Review of Contemporary Philosophy
ISSN: 1841-5261, e-ISSN: 2471-089X
Vol 22 (1), 2023
pp. 3952 - 3963

Blockchain and Healthcare Systems: Integration of Blockchain in Healthcare Informatics-An Updated Review

[1]-Mohammed Aedh Saeed Aljabri,[2]-Mashael Kamal Binsaeed ,[3]-Badr Mohammed Ali Alsahli ,[4]- Abdullah Ali Aldhmaly,[5]-Haya Saud Alanazi,[6]-Fatmah Ali Saeid Alqrnui,[7]-Ali Jabir Khuwairi,[8]-Nasser Mohamas Salem Al-Mutairi,[9]-Abdulkaream Farhan Owid Almotairi,[10]-Abduilh Abdulraman Hajer Al Harbl,[11]-Adel Mukhlid Dhahi Al Omayri ,[12]-Hejab Bin Abdullah Aldossary,[13]-Saud Ahmed Ail Kabani ,[14]-Ayman Mohammed Abudyah,[15]- Ali Yahya Mousa Mahash ,

[1] KSA, Ministry Of Health, Medina Health Cluster King Salman Bin Abdul-Aziz Medical City Paychlatric Hospital
[2] KSA, Ministry Of Health, Riyadh Specialized Dental Center
[3] KSA, Ministry Of Health, Rawidat Al-Ared General Hospital
[4] KSA, Ministry Of Health, Rawidat Al-Ared General Hospita
[5] KSA, Ministry Of Health, Riyadh Specialized Dental Center
[6] KSA, Ministry Of Health, Dental Center In Hafar Albatin
[7] KSA, Ministry Of Health, King Saud Medical City
[8] KSA, Ministry Of Health, Al Rass General Hospital
[9] KSA, Ministry Of Health, Al Rass General Hospital
[10] KSA, Ministry Of Health, Al Rass General Hospital
[11] KSA, Ministry Of Health, Riyadh Alkabra Hospital
[12] KSA, Ministry Of Health, ALSULAYIL HOSPITAL GENRAL
[13] KSA, Ministry Of Health, Damad General Hospital
[14] KSA, Ministry Of Health, Damad General Hospital
[15] KSA, Ministry Of Health, Damad General Hospital

Abstract:

Background: Healthcare systems face major challenges with data security, management costs, and inefficient information sharing across diverse stakeholders. Traditional healthcare information systems struggle to address these issues, especially concerning privacy and trust. Blockchain technology, with its decentralized, immutable, and secure nature, presents a promising solution to these challenges by improving data integrity and transparency.

Aim: This review aims to examine the integration of blockchain technology into healthcare informatics, exploring its potential to enhance data security, streamline data sharing, and improve the overall management of healthcare information.

Methods: The review synthesizes existing literature on blockchain's applications in healthcare. It evaluates various blockchain models, such as private, public, and consortium blockchains, and their specific uses in patient data management, medical record sharing, and cost management. Additionally, the review assesses the scalability and security of blockchain-based systems in healthcare contexts.

Results: The study identifies blockchain as a transformative tool that can address existing challenges in healthcare systems, such as data breaches, inefficiencies, and privacy concerns. Blockchain-based systems are found to enhance trust between healthcare providers and patients, ensuring secure and transparent sharing of health data. The use of consensus algorithms and Distributed Data Storage Systems (DDSS) further improves data management.

Conclusion: Blockchain technology has significant potential to disrupt healthcare systems by providing a decentralized and secure infrastructure for electronic health records (EHR). It can also address key issues such as privacy, security, and inefficiencies, ultimately leading to more effective and transparent healthcare management.

Keywords: Blockchain, healthcare informatics, data security, electronic health records, patient data management, decentralized systems.

Received: 16 october 2023 **Revised:** 29 November 2023 **Accepted:** 13 December 2023

Introduction:

One of the biggest problems facing modern healthcare systems is high maintenance and management costs [1]. Doctors, researchers, practitioners, support staff, management staff, and patients are only a few of the many domains that make up the extremely complex healthcare system [2]. As a result, managing and organizing patient data becomes extremely difficult [3,4]. The diverse workflows and heterogeneous data formats found in several healthcare domains exacerbate this challenge. Therefore, a significant barrier is the ineffective sharing of healthcare-related data among these different domains [5]. A system must be created, run, and maintained to handle the interchange and administration of health information. Despite the fact that third-party organizations usually create and manage traditional PHR and EHR systems, trust, privacy, and data security concerns remain major worries [6]. However, because of ongoing privacy and data security issues, these third-party-based solutions fall short of stakeholders' expectations about privacy [7], which results in a lack of transparency in the conventional electronic healthcare model.

