International Journal of Safety and Security Engineering
Vol. 14, No. 1, February, 2024, pp. 267-287
Journal homepage: http://iieta.org/journals/ijsse

A Review of Blockchain Applications and Healthcare Informatics

Shruthi Kumarswamy*, Poornima Athikatte Sampigerayappa

Department of Computer Science and Engineering, Siddaganga Institute of Technology, Tumkur, Visvesvaraya Technological University, Karnataka 590018, India

Corresponding Author Email: shruthik@sit.ac.in

https://doi.org/10.18280/ijsse.140127

Received: 13 July 2023
Revised: 23 January 2024
Accepted: 31 January 2024
Available online: 29 February 2024

Keywords:
blockchain, data security, health record, healthcare, MedRec

ABSTRACT

Blockchain technology is being used in the healthcare industry to create fair agreements. In the medical industry, a blockchain network is utilized to protect patient data that is acquired from pharmacies, doctors' offices, hospitals, and diagnostic facilities. Blockchain-based applications have the capability to detect and alert users to absurd or potentially dangerous mistakes in the medical domain. Blockchain technology can solve several issues with data management, interoperability, security, and transparency, which could result in major advancements in the healthcare sector. Blockchain technology could improve healthcare systems' efficiency, security, and transparency to overcome issues with conventional health data management systems. This could ultimately result in better patient outcomes. It's crucial to remember that interoperability, privacy, and regulatory concerns must all be carefully considered before implementing blockchain in the healthcare industry. To curb drug fraud and provide patients greater control over their information, the authors of this paper examine current trends and highlight the potential benefits of blockchain technology in the healthcare sector.

1. INTRODUCTION

Health IT, encompassing electronic health records (EHRs), telemedicine, data analytics, and artificial intelligence, has the potential to reshape healthcare in India. The convergence of technology and healthcare delivery is bridging gaps, improving access, enhancing quality, and increasing efficiency. Understanding the current state of Health IT and anticipating future trends is crucial to harnessing its full potential.

1.1 Present status of healthcare data management

1.1.1 Adoption of electronic health records (EHRs)

EHRs have witnessed significant adoption in India's healthcare ecosystem. These digital records are replacing paper-based systems, offering several advantages, current EHR issues are shown in Figure 1.

- Efficient Data Management.
- Improved Care Coordination.

1.1.2 Electronic health records

Patient files are stored in electronic health records, or EHRs. These were paper files in the past. To streamline patient documentation, the Affordable Care Act (ACA) of 2010 mandated that providers transition to electronic health record (EHR) systems. All clinical, health, and demographic data are included in EHRs.

1.1.3 Electronic medical records

Like EHRs are electronic medical records (EMRs). All the patient's medical history isn't always included in the electronic medical records (EMRs) that hospitals often employ. Doctors and nurses have access to a patient's electronic medical record (EMR) upon admission, which contains information about the patient's condition, treatment, and medical history.

1.1.4 Administrative and demographic data

Billing, insurance, reimbursement, scheduling, and payment details are examples of administrative data. Given that it contains private information like credit cards and Social Security numbers, this data needs to be very secure.
Their EHR system offers.

- Centralized Data Storage.
- Data Integration.
- Interoperability.

Health Information Exchanges (HIEs) are instrumental in enabling the secure exchange of patient data among healthcare providers. The interoperability enhances care continuity and reduces medical errors.

1.2 Blockchain for health records security

Blockchain technology holds immense promise for enhancing security, privacy of health records:

- **Data Security:** Patient records deployed on blockchain are immutable, safeguarded against unauthorized tampering. This ensures the integrity and authenticity of health data.
- **Consent Management:** Blockchain's smart contracts enable exact control over who can view and alter

health information. Patients can grant permission securely, ensuring privacy while allowing healthcare providers access when necessary.

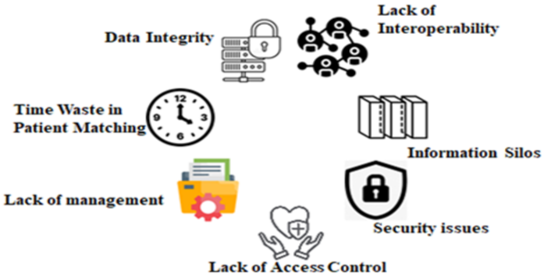

Figure 1. Current EHR issues

1.3 Future trend - blockchain-based health records

In the coming years, we anticipate the broader adoption of blockchain for health records in India. Patients are provided with:

- Complete control over the sharing and access of their data, allaying worries about data breaches.
- Enhanced data security, instilling trust in healthcare systems.
- Improved interoperability between healthcare providers, promoting seamless care coordination.

Blockchain is an advanced, open, decentralized ledger that syncs data across many computer platforms and prevents any record from being altered in the past without impacting subsequent blocks. A long chain is formed through blockchain demonstration and association with the prior block. Blockchain is ultimately the call of the archive. A fair establishment of obligation is provided by Blockchain because every exchange is registered and publicly verified. Nobody can alter any of the insights included in the Blockchain once they have been recorded. It demonstrates that the records are authentic and undamaged. In Blockchain, data is maintained on networks rather than a simple data file, enhancing security and demonstrating its propensity to be compromised. Blockchain enables advertisers to keep track of the products they have utilized [1, 2].

