Grenze International Journal of Engineering and Technology, June Issue

A Review of Blockchain for Secure Patient Data in Healthcare

Lucky Ghai[1], Shree Druthi Jalimenchi[2] and Palash Gourshettiwar[3]
[1-3]Department of Artificial Intelligence and Data Science, Faculty of Engineering & Technology, Datta Meghe Institute of Higher Education and Research, Wardha, Maharashtra, India 442001
Email: luckyghai.wr@gmail.com, shreedruthij@gmail.com, palashg.feat@dmiher.edu.in

***Abstract*—There are many hurdles that the healthcare industry goes through to protect patient data, which is always required since healthcare data is very sensitive. Blockchain technology is quite effective for maintaining data's perpetual integrities and privacies. This paper aims to analyse the applicability of the blockchain concept in the healthcare sector, where the emphasis is made on the technical ability of the idea to facilitate secure and comprehensive decentralised information management for patients. The first part of the paper introduces the topic and considers the growing need for secure data handling in healthcare. The second part provides an overview of the related studies and the development of blockchain solutions. A brief explanation of how the blockchain algorithms work is given, and then the different potential uses of blockchain in healthcare are discussed, such as in EHR and medical supply chain. The descriptive architecture of blockchain in the healthcare domain is also discussed, and then the implementation issues of the technology domain are explained. Lastly, the paper looks at the future direction and possible advancement concerning the use of blockchain in the health sector. The research analyses reveal that blockchain should be implemented to improve data protection, share, reuse, and identifiability of patient data with immense opportunities to increase the quality of patients' treatment and healthcare organisation effectiveness shortly.**

***Index Terms*— Blockchain, Healthcare, Patient Data, Security.**

I. INTRODUCTION

In Modern Healthcare System, Health information security for patients is essential because of technological advancements that require digital means to store patient data. Over time, Electronic Health Records (EHRs), Wearable health devices, and telemedicine platforms have changed how patient data is captured, managed, and transmitted, increasing convenience and effectiveness. They also increase the healthcare system's risk of exposure to data theft, illicit entry, and cybercrime. This data often includes and is usually not limited to the identifying particular of the patient, financial records and other personal and medical records. Thus, it becomes a valuable asset for the hackers. They stated that one breach may result in identification theft, money loss, and care compromise. In addition, that is dangerous for patients, and the lack of confidence is critical for healthcare organisations and their future. Data protection measures guaranteeing strong security guarantees are not only limited to legal standards of personal data protection, such as GDPR or HIPAA, but also raise the issue of trust, transparency, and responsibility. With integrated and interoperable solutions gradually integrated into healthcare IT structures, shielding patient information from new threats becomes critical [1].

Grenze ID: 01.GIJET.11.2.119_20

Data Privacy and Integrity in Healthcare are challenging, especially because patients' records are sensitive and uniquely identifiable information. An unbounded growth point is attributed to the rising utilisation of EHRs, wearable devices, and telemedicine platforms, which contribute sizable amounts of data and expose vast resources to cyber threats. Increased cross-healthcare stakeholders' data sharing with hospitals, Insurance companies and research organisations also increases the exposure to breaches and misuse. Most traditional healthcare systems are not very secure; thus, they can easily be vulnerable to the most advanced hacking. The fourth crucial question is what is at risk due to the actions of an employee with IT privileges who shares information unauthorised. Preserving data accuracy is also an issue because any change to the patient records may mislead personnel, cause improper treatment, and ruin trust. A dynamic and innovative approach is required to serve this purpose, simultaneously providing ready access to the data and applying security measures coupled with the need to satisfy various legislations like GDPR or HIPAA [2].