Blockchain technology offers interesting solutions to these security issues as well as the challenging problem of handling large amounts of heterogeneous data in healthcare systems [8]. Blockchain is a digital ledger, peer-to-peer network, and decentralized, distributed database [9]. It enables the safe transfer of data between people by connecting numerous computers via nodes and does not require transactions to generate new blocks. All approved and verifiable medical data is accessible to clients thanks to blockchain technology, which is supported by cryptography. The master key of a blockchain is a hash, which employs the hash function to generate unique identifiers for cryptocurrencies and add data. Anyone can select transactions and add a new chain to the block. Stakeholders are reluctant to work together and share health information since traditional PHR and EHR-based systems have not been able to adequately handle privacy and security concerns. As a result, both patients and healthcare providers are now burdened by the growing expenditures of healthcare. Researchers and governments are increasingly using blockchain technology to address these trust-related problems. By improving management systems and creating a decentralized foundation for the sharing of electronic health information, blockchain is expected to drastically disrupt the healthcare system, according to IBM and several top healthcare organizations [10]. The market for blockchain technology is anticipated to grow to a value of over USD 500 million by 2022 [11]. The use of blockchain in healthcare has been the subject of many studies, but the body of current research does not offer a thorough grasp of how it might be applied in different contexts. Thus, a thorough investigation of the possible uses of blockchain technology in the healthcare industry is unquestionably necessary. These days, a lot of servers are being created to provide services to customers using mobile devices. With mobile devices and a plethora of applications, it is possible to generate and send a significant amount of medical data every day or every week in today's digital environment. Cost limits, operational inefficiencies, the need for standardization, and individual behavioral restraints in service delivery are just a few of the challenges that the existing healthcare system may be able to overcome [12].

However, healthcare providers frequently do not take full advantage of the most recent technological developments in the supply chain. For example, new strategies for gathering and allocating medical supplies are frequently not carried out successfully. Indeed, according to a Healthcare Finance research, needless supply chain operations and administration cost close to USD 25.7 billion a year [13]. To overcome these constraints and satisfy the rising demand for better healthcare, considerable work is required to develop a more intelligent healthcare system. The design and development issues associated

with smart devices, tools, improved facilities, and modernized healthcare organizations could be the main focus of this system. Additionally, it might encourage the creation of intelligent healthcare solutions that make use of biosensors, customer-connected apps, and state-of-the-art emergency services [14]. To improve healthcare services, it is crucial to discover consensus algorithms that are currently in use across different blockchain networks and ascertain which are compatible with Internet of Things (IoT)-based infrastructures in order to create a more effective network [15]. Additionally, using Distributed Data Storage Systems (DDSS), a quicker data-sharing method, will help with the issue of huge data storage in blockchain [16]. This system tracks several documents with the same name that are kept in the same place by using file translation and data caching. In order to access the complete file using Distributed Hash Tables (DHT), a large file uploaded to DDSS is split up into smaller data objects, like 256 kb files, then linked together into an empty object [17]. With the use of some sensors, users' data can be automatically collected and sent to cloud systems or designated storage for additional analysis by medical staff, doctors, and nurses [18]. There are strict penalties for non-compliance with the rules and regulations that have been established to protect patient privacy. These requirements require strong security management for the control, sharing, and exchange of health data in electronic healthcare systems (EHRs) [19]. Nearly 70% of healthcare executives believe blockchain will have a big impact on the healthcare industry, especially in areas like clinical trials, regulatory compliance, and the development of a decentralized framework for the exchange of electronic health records (EHR), according to an IBM report [20].

Blockchain-based healthcare systems are quickly gaining traction in both real-world applications and research fields because of their improved data security and economic management. The amount of research on blockchain-based healthcare systems has grown rapidly during the last ten years. Nonetheless, there is a noticeable lack of thorough data gathering and representation of earlier studies in this field. Review articles that already exist usually provide succinct overviews of current advancements and highlight the benefits and drawbacks of different approaches put forth by scholars. These reviews, however, do not offer a thorough analysis of the various aspects of blockchain in healthcare systems, including the research topics being investigated, the particular healthcare domains where blockchain is most frequently used, the applications of blockchain in different fields, and the current blockchain-based healthcare systems. By offering a thorough review of the body of existing literature, pointing out possible blockchain applications in a variety of healthcare specialties, and discussing potential future research avenues, obstacles, and opportunities in the blockchain-based healthcare industry, this study aims to close these gaps. Presenting a thorough analysis of the body of existing literature is the study's ultimate contribution, which will help to consolidate the body of knowledge on the use of blockchain in healthcare.

Background Study of Blockchain

What Is Blockchain?

Blockchain represents a decentralized and immutable data structure designed to streamline the tracking of assets and recording of transactions across a network. It is composed of an expanding series of blocks, each securely linked to one another through cryptographic methods. These blocks contain transaction data, timestamps, and a cryptographic hash that refers to the preceding block, ensuring the continuity and integrity of the entire chain. The timestamp provides evidence of the data’s existence at the moment the block was created. The blocks form a sequential chain, as each block holds information about its predecessor, which ensures interconnection. Consequently, once a transaction is recorded, it becomes irreversible, as altering any block would necessitate changing all subsequent blocks, thus rendering blockchain transactions tamper-proof.

Key Features

A central attribute of blockchain technology is decentralization. There is no single governing body that controls the blockchain, but rather, each entry is validated and recorded by participants in a peer-to-peer network through various consensus protocols, as further explained in Section 2.1.4. The security of data is a critical aspect of blockchain transactions, as information is transferred directly between parties without the need for intermediaries, thereby minimizing the risk of data breaches or modifications. Another

significant feature is persistence; once data is entered into the blockchain, it becomes immutable and cannot be deleted, as it is recorded on a distributed ledger that spans multiple nodes [21]. Additionally, blockchain provides a degree of pseudonymity, where users' identities may be obscured, which is a common feature across various blockchain implementations. **Figure 1** provides a visual representation of the primary features of blockchain technology. Blockchain's design facilitates auditability and traceability by linking each new block to the preceding one, forming a chain structure. This linkage is verified through the creation of a Merkle tree, where each leaf value represents a transaction, and the root of the tree serves as the ultimate verification point. This structure allows the blockchain to maintain the integrity of the data and ensures that only the root of the tree is necessary for verification, as illustrated in **Figure 2**.