Distributed ledger technology, or blockchain, offers insights and never removes or changes them without unanimous agreement. A cryptographic hash that links each information block with newly added insights block information determines the price of a Blockchain hash. Measurements are not managed individually thanks to the distributed Blockchain record structure, which makes it accountable and accessible to all organized customers. The patient will follow the acquisition of their records by monitoring health data on a blockchain [3, 4].

We use wearable technology and the Internet of Things (IoT) to use real-time Blockchain for healthcare to preserve and update vital patient data, such as blood pressure and sugar levels. It is beneficial for doctors to identify patients who are very susceptible to risks and to suggest and notify their families and employers in the event of an emergency. Blockchain's decentralized architecture makes it difficult to exploit and prevents any one copy of the data from being compromised [5, 6]. The research queries addressed in this article are as follows:

RQ1: To see the blockchain generation and its full healthcare ambitions.

RQ2: Learning about the ways in which blockchain technology can enhance the global healthcare system.

RQ3: To educate oneself on the implementation of blockchain technology's unified work-flow process in the provision of healthcare facilities.

Blockchain is no longer dependent on any one source for information acquisition. Rather, Blockchain is replicated and propagated by a computer network. A new block is reflected in the blockchain on every internet-connected computer. The fundamental operational processes of Blockchain generation are depicted in Figure 2.

A Blockchain device operates at the very top of the internet, on a P2P network of computers where everyone uses the same protocol and has the same copy of the transaction ledger. This enables machine consensus to support P2P fee transactions without the need for an intermediary. Blockchain technology comes in many varieties, including public, private, hybrid, and consortium. Every Blockchain community has unique benefits and drawbacks that affect its key uses.

- The first generation of Blockchain is public Blockchain, and it was here that the idea for Bitcoin and other cryptocurrencies emerged, helping to advance distributed ledger technology (DLT). It eliminates the negative effects of centralization, like lack of security and transparency. DLT disseminates facts around a P2P network as opposed to preserving them in one location. It requires a few different techniques for fact authentication because of how decentralized it is.
- A private blockchain is a blockchain network that operates in a restricted setting, is closed, or managed by a single organization. It is noticeably smaller, but it performs similarly to a public blockchain community in terms of P2P networking and decentralization. In a non-public Blockchain, the network's creator is already familiar with the participants. On the public web, one cannot broaden a permission-based response, and users maintain complete anonymity.
- On occasion, companies seeking the best of both worlds will use hybrid blockchains, which blend elements of public and private blockchains. Businesses may build a public, permissionless system in addition to a private, permission-based one, allowing them to manage exactly what information is made public and who can access it on the Blockchain.

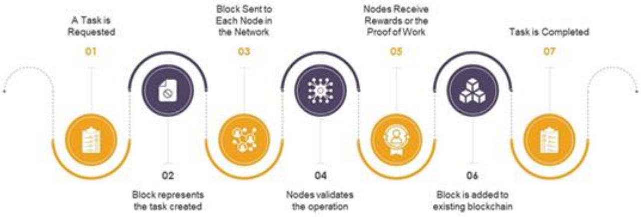
A Task is Requested
01
Block Sent to Each Node in the Network
03
Nodes Receive Rewards or the Proof of Work
05
Task is Completed
07
02
Block represents the task created
04
Nodes validates the operation
06
Block is added to existing blockchain

Figure 2. The procedures involved in using blockchain technology

2. BLOCKCHAIN AND HEALTHCARE SYSTEMS

As the technology that made Bitcoin possible, blockchain was first primarily used in the financial sector. However, efforts have been made to adapt the technology for a variety of industries, including healthcare, insurance, manufacturing, pharmacy, e-balloting, power, and many more applications implementable features of blockchain technology in healthcare is shown in Figure 3 [7].

The healthcare sector is a unique assignment since it has a complicated process, multiple powerful stakeholders, and a desire to disrupt using cutting-edge solutions. Blockchain technology offers potential uses for managing public health, remote monitoring, electronic health records (EHR), clinical data control, information security, and medication research, among other healthcare-related issues. Surprisingly, blockchain can alleviate worries about data ownership and share by letting patients personalize their data and choose with whom their miles are shared [8]. In Figure 4, Gaynor et al. [9] present a few possibilities offered by blockchain for replacing healthcare statistics, showing how these solutions might enable the healthcare sector to improve data exchange across all enterprise techniques, such as change, storage, and record monitoring. Blockchain offers exceptional opportunities to leverage the power of other emerging technologies and has the potential to address significant healthcare challenges. Despite interoperability challenges, such as the lack of an existing fashion for creating blockchain-based healthcare software, allowing blockchain to resolve many complex issues that the fitness care industry faces today shall allow a transformation with the assistance of researchers and practitioners from different fields towards improving and innovative ways of viewing the fitness care business [10].

