. Emerg. Technol. Account.* 2022, 19, 199–210.
30. Alnafrani, M.; Acharya, S. SecureRx: A blockchain-based framework for an electronic prescription system with opioids tracking. *Health Policy Technol.* 2021, 10, 100510.
31. Leng, J.; Chen, Z.; Huang, Z.; Zhu, X.; Su, H.; Lin, Z.; Zhang, D. Secure blockchain middleware for decentralized iiot towards industry 5.0: A review of architecture, enablers, challenges, and directions. *Machines* 2022, 10, 858.
32. Hasan, M.R.; Deng, S.; Sultana, N.; Hossain, M.Z. The applicability of blockchain technology in healthcare contexts to contain COVID-19 challenges. *Libr. Hi Tech* 2021, 39, 814–833.
33. Villarreal, E.R.D.; García-Alonso, J.; Moguel, E.; Alegría, J.A.H. Blockchain for healthcare management systems: A survey on interoperability and security. *IEEE Access* 2023, 11, 5629–5652.
34. Shae, Z.; Tsai, J. Transform blockchain into distributed parallel computing architecture for precision medicine. In *Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS)*, Vienna, Austria, 2–6 July 2018; pp. 1290–1299.
35. Kumar, R.; Kumar, J.; Khan, A.A.; Zakria; Ali, H.; Bernard, C.M.; Khan, R.U.; Zeng, S. Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. *Comput. Med. Imaging Graph.* 2022, 102, 102139.
36. Wang, Y.; Zhang, A.; Zhang, P.; Qu, Y.; Yu, S. Security-Aware and Privacy-Preserving Personal Health Record Sharing Using Consortium Blockchain. *IEEE Internet Things J.* 2022, 9, 12014–12028.
37. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage for healthcare data security and privacy. *J. Parallel Distrib. Comput.* 2022, 164, 152–167.
38. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy framework for Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. *J. Supercomput.* 2021, 77, 7916–7955.
39. Majdoubi, D.E.; Bakkali, H.E.; Sadki, S. SmartMedChain: A Blockchain-Based Privacy-Preserving Smart Healthcare Framework. *J. Healthc. Eng.* 2021, 2021, 4145512.
40. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F.; Chen, Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS ONE* 2020, 15, e0243043.
41. Younis, M.; Lalouani, W.; Lasla, N.; Emokpae, L.; Abdallah, M. Blockchain-Enabled and Data-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access. *IEEE Syst. J.* 2022, 16, 3746–3757.

42. Wu, G.; Wang, S.; Ning, Z.; Li, J. Blockchain-Enabled Privacy-Preserving Access Control for Data Publishing and Sharing in the Internet of Medical Things. *IEEE Internet Things J.* 2022, 9, 8091–8104.
43. Alzubi, O.A.; Alzubi, J.A.; Shankar, K.; Gupta, D. Blockchain and artificial intelligence enabled privacy-preserving medical data transmission in Internet of Things. *Trans. Emerg. Telecommun. Technol.* 2021, 32, e4360.
44. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* 2018, 39, 283–297.
45. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare Data Gateways: Found Healthcare Intelligence on Blockchain with Novel Privacy Risk Control. *J. Med. Syst.* 2016, 40, 218.
46. Mohammad Hossein, K.; Esmaeili, M.E.; Dargahi, T.; Khonsari, A.; Conti, M. BCHealth: A Novel Blockchain-based Privacy-Preserving Architecture for IoT Healthcare Applications. *Comput. Commun.* 2021, 180, 31–47.
47. Yugha, R.; Chithra, S.; Bhalaji, N.; Karthika, S. Privacy Protected IoT-Blockchain using ZKP for Healthcare application. *Control Eng. Appl. Inform.* 2022, 24, 76–87.
48. Ul Haque, R.; Hasan, A.S.M.T.; Jiang, Q.; Qu, Q. Privacy-preserving k-nearest neighbors training over blockchain-based encrypted health data. *Electronics* 2020, 9, 96.
49. Al-Otaibi, Y.D. K-nearest neighbour-based smart contract for internet of medical things security using blockchain. *Comput. Electr. Eng.* 2022, 101, 108129.

Retrieved from <https://encyclopedia.pub/entry/history/show/116222>