Naif Arab University for Security Sciences
Journal of Information Security and Cybercrimes Research
مجلة بحوث أمن المعلومات والجرائم السيبرانية
https://journals.nauss.edu.sa/index.php/JISCR
JISCR

Security in Health Information Management Records through Blockchain Technology: A Review

Yasir Hamid[1*], Rameez Yousuf[2], Atif Chowhan[1]

[1]Information Security Engineering Technology, Abu Dhabi Polytechnic, United Arab Emirates.

[2]Department of Computer Science, University of Kashmir, J&K, India.

Received 08 Feb. 2023; Accepted 01 May. 2023; Available Online 22 June. 2023

Abstract

Medical records play a crucial role in delivering high-quality healthcare by facilitating accurate diagnosis, treatment, and patient monitoring. However, manual, paper-based record-keeping systems present various challenges, including storage burden and retrieval difficulties. Although electronic medical records (EMRs) have gained popularity, they are not risk-free, such as data manipulation. Inadequate medical records administration contributes to inefficiencies in the healthcare system, increased costs, incorrect diagnoses, and compromised patient care. This literature review investigates the potential of blockchain technology in enhancing medical record management and improving the quality, efficiency, and limitations associated with traditional manual methods. Specifically, the study explores the benefits of utilizing blockchain in medical records management. The findings suggest that blockchain technology can enhance the security, interoperability, and accessibility of medical records thereby mitigating concerns related to data manipulation while providing a more cost-effective and efficient solution for medical records management.

I. Introduction

The maintenance of precise medical records is essential to the provision of high-quality healthcare. Precise medical records are also useful in the study of medical systems, illnesses, and health disparities. Moreover, such records aid in the eradication of healthcare inequalities. The proper diagnosis and treatment of illnesses must be documented by licensed medical experts to provide high-quality medical care. Medical fitness is a prerequisite for providing the kind of high-quality health care that ultimately benefits the population's health. [1] States that accurate medical records are vital to delivering better health care and lowering the health burden. For patients to get the best treatment possible and to guarantee continuity of care, accurate and complete medical records must be kept. What effect do you think organized medical records will have on the smooth operation of healthcare facilities? In conclusion, high-quality medical care relies heavily on accurate records [2]. The National Health Organization's Health Care Records Management Steering Committee defines records management as "systematic and consistent control of all records in which they are preserved throughout their life cycle". According to the World Health

Keywords: Cybersecurity, Blockchain, Electronic Medical Records (EMRs), Health Services, Smart Contracts.

Production and hosting by NAUSS

* Corresponding Author: Yasir Hamid
Email: yasir.hamid@adpoly.ac.ae

doi: 10.26735/QBIJ3667

Report, the health of a country must have quick and simple access to medical records. The World Health Organization (WHO) claims that the quality and management of health information records impact both the quality and efficiency of healthcare professionals and the accessibility of healthcare services. They also determine how much money is required to offer medical care. For the sake of monitoring both healthcare providers and their patients, accurate medical records must be kept. They are crucial in shaping and implementing health care policy, which has a direct impact on the health of a nation and the quality of life of its citizens.

An educated and healthy populace is essential to the national development and prosperity of any culture. Even though the disease is expected to be discovered and treated despite the everyday occurrence of sickness, injury, and emergency circumstances, the patient's health record is a collection of the patient's mental and physical health information from various healthcare providers. Information on a patient's medical history, physical exam, diagnosis, treatment, laboratory test results, imaging reports, warnings (such as those of allergies), and other pertinent information are all kept in the patient's health record. It is possible to save these medical records either manually or electronically. The majority of healthcare facilities still rely on manual, paper-based record-keeping methods. For all four of us [3] this method has several major downsides, including a high storage burden and a high barrier to entry retrieving previously stored data. Electronic medical records (EMRs) have become more popular in recent years due to the ease with which they can be stored and retrieved in digital form [4]. However, without adequate identification, there is a significant risk of manipulation. Patients' legal rights to hold healthcare providers harmless for any unauthorized disclosure of their medical records raise their concerns about the healthcare system. The authors in [5] argue that inaccurate paper records might lead to unnecessary procedures. This method is inefficient because it requires time-consuming manual record transfers through snail mail and fax machines. Poor medical records administration drives up healthcare costs owing to inefficient regulatory frameworks that scatter critical patient information among paper documents, digital photos, and electronic databases [6]. Neglect, incorrect diagnosis and treatment, and inadequate reporting all contribute to alarming death rates [7]. For example: despite South Africa's best intentions, the country's healthcare system is unable to meet the needs of its population because of insufficient funding, inefficient management, and the improper disposal of sensitive patient data [8]. Corruption and the acquisition of fake pharmaceuticals, which aggravate patients' health, have been made possible by the country's inadequate record-keeping. According to [9], poor medical records lead to iatrogenic injuries and impede clinical negligence claims and disciplinary proceedings. This study looks at whether or not digital technologies, and in particular blockchain technology, can enhance the management of medical records, the quality of care provided, and the efficiency with which services are delivered.

The rest of the paper is organized as follows, in section II we present a literature review of the recent works on blockchain and healthcare, section III identifies the role of blockchain in healthcare, in section IV we discuss blockchain architecture and its healthcare applications, in section V we propose a framework for using blockchain in healthcare, in section VI healthcare system issues and blockchain are discussed, while section VII discusses blockchain healthcare issues and finally, the paper concludes in section VIII.

II. Literature Review

The Information Records Management Task Force (IRMT) defines "record management" as "the process of ensuring that information acquired in any form and on any medium is managed effectively, efficiently, and cost-effectively." "Medical Records Management Provides Evidence of Activities or Business Transactions," [10] Medical records are supposed to help physicians offer future care by documenting past diagnoses and treatments. Proper health records management allows for better healthcare decisions and legislation, they say. The IRMT states that good health records administration is essential for high-quality health services and hospital and agency success [11]. According to [12], blockchain-based technology uses a shared

or distributed database to monitor a growing list of transactions, or "blocks." A distributed ledger called a "blockchain" stores transaction records in "blocks" linked in a "chain". "Chain of trust" is a common description. Blockchain technology's potential to increase governance trust, accountability, openness, participation, and transparency is generally accepted. It helps corporations trade and streamline processes. Satoshi Nakamoto created this system for Bitcoin trading in 2008. Bitcoin, Litecoin, and Ethereum use blockchain technology. Blockchain, which powers Bitcoin and other cryptocurrencies, is widely used in finance [13]. Modern blockchain uses include healthcare, insurance, pharmaceuticals, manufacturing, electronic voting, legal contracts, tourism, energy, and transportation [14]. Blockchain technology may enhance patient care, financial transactions, prescription fulfillment, medical records management, and governance. Technologists say blockchain, the fourth industrial revolution, will have far-reaching effects. Blockchain can tackle the complex issues facing the healthcare sector [15]. Blockchain is a decentralized database that stores patient data in time-stamped "blocks" that cannot be edited. Despite its early development [16], Healthcare Informatics editors named blockchain as one of the Top Technology Trends for HIT in 2017. By 2026, blockchain healthcare will be worth $5.50 billion and healthcare is expected to grow by 63.85% from 2018 to 2025 [17].