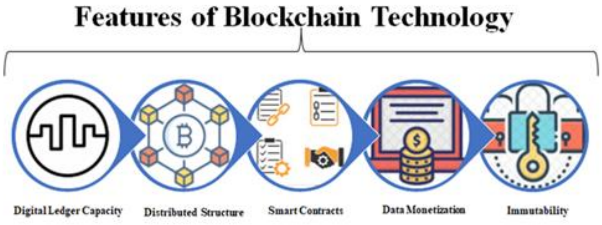

Figure 3. Implementable features of blockchain technology in healthcare

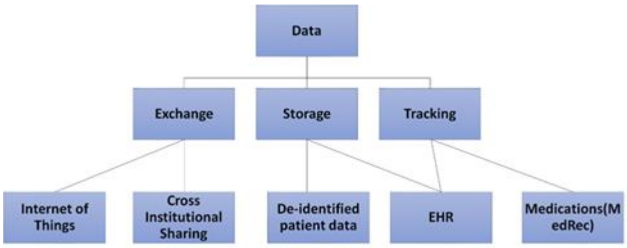

Figure 4. Data (electronic health record) exchange tree

2.1 The definition of health data management

The management of patient data collection, storage, and analysis is known as health data management, clinical data management, or health information management. This data consists of administrative (billing, scheduling, insurance, Medicare coding), medical history, treatments (family history, doctor visits), and demographic data (name, age, address, gender) healthcare data from variety of sources is shown in Table 1.

A single patient is estimated to produce more than 80 gigabytes of data annually. The Health Insurance Portability and Accountability Act (HIPAA) safeguards this data, which needs to be secured to preserve patient privacy. This is one more duty that health data managers have.

Table 1. Healthcare data from variety of sources

Sl.No.	Variety of Source	Meaning
1	Electronic Health Records	Electronic health records (EHRs) hold patient files. EHRs include all health, clinical, and demographic information.
2	Electronic Medical Records	Electronic medical records (EMRs) are similar to EHRs. EMRs don't always include the patient's entire medical history.
3	Public Health Data	The healthcare industry is gathering population data, which includes the overall health of a region.
4	Imaging Data	Imaging data includes results of X-rays, MRIs, mammograms, and other scans. Mammograms have mostly gone to digital imaging capture.
5	Administrative and Demographic Data	Administrative data includes billing, insurance, reimbursement scheduling, and payment information.
6	Wearables	Wearable electronics devices that can collect information and user activity are a new source of health data.

2.2 Limitations / Blockchain's shortcomings in the context of healthcare

2.2.1 Scalability

Scaling problems may arise in blockchain networks, particularly public ones, when the volume of transactions and participants rises. Costs may go up and transaction processing times may get longer as a result.

2.2.2 Integration with existing systems

Integrating blockchain with existing healthcare systems, such as Electronic Health Records (EHRs), can be complex and may require significant changes to current infrastructure. Legacy systems may not easily adapt to blockchain technology.

2.2.3 Regulatory uncertainty

The healthcare industry is highly regulated, and the legal and regulatory framework around the use of blockchain in healthcare is still evolving. Uncertainty about compliance with existing regulations poses a challenge to widespread adoption.

2.2.4 Data privacy concerns

Blockchain offers an unchangeable and safe record, but data privacy is one of its problems. Storing sensitive health data on a public blockchain might raise concerns about exposing patient information, even if it is encrypted.

2.4.5 Energy consumption

Some blockchain networks, particularly proof-of-work-based ones like Bitcoin, are criticized for their high energy consumption. This is an environmental concern and may not align with sustainability goals in healthcare.

2.2.6 Lack of standardization

The lack of standardized protocols and frameworks for implementing blockchain in healthcare can hinder interoperability. Different blockchain platforms may have varying features and capabilities.

2.2.7 Smart contract risks

While smart contracts automate and enforce predefined rules, they are not immune to vulnerabilities. Bugs or security flaws in smart contracts could lead to unexpected behaviors, impacting the security and reliability of the system.

2.2.8 User education and adoption

Users, including healthcare providers and patients, may not be familiar with blockchain technology. Education and training are essential for successful adoption, and resistance to change could slow down the transition.

2.2.9 Irreversibility of transactions

Once data is added to the blockchain, it is generally irreversible. This immutability, while a strength in terms of security, can become a limitation if there are errors or if data needs to be modified for legitimate reasons.

2.2.10 Costs and resource intensiveness

Implementing and maintaining a blockchain network can be resource-intensive and costly. This includes expenses related to infrastructure, development, and ongoing maintenance.

2.2.11 Identity management

While blockchain provides a level of anonymity, managing identities securely and ensuring that patients have control over who accesses their data can be challenging. Striking a balance between privacy and identity verification is crucial.

2.2.12 Long confirmation times

In some blockchain networks, especially those using proof-of-work consensus mechanisms, confirmation times for transactions can be relatively long. This delay may not be suitable for certain real-time healthcare applications. Limitations / Challenges of Blockchain Technology is shown in Figure 5.