Blockchain is emerging as a disruptive technology in various sectors, including healthcare, due to its inherent decentralisation, immutability, and transparency capabilities. Unlike traditional computer systems, which utilise centralised structural databases, blockchain for computer systems uses a distributed database, where information is distributed among multiple nodes, thereby eliminating susceptibilities to single points of failure. This decentralisation increases system reliability as it becomes difficult for an unauthorised person to tamper with data. In the healthcare industry, blockchain has the practical application of handling patient information in safe, secure, immutable ways and shared only with the right people. Offering a clear and trace-to-a-level trail within several business processes also helps improve accountability and confidence within several healthcare processes. Also, avoiding intermediaries becomes possible with blockchain, creating a push for lesser spending and quicker transactions. Integrating it into smart contracts can extend the efficiency in handling sophisticated healthcare processes while reducing the margin of error through using smart contracts in claim handling and patient consent. Identifying significant means of innovation using blockchain in transforming and providing secure healthcare systems with structures and frameworks in place, with extensive discussions on data privacy, in an open source to actualise more empowered patient and efficient administrative structures [3].

This review discusses the opportunity of blockchain technology applications in healthcare systems, emphasising the issues concerning patient records' security issues, using information concerning data privacy, data integrity and integration. It is to apprise the utilisation of blockchain and advance its effectiveness in the various tedious healthcare processes, including claim settlement and patients' consent, via a decentralised and automated system. The areas within the review's remit are principles of blockchain, the use of blockchain for managing EHRs, the fight against fraud and work in progress. Also, the review will discuss the limitations of implementing Blockchain System Management for secure healthcare data management based on regulation, ethical, and legal questions, as well as the prospects for future blockchain systems for healthcare information management.

II. Literature Review

Alhadhrami et al. [4] examine the applicability of blockchain technology to the administration and sharing of electronic health and medical records among stakeholders in the e-health industry. In the paper, the author focuses on the potential of blockchain technology in enhancing the exchange of interoperable data by patients, hospitals, clinics, and other stakeholders in the health sector. Alhadhrami et al. specify the issues concerning the blockchain structures, including such issues as the privacy of the patient's information and the stability of the blockchain networks against attacks. This study also brings out possible recommendations for the challenges, insisting that more attention needs to be paid to selecting the proper Blockchain architectures concerning actors in the network, privacy and data authenticity.

Ismail et al. [5] presented an efficient distributed architecture for managing and sharing health information through blockchain since current healthcare systems still have some limitations, including single points of failure, data privacy concerns, and vulnerabilities. The paper also focuses on the problems the Bitcoin permission-less network faces, such as high energy consumption, less scalability and low throughput and then presents a better solution. To lessen the computational and communication load, Ismail et al. propose a blockchain structure where all the participants in the network keep just one copy of the ledger, which is then grouped into clusters. The proposed solutions involve a dedicated channel for financially confidential transactions between the group of participants and the problem of forking, typical for the Bitcoin network. Through experimental analysis, the authors establish that their design logically outweighs the Bitcoin network by 11 times less traffic mean and 67% faster updates as the number of nodes grows.

Yang et al. [6] suggest a blockchain model for sharing health data, emphasising EHRs in healthcare organisations. The paper also focuses on the most striking technical issues of EHR sharing: confidentiality, privacy, integration and integrity. Yang et al. propose a method of MedRec that uses encryption and attribute-based Authentication (ABA) to reinforce security. The approach ensures that 1) EHR pieces are not damaged or lost and are protected against alteration, 2) the Provenance of an EHR statement is retrievable, 3) There is the ability to apply fine-grained access control, and 4) It is clear who did what and when. As this study shows, this blockchain-based system using the architecture of MedRec guarantees that the alteration of EHRs is documented irreversibly to protect the patient data and avoid any obscurity in audit accessibility. Further, data authenticity is achieved from the encryption aspect, and from the ABA aspect, there is a provable trail of users who want to request information from EHR.