The healthcare sector is studying blockchain technology. Deloitte surveyed 1,000 IT executives from companies with $500 million or more in yearly sales in seven countries and nine industries in 2018 to predict blockchain's future[18]. 11% of CEOs work in healthcare, and 55% believe blockchain technology will have a major influence. 74% of healthcare technology executives say they understand blockchain. More than two-thirds (63%) of the CEOs of healthcare firms questioned stated they would invest more than $1 million in blockchain technology in the coming year. 39% listed blockchain among their top five strategic goals.

Blockchain technology might greatly enhance patient care. Deloitte's 2019 blockchain technology report [18] shows an increase in blockchain-related financing. This survey questioned 1,300 senior executives from dozens of countries. 53% of respondents said blockchain was a key corporate endeavor this year. Cognizant surveyed 588 blockchain-savvy workers in 2017 [19]. The survey results were valuable. 57% indicated it would considerably change the sector, and 51% mentioned clinical administration data interoperability (EMR, EHR) as a key potential use case their organizations planned to examine [20]. Blockchain has several healthcare applications. Health data management is promising. Blockchain technology is valuable. Blockchain-based medical records solutions are popular [21]. Blockchain data management applications include global scientific data exchange for R&D, data management, cloud storage, and EHRs [22]. Distributing and immuting these records ensure patient data protection and accuracy. Data integrity is crucial to healthcare delivery because inaccurate or missing patient data may create complications[23]. Unauthorized parties may only partially access blockchain-stored patient health records [23]. This DLT is represented by the blockchain. Immutable transactions reduce data corruption. Patient data encryption boosts network security. Corruption and data breaches plague hospital IT systems. Some people withhold things from their physicians to protect their medical information [24]. Thus, blockchains provide the highest data security.

III. The Role of Blockchain Technology in the Health Sector

Authors in [24] showed how blockchain technology improves healthcare companies, patient outcomes, and medical records (2018: 68). This technology improves compliance, healthcare expenses, and data utilization. Blockchain technology safeguards medical records. This technology accesses patient data and efficiently connects patients and providers. [20] say blockchain technology may be permissioned or permissionless. Both aid healthcare data storage.

A. Patient Confidentiality

Blockchain-based healthcare solutions may address data security, privacy, sharing, and storage [25]. It will enable consolidated, easily accessible health records, thus improving care. Centralized

medical records are secure and convenient [26]. This improves resource utilization for patients and medical personnel. Blockchain safeguards patient data, medical data, and hospital operations. According to [27], blockchain technology protects medical records from being manipulated or stolen. It's a decentralized database that keeps data across numerous networks for optimum redundancy, safety, consistency, and resistance against attack while speeding up medical data transfers. Blockchain technology can decentralize medical records, giving people authority over their health so they may make improvements. A blockchain-based MedRec system "ensures the security of medical health records." MedShare system allows data provenance and administration in cloud repositories across institutions". To secure medical data in a blockchain network, [28] used the Hyperledger Fabric membership service and channel construction scheme. Ambulance crews and paramedics may use blockchain-based technology to record emergency medical data and offer high-quality pre-hospital care, according to [29]. [3] claims that blockchain networks ensure data integrity. Ethereum's blockchain regulates and secures patient medical records [30].

B. Medical Records Openness

Blockchain technology improves data exchange between physicians, specialists, hospitals, and therapists. Time, money, and patient care errors are saved. Patients who trust their medical records are more likely to collaborate with their physicians and get prompt treatment [31]. Blockchain manages identity, confidentiality, accountability, and data sharing. It encourages patient data interchange and rewards medical researchers for system maintenance. Blockchain technology provides patients with an encryption key that allows healthcare professionals to access their health data, creating a transparent and auditable system [12].

C. Optimizing Healthcare Recordkeeping

Poor medical records management and control have contributed to high death rates. Blockchain technology may improve medical health records governance and management, helping patients and clinicians by providing quick, unified access to a patient's entire medical history from all providers. Blockchain-based medical records management may speed up patients' medical histories. It makes sharing disintermediated medical records safer and easier. Blockchain technology lets doctors rapidly update patient records across all platforms. It also gives anybody who needs to examine the patient's data and medical history complete access [20].

D. Protecting Drug Development and Distribution

Pharmaceutical businesses may conduct clinical trials and trade medical samples securely using blockchain technology. Blockchain technology can monitor and label each clinical trial stage, ensuring the best data quality and reducing wasteful costs. Accountability and transparency increase clinical trial reporting. Blockchain also permits autonomous monitoring and preventive maintenance of medical equipment, uniting otherwise different healthcare procedures and improving regulatory compliance, patient experience, and cost. It also shortens the research cycle for new drugs [32] and might revolutionize healthcare systems by making users the center of the healthcare ecosystem. This improves medicine distribution by increasing individuals' trust in the healthcare system and drug-buying knowledge. Protection of creative works, counterfeiting, low-quality items, and drug trafficking must be handled.

IV. Blockchain Architecture for Healthcare

The basic architecture of blockchain consists of blocks that are linked in chronological order and are append-only. Each block consists of a block header and a block body. The header consists of information such as hash, previous hash, merkle root, timestamp, and nonce [33]. The body of the block consists of transactions. Fig. 1 shows the basic structure of a blockchain in healthcare.

The architecture of blockchain for healthcare typically consists of several components, including nodes, consensus mechanisms, and smart contracts.

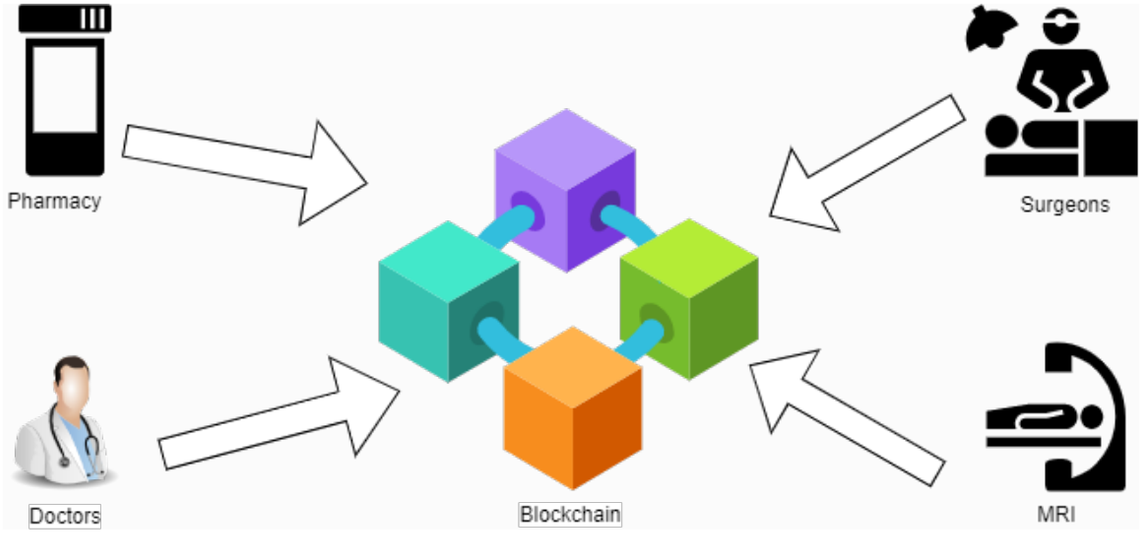

Fig.1 Blockchain architecture in healthcare.

A. Nodes: These are the devices or computers that participate in the network and maintain a copy of the blockchain. They can be operated by healthcare providers, patients, researchers, or other stakeholders. The use of nodes in healthcare blockchain helps to increase transparency, security, and interoperability of healthcare data.