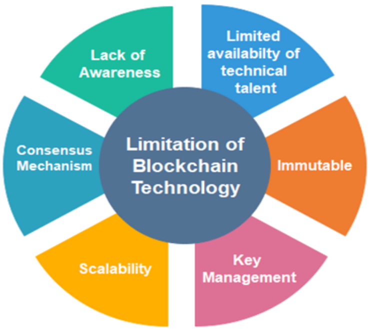
Lack of Awareness
Limited availabilty of technical talent
Consensus Mechanism
Limitation of Blockchain Technology
Immutable
Scalability
Key Management

Figure 5. Limitations / challenges of blockchain technology

3. A SURVEY ON BLOCKCHAIN FOR HEALTHCARE INFORMATICS

Numerous investigations were carried out to enhance the quality of healthcare by utilizing blockchain technology [11]. The healthcare sector is expanding both horizontally and vertically. The vertical direction of healthcare is expanding more quickly, bringing new drugs, vaccines, and medical equipment to the market and the capacities of blockchain technology for the healthcare domain is shown in Figure 6.

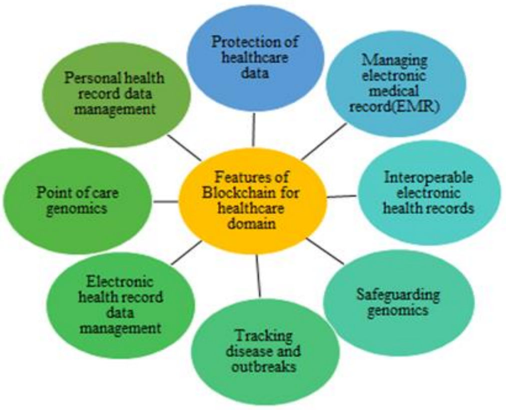
Protection of healthcare data
Personal health record data management
Managing electronic medical record(EMR)
Point of care genomics
Features of Blockchain for healthcare domain
Interoperable electronic health records
Electronic health record data management
Safeguarding genomics
Tracking disease and outbreaks

Figure 6. Capacities of blockchain technology for the healthcare domain

But because most hospitals have been recording and sharing patient electronic health records (EHRs) using outdated technology for the past 20 years, the horizontal direction is only slowly expanding.

Blockchain adoption as a new horizontal breakthrough has the potential to completely transform the healthcare sector. This is because blockchain technology offers answers for a number of challenges related to data management for electronic health records (EHRs) in the healthcare sector, including scalability concerns [12], data blocking across healthcare organizations, and EHR manipulation.

3.1 Applications

1. **MedRec** is a decentralized document control device to deal with EMRs, developed with the use of blockchain era designed [13]. The gadget advanced the use of Solidity and Ethereum (Geth), but it was no longer developed on the Ethereum community instead, it constructed a small-scale private blockchain with comprehensive, one-of-a-kind APIs [14]. MedRec permits patients get the right of entry to their clinical statistics across vendors and remedy website.
2. **Carechain**, lead by IT pioneers Johan Sellstrom and Stefan Farestam, Carechain is a Swedish business that just unveiled a blockchain-based personal healthcare information management system. The system concentrates on the protocol stage and creates a new infrastructure that is manageable by anybody but does not belong to anyone. The Carechain utilized the Ethereum method to build a national blockchain for fitness data that gives users ownership and control over their medical records. The device will place the character in the center and assign the character a regular virtual identification that is owned and controlled by the character. The system must ensure that facts are included with integrity, and an integrated policy must ensure traceability [15].
3. **Dovetail** Utilizing the Hyperledger material approach, Dovetail is a blockchain-based digital

consent application that facilitates the sharing of patient data to enhance healthcare systems, products, and services. The gadget offers an audited ledger of scientific facts interactions to confirm identify, record consent, and generate tamper-proof audit records of each records exchange. Additionally, it capitalizes on the advantageous features of distributed ledger manufacturing [16].

4. **MedHypChain** is a patient-focused, interoperable hyper-ledger-based medical healthcare and information exchange device that protects patient privacy. Every transaction is protected by an identification-based broadcast organization encryption method [17]. The device enables the secure deployment of patient-targeted interoperability (PCI) information sharing between the patient and medical server, as well as interoperability and malicious user tracing. There are several ways that blockchain technology can improve healthcare around the world. The Blockchain has a wide range of applications and features in the healthcare sector. By managing the drug delivery chain, supporting the secure transfer of patient clinical data, and facilitating the safe switch of patient medical data, ledger technology enables medical researchers to decipher genetic codes. Figure 6 illustrates the types of capabilities and essential Blockchain concept enablers in numerous healthcare and related sectors. Healthcare information security, extensive genome control, digital record management, clinical data, interoperability, digitalized tracking, problem emergence, and other technically complex and mind-boggling operations are some of the methods used to advance and implement the Blockchain era. The primary drivers behind the adoption of blockchain technology are its fully digitalized components and applications in healthcare-related products [18, 19]. With the help of Blockchain, the entire prescription process from manufacture to pharmacy shelves becomes transparent. Blockchain and IoT can be used to track speed, goods paths, and congestion.