Jennath et al. [7] present an efficient solution based on blockchain technology that connects the management of sensitive records to trusted AI-empowering e-health systems. The paper overviews cybersecurity threats and privacy violations in digital health platforms and proposes a blockchain approach to promote healthcare information security, openness, and audibility. So, Jennath et al. propose a framework by which patients own their data and can share it securely, which is verifiable and has an audit trail. The framework adopts consent-based data sharing and keeps a record of patient consent associated with the data shared, along with information on the usage of this data for training AI models. Based on this work, the need for using blockchain to develop trusted AI models is evident since it would allow for the decentralised management of patient data and the control of who has access to it. A Proof-of-Concept (PoC) implementation of Permissioned Blockchain can lead to a promising future, as discussed by the authors. However, these authors understand that more scaling, patient mobility, and role-based permission systems must be implemented.

Oladele et al. [8] developed a blockchain electronic health data system, BEHeDaS, for safe medical records exchange. The paper presents a permissioned blockchain architecture employing a hyper-fabric ledger with smart contracts offering limited openness other than applying sophisticated mathematics. Using the flows described by Oladele et al., the authors explain how the system enables various users – patients, practitioners, and health officers – to create, access, and store the patient's medical records. The study reveals that the above system can support as many as 2500 users with a query transaction time of 0.56 sec and an HTTPS response of 0.42 sec. The contribution is about implementing a permissioned blockchain ledger to solve security concerns, privacy, and integration of patients' records across various healthcare centres, particularly in the Nigerian environment. Looking at the factors that the proposed system comprises, its high performance and open-source character ensure that it can expand and meet the user need for secure management of medical records conveniently.

III. Blockchain Algorithm in Healthcare

Blockchain algorithms in healthcare include the secure and efficient process and decentralised sharing of highly sensitive patient information. Some of these are consensus, such as PoS, PBFT for approval of business deals, encryption, AES, and RSA for data enclosure and privacy, such as Zero Knowledge Proofs (ZKP) to maintain patient anonymity while facilitating data sharing among parties. Table 1 provides a summary of various blockchain algorithms that are used in the context of healthcare systems. The focus is on classifying each algorithm, its main applications, specifics, benefits, weaknesses, and practical applications in the healthcare sector. It is helpful to reference this table as a roadmap on how the following algorithms assist in creating secure, efficient, and privacy-preserving data management for health care. Complementing the identified opportunities offered by the technology in overcoming the mentioned challenges, such as data integrity, interoperability and scalability, the table identifies critical areas, such as consensus mechanisms, encryption and privacy, which blockchain technology can address effectively in healthcare settings.

These algorithms operate in a way that guarantees the validation, encryption, and decentralisation of all transactions regarding data in exchange for negating privacy invasions, data theft, and fraud. Implementations such as PoW or PBFT created the consensus, allowing for the validation of transactions without needing a single control. Data is encrypted utilising the AES and RSA, which ensures patient data confidentiality, but at the same time, it is comprehensible for other participants of the process. Also, to enhance user privacy, technologies such as Zero-Knowledge Proofs (ZKP) re-identify data and its owners without sharing personal information. This kills intermediaries and makes transactions more efficient, as a smart contract may cover a range of services, including patient consent or insurance claims.

Blockchain, at its simplest, is made up of blocks in which actual transaction data is stored, nodes are part of the network, and consensus types (like POW, POS, and PBFT) confirm the transaction's authenticity in the distributed network. These consensus algorithms are valuable for avoiding fraudulent actions for data integrity issues. The classification of the blockchain systems includes public blockchains, private blockchains and

