BLOCKCHAIN IN HEALTHCARE: UNLOCKING THE POTENTIAL OF BLOCKCHAIN FOR SECURE AND EFFICIENT APPLICATIONS FOR MEDICAL DATA MANAGEMENT- A PRESENTATION OF BASIC CONCEPTS

Zia Ahmed Shaikh[1], Azar Akbar Memon[1], Ahmed Muhammad Sheikh[2], Samiullah Soomro[1], Mehran Sayed[1],

[1]A.H.S Bukhari Postgraduate Institute of Information and Communication Technology, University of Sindh, Pakistan, [2]COMSATS University, Islamabad, Pakistan

Correspondence:
Zia Ahmed Shaikh,
A.H.S Bukhari Postgraduate Institute of Information and Communication Technology, University of Sindh, Pakistan
Email: ziaahmed-shaikh@gmail.com

DOI: 10.38106/LMRJ.2023.5.2-08
Received: 29.05.2023
Accepted: 27.06.2023
Published: 30. 06.2023

ABSTRACT

Medical data management presents significant challenges in terms of security, privacy, and efficiency. Blockchain technology has emerged as a promising solution to address these concerns in recent years. This comprehensive review explores the role of blockchain technology in secure and efficient medical data management. By providing a decentralized and immutable ledger, blockchain ensures data integrity, enhances privacy, and facilitates auditable access to medical information. The paper examines various applications of blockchain in medical data management, including electronic health records (EHRs), medical imaging, clinical trials, telemedicine, and drug supply chain management. It highlights the benefits and challenges of implementing blockchain in healthcare settings, discussing interoperability, consent management, scalability, and regulatory considerations. The review encompasses relevant research studies, industry initiatives, and real-world use cases to provide a comprehensive overview of the current state of blockchain technology in medical data management. The paper concludes with a discussion of future directions and potential areas for further research, emphasizing the transformative potential of blockchain in revolutionizing the way of medical data storage, sharing, and utilization.

Key Words: Blockchain, Medical data systems, Electronic health records, Security, privacy

INTRODUCTION

Effective medical data management has been crucial throughout healthcare for delivering high-quality medical services, advancing research, and improving patient outcomes. Traditional approaches such as databases and distributed data management systems have played a significant role in storing, retrieving, and processing medical information. However, they have encountered security, privacy, data integrity, and interoperability challenges. Databases have been widely used in healthcare sector to store patient records, diagnostic results, and medical histories. These systems have provided structured storage and efficient querying capabilities, enabling healthcare providers to access patient information as needed. While databases and distributed data management systems have served healthcare reasonably well, they are not without limitations. Centralized databases can be vulnerable to single points of failure, exposing them to data breaches and unauthorized access. Furthermore, data silos created by disparate systems hinder seamless information exchange between healthcare providers, leading to fragmented care and a lack of continuity. To address the interoperability challenges, Application Programming Interfaces (APIs) have played a crucial role in enabling data connectivity across various healthcare systems. Service Oriented Architectures (SOAs) based on Web-Services and Web-APIs facilitate data exchange between software applications and systems (1), allowing for interoperability and seamless communication. They provide a standardized interface for accessing and sharing medical data, fostering integration among electronic health records (EHRs), medical imaging systems, laboratory information systems, and other healthcare applications.

However, despite the role of APIs in promoting data interoperability, limitations exist. Healthcare APIs often face challenges with different data formats, varying data standards, and inconsistent implementation. Additionally, concerns regarding data privacy, security, and the lack of standardized APIs across different healthcare systems pose barriers to achieving full interoperability.

Introduction to Blockchain

Blockchain technology has emerged as a promising solution to address challenges related to medical data management (2). Originally developed as the underlying technology for cryptocurrencies, blockchain offers a decentralized, transparent, and immutable ledger that can revolutionize the way medical data is handled. By leveraging cryptographic algorithms and consensus mechanisms, blockchain ensures data integrity, immutability, and resistance to tampering (3). Since blockchain is transforming various industries nowadays (4-7).