Different Kinds of Blockchain

There are three main types of blockchain: private, public, and consortium [21]. Each type varies in terms of who can write, read, and access the data stored on the blockchain. A public blockchain allows anyone to view the data, participate in transactions, or even modify the original software. Public blockchains have gained popularity, especially in the context of cryptocurrencies such as Bitcoin [23] and Ethereum [24]. In contrast, a consortium blockchain is accessible only to a predefined group of participants, while a private blockchain is a closed system where access is restricted to a central authority, preventing external entities from interacting with the network. However, there is no universally accepted definition or classification system for blockchain types [25].

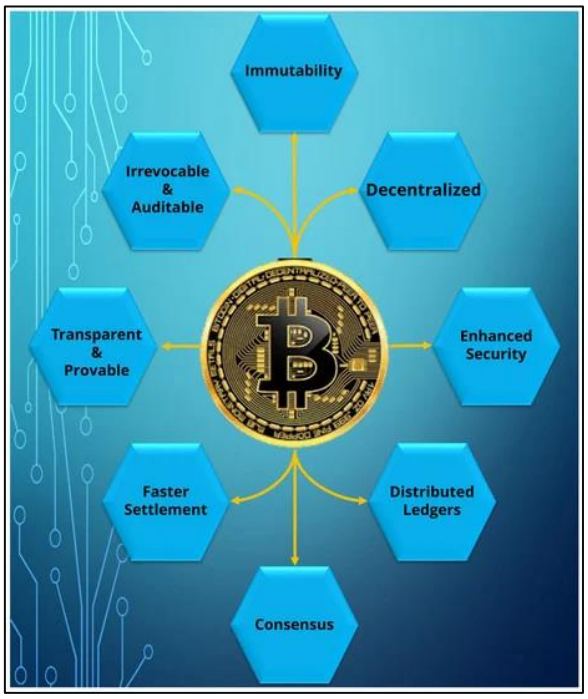

Figure 1: Key Features of Blockchain Technology.

The data below outlines the distinctions between the three blockchain types:

- **Private Blockchain**: Characterized by high efficiency, consensus determined by a single organization, and centralized control. Data on private blockchains can be tampered with, and participation is restricted.
- **Consortium Blockchain**: Features high efficiency and consensus determination by a selected group of nodes. It operates with partial centralization and may be subject to tampering, though to a lesser degree than private blockchains.
- **Public Blockchain**: Has low efficiency, with consensus achieved by all miners, and is decentralized. The data within public blockchains are publicly accessible, and tampering is highly improbable.

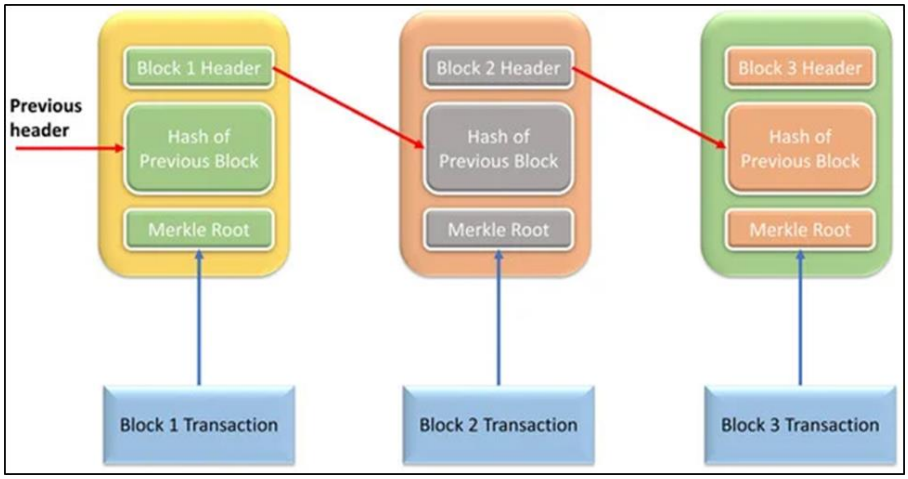

Figure 2: Blockchain Structure.

Difference between Blockchain in Healthcare and General Sectors

Since its inception with Bitcoin, blockchain technology has primarily been utilized for financial transactions. Over the last decade, numerous cryptocurrencies, including Ethereum, Tether, BNB, and Dogecoin, have been developed, taking advantage of blockchain's decentralized, secure, and immutable nature, making it an ideal solution for large-scale financial activities such as lending and insurance. In contrast, the key application of blockchain in healthcare revolves around the management of patient data, ensuring secure and protected information exchange. Blockchain in the healthcare sector is not limited to monetary transactions but extends to safeguarding personal data and facilitating secure medical record sharing. Blockchain's applications have significantly evolved in recent years. Initially designed for cryptocurrencies, blockchain is now being employed in various sectors such as voting, where its tamper-resistant features ensure integrity. The use of smart contracts enforces accountability and guarantees the consistency of agreements among parties. Furthermore, blockchain has been leveraged to address the security concerns of Internet of Things (IoT) systems by providing secure communication and data storage solutions. The potential applications of blockchain are virtually limitless, constrained only by the creativity of its users. In this study, while the primary focus is the impact of blockchain in healthcare, the technology's broader applicability across sectors is noteworthy. The healthcare sector utilizes all the functionalities offered by blockchain, including secure monetary transactions, personal data protection, logistics, and overall data security.