B. Consensus mechanism: This is the process by which the network agrees on the state of the blockchain and ensures its integrity. Examples of consensus mechanisms include proof of work, proof of stake, Stellar consensus protocol, and practical Byzantine fault tolerance.

C. Smart contracts: These are self-executing contracts with the terms of the agreement between buyer and seller being directly written into lines of code. They can be used in healthcare to automate the sharing of patient data, the management of clinical trials, and the tracking of medical supply chains. Formal methods are mathematical techniques used to verify the correctness of software and hardware systems. Given their critical role in ensuring the integrity of transactions, the use of formal methods for the verification of smart contracts is becoming increasingly important. Here are some ways in which formal methods can be used for the verification of smart contracts:

- *Formal specification:* It involves describing the behavior of a system using a mathematical language [34]. This can be used to specify the requirements of a smart contract and to check that the contract behaves correctly under all possible scenarios.
- *Model checking:* It is a technique for verifying the correctness of a system by checking that a model of the system satisfies certain properties. This can be used to verify that a smart contract behaves correctly under all possible inputs and in all possible states.
- *Theorem proving:* It involves using mathematical reasoning to prove that a system satisfies certain properties. This can be used to verify that a smart contract behaves correctly under all possible scenarios.
- *Program analysis:* It involves examining the source code of a program to identify potential errors or vulnerabilities. This can be used to identify potential flaws in a smart contract and to prevent them from being exploited.
- *Static analysis:* It involves the use of software tools to analyze the code of a smart contract without actually executing it. This can help identify potential security vulnerabilities and programming errors in the contract.
- *Formal verification tools:* There are several formal verification tools available for verifying the correctness and safety of smart contracts. Here are some examples:
- *Solidity Compiler:* Solidity is a high-level programming language used to write smart con-

tracts for the Ethereum blockchain. The Solidity Compiler includes a static analyzer that can detect potential bugs and vulnerabilities in the contract code.

- *Mythril:* It is a security analysis tool for smart contracts. It uses symbolic execution and SMT solvers to detect security vulnerabilities in the contract code, such as reentrancy attacks, integer overflows, and unhandled exceptions.
- *Oyente:* It is a security analysis tool for Ethereum smart contracts. It uses symbolic execution to analyze the contract code and identify potential vulnerabilities, such as callstack depth limit violations, integer overflows, and gas limit violations.
- *KEVM:* Itis a formal verification tool for smart contracts on the Ethereum blockchain. It uses formal methods, such as theorem proving, to verify the correctness of the contract code and ensure that it behaves as expected.
- *Securify:* It is a security analysis tool for smart contracts on the Ethereum blockchain. It uses a combination of static analysis and dynamic analysis to identify potential vulnerabilities in the contract code, such as reentrancy attacks and outofgas errors.
- *SmartCheck:* This is a static analysis tool for smart contracts on the Ethereum blockchain. It uses a set of predefined rules to analyze the contract code and detect potential vulnerabilities, such as uninitialized variables and unchecked return values.

These formal verification tools can help developers ensure that their smart contracts are correct, secure, and free from vulnerabilities before they are deployed on a blockchain network.

Moreover, the framework of blockchain for healthcare consists of users such as patients, doctors, administrators, and nurses. The blockchain layer receives the data from users and sends it to the cloud for storage and processing. Cloud storage for healthcare using blockchain can provide a secure and decentralized way to store and share patient data. Blockchain technology, with its immutability and decentralized nature, can ensure that patient data is tamper-proof and only accessible to authorized parties. This can help to protect patient privacy and improve data security in the healthcare industry [35], [36]. Additionally, the use of smart contracts can automate certain processes and make data sharing more efficient. One example of a blockchain healthcare platform that uses cloud computing is the MediBloc platform. All the components work together to provide a secure and decentralized platform for storing and sharing health data, while also ensuring privacy and compliance with relevant regulations. Fig. 2 shows the blockchain framework for healthcare.

Storing data on the cloud in a blockchain-based healthcare system involves several steps. Here is an overview of the typical process:

- *Data creation and capture:* The data is created and captured by a healthcare provider or patient using a device or application. It may include patient health records, diagnostic images, test results, and other medical information.
- *Data encryption:* Before storing data on the cloud, it is encrypted using strong encryption algorithms to ensure that it is protected from unauthorized access.
- *Data upload:* The encrypted data is then uploaded to the cloud, where it is stored securely. The cloud provider must ensure that the data is stored securely, and access to the data is restricted to authorized users.
- *Data hashing and blockchain transaction creation:* A cryptographic hash is created for the data, which is then used to create a transaction on the blockchain. The transaction contains the hash, as well as other metadata, such as a timestamp and the identity of the entity uploading the data.
- *Transaction validation and confirmation:* The transaction is then validated and confirmed by the nodes on the blockchain network using the consensus algorithm. Once the transaction is confirmed, it becomes a permanent part of the blockchain, and the data is considered securely stored.
- *Data access:* Authorized users can access the data on the cloud by decrypting it using a private key. The blockchain provides an audit

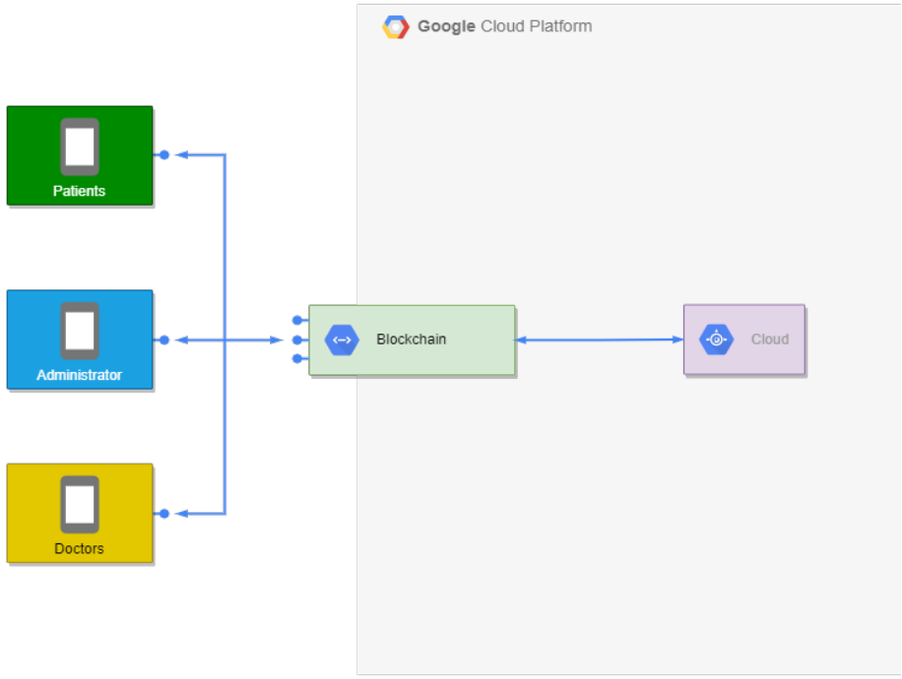

Fig. 2 Blockchain framework for healthcare.

trail of all transactions, ensuring that the data's integrity is maintained and can be traced back to its source.

