IJCRT.ORG ISSN : 2320-2882

INTERNATIONAL JOURNAL OF CREATIVE RESEARCH THOUGHTS (IJCRT)

An International Open Access, Peer-reviewed, Refereed Journal

DESIGNING A FRAMEWORK FOR HEALTHCARE INFORMATION SYSTEM USING ROBUST BLOCHAIN TECHNIQUE

[1]Mr. Atul A. Padghan,
[1]Student,
[1]CSE Department
[1]Rajarshi Shahu Collage of Engineering, Buldhana, Maharashtra

[2]Prof. Pallavi P. Rane,
[2]Asst. Professor,
[2]CSE Department
[2]Rajarshi Shahu Collage of Engineering, Buldhana, Maharashtra

[3]Prof. Nilesh N. Shingne
[3]Asst. Professor,
[3]CSE Department
[3]Sanmati Engineering College, Washim, Maharashtra

Abstract: Electronic medical records are an important part of healthcare organization. In recent years, there have been increasing concerns about privacy and integrity in the storage and use of patient information. In this case, for example, information provided under health and health insurance can be considered as evidence of health insurance and management. In the past few years, many problems in the management of medical records have threatened the privacy of patient information. The privacy of patient data is an important issue in smart medical applications. Therefore, blockchain is very necessary because it can increase transparency and security in medical practices. Therefore, this paper presents a secure blockchain framework for managing medical records using a research model. The proposed system consists of five elements: blockchain networks, smart contracts, self-regulation, data encryption, and integration with medical data. In this framework, healthcare institutions can manage health information for security and privacy. In addition, secure storage systems for electronic data have been requested to meet the needs of these institutions. It provides security and privacy for healthcare organizations, especially when managing health information, and also ensures that information that meets the needs of the organization is stored securely.

Keywords: Blockchain technology, design science, electronic healthcare records etc.

I. INTRODUCTION

Today, many medical, transportation and financial services use blockchain technology. In recent years, these machines have become fast and convenient. Blockchain or blockchain technology is a general certificate used to record transactions and track assets within a secure, immutable and peer-to-peer computer network instead of a central organization. A company's assets can be tangible, such as buildings or money, or intangible, such as patents or copyrights. In general, a blockchain consists of a set of information stored in a block structure. The hash value (digital fingerprint or unique identifier) uniquely identifies the block of data and groups the timestamps of recent transactions. Using this design, each block is linked in chronological order and is called a blockchain. Since

every block needs to be changed at the same time after the block is changed, it is almost impossible to change a block in the middle of the chain. Due to this mechanism, the blockchain network information is immutable.

Good health is the foundation of a prosperous and happy life, and medical technology plays a significant role in making today's life more fulfilling and enjoyable. Technology makes it easier for us to make decisions about issues that affect our health. The healthcare sector manages a lot of medical information about patients, doctors, and medications to provide better treatment. All healthcare organizations face the challenge of protecting this information from unauthorized users. Disclosure of medical information can reveal a patient's identity and illness, allowing them to be more understanding. Hospitals that store a lot of medical information need to have good security in this regard [2].

In many sectors, blockchain technology has helped advance and improve operations [3]. These systems record all the events that an object or subject goes through from its creation to its current state. It has different applications such as checking fresh food, verifying the authenticity of works of art, and verifying land ownership. Blockchain also allows smart contracts, which are codes of code that are executed according to predetermined conditions.

Healthcare is the industry most affected by data security breaches [4]. Many healthcare providers reported that more people were affected by medical data breaches between 2005 and 2019. For example, according to the Insurance Institute's Health Insurance Portability and Accountability Act (HIPAA), there was at least one health insurance breach every day in 2018. Between 2009 and 2018, more than 59% of the US population was exposed due to a data breach. improper sharing of identity [5]. Figure 1 shows the crime situation from 2009 to 2021 by number of reported crimes.