The overall vision of Blockchain to revolutionize the healthcare market in the coming years can be to address problems impacting the current structure. It enables doctors, patients, and chemists to easily gain access to all the information available at any given time. Blockchain technology is being investigated, tested, and discovered by medical companies inside the clinical space for health information day and night. By decentralizing patient fitness records data, improving payment alternatives, and following prescription medications, it has established itself as an indispensable tool in the healthcare industry. In addition, advanced technology includes artificial intelligence and technologies that learn. Blockchain is a rather important component of the market. The way that blockchain is changing the healthcare sector has some real applications. To streamline the clinical delivery chain, the program is built using Blockchain monitoring technology [20-22].

The potential of blockchain allows for the creation of a complex data storage system that maintains a person's whole medical history, including diagnoses, examination results, previous regimens, and even measures from intelligent sensors. A doctor can quickly acquire all the data required to provide precise diagnoses and recommendations for the application of this method. Because every statistic is recorded in a single Blockchain device, it is protected from loss and change. It might use Blockchain to avoid a company's internal networks. Rescue assaults and other issues, including laptop corruption or hardware failure, could be eliminated if a healthcare organization successfully deploys a Blockchain community [23, 24].

3.2 Decentralized and secure affected person statistics control

Transferring paper medical records between several hospitals utilizing patients themselves is inconvenient and ineffective. A key strategy to raise the caliber of healthcare professionals and lower clinical costs is the sharing of medical data.

Although modern EHR systems offer numerous benefits, there are still many limits in place in healthcare data systems, which prevent comfortable and scalable data sharing among various organizations and, as a result, restrict the advancement of scientific research and decision-making. As mentioned previously, there are risks associated with a centralized device's information leaking attack. However, patients are unable to retain ownership of their personal information that they could share with a partner. It might lead to the unauthorized usage of confidential information by inquiring organizations. Furthermore, separate competing groups that lack relationships are less likely to share information, which could impede the growth of information sharing.

In this situation, it is essential to ensure protection and privacy protection and return to properly handling information returned to users to promote information exchange. When records are contained in a single organization, it is much easier to solve security and privacy concerns; but, when comfortable health information interchange occurs across different domain names, it will be more challenging. In the meanwhile, it also wants to continue to think about how to promote effective teamwork in the healthcare sector.

As one of the common strategies, a comfortable access control system demands only authorized entities to have access to sharing information. This approach consists of gaining universal access to the policy as well as the ability to manage a list (ACL) relevant to the data owner. ACL is a list of users with the appropriate permissions (examine, write, and update) to access specific statistics. Giving authenticated users permission to access the protected sources under established access rules is known as authorization. The authorization procedure is always carried out after the authentication system.

Combining blockchain technology with gaining access to control mechanisms to build an honest machine is promising. Customers can casually handle their data and keep shared information private. According to this new paradigm, patients can predefine the operations (read, write, update, delete), access permissions (authorize, refuse, revoke), and time to share their data using smart contracts on the blockchain without losing the ability to control it. Once all the prerequisites are satisfied, smart contracts can be created on the blockchain and can also offer an audit mechanism for each request entered the ledger. Smart contracts are being used in several current studies and programs to facilitate the sharing of healthcare data. Table 2 represents the main contributions and gaps identified in decentralized and secure patient data management.

Figure 7 shows how the database's patient records are organized, with access control rules contained in the block and medical metadata in the smart agreement, Figure 8 shows the combination of access control mechanism by smart contract.

The machine-getting-to-know technique can effectively provide innovative products and encourage the optimization of healthcare systems. How to store, distribute, and educate sensitive material securely is a major difficulty for practical systems using machine learning. To improve the security and privacy of datasets, system learning, and blockchain integration are becoming increasingly popular.

Table 2. Main contributions and gaps identified in decentralized and secure patient data management