Storing data on the cloud in a blockchain-based healthcare system involves encrypting the data, uploading it to the cloud, creating a blockchain transaction with a cryptographic hash, validating and confirming the transaction using the consensus algorithm, and providing authorized users with access to the data. The use of blockchain technology ensures that the data is stored securely and that its integrity is maintained, providing a transparent and secure way to store and access healthcare data.

Blockchain technology has several potential applications in the healthcare industry as shown in Fig. 3, including:

- *Electronic Health Records (EHRs):* Blockchain can be used to securely store and share patient health records, ensuring that sensitive information is protected and accessible only to authorized parties.
- *Clinical Trials:* Blockchain can be used to track and manage clinical trial data, ensuring that results are secure, transparent, and tamper-proof.
- *Supply Chain Management:* Blockchain can be used to track the movement of medical supplies and drugs from manufacturers to patients, helping to prevent counterfeit drugs and improving transparency in the supply chain.
- *Remote Patient Monitoring:* Remote Patient Monitoring (RPM) using blockchain technology involves the use of wearable devices, sensors, and other digital health tools to collect and transmit patient data to healthcare providers. Blockchain technology can be used to securely store and manage this data, providing several benefits for RPM applications.
- *Health Data Exchange:* Blockchain can be used to securely exchange health data between different organizations and systems, reducing the risk of data breaches and improving data interoperability.
- *Personalized Medicine:* Blockchain can be used to securely store and share genetic and health data, enabling the development of personalized medicine and precision healthcare.
- *Insurance Claims Processing:* Blockchain can be used to streamline and secure the processing of insurance claims, reducing fraud and administrative costs.

- *General Data Protection Regulation (GDPR):* All people living in the European Union (EU) and the European Economic Area must abide by the General Data Protection Regulation (GDPR), which is a provision of EU law (EEA). GDPR has consequences for how patient data is gathered, kept, and processed in the context of blockchain in healthcare.

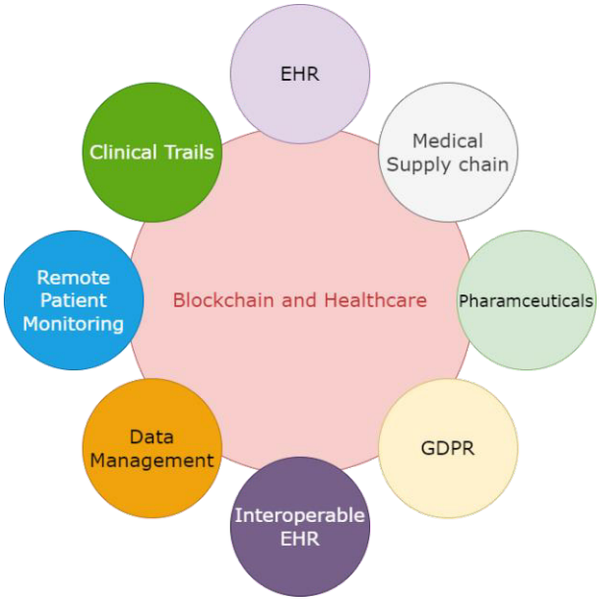

Fig. 3 Blockchain applications in healthcare.

The blockchain as a novel technology is still in its early stages, but its potential for improving the security, efficiency, and accessibility of healthcare data is significant.

(I) Platforms for Blockchain-Based Healthcare Systems

Several blockchain-based platforms are being developed or used in healthcare systems. Some of these platforms are summurized in Table I.

Blockchain-based platforms offer several advantages for healthcare systems, including improved security, transparency, and efficiency. The choice of platform will depend on the specific needs and requirements of the healthcare system in question.

(II) Consensus Algorithms for the Healthcare System

Consensus algorithms play an important role in ensuring the accuracy and consistency of data in healthcare systems, particularly in decentralized or distributed systems. Here are some consensus algorithms that can be used in healthcare systems, summarized in Table II.

The choice of consensus algorithm for a healthcare system will depend on factors such as the number of nodes, the level of security and privacy required, and the computational resources available.

TABLE I
PLATFORMS FOR BLOCKCHAIN-BASED HEALTHCARE SYSTEMS

Platform	Brief of the platform
Hyperledger Fabric	It is a permissioned blockchain platform that provides a flexible and modular architecture, making it suitable for building healthcare systems. It offers features such as confidentiality, privacy, and smart contracts, which can be used to develop secure and transparent healthcare applications.
Ethereum	It is a public blockchain platform that supports the development of decentralized applications (dApps) using smart contracts. It can be used to build healthcare systems that require transparency and decentralization, such as supply chain management or clinical trials.
Hashed Health	It is a blockchain-based platform that provides solutions for the healthcare industry. It offers features such as identity management, data sharing, and secure messaging, which can be used to improve the efficiency and security of healthcare systems.
Medicalchain	It is a blockchain-based platform that enables patients to store and share their medical data securely. It uses smart contracts to ensure that patients have control over their data and can grant access to healthcare providers as needed.

TABLE II
CONSENSUS ALGORITHMS FOR THE HEALTHCARE SYSTEM

Consensus Algorithms	Brief of the algorithm
Practical Byzantine Fault Tolerance (PBFT)	PBFT is a consensus algorithm that is designed to provide fault tolerance in a distributed system with a small number of nodes. It is a proven algorithm that is used in various applications, including healthcare systems. PBFT ensures that all nodes agree on the order of transactions and that the transactions are executed correctly.
Proof of Authority (PoA)	PoA is a consensus algorithm that is designed to provide a high level of security in private blockchain networks. It is used to ensure that only authorized nodes can participate in the consensus process. PoA is a good choice for healthcare systems where data privacy and security are critical.
Proof of Work (PoW)	PoW is a consensus algorithm that is widely used in public blockchain networks, such as Bitcoin. It requires participants to perform complex calculations to validate transactions, which can be time-consuming and energy-intensive. While PoW can provide a high level of security, it may not be suitable for healthcare systems due to its high computational requirements.
Proof of Stake (PoS)	PoS is a consensus algorithm that allows validators to participate in the consensus process based on their stake in the network. Validators can earn rewards for validating transactions and are incentivized to act honestly. PoS can provide a high level of security and energy efficiency, making it a good choice for blockchain-based healthcare systems.
Delegated Proof of Stake (DPoS)	DPoS is a consensus algorithm that is used in blockchain networks that require high throughput and low latency. It allows stakeholders to delegate their voting power to a set of block producers, who are responsible for validating transactions. DPoS can provide fast transaction processing and a high level of security, making it a good choice for healthcare systems that require high performance.

V. BLOCKCHAIN-BASED FRAMEWORK FOR HEALTH INFORMATION RECORDS MANAGEMENT

Blockchain technology replaces centralized databases in our medical records management system. The blockchain's smart contracts can safeguard patient data on the distributed ledger's nodes. Smart contracts for administrative chores may save time and effort in healthcare.

Health information records management uses Ethereum's blockchain technology. The framework is based on smart contract dependencies. [37], [38] inspired the design. An encrypted, private blockchain network secures, protects, and verifies all medical records. An innovative combination of Nchinda and Cameron's data transmission mechanism protects blockchain data integrity by instantly recognizing the user and authorizing the corresponding authorization (2019).

A. Registrar Contract (RC)

This contract connects member ID strings to specific Ethereum addresses. Those who have joined include both patients and medical professionals. The proposed method allows for varying degrees of access based on the identity being used.

It is acceptable to provide patients with access to their medical records. In subparagraph (b), affix your signature to your health records. Staff members in the medical field are allowed to create and alter patient records. The first step is to review legal health documentation. There are special protections in place for medical workers.