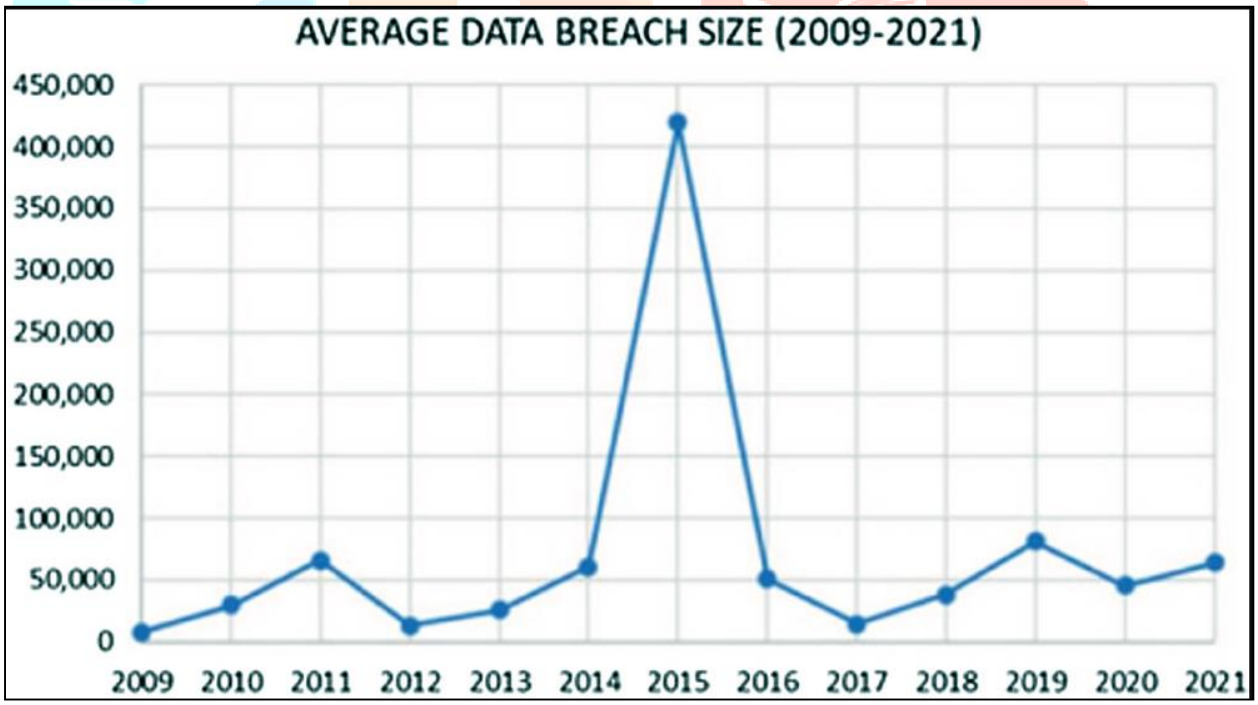

Fig. 1: Data violations from 2009 to 2021

The concept of blockchain first appeared in the Bitcoin whitepaper and was designed to solve the problem of double spending without the need for a trusted third party such as a bank or financial institution [7]. Decentralized currencies and peer-to-peer electronic cash applications are one of the unique features of the first public blockchain behind Bitcoin. Therefore, the Bitcoin blockchain is difficult to customize with scripts or other scripting systems. The Ethereum blockchain platform [8], developed by Vitalik Buterin, has a Turing-complete language for writing smart contracts. There are rules that can be used to leverage Ethereum's currency, identity, and

reputation[5]. After the launch of the Ethereum platform, people realized the value of blockchain applications and started to research other blockchain-based applications. The success of blockchain continues to grow as new blockchains and software stacks are developed to create new blockchain technologies. Compared to the Internet era, where value was captured at the application layer, the technology has snowballed in adoption and investment. Therefore, education and business need to understand and deploy blockchain technology. Scalability has become a critical issue for blockchain-based cryptocurrencies [9]. Multitasking is one of the keys to scaling blockchains, and very few transactions have been known for a long time.

In recent years, according to [10, 11], blockchain technology has become increasingly important due to its many features, as shown in the figure below and figure 2.

1. **Decentralization**: Using this technology, you can store your assets on the network instead of having them under the care and control of a single person or organization. If you use algorithms to run systems, you can't cheat because people can't cheat on you. No one can use blockchain technology for personal gain. However, in most current organizations and healthcare environments, this is often done through centralized processes where one school powers many other buildings.
2. **Transparency:** Data transparency helps create accurate, complete and correct data that can be used in the healthcare sector. There is currently no solution that simultaneously provides transparency, confidentiality and security for managing medical information. Blockchain technology can also be transparent by ensuring data security, ensuring that people have the right to access medical information and achieving this through access and control procedures.
3. **Immutability:** One of the biggest benefits of Blockchain is that such a list can be immutable for a long time, which is its most important feature. By analyzing the perspective, it is possible to redesign and redesign the process to be more efficient, faster and more profitable in the long run. Due to this feature, users cannot edit or delete files on the internet. Cryptographic hashing is one of the methods that can be used to accomplish this task.
4. **Production of information in the health sector:** In order to ensure public confidence in the use of health information, all important information regarding the development, creation, access and distribution of data must be provided in the medical record. The ability to track changes made from the creation of the profile to its current state provides this security. Using blockchain technology, timestamping is done through a process that includes evaluating the hash value of the certificate to ensure that the certificate is trusted in all legitimate transactions. Once the hash is determined, it is sent to consensus for verification.
5. **Minting:** Blockchain can solve many governance issues. This is why people and businesses in the West believe that banks and international tech companies like Google and Meta can be more trustworthy and accountable if they use blockchain [12]. Blockchain has the opportunity to be a new technology not only in countries where mining industries are ongoing, but also in countries that have not yet reached the adoption stage.
6. **Privacy and programmability:** Blockchain is characterized by anonymity and programmability. Programmable smart contracts can revolutionize transactions by creating new anonymity rules that ensure that the identity of the sender and the recipient remains anonymous during business hours. Smart contracts are called self-service based on the agreement between the buyer and the seller.
7. **Decentralized Ledgers and Protocols:** Blockchain is likely to offer many advantages in the future because it combines technologies such as distributed ledgers and consensus technology. Consensus is a decision-making process among active nodes in the network where millions of nodes complete transactions simultaneously. This algorithm is crucial for the proper functioning of the system. Decentralized ledger systems (DLT) make the process transparent and reliable by allowing anyone with access rights to see the ledger instantly.