Existing Blockchains

There are now several established blockchain frameworks and platforms that facilitate the development of decentralized applications. Prominent examples include Hyperledger [26] and Ethereum [24], both of which provide developers with the tools to build new applications upon existing blockchain infrastructures and create custom test networks based on their protocols.

Mechanisms for Consensus

Data entries within a blockchain network are accepted through distributed ledgers and data entry protocols that rely on distributed consent mechanisms. Three of the most commonly employed consensus protocols. The proof-of-work (PoW) consensus protocol is integrally linked to Bitcoin, making it a central component of blockchain technology. In PoW, miners engage in competition to solve a computationally intensive puzzle. They use brute force methods to find a hash for the proposed block that meets a predefined value. Miners who successfully compute the hash and validate a transaction within the block are rewarded. However, the major drawback of the PoW protocol is its substantial energy consumption, particularly when applied to large-scale blockchains [27].

On the other hand, the proof-of-stake (PoS) protocol operates by selecting a node based on its stake in the blockchain. In PoS, stakes represent the portion of cryptocurrency held by a participant. This model

has been criticized for disproportionately benefiting wealthier nodes. To mitigate this, several variations of PoS have been proposed, incorporating randomization to select the authorized node. Ethereum, for example, is transitioning from a PoW to a PoS protocol [21]. The practical tolerance of the Byzantine defect is addressed through the Byzantine Convention [28]. In the case of practical Byzantine fault tolerance (PBFT), the network of nodes must be predetermined, which limits its applicability to universal blockchains. PBFT is divided into three categories: committed, pre-prepared, and prepared. Transitioning between these stages requires a consensus of (2/3) of the nodes. Currently, PBFT is implemented in Hyperledger Fabric [29]. When comparing the three protocols, it is evident that PBFT employs authorized nodes, PoS relies on accessible nodes, and PoW also uses accessible nodes. In terms of adversarial tolerance, PBFT can withstand up to 33.3% faulty replicas, PoS can tolerate stakes less than 51%, and PoW can withstand up to 25% of computational power being controlled by adversaries. Energy expenditure in these protocols varies, with PoW consuming the highest energy, followed by PoS, and PBFT requiring the least. Notable implementations of these protocols include Hyperledger Fabric for PBFT, Peercoin for PoS, and Bitcoin for PoW [29][21][23].

Smart Contracts

Ethereum, a prominent blockchain infrastructure, offers a noteworthy feature: the support of smart contracts [24]. These contracts are self-executing, with the terms of the agreement encoded in predefined source code. Cryptographic contracts eliminate the need for intermediaries, streamlining processes by directly activating functions within the blockchain. This feature is increasingly used across various domains, particularly in healthcare, where it facilitates secure and automated operations [24].

Blockchain Potential in Healthcare

The healthcare sector faces challenges involving staff-intensive environments and the need for secure data access from diverse sources. The data generated within healthcare systems must be accurately edited and processed to maintain trust across all operational sectors. These operations encompass a variety of activities, including health problem-solving, knowledge-based care, clinical decision-making, triage, and evaluation. Depending on the nature of the care provided, patients should have access to the latest technology, expertise, and experiences. Collaboration with educational institutions further facilitates the development of skilled healthcare workers, while clinical research and trials benefit from such partnerships. Healthcare organizations support research by providing informants, samples, and other resources, while research institutions contribute methodologies and tools. In these collaborations, the secure exchange of patient data, consent, and evidence, as well as payment processing, is necessary.

Data integrity and access control are paramount to ensuring the confidentiality of patient information and securing data exchanges. Effective access management fosters trust between data owners and institutions, with the server playing a critical role in defining and enforcing access policies [30]. Interactivity, which allows various information systems and devices to connect and share data across organizational boundaries, is crucial for improving individual and collective health outcomes. The provenance of healthcare data, specifically Electronic Health Records (EHRs), enables better tracking and validation of information, thereby enhancing trust in the system. As Courtney and Ware [31] highlight, data integrity refers to the alignment of data with expected quality standards, and the extent to which data meets the required quality defines its integrity. At present, healthcare organizations are increasingly reliant on data requests from research institutes [32]. Unauthorized data sharing and theft undermine public trust in the healthcare system, with malpractice further eroding confidence. To address these concerns, blockchain's decentralized nature can ensure secure data sharing, integrity, and access control without the need for third-party intermediaries, thereby reinforcing trust among stakeholders.

Types of Blockchain in Healthcare System: Public, Private, and Consortium

Blockchain networks connect nodes to validate transactions within the system, with various types of blockchain protocols based on node familiarity and network permissions. Authorized blockchains, such as Ripple [33] and Hyperledger Fabric [34], involve participants who are already known within the

network. Public blockchains, exemplified by Bitcoin [35] and Ethereum [36], are open networks where anyone can join and become a member, providing decentralized data transfer capabilities within a peer-to-peer (P2P) network. This decentralized structure significantly reduces the costs associated with arbitration, modification, and system maintenance. Despite these advantages, public blockchains often face scalability challenges [37].

Public Blockchain

A public blockchain is an open network that allows anyone to access and participate in the system. Members can engage in the consensus process through mechanisms like proof of work embedded in smart contracts. The goal of public blockchains is to eliminate centralized control, ensuring decentralization through the use of P2P blocks and the Merkle hash cryptography tree. Transactions are synchronized across all nodes, and any participant can become a node, providing them with blockchain files. However, the energy consumption of public blockchains increases with the number of connected nodes, as substantial power is needed to validate transactions [38].