Ref.	Main Contributions	Gaps Identified
[13]	MedRec: A cutting-edge, blockchain-based decentralised record management solution for electronic medical records (EMRs). Patients benefit from the system's simple access to their medical records across providers and treatment locations as well as its comprehensive, unchangeable log. MedRec handles data exchange, accountability, secrecy, and authentication—all important factors to take into account when working with sensitive data—by utilising special blockchain features. A modular design facilitates interoperability and makes the system convenient and flexible by integrating with providers' current local data storage solutions.	Provide the framework as a starting point for additional development.
[25]	Owing to blockchain's growing popularity, numerous blockchain applications, including electronic health record (EHR) systems, have been suggested for the healthcare industry. As a result, they conducted a thorough literature analysis of blockchain techniques intended for EHR systems in this work, concentrating solely on the privacy and security issues. Before delving into how blockchain is used in EHR systems, they provide essential background information on both systems as part of the review. They also noted a number of chances and obstacles for further investigation.	will help the ageing population by providing more understanding into the design and application of next-generation EHR systems.
[26]	The goal of the study is to develop a diagrammatic conceptual model of a medical app that uses blockchain technology to handle patient and physician databases during surgery. The model is constructed on the shortcomings of earlier models, which mostly used blockchain technology in the banking and financial industry. This study will continue to offer a simulation space conceptual models in current studies, with a focus on the development of mission space conceptual models, particularly considering the rarity of models utilising blockchain in the healthcare industry. Following the development of this model, a smartphone app that accepts Bitcoin payments might be developed to enable doctors handle every patient directly and efficiently while also assisting patients in making an informed decision about preparation, procedure, or cost, procedure or preparation of pre and post- surgery.	-
[27]	They suggest a brand-new architecture for exchanging electronic health records (EHRs) that integrates IPFS and blockchain on a mobile cloud platform. They create a reliable access control system with smart contracts to enable safe exchange of electronic health records between various patients and healthcare professionals. They demonstrate a working prototype that uses the Ethereum blockchain in a mobile app that uses Amazon cloud computing to share actual data. Based on empirical findings, the concept offers a workable way to provide secure data transfers on mobile clouds while protecting private health information from security risks.	Compared to traditional schemes, this framework only permits medical users to share medical data across mobile cloud environments in a dependable and efficient manner.
[28]	One important source of health care intelligence is healthcare data. One crucial step in improving the intelligence of the healthcare system and the calibre of healthcare services is the sharing of healthcare data. To allow patients to easily and securely own, control, and share their own data without violating privacy, we proposed an app called Healthcare Data Gateway (HGD) architecture based on blockchain. This offers a new potential way to improve the intelligence of healthcare systems while maintaining patient data privacy.	-
[29]	BPDS, or blockchain-based privacy-preserving data sharing, is used for EMRs. The original EMRs are safely kept in the cloud with BPDS, and the indexes are reserved in a consortium blockchain that is impenetrable to tampering. By doing this, there is a far lower chance that medical data would escape, and the blockchain's indexes guarantee that EMRs cannot be changed at will. Using blockchain smart contracts, secure data sharing can be carried out automatically based on patients' pre-defined access permissions.	The original EMRs are encrypted by the patient and are now stored in the cloud via an extensible approach. Instead of using homomorphic encryption, distributed storage and CP-ABE-based access control schemes are employed.
[30]	A summary of the usage of EMRs in mental health and medical settings, with an emphasis on an implementation experience in an integrated health care context. Psychologists can assist in the creation and implementation of electronic medical records (EMRs) in mental health settings. The presentation highlights the potential for an EMR to improve the efficacy of mental health treatment in the communication, coordination, and delivery of mental health care.	A greater interest in and involvement from psychologists regarding how they may play a significant role in carefully implementing these tools as electronic medical records (EMRs) become a more standard component of mental health care. It is not limited to mental health services.

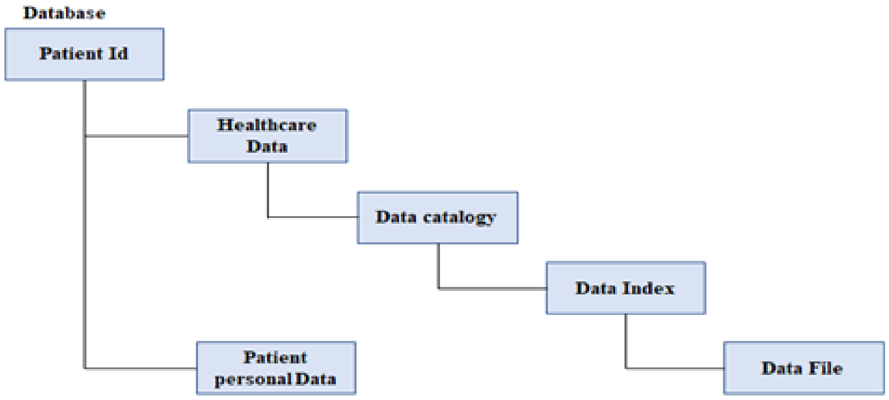

Figure 7. Patient database

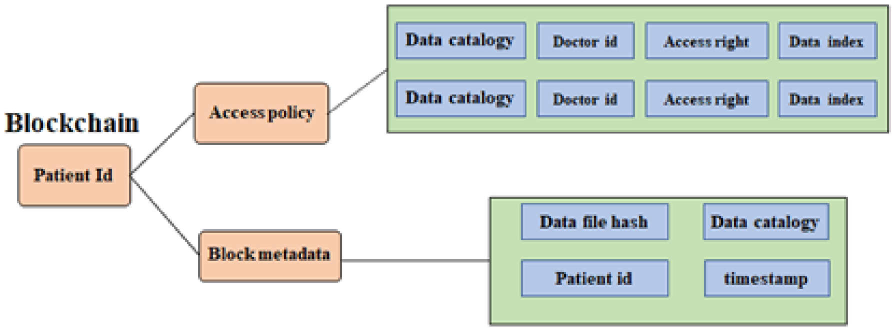

Figure 8. Integration of smart contracts with access control mechanisms

Federated mastery is an effective system learning technique that is accomplished among numerous computing nodes under the condition that sensitive data is kept secure and private during information exchange. Sharing encrypted datasets enables collaboration between various clinical settings to develop high-accuracy prediction algorithms. To ensure accountability and reliable collaboration, blockchain as a regulator can record associated training transactions in an unaltered and transparent manner. In this case, medical companies and researchers might be more eager to share encrypted datasets to advance the creation of medical treatments and public health.