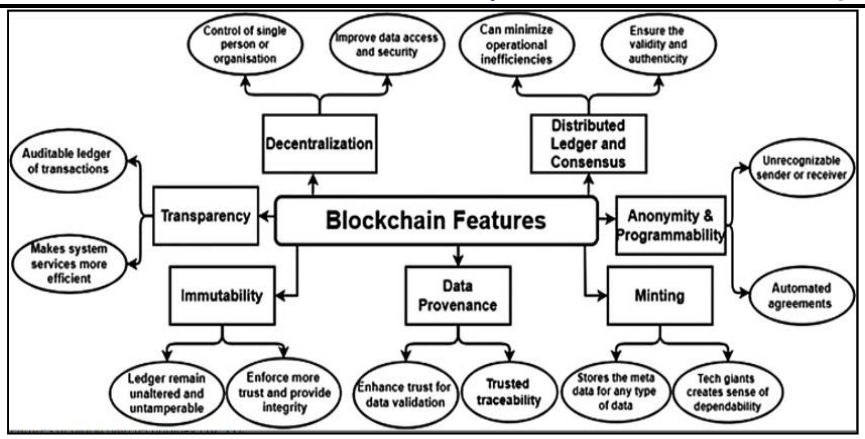

Fig. 2: Features of blockchain technology

Therefore, there is no doubt that electronic medical records are important for any healthcare organization. In the past few years, many concerns have been raised about the storage and use of patient information, especially privacy and reputation. Therefore, the information provided can be considered as part of a health policy or health insurance, for example, as evidence of health insurance and management. In the past few years, the privacy of patient information has been at risk due to some problems in the management of medical records. One of the most important issues in smart healthcare applications is the confidentiality of patient information.

Therefore, this paper presents a secure blockchain architecture for managing medical records using a research model. The proposed system will include five elements: blockchain networks, smart contracts, self-regulation, data encryption, and integration with medical data. Establishing a secure blockchain framework for managing medical information can lead to greater collaboration, improve patient information security, tracking, privacy, interaction, and accurate information. By leveraging the potential of blockchain technology, healthcare providers can overcome the limitations and challenges of traditional data management, and pave the way for greater efficiency, safer, and patient-centered treatment.

A secure blockchain project for medical information management has many contributions that can increase the efficiency and security of medical information management. These partnerships include improving data security and privacy protection, integration and sharing, and improving data accuracy and integrity. Using blockchain technology, healthcare organizations can unlock all the resources of electronic medical records and provide patients and other stakeholders with secure and easy access to medical information.

The remainder of this paper is organized as follows: Section 2 discusses the existing literature. Section 3 presents the methodology and development. Sections 4 and 5 present the discussion and conclusions, respectively.

II. RESEARCH DATA

The document presents various studies on medical data, blockchain, and the role of blockchain in this data. This section focuses on two things: medical information and blockchain technology.

The authors in [13] proposed a blockchain-based project for self-management of health information sharing with healthcare providers. Its aim is to provide better care to patients. The planning process includes the process of managing data to avoid risk.

Blockchain technology offers many solutions to these problems[14]. The authors then demonstrate a blockchain-based workflow for the healthcare sector. The framework provides effective access rules to users of the system, aiming to ensure the security and

efficiency of patient-related medical information. A scalability framework using blockchain technology is also planned as part of the framework.

The authors proposed a new model [15] to provide shared security so that participants can get the best results from the special features of the blockchain. The study found that the design increases the security of the device by making the information more accurate. Consensus-based marketing is used to create a more interactive and efficient way of doing business using the consensus model. In order to strengthen the collaboration of blockchain network nodes managed by the third layer of the system, the system is built with a triple structure at various levels, including the blockchain framework, middle application, and smart contracts, all of which are part of the system. revolution. .

According to [16], IoT medical networks should be shared with patients. Their design separates the data from the smart energy-saving biosensor, sends the data to the microcontroller, and stores it in a MySQL database. Raw data and research data should be carefully analyzed, collected, analyzed, and documented for healthcare professionals and patients around the world. However, the authors did not examine the security features in the solutions.

In [17], a product development project uses the blockchain paradigm to improve the accuracy and quality of work in medical diagnosis. Newly developed healthcare systems will be able to track the model presented to the patient by creating and understanding the connections between human and simulated doctors.

The authors in [18] addressed the economic and financial aspects of the health sensor problem. Some concepts of the software include encrypted messaging, medical devices, and remote access. Also, the software applications are included in new applications, online video sharing, messaging, medical applications, and medical device messaging.

In [19], the authors examined the benefits of modern blockchain-based solutions for protecting medical data in cloud-based and non-cloud-based situations, comparing blockchain with traditional methods.

Researchers in [20] proposed a permissioned blockchain solution based on the Hyperledger Fabric framework for storing and distributing electronic medical records. The proposed system has many advantages, such as providing patients with full control over their electronic medical records and allowing physicians to review these records and add new EHR products using methods such as authorization and revocation.