B. Patient-Provider Relationship (PPR) Contract

PPR smart contracts are medical certificates. The PPR smart contract maintains medical data, diagnosis,

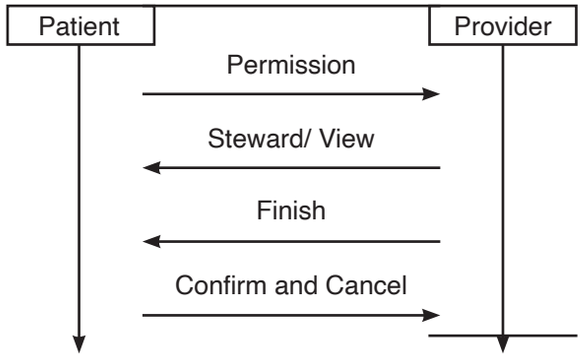

Fig. 4: Authorization procedure for getting medical record permission.

and summary of contract access permissions. Other important PPR diagnostic information may be given. The PPR contract owner must license all smart contract summaries to access them.

Fig. 4 shows that after receiving permissions, medical staff may only alter or view summary contracts. PPR contracts help the administration system monitor current diagnoses.

C. Summary contract (SC)

PPRs and other patient medical data are listed in this agreement. In the proposed system, a method is devised for classifying patients' medical records. Information is stored in the form of PPR smart contracts. The structure of a medical record is shown in Fig. 5.

D. Private Blockchain Network

Fig. 5 shows how the private blockchain network affects care quality. The main private blockchain is solid. Healthcare institutions handle critical network nodes and coordinate database changes across several sites. Clinics may update their databases by synchronizing with nearby blockchain nodes.

The dotted lines depict patient requests for their medical records to be sent to them through the blockchain. The most important nodes in the blockchain network (like a hospital or medical center) answer the inquiries because their infrastructure can

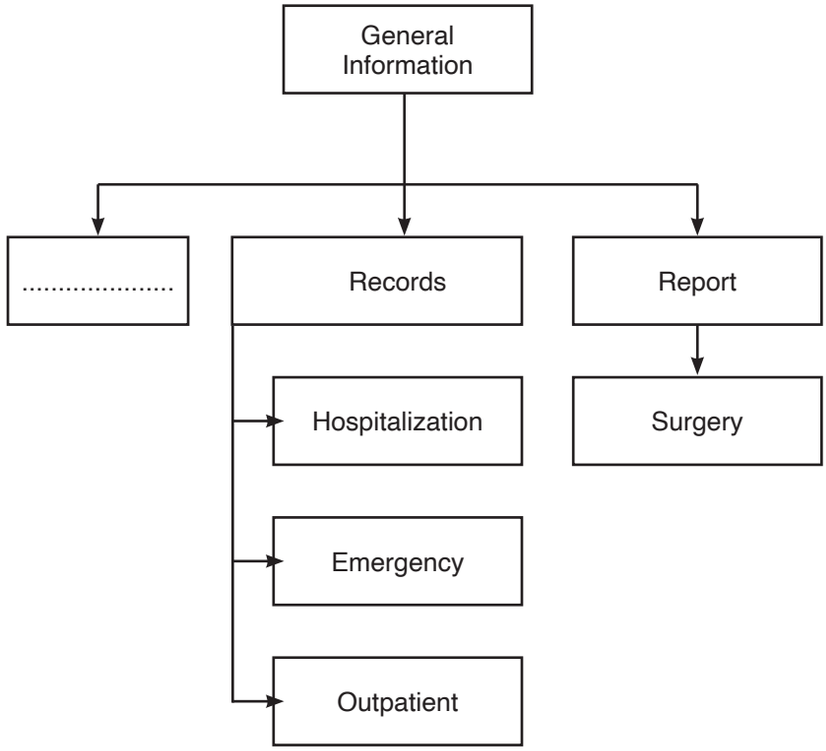

Fig. 5. Proposed personal medical record.

manage the influx of traffic created by the questions. For a pivotal node in a blockchain network, synchronization speed and precision are essential.

E. External Process and Outside Process

The external management system picks up on changes made to the blockchain databases, verifies the most recent information, and alerts the patients.

F. Update Nodes

The blockchain network instantly updates all nodes to provide the most recent data to the waiting node.

G. Notification from provider B

Patients may verify the accuracy of the changes made to their medical records by contacting the person or organization that made the changes.

VI. Healthcare System Issues and Blockchain

Important challenges to interoperability that continue to hinder access and use of electronic health information were noted in the 2018 annual report given to the U.S. Congress on the development of a national system for the electronic use and sharing of health information. The technological, monetary, and trust obstacles constitute all factors. Lack of standardized development, poor data quality, and difficulties in linking patient and healthcare provider records are all examples of technical challenges. Costs associated with creating, deploying, and optimizing HIT represent another economic challenge. To optimize HIT, it is necessary to adapt to the ever-evolving demands of healthcare programs, offer enough incentives for information sharing across healthcare providers, and overcome trust hurdles (such as legal and financial motivations) that prevent data from flowing.

A. Lost Opportunities in Healthcare

Utilizing current technology or adopting novel techniques, healthcare systems are unable to reduce waste. Researchers have looked at the issue of healthcare waste. In 2009 [39] looked at what factors contribute to healthcare spending above what is necessary for the United States. They identified six categories of healthcare waste in the United States, totaling $210 billion: unnecessary services, $190 billion in excess administrative costs, $130 billion in inefficiently delivered services, $105 billion in excessive prices, $75 billion in fraud, and $55 billion in missed prevention opportunities. Kelley conducted research in 2009 that predicted healthcare waste in the United States would amount to $700 billion [40]. It is estimated that in the United States healthcare waste accounts for five percent of GDP [41]. According to other research, over 20%, or $1.2T, of health expenditure in OECD nations is regarded to be waste. There is an estimated 20% waste in overall healthcare spending in the United States [42]. Overtreatment, poor care coordination, poorly executed care procedures, complex management, incorrect pricing, and misuse and fraud all contribute to waste (Hackbarth, 2012). The yearly cost to the United States healthcare system due to medical mistakes is estimated between $17 billion and $29 billion. If HIT is used to its full potential, it might save roughly $80 billion [43]. Overtreatment was identified by [44] as a source of avoidable damage and expense in healthcare in a study of 2,106 doctors. According to the findings, 20.6% of all medical treatment was inappropriate. Prescription drugs (22%), laboratory testing (24%), and surgical treatments (11.1%) all contribute to landfill trash. Overtreatment occurs for a variety of reasons, the most common of which is an apprehension of legal repercussions for doctors (84.7%), patient requests or insistence (50.0%), and a lack of easy access to previous medical information (38.2%). The use of computers has helped reduce waste as technology has progressed.