Blockchain ensures the security of data entry by acting as the solid foundation for device-mastering algorithms. The key problem identified by and the sharing of enormous datasets using specialized software and domain names. To execute system learning on encrypted data, homomorphic encryption is a topic of ongoing research Gentry. However, in practice, homomorphic encryption has a high computational expense. In the future, sensitive data might be encrypted without affecting the system's search for intelligent options. Additionally, artificial intelligence can be used to create smart contacts automatically, enhancing flexible and comfortable operations. Additionally, blockchain could be used to improve the security of network slice sellers and the 5G community control layer.

3.3 Prescription and billing

Healthcare organizations can more effectively influence patients' data, such as their prescription history, thanks to virtual healthcare architecture. Through computational and multiplatform virtual tools, using technology to transmit patient information allows for more effective communication between healthcare experts and businesses (during times of social distance). When compared to paper-based prescriptions, the use of virtual prescriptions enables effective communication while minimizing discrepancies, providing the patient with higher-quality first-class medical care [31]. To govern scientific statistics, however, most methods use centralized digital systems. The single point of failure problem that plagues centralized architectures makes it possible for healthcare providers to alter or abuse patient records. As a result, think about how records are accessible to healthcare organizations and how this is dependent on a single important server, as shown in Figure 9.

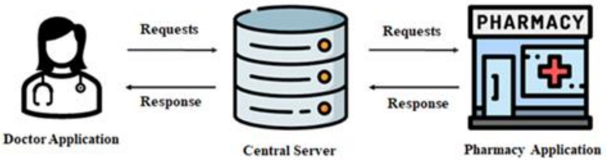

Figure 9. Electronic prescribing using a centralized architecture

On the other hand, decentralized blockchain technology guarantees the accuracy of statistics. The layout enables the blockchain to run independently of a central authority or middleman, and statistics are added to the chain by network node consensus, a decentralised architecture-based concept for electronic prescription is shown in Figure 10.

With the help of clever contracts, which are executable programs saved and operated on the blockchain, tasks like validating transactions may be automated without the need for 1/3-celebration interaction [32]. Ethereum is one of the most well-known decentralized application enhancement frameworks that make use of smart contracts. However, it makes use of the proof of work (Pow) consensus process, which has a high operational cost and requires the mining node to solve a cryptographic assignment [33, 34]. As these systems achieve consensus without mining, Sensible Byzantine Fault Tolerance 1 (PBFT) platforms, such as Tendermint and Istanbul Byzantine Fault Tolerance 2 (IBFT2), offer an alternative to PoW blockchains high processing costs. The consensus is broken down into stages, and the participants known as validators take part by presenting and validating blocks.

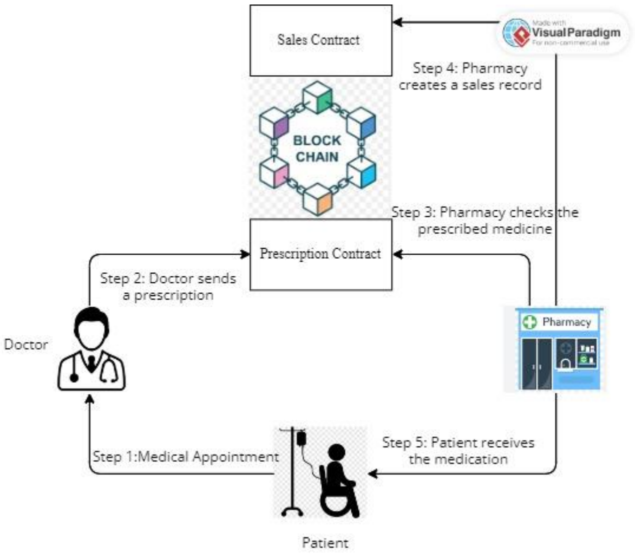
Sales Contract
Step 4: Pharmacy creates a sales record
BLOCK CHAIN
Step 3: Pharmacy checks the prescribed medicine
Prescription Contract
Step 2: Doctor sends a prescription
Doctor
Pharmacy
Step 5: Patient receives the medication
Step 1:Medical Appointment
Patient

Figure 10. A decentralised architecture-based concept for electronic prescription

Blockchain technology satisfies most of these requirements for combating fraud and prescription forgery under its inherent properties and decentralized architecture. In this way, it stops the patient from experiencing fitness issues because of prescription abuse. It offers the advantages listed below to e-prescription applications:

- Has no centralized authority and operates decentralized (no single point of failure).
- Maintains patient data on backup storage.
- Prevents the alteration of information for personal gain.
- Selling medications only with valid prescriptions.
- Effective and transparent communication between stakeholders.
- Decrease in medication errors and consistency.

As a result, developing a decentralized and fault-tolerant prescription model is highly feasible. A distributed consensus among the users of the network is used to add recent medical information or to complete the sale of medication. As a result, stakeholder dialogue will be more comfortable than with centralized systems and written prescriptions. An example of scientific truths. We investigate the use of blockchain technology and smart contracts to enable the selling of drug treatments best with valid data that is, data that was developed and signed by a doctor while also ensuring the availability, integrity, and transparency of the data. Table 3 shows the significant contributions of several writers in a decentralized architecture electronic prescription approach.