To solve the medical IoT problems in a secure and immutable manner, the authors in [21] proposed a blockchain concept based on the immutability principle, where hospitals and users can perform many treatments as part of the agreement regarding the secure and reliable operation of the lightweight private blockchain network.

[22] developed an innovative patient-centric blockchain-based EHR management system that enables the management of medical information across multiple stakeholders without the need for a central database. The system provides patient privacy and allows or revokes access or viewing of patient information without the need for a central system.

As a way to ensure the security of EHR sharing between different electronic systems, researchers in [23] proposed a blockchain architecture based on proof of participation eligibility (POS), cryptographic approval mechanism, and security hash algorithm (SHA256) to identify the EHR.

The authors of [24] proposed a method to secure shared medical information in patient management using blockchain technology. Blockchain technology and the Interstellar File System are part of the scheme.

[25] proposed a healthcare electronic medical information exchange based on blockchain technology. The design strategy identifies and prevents malicious activities of outsiders and insiders in storing and sharing EHRs. It can also establish standards that can be easily understood by different healthcare systems to ensure the integrity and reliability of EHR requests and responded messages.

Therefore, it is absolutely correct to say that electronic medical records are an important part of any medical organization today. In the past few years, many concerns have been raised regarding the storage and use of patient information. These concerns mostly concern the private hospital and its reputation. In this case, the information provided under the health insurance policy can be considered as an indicator of health insurance and management responsibility, as well as the information provided under the health insurance policy. The privacy of patient information has been at risk for more than a decade, mainly due to the many problems related to the management of medical information in the last few decades. One of the most important challenges in smart health applications is keeping patient information confidential.

III. PROCESS AND DEVELOPMENT STEPS

This section describes the process and development steps used in this study. This paper uses a research model to create a secure blockchain framework for managing medical records. This model is used to create a model of the material and the material itself to determine the material [26]. Figure 3 shows the methodology used in this study.

1) Determine search criteria: The author used keywords related to the topic, such as “electronic medical records” and “blockchain technology,” to narrow down the search scope of the article. Articles published in journals or conferences.
2) Identify search engines: This study identified five search engines that should be used to search for the desired information. The search engines include Scopus, IEEE Xplore Springer Link, Web of Science, and Google Scholar.
3) Collect data from search engines: In this process, the main publications related to EHR blockchain technology are collected by searching the rules we mentioned in step 1. Tom then examines the conclusion of the article and the content of the entire article.
4) Building a secure blockchain foundation for medical data management: Building a secure blockchain foundation for medical data management involves several steps. This section of the article will provide a comprehensive overview of these stages. Here is the list of stages offered by the design framework:

    a) Reducing risks: Blockchain technology uses technology encryption to protect data protection. So data is not allowed to be reduced, so reduce data.
    b) Do not change medical data: Distributed blockchain architecture ensures that no one can change medical data. Provide a blockchain audit system to help verify the accuracy of information and prevent fraud through fraud prevention.
    c) Patient Authorization: Patients can own and manage their own medical records. They will be able to access them whenever they want, access their information and share them with any doctor they want without any problems.

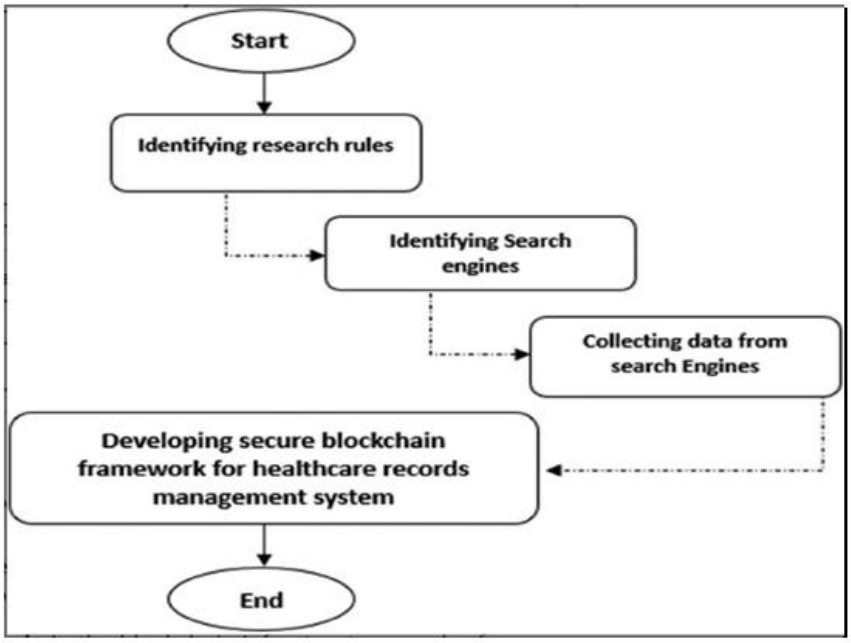

Fig. 3: Research methodology and development processes.