B. Expenses for Administration and Commerce

Global healthcare expenditures are substantial and rising. In 2018, healthcare expenditure in the United States was $3.6 trillion, or 17.7 percent of the GDP. This was an increase of 4.6 percent over 2017 spending levels. When compared to the 4.7% rise seen in 2017, 2018 saw a decrease in hospital

spending of $4.5% ($1,191.8 billion). As much as half of all healthcare expenditures are thought to be fraudulent due to overbilling or charging for services that were never provided [45]. The transaction costs associated with medical claims were studied in a study issued by the Council for Affordable Quality Healthcare. This organization is a non-profit partnership of health plans and trade organizations to streamline the business of healthcare. It takes a lot of time for a provider to manually execute medical transactions. It is believed that each transaction processed manually takes five minutes longer than an automated one. A single claim might be processed in as little as 40 minutes using electronic transaction processing. The administrative transaction expenses decreased as a consequence of EHR adoption. Whether the exchange is completed entirely digitally, partly digitally, or manually, determines these fees. The sending and receiving of 58 transactions incur fees. Possible expenses include those associated with sending a fax to the insurance company to report a claim, as well as any time or effort put into processing the claim. The healthcare sector and providers stand to save money and time if they can streamline their processes. In all, we expect to save around $700 million. Full implementation of computerized administrative processes may save the medical and dentistry sectors, combined, $12.4 billion annually, according to the same analysis.

C. Security

Healthcare providers and healthcare regulators place a premium on the safety of HIT resources like patient records. Security concerns are not being adequately addressed by existing HIT procedures. The current system is not secure enough to protect sensitive patient information. Between 2014 and 2015, the number of PHI breaches jumped from about 1.8 million to over 111.9 million. During 2018, the "Hacking/IT incident" accounted for six of the top 10 breaches. The HHS's Office for Civil Rights (OCR) created a gateway for data breaches. There is a record of breaches involving 500 or more persons' unprotected health information on the breach site. At present, healthcare practitioners are exclusively accountable for the safety and accuracy of their patient's medical files. Medical history isn't always easy to find. They protect information against corruption if the original record is tampered with.

D. Trading Medical Records

Quality of treatment relies heavily on the free flow of information about individual patients across different medical facilities. Interoperability, data integrity, accuracy, and availability are only a few of the problems that surround health information exchange. There are a variety of EHRs used by the healthcare industry, and they all follow somewhat different protocols. Throughout the city of Boston, 26 distinct EMRs are in operation, each having its own not just representation but also shared language [46]. As a result of patients' data being stored in many locations, they are not always easy to retrieve. According to [47], the present referral procedure is unsatisfactory to 63% of referring primary care doctors owing to insufficient information and substance in reference letters. About 30% of tests are reordered because the findings cannot be obtained or are of no use due to interoperability challenges among healthcare providers. Due to inefficiency, a lot of material is wasted. According to another survey [39], over a quarter of American patients said their medical data and test results were not transmitted in time for their appointment when they switched doctors. Nearly 81% of doctors indicated that they had difficulty locating the information they need to make educated treatment choices during patient visits [48].

E. Whole Patient Record

Medical histories of individual patients are dispersed over several databases. Electronic health records are not supposed to be a permanent record of a patient's medical history [10]. Experts have introduced blockchain technology to the discussion as the ideal method to centralize the EHR into a single, permanent record. The distributed ledger technology used in blockchains permits protected access to patient longitudinal health data.

F. Efficiency

Healthcare has always been an early adopter of many technologies, including fax machines. In

comparison to more modern electrical systems, the efficiency of this technology is rather poor. When comparing the success rates of fax and web-based referral systems, researchers found that only 54% of over 40,000 referrals resulted in booked specialist appointments utilizing fax [49]. Technical concerns, such as referrals being lost, not officially approved, missing information, and taking too long to reach patients, reduced the appointment rate for faxed referrals.

VII. Blockchain Healthcare Issues

Before it can be widely used in healthcare, blockchain technology must overcome several obstacles. Blockchain technology in healthcare poses some challenges and considerations. There are technological, legal, commercial, trust, and socio-technical issues [50]. Initial cost, cost of joining the network, cost of overcoming standardization issues, cost of operation, cost of sharing data, cost of following regulatory guidelines, and cost of maintenance are all factors to consider when deciding whether to use a blockchain to manage and share patient records [51]. Implementing the blockchain and convincing market players to join will cost these amounts. Verifying financial transactions is part of data transfer. Transaction verification costs also depend on electricity use and capital equipment [52]. Due to their limited use in healthcare, blockchain installations are financially ambiguous [36]. Another challenge is convincing market players to join the blockchain. Participants in the market must agree to let the market use their personal information to join the network. Data can be synchronized across sources without a single authoritative source, eliminating the need for reconciliation. Integrating disparate data sets takes time and resources. With a blockchain, everyone uses the same verified data, and these service providers lose their central authority. Everyone has equal control over collective data access and modification. Blockchain networks must try to win over healthcare providers. Blockchain technology in healthcare is hampered by scalability. The number of sales that can be approved and processed per second should be calculated. The original blockchain program, Bitcoin, can handle seven transactions per second. IBM achieved 3,500 transactions per second by optimizing blockchain technology[53]. In private blockchains, some transactions are kept on the chain while others are kept off to reduce blockchain strain and increase speed and scalability. For everyone to have the "same version of the truth," healthcare data sharing will need more storage. As more advanced tools are used, clinical data transactions increase dramatically [54]. Several methods have been proposed to address blockchain scalability, despite its difficulty. Healthcare institutions may store some data off-chain, and smart contracts can help share other data. Healthcare institutions can use blockchain connections to access off-chain data when needed. Thus, some data may be kept off-chain for security and privacy. The lack of clarity in blockchain regulation is also important. Blockchain adoption in healthcare systems is slow due to government restrictions on healthcare data. The Health Insurance Portability and Accountability Act (HIPAA) and other data privacy laws, general data protection regulations, and patient health information security policies must be followed by entities. Blockchain projects in healthcare should be known and adaptable to the ever-changing regulatory framework [55].

VIII. Conclusions and Future Research

Health is wealth, but health records may also be wealth. Thus, medical secrecy is more important than ever. Patient-driven interoperability, where patients provide on-demand access to their health data, is increasingly common. The patient decides who gets their medical history. Blockchain, by decentralizing the process, solves the problems of switching from an institution-driven to a patient-driven approach. 16% of IBM's Institute for Business Value Blockchain's 200 executives in the health sector are ready to deploy commercial blockchain. Blockchain can verify and validate data, offer real-time data access, maintain data confidentiality, effectively handle enormous data amounts, and decentralize data.

After all, parties agree on protocols, and "smart contracts" operate automatically under our technique. The patient and hospital management will be the end users. Smart contract execution involves

invoking, producing, and validating a record. Blockchain technology is one of several ways to improve health record management, as discussed in this paper. Blockchain technology may be used for utility payments, finance, e-voting, transportation, supply chain management, and more besides healthcare record keeping. Blockchain needs further research to be applied anywhere it can ease people's lives.

Funding

This article did not receive any specific grant from funding agencies in the public, commercial, or not-for-profit sectors.

Conflict of Interest

Authors declare that they have no conflict of interest.

References

[1] L. P. Luthuli and T. Kalusopa, "The management of medical records in the context of service delivery in the public sector in KwaZulu-Natal, South Africa : the case of Ngwelezana hospital," *South Afr. J. Libr. Inf. Sci*., vol. 83, no. 2, pp. 1–11, Dec. 2017, doi: 10.7553/83-2-1679.

[2] A. Rabiu, M. Mukhtar, F. Abbas, and A. Yusuf, "ICT Utilization and its Barriers in Jigawa State Primary Health Care Centers," *Inf. Technol.*, vol. 16, no. 2, Dec. 2019.

[3] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "MedRec: Using Blockchain for Medical Data Access and Permission Management," in *2016 2nd Int. Conf. Open Big Data (OBD)*, Aug. 2016, pp. 25–30. doi: 10.1109/OBD.2016.11.