Private Blockchain

Private blockchains are restricted to authorized participants, with data access and transaction verification requiring permission. Unlike public blockchains, which operate under a decentralized system, private blockchains do not offer the same level of decentralization. While private blockchains can achieve a high degree of expertise in transaction validation, they are less flexible in terms of access, as only authorized entities can participate in transaction verification [39].

Consortium Blockchain

Consortium blockchains represent a hybrid model that blends elements of both public and private blockchains. They are partially decentralized, with pre-selected nodes performing data transactions in both private and public blockchains. This model combines the trusted entities of private blockchains with the openness of public blockchains, though strong encryption is required to secure transactions. While consortium blockchains offer a balance between reliability, legitimacy, and decentralization, they still face challenges in ensuring flawless operation across all participants [40][41].

Blockchain Integration in Healthcare Information System:

Blockchain technology, originally designed for cryptocurrency transactions, has gradually found significant applications across various industries, including healthcare. Its potential to revolutionize the healthcare sector stems from its ability to enhance data security, improve patient privacy, streamline operations, and provide better interoperability between different healthcare systems. Integrating blockchain into healthcare information systems could address several long-standing challenges, such as data breaches, inefficiency in administrative tasks, and difficulties in managing patient records across disparate organizations. One of the most notable advantages of blockchain in healthcare is its capability to provide secure and immutable records. Blockchain operates on a decentralized ledger system, where each transaction or data entry is encrypted and linked to previous entries, forming a chain of blocks. Once data is entered into the blockchain, it cannot be altered or deleted without the consensus of the majority of network participants. This feature significantly reduces the risk of data manipulation and unauthorized access, which is a growing concern in healthcare, where sensitive patient data is frequently targeted by cyberattacks. Moreover, blockchain technology offers greater transparency in data sharing. In healthcare, numerous stakeholders, including doctors, hospitals, insurance companies, and patients, need access to health data at various stages of care. Traditional systems often face challenges in maintaining the integrity and privacy of data while ensuring that the right people have access to it. Blockchain's decentralized nature means that only authorized parties have access to specific data, and all transactions are recorded transparently, offering an auditable trail of actions taken. This ensures that patients have control over their personal health data and can give or revoke access to authorized entities at any time.

The integration of blockchain into healthcare systems can also improve data interoperability, which is a significant issue in the sector. Health data is often stored in siloed systems, making it difficult to share and access crucial information. The lack of standardization in data formats and protocols further exacerbates this challenge. Blockchain's ability to create a unified, distributed ledger accessible to all parties involved could enable seamless sharing of patient information across different institutions, regardless of the underlying technologies they use. This could facilitate better coordination of care and lead to improved patient outcomes, especially in emergency situations where rapid access to comprehensive health records is crucial. Additionally, blockchain can address issues related to medical supply chain management. Counterfeit drugs and medical supplies are a significant concern in healthcare, as they can lead to serious harm and even fatalities. Blockchain's ability to track and authenticate products from their origin to their end-users can help reduce the prevalence of counterfeit goods. Each stage of the supply chain, from manufacturing to distribution, can be logged into a blockchain, providing a transparent record that can be accessed by authorized entities. This enables stakeholders to verify the authenticity of products and ensure their safety before they reach the patient.

In the context of clinical trials, blockchain could also play a critical role. Clinical trials often face challenges related to data integrity and transparency, with issues such as selective reporting and data tampering. Blockchain can provide an immutable record of trial data, ensuring that the information collected throughout the process remains unchanged and transparent. This can foster trust in the results of clinical trials and encourage more participation from both patients and researchers. Moreover, blockchain can enhance the management of consent in clinical trials. Patients can give or withdraw consent for participation through secure blockchain-based systems, ensuring that their rights are protected throughout the research process. Despite its numerous benefits, integrating blockchain into healthcare systems comes with its challenges. One of the main obstacles is the need for regulatory alignment. Healthcare is a highly regulated industry, and any new technology, including blockchain, must comply with existing laws and standards, such as the Health Insurance Portability and Accountability Act (HIPAA) in the United States. Regulations surrounding the use of blockchain for patient data must be clear and standardized to ensure that the technology can be adopted safely and effectively. Additionally, the implementation of blockchain systems requires significant investment in infrastructure and training, which could be a barrier for smaller healthcare organizations or those with limited resources.

Furthermore, while blockchain offers enhanced security, it is not completely immune to vulnerabilities. The security of the blockchain network itself relies on the consensus mechanism and the ability of the network participants to maintain integrity. If a large proportion of the network is compromised, there could be potential risks to the data stored on the blockchain. Therefore, careful attention must be paid to ensure that blockchain networks are secure and that appropriate safeguards are in place to prevent attacks. Another challenge is the scalability of blockchain solutions. Blockchain networks, especially those using proof-of-work consensus mechanisms, can be energy-intensive and may struggle to handle the vast amounts of data generated by healthcare systems. The current limitations of blockchain in terms of transaction speed and cost need to be addressed before it can be fully integrated into large-scale healthcare information systems. Solutions such as the use of hybrid blockchain models or the development of more efficient consensus algorithms may help overcome these challenges.