Therefore, the creation of a secure blockchain framework for the management of medical information has the following main points (see Figure 4):

1. **Blockchain Network:** In a blockchain infrastructure, nodes form a decentralized network that forms a chain. Nodes are responsible for ensuring the integrity of the network by confirming transactions and adding new blocks to the chain every day. Blockchain networks have many advantages, including:

   - ✓ **Decentralization:** Since it is a decentralized organization that is not controlled by any organization, it cannot be controlled by any control system and there is no failure. This increases the security and reliability of the system.
   - ✓ **Security:** Since the blockchain network makes all transactions immutable and unchangeable, their security and reputation are not compromised. This means they are resistant to fraud and tampering.
   - ✓ **Immutable data:** Once a transaction is recorded on the blockchain, it cannot be deleted or changed. Therefore, all changes are recorded in the repository, ensuring the most transparency and security.
   - ✓ **Transparency:** The network ensures that all transactions are transparent and accountable as every node has access to every transaction, allowing all transactions to be tracked as they are completed.
   - ✓ **Speed and efficiency:** The blockchain network is a network of nodes controlled by consensus standards that execute and confirm transactions instantly, creating efficiency and speed.

2. **Smart Contracts:** Smart contracts can perform various business functions, thereby increasing the efficiency and productivity of businesses using blockchain technology. Contracts can be executed on the blockchain, subject to certain conditions or terms. Among its significant benefits, automating contract execution can simplify and implement complex processes. These processes often require human intervention, which can lead to errors and delays. Smart contracts do not require human intervention because their rules can be built directly into the software. Smart contracts also have many advantages, including flexibility and operational management. Using blockchain, contract terms and conditions can be entered into and executed as soon as the conditions are met. Therefore, no human intermediaries are allowed, reducing the possibility of fraud and errors. Smart contracts include three applications:

- ✓ **Access control:** Smart contracts can provide access control in many applications; organizations can grant access to different resources to specific individuals by creating personal agreements that allow them to share rights and permissions before granting access to resources to specific individuals based on specific criteria.

- ✓ **Proof:** Smart contracts can also verify the authenticity and accuracy of information, eliminating the possibility of information being contradicted. Blockchain technology can be used in any way that allows users of such contracts to ensure that the data they are working on cannot be altered, tampered with, or modified in any way by the user.

- ✓ **Authentication:** Smart contracts provide a simple and secure authentication solution. Smart contracts are a great and secure way to create real-time transactions. Blockchain technology is used to create unique identifiers for users and devices using these contracts, eliminating the need for usernames and passwords for onboarding and other identification processes. The security of the system will also be increased, allowing different systems and programs to interact with each other at the same time, increasing their benefits and security.

3. **Privacy key management:** Privacy management should be used to ensure that all information is secure, confidential, and authentic when managing medical records. This will increase patient safety and ensure compliance with government regulations. Self-regulation provides the following resources for medical records:

- ✓ **Encryption:** Private keys can be used to access medical information, ensuring that only authorized parties can access and decrypt the information.
- ✓ **Verification:** These keys help users verify the accuracy and completeness of medical records.
- ✓ **Privacy:** The nature of blockchain technology allows medical information to be stored securely across multiple nodes, thus increasing privacy and reducing the risk of information leaking out.
- ✓ **Auditability:** Dedicated management ensures auditability, accountability, and tracking of medical records.
- ✓ **Scalability:** The privacy management system can be easily expanded to accommodate the growth of overall medical data.

- ✓ **Interoperability:** This system can be easily integrated with other medical systems, such as electronic medical records, to allow information to be shared easily and securely.

4. **Data encryption:** Data encryption can be defined as the process of scrambling data using a key or algorithm and making it unreadable and unintelligible to anyone who does not have the key. The decryption key is used to decrypt and decode the data. Hospitals can ensure the security of patient data through encryption to prevent unauthorized access, destruction or modification. Managing medical records using data encryption has the following advantages:

- ✓ **Confidentiality and security:** Data encryption ensures the confidentiality of patient information and prevents unauthorized personnel from accessing or using sensitive information.
- ✓ **Compliance:** Healthcare companies must comply with data security regulations like HIPAA and GDPR. Data encryption helps organizations meet these regulatory requirements.
- ✓ **Data Integrity:** Data is encrypted while in transit or stored, and there is no risk of data corruption or fraud as encryption ensures that data is not compromised.
- ✓ **Data resilience:** Blockchain frameworks often use shared networks, making data encryption all the more important to protect patient data.
- ✓ Information Sharing: Information encryption allows for the secure sharing of information between healthcare providers and researchers on a regular basis without compromising privacy.

5. **Integration with medical IT systems:** A secure blockchain framework for EHR products must be integrated with medical IT systems to ensure the efficiency and integrity of patient information. Integrating blockchain technology into the healthcare sector is critical to maximize its potential. Healthcare providers can integrate blockchain technology into their healthcare IT systems. With this integration, patient information can be shared across hospitals, clinics, and laboratories. Healthcare IT systems that use blockchain technology to ensure the security and privacy of patient health information can benefit from the advantages and disadvantages of blockchain in these circumstances. Use blockchain encryption algorithms to encrypt and authenticate patient information, ensuring only sensitive information is secured. Additionally, blockchain's integration with health IT systems enables information sharing and collaboration. Clinicians in different locations can instantly view and update patient information, improving collaboration and continuity of care.