Characteristics of Blockchain

Figure 1 presents blockchain's key characteristics: decentralization, immutability, security, transparency, trust and consensus, data privacy, scalability, smart contracts, interoperability and auditability. These characteristics collectively contribute to the unique value proposition of blockchain technology in a number of fields including healthcare.

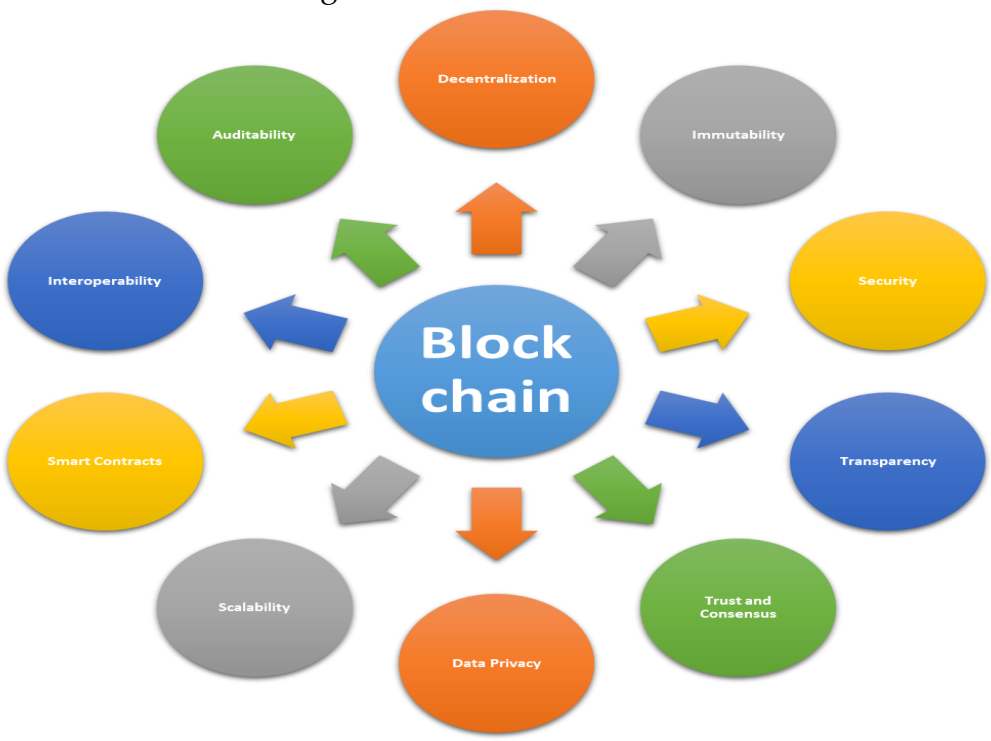

Figure 1. Key characteristics of Blockchain network

Decentralization: Blockchain works in a decentralized network, where there is no need to have a central control. This allows for peer-to-peer transactions and consensus among participants, promoting trust and transparency.

Immutability: As the data is added to the blockchain, it cannot be altered or deleted. The immutability feature ensures data integrity and enhances trust in the system.

Security: Blockchain operates upon cutting-edge cryptographic algorithms to provide highly secure data. Transactions are recorded in a transparent and tamper-resistant manner, making it difficult for unauthorized parties to manipulate or access sensitive information.

Transparency: Blockchain provides transparency by allowing all participants in the network to have access to the same information. Each transaction is recorded in a public ledger, promoting accountability thus reducing the risk of fraud.

Trust and Consensus: Blockchain relies on consensus mechanisms, like proof of work to authenticate transactions. This decentralized consensus ensures trust among participants without the need for a centralized authority.

Data Privacy: While blockchain promotes transparency, it also ensures privacy through the use of cryptographic techniques. Participants can maintain control over their personal data and determine the level of access granted to others.

Scalability: Scalability has been a challenge for blockchain technology due to limitations in transaction processing speed and storage capacity. However, various solutions are being developed to address these scalability concerns, such as off-chain transactions and layer-two solutions.