Despite these challenges, the integration of blockchain into healthcare holds immense promise. As the technology continues to evolve, its potential to improve the efficiency, security, and interoperability of healthcare information systems will become more apparent. By addressing the concerns related to scalability, regulatory compliance, and security, blockchain can be transformed into a valuable tool for the healthcare industry. The ongoing research and pilot projects in blockchain applications in healthcare show that the industry is moving towards adopting this transformative technology, paving the way for a more secure, efficient, and patient-centered healthcare ecosystem. In conclusion, blockchain has the potential to significantly improve healthcare information systems by enhancing data security, transparency, and interoperability. Its ability to securely store and share health records, track the supply chain, and ensure data integrity in clinical trials can revolutionize the way healthcare is delivered. However, challenges such

as regulatory compliance, scalability, and security must be addressed before blockchain can be fully integrated into healthcare systems. With ongoing advancements, blockchain may become a cornerstone of the future healthcare ecosystem, providing safer and more efficient care for patients.

Conclusion:

The integration of blockchain technology into healthcare systems offers a transformative approach to managing patient data, ensuring security, and improving efficiency. Traditional healthcare systems face numerous challenges, particularly in handling vast amounts of sensitive information across a range of stakeholders, including patients, healthcare providers, and administrators. Blockchain's decentralized nature enables secure, transparent, and efficient sharing of health data, addressing many of the inefficiencies and trust issues inherent in current systems. A significant advantage of blockchain is its ability to ensure the privacy and integrity of patient data. Through cryptographic techniques and consensus algorithms, blockchain allows for the secure sharing of medical records among authorized parties without the need for intermediaries. This transparency not only enhances trust between patients and healthcare providers but also ensures that data is tamper-proof, preventing unauthorized modifications. Furthermore, the implementation of Distributed Data Storage Systems (DDSS) in blockchain networks resolves concerns regarding the scalability and storage of large data volumes, ensuring fast and efficient access to health records. Blockchain's impact on healthcare extends beyond data management. It has the potential to reduce administrative costs, improve supply chain management, and streamline processes such as medical billing and insurance claims. By eliminating inefficiencies and reducing reliance on intermediaries, blockchain can significantly lower the operational costs of healthcare systems. Moreover, it facilitates real-time updates and tracking of patient data, enhancing decision-making and patient care. However, there are challenges to blockchain integration, including technical barriers, regulatory hurdles, and the need for widespread adoption across healthcare systems. Despite these challenges, the growing interest in blockchain applications by healthcare stakeholders indicates a promising future for the technology. By fostering more secure, efficient, and transparent systems, blockchain can help address many of the pressing issues facing modern healthcare, ultimately improving patient outcomes and the overall healthcare experience. Future research should focus onz refining blockchain frameworks, addressing interoperability issues, and exploring additional applications in the healthcare sector.

References:

[1] McClean, S.; Gillespie, J.; Garg, L.; Barton, M.; Scotney, B.; Kullerton, K. Using phase-type models to cost stroke patient care across health, social and community services. *Eur. J. Oper. Res.* **2014**, *236*, 190–199.

[2] Soltanisehat, L.; Alizadeh, R.; Hao, H.; Choo, K.K.R. Technical, Temporal, and Spatial Research Challenges and Opportunities in Blockchain-Based Healthcare: A Systematic Literature Review. *IEEE Trans. Eng. Manag.* **2023**, *70*, 353–368.

[3] Xing, W.; Bei, Y. Medical Health Big Data Classification Based on KNN Classification Algorithm. *IEEE Access* **2020**, *8*, 28808–28819.

[4] Khan, A.A.; Wagan, A.A.; Laghari, A.A.; Gilal, A.R.; Aziz, I.A.; Talpur, B.A. BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts. *IEEE Access* **2022**, *10*, 78887–78898.

[5] Quadery, S.E.U.; Hasan, M.; Khan, M.M. Consumer side economic perception of telemedicine during COVID-19 era: A survey on Bangladesh's perspective. *Inform. Med. Unlocked* **2021**, *27*, 100797.

[6] Tomlinson, M.; Rotheram-Borus, M.J.; Swartz, L.; Tsai, A.C. Scaling up mhealth: Where is the evidence. *PLoS Med.* **2013**, *10*, e1001382.

[7] Chanda, J.N.; Chowdhury, I.A.; Peyaru, M.; Barua, S.; Islam, M.; Hasan, M. Healthcare Monitoring System for Dedicated COVID-19 Hospitals or Isolation Centers. In Proceedings of the 2021 IEEE Mysore Sub Section International Conference (MysuruCon), Hassan, India, 24–25 October 2021; pp. 405–410.

[8] Cagigas, D.; Clifton, J.; Diaz-Fuentes, D.; Fernández-Gutiérrez, M. Blockchain for Public Services: A Systematic Literature Review. *IEEE Access* **2021**, *9*, 13904–13921.

[9] Jabeen, F.; Hamid, Z.; Akhunzada, A.; Abdul, W.; Ghouzali, S. Trust and Reputation Management in Healthcare Systems: Taxonomy, Requirements and Open Issues. *IEEE Access* **2018**, *6*, 17246–17263.

[10] Ghayvat, H.; Pandya, S.; Bhattacharya, P.; Zuhair, M.; Rashid, M.; Hakak, S.; Dev, K. CP-BDHCA: Blockchain-Based Confidentiality-Privacy Preserving Big Data Scheme for Healthcare Clouds and Applications. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1937–1948.

[11] Wang, S.; Ouyang, L.; Yuan, Y.; Ni, X.; Han, X.; Wang, F.Y. Blockchain-Enabled Smart Contracts: Architecture, Applications, and Future Trends. *IEEE Trans. Syst. Man Cybern. Syst.* **2019**, *49*, 2266–2277.