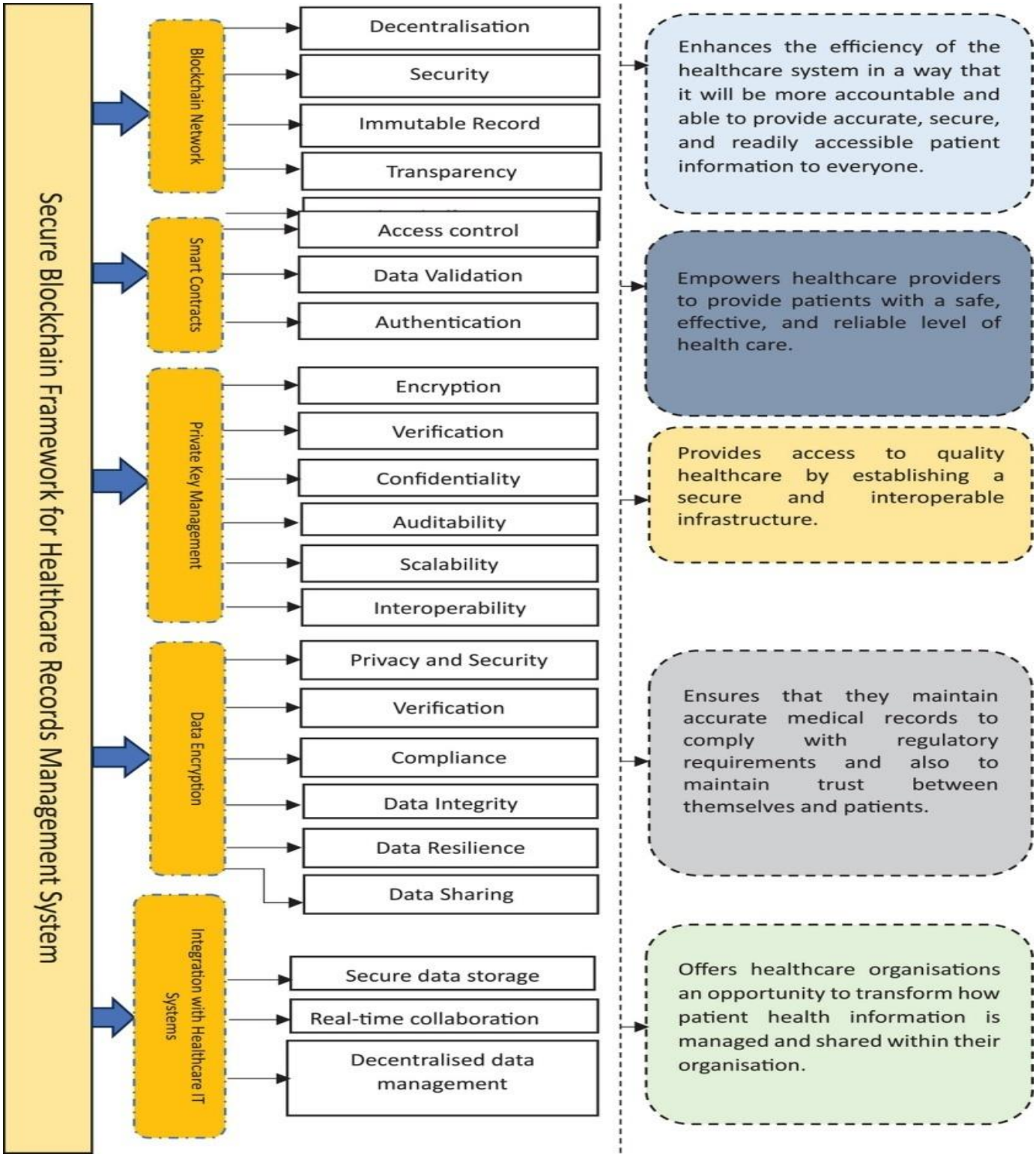

Fig. 4: Secure blockchain framework for healthcare records management system.

IV. DISCUSSION

This paper aims to discuss the results and recommendations of the study. This study develops the EHR framework for medical records using blockchain technology. This framework ensures the confidentiality, accuracy and accessibility of electronic medical records. Medical information management using this framework is designed to meet the needs of medical organizations. It provides encryption, controls access to patient information and provides a consensus algorithm for data security.

One of the main conclusions of this study is that blockchain technology has many advantages over traditional EHR systems. Decentralized infrastructure and encryption increase the security, immutability and traceability of electronic medical records.

Blockchain technology has proven to have many advantages over traditional EHR systems, particularly in the areas of security, flexibility, and traceability.