TABLE I. BLOCKCHAIN ALGORITHM IN HEALTHCARE

Classification	Algorithm	Use Case	Specialty	Advantages	Limitations
Consensus Algorithm [9]	Proof of Work (PoW)	Validates transactions in blockchain networks (rarely used in healthcare).	High security and immutability.	Proven security in distributed environments.	High energy consumption; unsuitable for real-time healthcare applications.
	Proof of Stake (PoS)	Validates transactions in healthcare networks requiring scalability.	Energy-efficient and supports faster validation.	Reduces environmental impact; speedier transaction speeds.	Requires initial stake; risk of centralisation.
	Practical Byzantine Fault Tolerance (PBFT)	Validates healthcare transactions in private/consortium blockchain networks.	Fault-tolerant and highly efficient for permissioned systems.	Ideal for small to medium-sized private networks.	Limited scalability with an increasing number of nodes.
Symmetric Encryption Algorithm [10]	Advanced Encryption Standard (AES)	Encrypts sensitive healthcare data like patient records and test results.	Strong symmetric encryption for data confidentiality.	Simple to implement; widely supported.	Vulnerable if encryption keys are compromised.
Asymmetric Encryption Algorithm [11]	Rivest-Shamir-Adleman (RSA)	Enables secure communication and data sharing between healthcare entities.	Strong asymmetric encryption for secure key exchange.	Effective for small-scale data sharing.	Computationally expensive for large-scale systems.
Hashing Algorithm [12]	SHA-256 (Secure Hash Algorithm)	Hashes healthcare data to ensure immutability and verification.	Creates tamper-proof records with unique digital fingerprints.	Reliable for maintaining data integrity.	Potential vulnerability to future quantum attacks.
Digital Signature Algorithm [13]	Elliptic Curve Digital Signature Algorithm (ECDSA)	Verifies the authenticity and integrity of healthcare transactions.	High security with smaller key sizes.	Low computational overhead; efficient for mobile devices.	Susceptible to implementation flaws if randomness is weak.
Contract Automation [14]	Smart Contract Logic	Automates insurance claim processing, consent management, and supply chain tracking tasks.	Reduces fraud and intermediaries.	Enhances operational efficiency; ensures rule compliance.	Vulnerable to coding bugs; may expose sensitive data if improperly coded.

consortium blockchains, which vary in their openness, permission and scalability level. Public blockchains allow complete decentralisation to anybody and could be more scalable, like Bitcoin. On the other hand, private blockchains have superior control with anonymity. Consortium blockchains are in between, with multiple organisations controlling the consensus in the network. Also, smart contracts, which are self-generated contracts written into the blockchain, can perform patient consent, insurance claims, and medical records verifications, thus cutting out most of the administrative work and errors and building credibility and integrity of the health care transactions. That is why the characteristics of blockchain discussed above help provide safe, fast, and non-interference with the storage and transfer of health-related records between parties, as well as enhance the condition of patients and the functionality of various organisations.

IV. APPLICATIONS OF BLOCKCHAIN IN HEALTHCARE

Blockchain is used in many areas of health care and presents new opportunities to address some of the sector's issues. From storing patient information to achieving the compatibility levels of various healthcare systems, blockchain solves the problem of increasing operational transparency, data protection, and the effective communication and sharing of information. It re-positions control of a patient's medical information back into the hands of the patient while, at the same time, it reduces fraud in both insurance and clinical trials. The table below analyses various blockchain applications in the healthcare field with relevant use cases, the nature of blockchain solutions, benefits offered and barriers to applying each solution. Table 2 describes the various applications of blockchain in healthcare.

Concerning patient data management, one of the most significant advantages of blockchain is the creation of a secure, transparent, and non-tamperable electronic health records (EHR) repository, which will grant healthcare practitioners immediate and direct access to accurate and comprehensive patient information. Another advantage is that data can be shared across multiple healthcare systems since blockchain assures interoperability, which is vital for seamless healthcare services. Another area where Blockchain is advantageous to healthcare is Data Ownership, and it will allow patients to determine who can view their detailed health data, thus fostering trust