[12] Khatri, S.; Alzahrani, F.A.; Ansari, M.T.J.; Agrawal, A.; Kumar, R.; Khan, R.A. A Systematic Analysis on Blockchain Integration with Healthcare Domain: Scope and Challenges. *IEEE Access* **2021**, *9*, 84666–84687.

[13] Omar, I.A.; Jayaraman, R.; Debe, M.S.; Salah, K.; Yaqoob, I.; Omar, M. Automating Procurement Contracts in the Healthcare Supply Chain Using Blockchain Smart Contracts. *IEEE Access* **2021**, *9*, 37397–37409.

[14] Shynu, P.G.; Menon, V.G.; Kumar, R.L.; Kadry, S.; Nam, Y. Blockchain-Based Secure Healthcare Application for Diabetic-Cardio Disease Prediction in Fog Computing. *IEEE Access* **2021**, *9*, 45706–45720.

[15] Sun, Z.H.; Chen, Z.; Cao, S.; Ming, X. Potential Requirements and Opportunities of Blockchain-Based Industrial IoT in Supply Chain: A Survey. *IEEE Trans. Comput. Soc. Syst.* **2022**, *9*, 1469–1483.

[16] Fernández-Caramés, T.M.; Fraga-Lamas, P. A Review on the Use of Blockchain for the Internet of Things. *IEEE Access* **2018**, *6*, 32979–33001.

[17] Liu, Q.; Liu, Y.; Luo, M.; He, D.; Wang, H.; Choo, K.-K.R.C. The Security of Blockchain-Based Medical Systems: Research Challenges and Opportunities. *IEEE Syst. J.* **2022**, *16*, 5741–5752.

[18] Wu, G.; Wang, S.; Ning, Z.; Zhu, B. Privacy-Preserved Electronic Medical Record Exchanging and Sharing: A Blockchain-Based Smart Healthcare System. *IEEE J. Biomed. Health Inform.* **2022**, *26*, 1917–1927.

[19] Ahmed, I.; Mousa, A. Security and Privacy Issues in Ehealthcare Systems: Towards Trusted Services. *Int. J. Adv. Comput. Sci. Appl.* **2016**, *7*, 229–236.

[20] Ren, J.; Li, J.; Liu, H.; Qin, T. Task offloading strategy with emergency handling and blockchain security in SDN-empowered and fog-assisted healthcare IoT. *Tsinghua Sci. Technol.* **2022**, *27*, 760–776.

[21] Chinaei, M.H.; Gharakheili, H.H.; Sivaraman, V. Optimal Witnessing of Healthcare IoT Data Using Blockchain Logging Contract. *IEEE Internet Things J.* **2021**, *8*, 10117–10130.

[22] Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-Based Framework for Security and Privacy-Assured Internet of Medical Things With Effective Access Control. *IEEE Internet Things J.* **2021**, *8*, 11717–11731.

[23] Li, P.; Xu, C.; Jin, H.; Hu, C.; Luo, Y.; Cao, Y.; Mathew, J.; Ma, Y. ChainSDI: A Software-Defined Infrastructure for Regulation-Compliant Home-Based Healthcare Services Secured by Blockchains. *IEEE Syst. J.* **2020**, *14*, 2042–2053.

[24] Qahtan, S.; Sharif, K.Y.; Zaidan, A.A.; Alsattar, H.A.; Albahri, O.S.; Zaidan, B.B.; Zulzalil, H.; Osman, M.H.; Alamoodi, A.H.; Mohammed, R.T. Novel Multi Security and Privacy Benchmarking Framework for Blockchain-Based IoT Healthcare Industry 4.0 Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 6415–6423.

[25] Kapadiya, K.; Patel, U.; Gupta, R.; Alshehri, M.D.; Tanwar, S.; Sharma, G.; Bokoro, P.N. Blockchain and AI-Empowered Healthcare Insurance Fraud Detection: An Analysis, Architecture, and Future Prospects. *IEEE Access* **2022**, *10*, 79606–79627.

[26] Kumar, R.; Kumar, P.; Tripathi, R.; Gupta, G.P.; Islam, A.N.; Shorfuzzaman, M. Permissioned Blockchain and Deep Learning for Secure and Efficient Data Sharing in Industrial Healthcare Systems. *IEEE Trans. Ind. Inform.* **2022**, *18*, 8065–8073.

[27] Saini, A.; Wijaya, D.; Kaur, N.; Xiang, Y.; Gao, L. LSP: Lightweight Smart-Contract-Based Transaction Prioritization Scheme for Smart Healthcare. *IEEE Internet Things J.* **2022**, *9*, 14005–14017.

[28] Singh, A.P.; Pradhan, N.R.; Luhach, A.K.; Agnihotri, S.; Jhanjhi, N.Z.; Verma, S.; Ghosh, U.; Roy, D.S. A Novel Patient-Centric Architectural Framework for Blockchain-Enabled Healthcare Applications. *IEEE Trans. Ind. Inform.* **2021**, *17*, 5779–5789.

[29] Hasselgren, A.; Kralevska, K.; Gligoroski, D.; Pedersen, S.A.; Faxvaag, A. Blockchain in healthcare and health sciences—A scoping review. *Int. J. Med. Inform.* **2020**, *134*, 104040.

[30] Aujla, G.S.; Jindal, A. A Decoupled Blockchain Approach for Edge-Envisioned IoT-Based Healthcare Monitoring. *IEEE J. Sel. Areas Commun.* **2021**, *39*, 491–499.