Smart Contracts: Blockchain platforms support self-executin agrrements having pre-defined conditions. Once the pre-defined conditions are meet, smart contracts automate processes and enable the execution of transactions.

Interoperability: Interoperability refers to the ability of different blockchain networks or systems to communicate and share data seamlessly. Standards and protocols are being developed to enhance interoperability and facilitate the exchange of information across various blockchain platforms.

Auditability: The transparent nature of blockchain allows for easy auditing of transactions. Every transaction on the blockchain can be traced and verified, providing an auditable record of events and enhancing accountability.

Blockchain Data Structure

Blockchain works in a decentralized computer network (i.e. nodes), where each node maintains a copy of the entire ledger. A ledger is a collection of blocks, and each block consists of various transactions which contain data. In healthcare it will be patient's data, ensuring redundancy and resilience. The distributed nature of the network enhances security and eliminates the need for a central authority(8, 9).

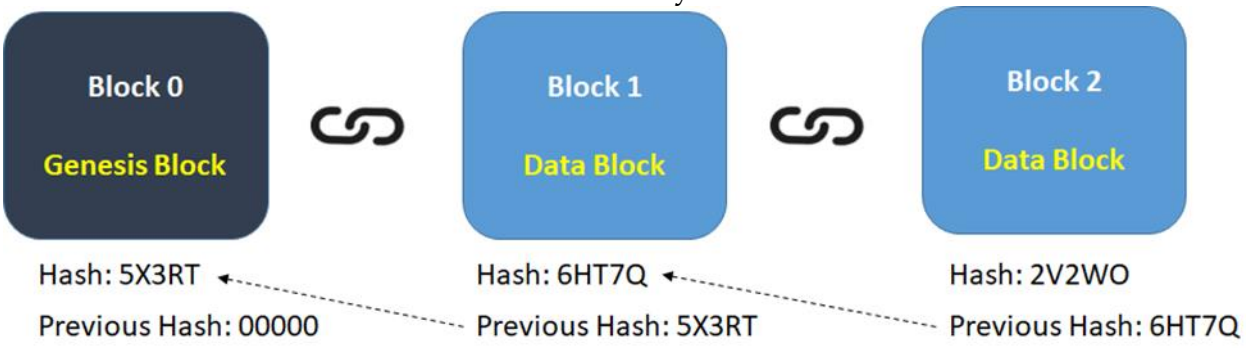

Figure 2: Connected blocks forming a blockchain

Each block contains different kind of data such as index, timestamp, hash, previous block hash and most importantly the data. Here, each block stores the information about its previous block's hash, which forms a chain of blocks. Some key components of blockchain are discussed here under. Figure 2 presents the format of block formation.

Components of blockchain

Index: The index or block number represents the position of the block within the blockchain. It is a unique identifier for each block and helps maintain the chronological order of the blocks in the chain.

Hash: The hash is a unique digital fingerprint generated by applying a cryptographic hash function to the data contained within the block. It serves as a digital signature that uniquely identifies the block and ensures its integrity. Even a minor change in the block's data would result in a different hash, alerting the network to potential tampering attempts.

Previous Hash: Each block (except the first block, also known as the genesis block) contains a reference to the hash of the previous block in the chain. This linking of blocks via their previous hash creates a sequential and tamper-resistant structure. Any modification to a previous block would require recalculating the hash of that block and all subsequent blocks, making it computationally infeasible to alter the blockchain undetected.

Timestamp: The timestamp represents the point in time when the block was created or added to the blockchain. It provides information about the order of events and helps maintain the chronological order of the blocks. Additionally, the timestamp adds a temporal dimension to the blockchain, enabling the tracking of events and ensuring that blocks are added in a logical sequence.

Data: The data component of a block contains the actual information or payload that is stored within the blockchain. In the context of a medical data system, this could include patient records, treatment information, diagnostic results, genomic data, or any other relevant healthcare-related data. The data is typically represented in a structured format and may be encrypted to protect patient privacy and ensure data security.

Blocks: Blocks are containers that store a set of data and transactions. Each block typically includes a unique identifier called a hash, a timestamp, and a reference to the previous block's hash. The blocks are linked together in a chronological order, forming a chain of blocks.