TABLE II. APPLICATION OF BLOCKCHAIN IN HEALTHCARE

Sr. No	Application	Use Case	Blockchain Solution	Benefits	Challenges
1.	Patient Data Management [15]	Secure storage, sharing, and retrieval of Electronic Health Records (EHRs).	Blockchain ensures patient data is securely encrypted and stored in a decentralised ledger, allowing easy sharing across healthcare entities.	Enhanced data security, immutability, and transparency, ensuring the integrity of EHRs.	Scalability issues, potential for data fragmentation, and integration with legacy systems.
2.	Interoperability [16]	Blockchain as a solution for cross-system data exchange.	Blockchain enables seamless, trusted data exchange between different healthcare systems, ensuring compatibility and consistency.	Enables faster and more secure health data sharing across multiple systems, improving clinical decision-making.	Lack of standardisation, resistance from traditional systems, and complexity in adopting new technologies.
3.	Data Ownership [15]	Empowering patients through blockchain-enabled control over their data.	Blockchain allows patients to maintain control over access to their medical records using cryptographic keys and permissioned access.	Patients have complete control over who accesses their data, improving privacy and trust.	Educating patients about managing access and potential data breaches in shared access mechanisms.
4.	Fraud Prevention [17]	Combatting fraudulent claims and unauthorised access.	Smart contracts and immutable records in blockchain prevent unauthorised changes to data and enforce conditions for accessing medical records and claims.	Reduced fraud in insurance claims and patient data tampering transparent access auditing.	The complexity of smart contract implementation and ensuring compliance with healthcare regulations.
5.	Clinical Trials and Research [17]	Data integrity and transparency in research.	Blockchain can record research data immutable and transparently, ensuring all changes and results are logged in a tamper-proof ledger.	Increased trust in clinical trial data ensures that results cannot be altered and promotes research transparency.	Data privacy concerns, ensuring compliance with ethical standards in research, and integration with existing research frameworks.

and privacy. A key advantage of implementing blockchain is that it is also far more effective in fraud prevention, as there is no extended scope for concealing fraudulent transactions concerning medical services and insurance claims. Last but not least, through its features such as immutability, blockchain has the potential to verify Clinical Trial and Research data and subsequently alleviate doubts regarding data falsification while increasing the reliability of the research results. Although these applications are excellent examples of the tremendous capabilities of the blockchain, it is crucial to imagine the issues that arise when adopting such a technology, like legal restrictions, compatibility of blockchain with pre-existing systems, or the ability to scale up. However, from the discussed activities, it is possible that blockchain has a future in healthcare and might benefit effectiveness, safety, and patient experiences worldwide.

V. BLOCKCHAIN ARCHITECTURE IN HEALTHCARE

Secure patient data in blockchain healthcare architecture comprises several fundamental constituents outlined below. However, the basic idea is based on the distributed database regime, which means that the patient data is spread across many network nodes and cannot easily be centralised or controlled. Every piece of the patient's information is saved in a single block that can be shared and synchronised among other blocks and cannot be changed once recorded. This feature responds to one of the most pressing issues in the healthcare domain – data quality and guarantees the credibility of medical records.

The system uses cryptography to control users of specific data. The data is encoded so that only other parties to the decryption key, including the doctors and the patient himself, can retrieve it, making it completely secure. Smart contracts are another vital constituent of architecture. These smart contracts perform several healthcare tasks, including consent management and data sharing. It not only lessens bureaucracy but also inaugurates the idea that access to patient data has become decisive by preconditions, not arbitrary, thereby enhancing the efficiency of the process. A P2P network provides direct connectivity between the different nodes in the blockchain, thus allowing for a smooth transfer of information at the decentralised real-time network. This makes the system more secure and easily scalable since no single point of failure is constructed. Moreover, it directly organises the data in the system architecture at the application layer. It can be interfaced with existing hospital Information Technology systems through middleware solutions to transfer data between blockchain networks and Electronic Health Records (EHR) systems. The architecture also takes care of the integration to ensure that different healthcare organisations like hospitals, clinics, and laboratories, among others, can freely share patient information without threatening the quality and privacy of information. Integrating these Technologies, the blockchain of healthcare architecture offers a highly secure, transparent system of managing patient data that holds a solution to many of the issues related to healthcare at the present moment, including Data breaches, unauthorised access, and the sharing of data between numerous systems.

Blockchain technology is gradually emerging in the healthcare sector. It is key to many sector problems, encompassing data integrity, compatibility, and connectivity issues. Several avenues and programs have been developed to address the issue of deploying blockchain systems to enhance the delivery of healthcare services. MediBloc is one of the two specific examples. This company uses blockchain in healthcare by applying different strategies from Guardtime.