[31] Saini, A.; Zhu, Q.; Singh, N.; Xiang, Y.; Gao, L.; Zhang, Y. A Smart-Contract-Based Access Control Framework for Cloud Smart Healthcare System. *IEEE Internet Things J.* **2021**, *8*, 5914–5925.

[32] Akash, S.S.; Ferdous, M.S. A Blockchain Based System for Healthcare Digital Twin. *IEEE Access* **2022**, *10*, 50523–50547.

[33] Bansal, G.; Rajgopal, K.; Chamola, V.; Xiong, Z.; Niyato, D. Healthcare in Metaverse: A Survey on Current Metaverse Applications in Healthcare. *IEEE Access* **2022**, *10*, 119914–119946.

[34] Yazdinejad, A.; Srivastava, G.; Parizi, R.M.; Dehghantanha, A.; Choo, K.K.R.; Aledhari, M. Decentralized Authentication of Distributed Patients in Hospital Networks Using Blockchain. *IEEE J. Biomed. Health Inform.* **2020**, *24*, 2146–2156.

[35] Kumar, Y.; Nakamoto, S. Bitcoin 6.0: Military Grade e-Payment System. *SSRN Electron. J.* **2020**.

[36] Jolfaei, A.A.; Aghili, S.F.; Singelee, D. A Survey on Blockchain-Based IoMT Systems: Towards Scalability. *IEEE Access* **2021**, *9*, 148948–148975.

[37] Dinh, T.T.A.; Liu, R.; Zhang, M.; Chen, G.; Ooi, B.C.; Wang, J. Untangling Blockchain: A Data Processing View of Blockchain Systems. *IEEE Trans. Knowl. Data Eng.* **2018**, *30*, 1366–1385.

[38] Anoaica, A.; Levard, H. Quantitative Description of Internal Activity on the Ethereum Public Blockchain. In Proceedings of the 2018 9th IFIP international conference on New technologies, Mobility and security (NTMS), Paris, France, 26–28 February 2018; pp. 1–5.

[39] Feng, L.; Zhang, H.; Tsai, W.T.; Sun, S. System architecture for high-performance permissioned blockchains. *Front. Comput. Sci.* **2019**, *13*, 1151–1165.

[40] Khan, C.; Lewis, A.; Rutland, E.; Wan, C.; Rutter, K.; Thompson, C. A Distributed-Ledger Consortium Model for Collaborative Innovation. *Computer* **2017**, *50*, 29–37.

[41] King, S.; Nadal, S. PPCoin: Peer-to-Peer Crypto-Currency with Proof-of-Stake. In Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security—CCS'16, Vienna, Austria, 24–28 October 2016; Volume 1918, pp. 1–27.

الملخص:

الخلفية: تواجه أنظمة الرعاية الصحية تحديات كبيرة تتعلق بأمن البيانات، وتكاليف الإدارة، وعدم كفاءة تبادل المعلومات بين الأطراف المعنية المتنوعة. تكافح أنظمة المعلومات الصحية التقليدية لمعالجة هذه القضايا، خاصة فيما يتعلق بالخصوصية والثقة. تقدم تقنية البلوكشين، بطبيعتها اللامركزية، الثابتة، والآمنة، حلاً واعدًا لهذه التحديات من خلال تحسين نزاهة البيانات وشفافيتها.

الهدف: تهدف هذه المراجعة إلى دراسة دمج تقنية البلوكشين في معلومات الرعاية الصحية، واستكشاف إمكانياتها في تعزيز أمان البيانات، وتبسيط مشاركة البيانات، وتحسين إدارة المعلومات الصحية بشكل عام.

الطرق: تدمج المراجعة الأدبيات الحالية حول تطبيقات البلوكشين في الرعاية الصحية. كما تقيم نماذج البلوكشين المختلفة، مثل البلوكشين الخاص، والعام، وبلوكشين الاتحادات، واستخداماتها المحددة في إدارة بيانات المرضى، ومشاركة السجلات الطبية، وإدارة التكاليف. بالإضافة إلى ذلك، تقيّم المراجعة قابلية التوسع وأمان الأنظمة المبنية على البلوكشين في سياقات الرعاية الصحية.

النتائج: تحدد الدراسة البلوكشين كأداة تحوّلية يمكنها معالجة التحديات الحالية في أنظمة الرعاية الصحية، مثل تسريبات البيانات، وعدم الكفاءة، والمخاوف المتعلقة بالخصوصية. تم العثور على أن الأنظمة المعتمدة على البلوكشين تعزز الثقة بين مقدمي الرعاية الصحية والمرضى، مما يضمن مشاركة آمنة وشفافة للبيانات الصحية. كما أن استخدام خوارزميات الإجماع وأنظمة تخزين البيانات الموزعة (DDSS) يُحسن إدارة البيانات.

الخاتمة: تتمتع تقنية البلوكشين بإمكانات كبيرة لإحداث تغيير في أنظمة الرعاية الصحية من خلال توفير بنية تحتية لامركزية وآمنة للسجلات الصحية الإلكترونية (EHR). يمكنها أيضًا معالجة القضايا الرئيسية مثل الخصوصية، والأمان، وعدم الكفاءة، مما يؤدي في النهاية إلى إدارة رعاية صحية أكثر فعالية وشفافية.

الكلمات الرئيسية: البلوكشين، معلومات الرعاية الصحية، أمان البيانات، السجلات الصحية الإلكترونية، إدارة بيانات المرضى، الأنظمة اللامركزية.