Consensus Mechanism: Consensus mechanisms enable nodes in the blockchain network to agree on the validity of transactions and the order in which they are added to the blockchain. Popular consensus mechanisms include proof of work (PoW)(10), proof of stake (PoS)(11), delegated proof of stake (DPoS), and practical Byzantine fault tolerance (PBFT)(12).

Cryptography: Blockchain relies on cryptographic techniques to secure data and provide privacy and authenticity. Public-key cryptography is commonly used for identity verification, digital signatures, and encryption of data within the blockchain. Cryptographic hashes ensure the integrity and immutability of the blocks(13).

Governance: Blockchain networks may have governance mechanisms in place to make decisions about protocol upgrades, changes, or other network parameters. Governance can be implemented through voting systems, committees, or community-driven processes to ensure the evolution and improvement of the blockchain network.

User Interfaces and Wallets: User interfaces and wallets provide an interface for users to interact with the blockchain network. They allow users to view their account balance, initiate transactions, interact with smart contracts, and manage their cryptographic keys (14).

These components collectively contribute to the functioning and security of a blockchain. The distributed network, blocks, consensus mechanism, cryptography, smart contracts, consensus incentives, governance (if applicable), and user interfaces form the foundation for building secure, transparent, and decentralized systems for various applications.

Blockchain in Medical Data Systems

Blockchain technology can play a role in various areas of medical science. Here are some key areas where blockchain can be applied:

Medical Data Management: Blockchain can enhance the security, privacy, and integrity of medical data, including electronic health records (EHRs), medical imaging, patient-generated data, and clinical research data. It enables decentralized storage, secure sharing, and auditable access to sensitive medical information while maintaining patient confidentiality.

Interoperability and Health Information Exchange: Blockchain can facilitate seamless interoperability and standardized exchange of medical data among different healthcare providers, healthcare systems, and medical devices. It enables the creation of a unified and comprehensive patient health record by securely integrating data from disparate sources.

Clinical Trials and Research: Blockchain can streamline and enhance transparency in clinical trials by securely recording and verifying trial protocols, participant consent, and data collection processes. It can also enable secure sharing and collaboration among researchers, while protecting intellectual property rights and ensuring data integrity.

Genomic Data Sharing: Blockchain can provide a secure and decentralized platform for sharing genomic data among researchers, healthcare institutions, and individuals. It ensures data privacy by allowing individuals to control access to their genomic information while still facilitating collaboration and data-driven research.

Immutable Storage and Traceability of Data: Blockchain's immutability can ensure the integrity and traceability of genomic and proteomic data. By recording data transactions on the blockchain, it becomes difficult to alter or manipulate the data, thereby enhancing the reliability and trustworthiness of research findings and clinical outcomes.

Personalized Medicine and Pharmacogenomics: Blockchain can support personalized medicine by securely storing and managing genomic and proteomic data. Smart contracts on the blockchain can enable the execution of personalized treatment plans based on individual genetic profiles and proteomic markers, improving therapeutic outcomes and reducing adverse drug reactions.

Drug Supply Chain Management: Blockchain can improve the traceability and transparency of the pharmaceutical supply chain. It enables tracking the journey of drugs from manufacturers to patients, reducing the risk of counterfeit drugs, and ensuring the authenticity and quality of medications.

Telemedicine and Remote Patient Monitoring: Blockchain can facilitate secure and private telemedicine consultations, remote patient monitoring, and the exchange of patient data between healthcare providers and patients. It can enable patients to maintain control over their health data and grant temporary access to healthcare professionals.

Medical Device Data Security: Blockchain can enhance the security and integrity of medical device data by providing an immutable record of device configurations, usage logs, and maintenance history. It can help detect tampering attempts and ensure the accuracy and reliability of device-generated data.

Healthcare Payment Systems: Blockchain can improve the efficiency and transparency of healthcare payment systems, reducing administrative costs and minimizing fraud. It can enable secure and automated transactions, streamlined claims processing, and accurate billing and reimbursement processes.