MediBloc is a decentralised platform for consolidated patient data in a world where patients own their information. It applied blockchain to create and implement the patient's electronic health records (EHRs) that can be accessed, jointly used, and modified by patients and related healthcare professionals only. It uses the permissioned blockchain framework, meaning only relevant actors (doctors, hospitals or insurance companies) can access the patient's data. Facing tremendous challenges of interoperability in the different healthcare providers' systems, MediBloc has been designed to enable convenient data sharing advantages. Also, smart contracts eliminate intermediaries for receiving patients' consent in data sharing and enforce the patients' rights throughout the entire continuum of care. The platform's goals are to completely protect patients' records and free them from the dangers inherent in data hacking and other security threats [18].

Guardtime, a blockchain-based organisation, is concerned mainly with data integrity and security issues, especially in the health sector. Blockchain is applied to validate and encrypt medical records to guarantee that they have not been altered at a particular time. Medical records have been signed with the help of Keyless Signature Infrastructure (KSI), a cryptographic system based on a decentralised ledger at Guardtime's platform. Information asymmetry can be eliminated with the help of this system, which means that HI organisations can ensure the actuality of medical data without a third party. With the help of this approach, Guardtime improves data provenance and provides healthcare professionals with a way to track the origin and history of patient records while protecting the patient's data. Government and healthcare organisations use Guardtime solutions to safeguard their vulnerable health information from attacks by hackers, thus meeting the regulations set by bodies such as HIPAA in the United States [19].

VI. Challenges and Limitations

Table 3 summarises the key challenges and limitations of implementing blockchain in healthcare, potential solutions, and impacts. Increased data means scalability occurs slower and incurs more costs; this can be solved using a private blockchain, layer-2 solutions, or sharding. Data privacy and confidentiality may be an issue of concern due to regulations such as GDPR and HIPAA. Still, encryption, Zero-Knowledge Proofs (ZKP), and Off-chain storage solve this problem. Some unresolved questions include data ownership and compliance on the regulatory and legal levels. Integrating EHRs and HIEs costs money and time but can be handled with Interoperability. The reason for adoption resistance is either a lack of trust or a lack of comprehension, and both pilot programs and education can help alleviate this. It is, therefore, essential to deal with these challenges to enhance the security and operations of information health data.

TABLE III. Challenges of Blockchain in Healthcare

Sr. No	Challenges	Description	Potential Solutions	Impact on Healthcare
1.	Scalability	Blockchain networks may need help handling large volumes of healthcare data, leading to slower processing and higher costs.	Implement private/permissioned blockchains, layer-2 solutions, or sharding techniques to improve scalability.	Slower data processing and higher operational costs may hinder efficient healthcare service delivery.
2.	Data Privacy & Confidentiality	Blockchain's transparency and immutability may conflict with maintaining patient privacy under regulations like GDPR and HIPAA.	Use encryption, Zero-Knowledge Proofs (ZKPs), and off-chain storage to preserve privacy.	Legal issues and patient trust concerns could arise if patient data is exposed or mishandled.
3.	Regulatory & Legal Issues	There is a lack of clear regulations regarding blockchain's use in healthcare, such as data ownership and cross-jurisdictional compliance.	Develop standardised frameworks in collaboration with regulatory bodies to ensure compliance with privacy laws.	Regulatory uncertainty may delay or prevent blockchain adoption in healthcare, complicating implementation.
4.	System Integration	Integrating blockchain with	Focus on interoperability	High integration costs and system

		healthcare systems like EHRs and HIEs can be complex and costly.	solutions and use bridging technologies for seamless integration.	complexity may slow adoption and increase financial burdens.
5.	Adoption Resistance	Healthcare stakeholders may resist blockchain adoption due to a lack of trust, understanding, or perceived complexity.	Increase awareness through pilot programs, case studies, and educational efforts to build trust and acceptance.	Slower adoption and inefficiencies as healthcare providers may be reluctant to transition to blockchain.