[4] V. M. Harshini, S. Danai, H. R. Usha, and M. R. Kounte, "Health Record Management through Blockchain Technology," in *2019 3rd Int. Conf. Trends Electron. Inform. (ICOEI)*, Apr. 2019, pp. 1411–1415. doi: 10.1109/ICOEI.2019.8862594.

[5] G. Kamau, C. Boore, E. Maina, and S. Njenga, "Blockchain Technology: Is this the Solution to EMR Interoperability and Security Issues in Developing Countries?," in 2018 *IST-Africa Week Conf. (IST-Africa)*, May 2018, pp. Page 1 of 8-Page 8 of 8.

[6] J. Medeiros and C. Schwierz, "Efficiency estimates of health care systems," , Jun. 2015. [Online]. Available: https://ec.europa.eu/economy_finance/publications/economic_paper/2015/pdf/ecp549_en.pdf (Accessed: May 03, 2023)

[7] E. B. Niyitunga, "The current and potential role of blockchain-based technology in managing medical records in Africa," *Digit. Policy Stud.,* vol. 1, no. 1, Art. no. 1, May 2022, doi: 10.36615/dps.v1i1.1253.

[8] D. Kaseje, "Health Care in Africa: Challenges, Opportunities and an Emerging Model for Improvement," Nov. 2, 2006. [Online]. Available: https://www.wilsoncenter.org/sites/default/files/media/documents/publication/Kaseje2.pdf

[9] M. Md Zali, S. Farik Mat Yatin, M. Razilan Abdul Kadir, S. Noraini Mohd Tobi, N. Hanis Kamarudin, and N. Nurul Emyliana Nik Ramlee, "Managing Medical Records in Specialist Medical Centres," *Int. J. Eng. Technol.,* vol. 7, no. 3.7, p. 232, Jul. 2018, doi: 10.14419/ijet.v7i3.7.16358.

[10] N. Kshetri, "Blockchain and Electronic Healthcare Records [Cybertrust]," *Computer*, vol. 51, no. 12, pp. 59–63, Dec. 2018, doi: 10.1109/MC.2018.2880021.

[11] K. Monica, "EHR Design, Interoperability Top List of Physician Pain Points," Sep. 18, 2018. [Online]. Available:https://ehrintelligence.com/news/ehr-design-interoperability-top-list-of-physician-pain-points (accessed May 03, 2023).

[12] M. N. O. Sadiku, K. G. Eze, and S. M. Musa, "Block chain Technology in Healthcare," *Int. J. Adv. Sci. Res. Eng*., vol. 4, no. 5, 2018, doi: 10.31695/IJASRE.2018.32723.

[13] Z. Shae and J. J. P. Tsai, "On the Design of a Blockchain Platform for Clinical Trial and Precision Medicine," in *2017 IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS),* Jun. 2017, pp. 1972–1980. doi: 10.1109/ICDCS.2017.61.

[14] M. Engelhardt, "Hitching Healthcare to the Chain: An Introduction to Blockchain Technology in the Healthcare Sector," *Technol. Innov. Manag. Rev.,* vol. 7, no. 10, pp. 22–34, 2017, doi: 10.22215/timreview/1111.

[15] M. C. Wong, K. C. Yee, and C. Nøhr, "Socio-Technical Considerations for the Use of Blockchain Technology in Healthcare," *Stud. Health Technol. Inform.,* vol. 247, pp. 636–640, Jan. 2018, doi: 10.3233/978-1-61499-852-5-636.

[16] S. M. Hosseini Sarkhosh and P. Akhavan, "Evaluating preparedness in using blockchains for electronic health record systems," *Electron. Libr*., vol. 41, no. 1, pp. 87–110, Jan. 2023, doi: 10.1108/EL-05-2022-0104.

[17] "Global Blockchain in Healthcare Market: Focus on Industry Analysis and Opportunity Matrix - Analysis and Forecast, 2018-2025." 2018. [Online].Available: https://bisresearch.com/industry-report/global-blockchain-in-healthcare-market-2025.html (accessed May 03, 2023).

[18] M. Budman, B. Hurley, A. Khan, and N. Gangopadhyay, "Deloitte's 2019 Global Blockchain Survey," 2019. [Online]. Available: https://www2.deloitte.com/content/dam/insights/us/articles/2019-global-blockchain-survey/DI_2019-global-blockchain-survey.pdf (accessed May 03, 2023).

[19] G. Meyer and F. McCraw,"Healthcare: Blockchain's Curative Potential for Healthcare Efficiency and Quality," Cognizant, 2017> [Online]. Available: https://dokumen.tips/documents/healthcare-blockchainas-curative-potential-for-healthcare-efficiency-2020-04-05.html (accessed May 03, 2023).

[20] Z. Alhadhrami, S. Alghfeli, M. Alghfeli, J. A. Abedlla, and K. Shuaib, "Introducing blockchains for healthcare," in *2017 Int. Conf. Electr. Comput. Technol. Appl.* (ICECTA), Nov. 2017, pp. 1–4. doi: 10.1109/ICECTA.2017.8252043.

[21] P. J. Korsten, "Healthcare rallies for blockchains: Keeping patients at the center," 2017. [Online]. Available: https://www.linkedin.com/pulse/healthcare-rallies-blockchains-keeping-patients-center-korsten/ (accessed May 03, 2023).

[22] S. Khezr, M. Moniruzzaman, A. Yassine, and R. Benlamri, "Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research," *Appl. Sci.,* vol. 9, no. 9, Art. no. 9, Jan. 2019, doi: 10.3390/app9091736.

[23] G. G. Dagher, J. Mohler, M. Milojkovic, and P. B. Marella, "Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology," *Sustain. Cities Soc.,* vol. 39, pp. 283–297, May 2018, doi: 10.1016/j.scs.2018.02.014.

[24] K. Clauson, E. Breeden, C. Davidson, and T. Mackey, "Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare," *Blockchain Healthc. Today,* vol. 1, Mar. 2018, doi: 10.30953/bhty.v1.20.

[25] G. Carter, D. White, A. Nalla, H. Shahriar, and S. Sneha, "Toward Application of Blockchain for Improved Health Records Management and Patient Care," *Blockchain Healthc. Today,* vol. 2, Jun. 2019, doi: 10.30953/bhty.v2.37.

[26] J. Frizzo-Barker, P. A. Chow-White, P. R. Adams, J. Mentanko, D. Ha, and S. Green, "Blockchain as a disruptive technology for business: A systematic review," *Int. J. Inf. Manag.,* vol. 51, p. 102029, Apr. 2020, doi: 10.1016/j.ijinfomgt.2019.10.014.

[27] H. S. A. Fang, T. H. Tan, Y. F. C. Tan, and C. J. M. Tan, "Blockchain Personal Health Records: Systematic Review," *J. Med. Internet Res.*, vol. 23, no. 4, p. e25094, Apr. 2021, doi: 10.2196/25094.

[28] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th Annu. Int. Symp. Pers. Indoor Mob. Radio Commun. (PIMRC),* Oct. 2017, pp. 1–5. doi: 10.1109/PIMRC.2017.8292361.

[29] K. Osei-Tutu, S. Hasavari, and Y.-T. Song, "Blockchain-based Enterprise Architecture for Comprehensive Healthcare Information Exchange (HIE) Data Management," in *2020 Int. Conf. Comput. Sci. Comput. Intell. (CSCI),* Dec. 2020, pp. 767–775. doi: 10.1109/CSCI51800.2020.00145.