- ✓ **Security:** Blockchain uses encryption techniques such as hashing and public-private key encryption to ensure that information is secure and accessible only to authorized individuals. All transactions or data entered into the blockchain are encrypted and linked to previous transactions, creating a proven, secure system. This method of data protection has been widely researched and demonstrated in many areas, including medical care. For example, Kumar and Tripathi [27] showed that the encryption process of blockchain reduces the risks associated with unauthorized data access and leakage compared to traditional systems.
- ✓ **Immutability:** One of the most important features of blockchain technology is immutability. Once information is recorded on the blockchain, it is nearly impossible to change or delete it without changing every part of the chain, which requires the agreement of most nodes in the network. This immutability is particularly useful for EHR systems because it ensures that patient information does not change over time, provides an audit trail, and increases confidence in the accuracy of medical records. Khan et al. [28] emphasized the effectiveness of immutability in preventing falsification of medical data.
- ✓ **Traceability:** The decentralized nature of blockchain allows for real-time tracking of data entry and changes. Every time a physician, insurer, or patient accesses or updates information, the change is recorded on the blockchain. This increases accountability and evidence by ensuring that every interaction with patient data has a clear and transparent history. Some studies, including that of Shahnaz et al. [29].

Security, immutability, and traceability are some of the challenges faced by traditional EHR management systems. This can increase patient and healthcare risks associated with the use of electronic health records. However, it should be noted that blockchain technology has many unique features that make it useful as a platform for managing electronic medical records. This solution solves all these problems. Cryptozoology has many advantages, one of which is its classification, meaning that it does not allow information to be obtained from any person or entity. This is one of the main benefits of cryptography. If organizations use this type of division of labor, hackers and other cybercriminals will have a hard time obtaining information. Therefore, the possibility of a data breach resulting from this measure is reduced. Also, since blockchain is immutable, once an EHR record is created or updated, it cannot be changed or deleted in the future. Therefore, according to this example, the data needs to remain reliable and proven, providing a comprehensive and transparent path for the future. In addition to the ability to track, blockchain technology has some additional benefits for doctors, such as tracking medical information across various stakeholders such as hospitals, medical facilities, and insurance companies. Additionally, this feature encourages collaboration among healthcare providers, ensuring data accuracy and reducing errors. The key benefits of Blockchain over traditional EHR management systems are security, immutability, and traceability. Implementing these features can improve patient outcomes by ensuring the integrity, accuracy, and confidentiality of electronic medical records.

Blockchain technology also uses advanced encryption techniques such as asymmetric (public-private key) encryption and hashing to ensure that only two parties have the authority to access or modify medical information. This encryption technology provides better

protection compared to centralized systems where a leak in the central storage can expose a lot of sensitive information. In contrast, the decentralized nature of the blockchain reduces this risk by ensuring that the entire system remains secure even if one of them is compromised. Research by Kumar and Tripathi [26] confirmed that blockchain encryption technology provides security and privacy for medical information and reduces the risk of information leakage.

In addition, blockchain provides an effective solution by reducing the overhead associated with centrally managing and securing big data. Traditional EHR systems usually require high operating costs for data storage, physical maintenance, and security measures to prevent data breaches. However, blockchain eliminates the need for a central authority to manage the system by distributing the stored data across the network of nodes, thereby reducing the costs associated with development in the middle. Vidap et al. [30] The decentralized nature of blockchain reduces operating and maintenance costs as it requires fewer resources to maintain and manage data.

Data transmission continuously enhances the security of blockchain systems by recording all changes in a transparent and tamper-proof manner. Unlike traditional systems where data can be modified or deleted, blockchain ensures that once data is entered, it cannot be changed without network approval. A study by Mahajan et al. shows that this immutable function is important in preventing fraud and unauthorized access. [31] highlighted the role of blockchain in protecting medical information from tampering.

Therefore, blockchain technology, which uses encryption, decentralized management and immutability features, is not only more secure than traditional systems, but also provides great benefits in terms of information management.

The study revealed several important implications for the healthcare industry. Blockchain frameworks can increase the security, integrity, and accessibility of EHRs. Patient safety can be increased by improving quality and improving medical procedures. Blockchain technology can also help reduce the amount of data in medical records management. Blockchain centralizes the distribution of information, ensuring there is no unauthorized access or less control.

Additionally, a blockchain framework for electronic medical records can reduce costs. Healthcare organizations can also eliminate data logging, reduce storage costs, and reduce errors associated with manual entry. Integrating blockchain into medical information management can improve collaboration between hospitals. Blockchain enables seamless information transfer between facilities, systems, and patients, reducing the inefficiency and complexity of current information exchange practices.

V. CONCLUSION

The most important part of any medical organization is the electronic EHR. In recent years, many privacy and reputation issues have arisen due to concerns about the storage and use of patient information. Therefore, for example, information provided by health insurance, health insurance, etc. can be considered evidence of health insurance and management respected in society. In the past few years, many problems related to the management of medical records have emerged and pose a threat to the privacy of patient information. One of the most important issues in patient information security in new medical applications is to ensure the confidentiality of patient information. Therefore, it is necessary to use blockchain to solve this problem. Transparency and security can be achieved in healthcare using blockchain technology. This paper uses the research design as the basis for development and proposes a secure blockchain system as a research design for managing medical information. The proposed system consists of five elements: Blockchain network, smart contracts, self-regulation, data encryption, and integration with medical information technology. The proposed system takes into account the possibility of providing security and privacy for healthcare organizations when managing medical information. In addition, secure storage systems for electronic data are also demanded to meet the needs of these organizations. Much work remains to be done through future research, including application of the design process in real-world organizations, to demonstrate its effectiveness and affordability.