These are just a few examples, and the potential applications of blockchain in medical science are continually expanding. Blockchain's inherent properties make it an attractive technology for healthcare. Its decentralized nature eliminates the need for intermediaries and provides a secure and transparent environment for data transactions. By distributing data across a network of participants, blockchain can enhance data security, privacy, and interoperability. Moreover, the immutable nature of blockchain ensures the integrity of medical data, reducing the risk of data manipulation or tampering.

CONCLUSION

This review presented basic concepts of blockchain data management system in healthcare, including EHRs, medical imaging, clinical trials, telemedicine, and drug supply chain management.

CONFLICT OF INTEREST: Authors declare no conflict of Interest

REFERENCES

1. ZH Khuhro; N Zaman; ZA Shaikh, "Service-Oriented Architecture and Web Services," J. Inf. Commun. Technol., vol. 3, no. 2, pp. 71–76, 2009.
2. I. A. I. K. Dahri, M.A. Memon, K. Khoumbati, "Interoperable Health Care System Using Blockchain Technology," SI NDH Univ. Res. (SCIENCE Ser., vol. 51, no. 03, pp. 437–440, 2019.
3. K. Dahri, B. Memon, M. Aquib, and Z. A. Shaikh, "Blockchain Implementation Challenges and Limitations: A Critical Review," Univ. Sindh J. Inf. Commun. Technol., vol. 4, no. 4, pp. 245–248, 2020.
4. M. Aquib, L. Das Dhomeja, K. Dahri, and Y. A. Malkani, "Blockchain-based Land Record Management in Pakistan," in 2020 3rd International Conference on Computing, Mathematics and Engineering Technologies (iCoMET), Jan. 2020. doi: 10.1109/iCoMET48670.2020.9073927.
5. S. L. K. Pournader, Mehrdokht, Yangyan Shi, Stefan Seuring, "Blockchain applications in supply chains, transport and logistics: a systematic review of the literature," Int. J. Prod. Res. 58, no. 7, 2020.
6. N. C. Komal Gilani, Emmanuel Bertin, Julien Hatin, "A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data," BRAIN 2020 2nd Conf. Blockchain Res. Appl. Innov. Networks Serv., pp. 97–101, 2020, [Online]. Available: https://hal.archives-ouvertes.fr/hal-02650705/document
7. K. Christidis and M. Devetsikiotis, "Blockchains and Smart Contracts for the Internet of Things," IEEE Access. 2016. doi: 10.1109/ACCESS.2016.2566339.
8. A. Alharby, Maher; van Moorsel, "Blockchain Based Smart Contracts - A Systematic Mapping Study," Comput. Sci. Inf. Technol., pp. 125–140, 2017, doi: 10.5121/csit.2017.71011.
9. C. Q. Mingxiao, Du, Ma Xiaofeng, Zhang Zhe, Wang Xiangwei, "A review on consensus algorithm of blockchain.," in IEEE international conference on systems, man, and cybernetics (SMC), pp. 2567-2572. IEEE, 2017.
10. wackerow, "Proof-of-work (PoW) | ethereum.org," Sep. 27, 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/pow/ (accessed Oct. 27, 2022).
11. "Proof-of-stake (PoS) | ethereum.org," Oct. 22, 2022. https://ethereum.org/en/developers/docs/consensus-mechanisms/pos/ (accessed Oct. 27, 2022).
12. M. C. B. Liskov;, "Practical Byzantine fault tolerance," Proc. OSDI, vol. 99, pp. 173–186, 1999.
13. A. Kosba, A. Miller, E. Shi, Z. Wen, and C. Papamanthou, "Hawk: The Blockchain Model of Cryptography and Privacy-Preserving Smart Contracts," in Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016, 2016, pp. 839–858. doi: 10.1109/SP.2016.55.
14. P. J. Nitin Naik, "Govern Your Identity Through Your Digital Wallet using Blockchain Technology," in 2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud), 2020. [Online]. Available: https://publications.aston.ac.uk/id/eprint/41998/1/SSI_Specifications_uPort_SovrinDrNitinNaik.pdf