VII. Advantages of Blockchain in Healthcare

Blockchain-based solutions in healthcare encompass an incredible advantage in terms of security and management of patient data over traditional solutions. This remains decentralised, and once the data is posted online, its capacity cannot be changed as this will present numerous loopholes for hacking, as with central systems. Using some of the most advanced cryptography measures, information organisations in the blockchain guarantee the privacy of health information without compromising openness, which allows a trail of checks to be made when there is a perceived violation. The patients obtain unprecedented control over their data, and shareholders receive the means to maintain secure permission management, leading to trust development.
Blockchain also helps to improve communication with other healthcare systems by standardising data exchange and reducing and improving efficiency in care transitions. Adding on, it simplifies billings, consent, and insurance claim standards and eliminates extra operating costs. The technology also addresses fraud within clinical trials and insurance by affirming data tamper-proof and sourcing. New technological improvements such as encryption and zero-knowledge proofs make it possible to ensure patient data security while sharing them on the blockchain. On an international level, blockchain interoperability fosters the integration and consolidation of numerous common approaches to public health and enhances medical research. These singular benefits serve to place the blockchain as a game changer capable of revolutionalising the solution of some of the most pressing problems related to the safe storage and utilisation of health information for patient-centric, efficient and effective healthcare solutions.

VIII. Future Scope

Blockchain in healthcare focuses on securing patient data in the future, with solutions to upcoming problems related to patient data privacy, security, and integrability. Blockchain is believed to be a key technology for Decentralized Electronic Health Records (D-EHR), which allows patients to manage their medical records by sharing their records between multiple parties while having complete control of their medical record data. That shall improve patient-centered care since it will make data more accessible and reduce duplicities. Blockchain will also advance precision medicine by enabling the safe exchange of clinical and genomic data anonymised to advance research in individualised treatment. Connecting with AI and IoMT will result in intelligent, accurate, secure decision-making despite the large and constantly changing data. On the same note, blockchain technology presents nearly unlimited opportunities in supply chain management by enhancing the trackability and accuracy of drugs and other medical equipment to minimize fake products. Introduction The following sectors will also benefit from the application of blockchain: Public health vaccination records, disease surveillance, and pandemic response strategies. Harnessing, scalability, optimisation regarding energy consumption, and the future of privacy-preserving techniques, such as zero-knowledge proofs, will only strengthen its position. Through trust, transparency, and efficiency, blockchain is set to emerge as a disruptive technology that will enable a secure, integrated, patient-centric universal healthcare system.

IX. Conclusion

This paper reviews the use of the blockchain in managing critical patient data where enhanced security is essential to aiding the healthcare sector. Current systems face data breaches, a lack of integration between different systems, and a centralised nature of decision-making. Still, through the exploitations of the features of decentralisation, transparency and immutability, blockchain can address these challenges. Practical issues include scalability, where more significant and complex transactions may prove challenging, legal hurdles and, perhaps the most important one, the hurdle of adoption. These barriers will be best addressed through multistakeholder engagement with parties from the healthcare system, technologists, and policymakers. As posited in this review, blockchain promises to disrupt the current paradigms of healthcare data security by harnessing an opportunity to achieve more efficient, reliable, and patient-sensitive models. The direction of subsequent studies and developments will be crucial for the failure and success of this unique technology.

REFERENCES

[1] A. Almalawi, A. I. Khan, F. Alsolami, Y. B. Abushark, and A. S. Alfakeeh, "Managing security of healthcare data for a modern healthcare system," *Sensors*, vol. 23, no. 7, p. 3612, 2023.

[2] S. Duggineni, "Data integrity and risk," *Open Journal of Optimization*, vol. 12, no. 2, pp. 25–33, 2023.