REFFERENCE

[1] Kanna, G.P., Abinash, M.J., Kumar, Y., Kumar, J., Suganya, E.: A review of security and confidentiality concerns in blockchain technology. In: Wireless Communication for Cybersecurity, p. 129. Wiley, New York, NY (2023).

[2] Engelhardt, M.A.: Exploring the role of blockchain technology in the healthcare sector. Technol. Innov. Manag. Rev. 7(10), 22–34 (2017).

[3] Kumar, R., Tripathi, R.: A secure framework for healthcare based on blockchain and public key cryptography. In: Blockchain Cybersecurity, Trust, and Privacy, pp. 185–202. Wiley, New York, NY (2020).

[4] Angst, C.M., Block, E.S., D'Arcy, J., Kelley, K.: The impact of IT security investments in healthcare data breaches considering institutional factors. MIS Q. 41(3), 893–916 (2017).

[5] Tikhomirov, S.: Ethereum: current knowledge and future research opportunities. In: 10th International Symposium on the Foundations and Practice of Security: FPS 2017, pp. 206–221. Springer, Cham (2018).

[6] Zubaydi, H.D., Chong, Y.-W., Ko, K., Hanshi, S.M., Karuppayah, S.: A comprehensive review of blockchain technology's role in healthcare. Electronics 8(6), 679 (2019).

[7] Gamage, H.T.M., Weerasinghe, H.D., Dias, N.G.J.: An overview of blockchain technology, its applications, and related challenges. SN Comput. Sci. 1, 1–15 (2020).

[8] Tikhomirov, S.: Ethereum blockchain platform overview, including its Turing-complete programming language for smart contracts. In: Foundations and Practice of Security: 10th International Symposium, FPS 2017, pp. 206–221. Springer, Cham (2018).

[9] Hader, M., Tchoffa, D., El Mhamedi, A., Ghodous, P., Dolgui, A., Abouabdellah, A.: Integrating blockchain and big data technologies to enhance supply chain traceability in the textile industry. J. Ind. Inf. Integr. 28, 100345 (2022).

[10] Kumar, T., Ramani, V., Ahmad, I., Braeken, A., Harjula, E., Ylianttila, M.: Challenges and key requirements for blockchain in healthcare. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications, and Services (Healthcom), pp. 1–7. IEEE, Piscataway, NJ (2018).

[11] McGhin, T., Choo, K.-K.R., Liu, C.Z., He, D.: Opportunities and research challenges of blockchain in healthcare applications. J. Network Comput. Appl. 135, 62–75 (2019).

[12] Frizzo-Barker, J., Chow-White, P.A., Adams, P.R., Mentanko, J., Ha, D., Green, S.: A systematic review of blockchain's impact as a disruptive technology in business. Int. J. Inf. Manage. 51, 102029 (2020).

[13] Amofa, S., et al.: Blockchain-based architecture for the secure sharing of personal health data. In: 2018 IEEE 20th International Conference on e-Health Networking, Applications, and Services (Healthcom), pp. 1–6. IEEE, Piscataway, NJ (2018).

[14] Shahnaz, A., Qamar, U., Khalid, A.: A blockchain approach to electronic health records. IEEE Access 7, 147782–147795 (2019).

[15] Theodouli, A., Arakliotis, S., Moschou, K., Votis, K., Tzovaras, D.: Designing a blockchain-based system for healthcare data sharing. In: 2018 17th IEEE International Conference on Trust, Security, and Privacy in Computing and Communications/12th IEEE International Conference on Big Data Science and Engineering (TrustCom/BigDataSE), pp. 1374–1379. IEEE, Piscataway, NJ (2018).

[16] Budida, D.A.M., Mangrulkar, R.S.: Developing and implementing a smart healthcare system using IoT. In: 2017 International Conference on Innovations in Information, Embedded, and Communication Systems (ICIIECS), pp. 1–7. IEEE, Piscataway, NJ (2017).

[17] Wang, S., et al.: Blockchain-enhanced parallel healthcare systems using the ACP method. IEEE Trans. Comput. Soc. Syst. 5(4), 942–950 (2018).

[18] Raj, C., Jain, C., Arif, W.: HEMAN: IoT-based e-healthcare system for remote monitoring and telemedicine. In: 2017 International Conference on Wireless Communications, Signal Processing, and Networking (WiSPNET), pp. 2115–2119. IEEE, Piscataway, NJ (2017).

[19] Mahajan, H.B., et al.: Integrating Healthcare 4.0 with blockchain for secure cloud-based electronic health record systems. Appl. Nanosci. 13(3), 2329–2342 (2023).

[20] Vidap, P., Bhargav, A., Paswan, R., Jewalikar, A.: A blockchain-based solution for managing electronic healthcare records. In: 2023 International Conference on Intelligent and Innovative Technologies in Computing, Electrical and Electronics (IITCEE), pp. 659–664. IEEE, Piscataway, NJ (2023).

[21] Khan, M.A., Alsuhibany, S.A., El-Shafai, W., Rehman, M.U., Ahmad, J.: An immutable blockchain framework for smart healthcare. Comput. Syst. Sci. Eng. 46(1), 165–179 (2023).