[30] N. Nchinda, A. Cameron, K. Retzepi, and A. Lippman, "MedRec: A Network for Personal Information Distribution," in *2019 Int. Conf. Comput. Netw. Commun. (ICNC),* Feb. 2019, pp. 637–641. doi: 10.1109/ICCNC.2019.8685631.

[31] P. Tagde et al., "Blockchain and artificial intelligence technology in e-Health," *Environ. Sci. Pollut.* Res., vol. 28, no. 38, pp. 52810–52831, Oct. 2021, doi: 10.1007/s11356-021-16223-0.

[32] M. Mettler, "Blockchain technology in healthcare: The revolution starts here," in *2016 IEEE 18th Int. Conf. e-Health Netw. Appl. Serv.* (Healthcom), Sep. 2016, pp. 1–3. doi: 10.1109/HealthCom.2016.7749510.

[33] R. Yousuf, Z. Jeelani, D. A. Khan, O. Bhat, and T. A. Teli, "Consensus Algorithms in Blockchain-Based Cryptocurrencies," in *2021 Int. Conf. Adv. Electr. Comput. Commun. Sustain. Technol. (ICAECT)*, Feb. 2021, pp. 1–6. doi: 10.1109/ICAECT49130.2021.9392489.

[34] M. Krichen, M. Lahami, and Q. A. Al–Haija, "Formal Methods for the Verification of Smart Contracts: A Review," in *2022 15th Int. Conf. Secur. Inf. Netw. (SIN),* Nov. 2022, pp. 01–08. doi: 10.1109/SIN56466.2022.9970534.

[35] R. Yousuf, D. A. Khan, and Z. Jeelani, *Security and Privacy Concerns for Blockchain While Handling Healthcare Data,*Florida, USA: CRC Press, 2021.

[36] T. Teli, R. Yousuf, and D. Khan, "Ensuring Secure Data Sharing in IoT Domains Using Blockchain," in *Cyber Security and Digital Forensics,* M. Ghonge, S. Pramanik, R. Mangrulkar. and D-N Le, Eds. MA, USA: Scrivener Publishing LLC, 2022,ch. 9, pp. 205–221.

[37] E. D.-Y. Liao, *Smart Biofeedback: Perspectives and Applications,* London, United Kingdom: Intechopen Limited, 2020.

[38] N. Rifi, E. Rachkidi, N. Agoulmine and N. C. Taher, "Towards using blockchain technology for eHealth data access management," in 2017 Fourth Int. Conf. Adv. Biomed. Eng. (ICABME), Beirut, Lebanon, 2017, pp. 1-4, doi: 10.1109/ICABME.2017.8167555.

[39] M .Smith, R. Saunders, L. Stuckhardt, and M. McGinnis,

Best Care at Lower Cost: The Path to Continuously Learning Health Care in America, D. C., USA: National Academies Press, 2013.

[40] M. Speer, J. M. McCullough, J. E. Fielding, E. Faustino, and S. M. Teutsch, "Excess Medical Care Spending: The Categories, Magnitude, and Opportunity Costs of Wasteful Spending in the United States," *Am. J. Public Health*, vol. 110, no. 12, pp. 1743–1748, Dec. 2020, doi: 10.2105/AJPH.2020.305865.

[41] J. J. Doyle, J. A. Graves, and J. Gruber, "Uncovering waste in US healthcare: Evidence from ambulance referral patterns," *J. Health Econ.,* vol. 54, pp. 25–39, Jul. 2017, doi: 10.1016/j.jhealeco.2017.03.005.

[42] D. M. Berwick and A. D. Hackbarth, "Eliminating waste in US health care," *JAMA,* vol. 307, no. 14, pp. 1513–1516, Apr. 2012, doi: 10.1001/jama.2012.362.

[43] T. G. K. Bentley, R. M. Effros, K. Palar, and E. B. Keeler, "Waste in the U.S. Health care system: a conceptual framework," *Milbank Q.,* vol. 86, no. 4, pp. 629–659, Dec. 2008, doi: 10.1111/j.1468-0009.2008.00537.x.

[44] H. Lyu, et al. "Overtreatment in the United States," *PLOS ONE,* vol. 19, no. 9, e0181970, 2017, doi: 10.1371/journal.pone.0181970.

[45] H. Treiblmaier and T. Clohessy, *Blockchain and Distributed Ledger Technology Use Cases,* Switzerland: Springer Cham, 2020.

[46] M. Orcutt, "Who will build the health-care blockchain?," Sept. 2017. {online].Available: https://www.technologyreview.com/2017/09/15/149153/who-will-build-the-health-care-blockchain/ (accessed May 03, 2023).

[47] T. K. Gandhi, D. F. Sittig, M. Franklin, A. J. Sussman, D. G. Fairchild, and D. W. Bates, "Communication breakdown in the outpatient referral process," *J. Gen. Intern. Med.,* vol. 15, no. 9, pp. 626–631, Sep. 2000, doi: 10.1046/j.1525-1497.2000.91119.x.

[48] S. Tarkan, C. Plaisant, B. Shneiderman, and A. Z. Hettinger, "Reducing missed laboratory results: defining temporal responsibility, generating user interfaces for test process tracking, and retrospective analyses to identify problems," *AMIA Annu. Symp. Proc. AMIA Symp.,* vol. 2011, pp. 1382–1391, 2011.

[49] M. Weiner et al., "A web-based generalist-specialist system to improve scheduling of outpatient specialty consultations in an academic center," *J. Gen. Intern. Med.,* vol. 24, no. 6, pp. 710–715, Jun. 2009, doi: 10.1007/s11606-009-0971-3.

[50] G. J. Katuwal, S. Pandey, M. Hennessey, and B. Lamichhane, "Applications of Blockchain in Healthcare: Current Landscape & Challenges." arXiv:1812.02776, 2018. [Online]. Available: https://arxiv.org/abs/1812.02776.

[51] T. Clohessy, H. Treiblmaier, T. Acton, and N. Rogers, "Antecedents of blockchain adoption: An integrative framework," *Strateg. Change*, vol. 29, no. 5, pp. 501–515, 2020, doi: 10.1002/jsc.2360.

[52] K. Cromanet al., "On Scaling Decentralized Blockchains," in *Int. Conf. Financ. Cryptography Data Secur.*, in Financial Cryptography and Data Security, J. Clark et al., Eds, in Lecture Notes in Computer Scienc, vol. 9604, 2016, doi: 10.1007/978-3-662-53357-4_8.

[53] A. Pedersen, M. Risius, and R. Beck, "A Ten-Step Decision Path to Determine When to Use Blockchain Technologies," MIS Q. Exec., vol. 18, pp. 99–115, Jun. 2019, doi: 10.17705/2msqe.00010.

[54] W. J. Gordon and C. Catalini, "Blockchain Technology for Healthcare: Facilitating the Transition to Patient-Driven Interoperability," *Comput. Struct. Biotechnol. J.,* vol. 16, pp. 224–230, 2018, doi: 10.1016/j.csbj.2018.06.003.

[55] P. B. Nichol, "IBM blockchain in healthcare rallies for patients," Dec. 2016. {online]. Available:https://www.cio.com/article/236871/ibm-blockchain-in-healthcare-rallies-for-patients.html (accessed May 04, 2023).