[3] A. A. Bakri, E. Sudarmanto, N. D. P. S. Fitriansyah, A. Y. Rukmana, and E. Y. Utami, "Blockchain technology and its disruptive potential in the digital economy," *West Science Journal Economic and Entrepreneurship*, vol. 1, no. 8, pp. 338–347, 2023

[4] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abella, and K. Shuaib, "Introducing blockchains for healthcare," in *Proc. Int. Conf. Electr. and Comput. Technol. and Appl. (ICECTA)*, Ras Al Khaimah, UAE, Nov. 2017, pp. 1–4.

[5] L. Ismail, H. Materwala, and S. Zeadally, "Lightweight blockchain for healthcare," *IEEE Access*, vol. 7, pp. 149935–149951, 2019.

[6] H. Yang and B. Yang, "A blockchain-based approach to secure healthcare data sharing," in *Proc. Norwegian Information Security Conf.*, Oslo, Norway, Nov. 2017, pp. 100–111.

[7] H. S. Jennath, V. S. Anoop, and S. Asharaf, "Blockchain for healthcare: securing patient data and enabling trusted artificial intelligence," unpublished.

[8] J. K. Oladele *et al.*, "BEHeDaS: A blockchain electronic health data system for secure medical records exchange," *J. Comput. Theories and Appl.*, vol. 1, no. 3, pp. 231–242, 2024.

[9] A. Kumar and S. Jain, "Proof of game (PoG): A proof of work (PoW)'s extended consensus algorithm for healthcare application," in *Proc. Int. Conf. Innov. Comput. and Commun. (ICICC)*, vol. 1, Singapore, 2021, pp. 23–36.

[10] N. M. Hamed and A. A. Yassin, "Secure patient authentication scheme in the healthcare system using symmetric encryption," *Iraqi J. Electron. & Electron. Eng.*, vol. 18, no. 1, pp. xx–xx, 2022.

[11] S. A. Ajagbe, A. O. Adesina, and J. B. Oladosu, "Empirical evaluation of efficient asymmetric encryption algorithms for protecting electronic medical records (EMR) on web applications," *Int. J. Sci. and Eng. Res.*, vol. 10, no. 5, pp. 848–871, 2019.

[12] M. D. Mohanty, A. Das, M. N. Mohanty, A. Altameem, S. R. Nayak, A. K. J. Saudagar, and R. C. Poonia, "Design of innovative and secured healthcare service using deep learning with a modified SHA-256 algorithm," *Healthcare*, vol. 10, no. 7, p. 1275, Jul. 2022.

[13] J. A. Alzubi, "Blockchain-based Lamport Merkle digital signature: Authentication tool in IoT healthcare," *Comput. Commun.*, vol. 170, pp. 200–208, 2021.

[14] A. McNamara, "Automating the chaos: Intelligent construction contracts," in *Smart Cities and Construction Technologies*, IntechOpen, 2020.

[15] I. Yaqoob, K. Salah, R. Jayaraman, and Y. Al-Hammadi, "Blockchain for healthcare data management: Opportunities, challenges, and future recommendations," *Neural Comput. and Appl.*, pp. 1–16, 2022.

[16] R. Belchior, A. Vasconcelos, S. Guerreiro, and M. Correia, "A survey on blockchain interoperability: Past, present, and future trends," *ACM Comput. Surv. (CSUR)*, vol. 54, no. 8, pp. 1–41, 2021.

[17] M. Benchoufi, D. Altman, and P. Ravaud, "From clinical trials to highly trustable clinical trials: Blockchain in clinical trials, a game changer for improving transparency?," *Front. Blockchain*, vol. 2, p. 23, 2019.

[18] B. Shrimali, S. Surati, and H. Trivedi, "MediBlock: A blockchain-based architecture for the secure healthcare system," in *Proc. Int. Conf. Adv. Comput. and Comput. Technol. (InCACCT)*, May 2023, pp. 750–755.

[19] S. Kaneko *et al.*, "Photonic gateway architecture extension and guard time-free initial connection method with point-to-multipoint remote control for metro/access converged all-photonics network," *J. Opt. Commun. and Netw.*, vol. 16, no. 12, pp. 1229–1240, 2024.