- Growing fake virtual prescriptions (without the digital signature of the doctor).
- Tampering with scientific documents, such as digital prescriptions. By doing so, it prevents the misuse of prescription pharmaceuticals and their side effects, such as overdosing [35].

Table 3. Significant contributions of several writers in a decentralized architecture electronic prescription approach

Ref.	Main Contributions
[31]	Compared the e-prescription systems that were chosen. The security and privacy procedures as well as the architecture of the systems serve as the foundation for the comparison process. Additionally, we assessed the systems' potential to advance towards utilizing cutting-edge technology like blockchain and artificial intelligence. The results of this study may help create a global e-Prescription system that patients can use when visiting countries other than their own.
[32]	This study described the use of blockchain technology and smart contracts in the healthcare industry, with an emphasis on the advancement of EHR access control.
[33]	One of the fundamental technologies of blockchain is the consensus algorithm, which is the subject of this study. In this study, we present a process model for unified consensus algorithms that works well for blockchains based on directed acyclic graphs (DAGs) as well as chains. Next, we examine several popular Blockchain consensus algorithms and categorize them based on how they were designed for the various stages of the process model.
[34]	The purpose of this study is to compare the effectiveness of PoW, PoS, and mixed consensus procedures in terms of dependability, fairness, and energy usage. Using NetLogo, an agent-based model of a typical block-chain system outfitted with several consensus techniques is constructed. This model replicates and assesses the various consensus methods in use within the blockchain.
[35]	This article gives a general overview of the subject and focuses on a variety of medications, including over-the-counter medications like loperamide, dextromethorphan, benzydamine, promethazine, chlorphenamine, diphenhydramine, and hyoscine butylbromide and prescription medications like quetiapine, gabapentinoids, Z-drugs, bupropion, and venlafaxine, which have been identified as being misused and diverted or have already been documented in the literature and on websites maintained by drug users that document new trends and experiments in drug abuse.

3.4 Healthcare interoperability and scientific statistics systems

- **Healthcare information and Interoperability:** Interoperability within the Blockchain community improves data exchange between players in this industry because every piece of information within the Blockchain adheres to a specific standard, making information exchange more effective. Information security in the healthcare industry Blockchain community skills like hashing and information immutability make data healthcare more comfortable.
- **Lower cost of healthcare statistics management:** Because the records are kept in several locations and databases, the value of data management in traditional healthcare information systems is far higher than storing that information smoothly in a Blockchain network.
- **Global sharing of healthcare records:** A patient may receive treatment in one nation before traveling

to another to continue receiving it. If standard hospital treatment procedures are used in this situation, transferring patient records among many special nations may not even be conceivable. Affected people's records may be easily shared internationally using a Blockchain network.

- **Enhancing the audit of healthcare facts through the usage of Blockchain:** The use of records audits in healthcare guarantees that organizations and stakeholders in this sector properly adhere to all laws and standards. The audit of healthcare data is improved since the Blockchain contains verifiable information and non-manipulative facts.

Interoperability, in a nutshell, is the main ability of specialized record-keeping systems to communicate, exchange, and use statistics in the healthcare environment. Following international standards, EHR systems can achieve interoperability and direct information sharing across a few healthcare carriers and institutions.

3.5 Pharmaceutical product authenticity and legitimacy

With the advent of device mastery and AI, providing opportunities to access information via smartphones, chemists might have clear and secure access to lab information for patients using a blockchain framework. This might facilitate better communication between chemists and prescribers in terms of maximizing pharmaceutical therapy. Pharmacists could play a stronger role in following patients to improve drug adherence and fitness outcomes if they have access to test findings and EHR.

We can go over the operation of a blockchain-based system for managing the entire pharmaceutical distribution chain. Let's imagine we've established a secure and reliable network where the parties who can be relied upon can join the community. The necessary transactions are stored on a blockchain on the backend, and once the information is recorded, it cannot be changed. In addition, we have a user-friendly mobile application that participants will utilize to conduct blockchain transactions.

A factory will generate a special hash and assign it to each new product as it is produced. The product's hash (unique identity) can be used to register it on the blockchain. The item might be viewed as a digital asset on the blockchain network, and its hash can be used to locate it at any moment. Depending on the manufacturer's preferences, any additional product records may be held either off-chain or on-chain backed by a trusted third party. Using an identifier, off-chain data can be blended with on-chain data. A hash-digest (for example, SHA-256) of all the off-chain data is typically generated and linked to the on-chain data in most blockchain-based programs. The best practice is to store text-only data on-chain and big documents (such as pictures) off-chain. A user-friendly mobile app can be used to quickly transfer ownership of a product to another participant after the maker has registered it on the blockchain. According to the license, the wholesaler must buy the pharmaceuticals from the manufacturer, who will then physically deliver them to the wholesaler while simultaneously registering the transfer transaction on the blockchain. The same process will be repeated by the wholesaler to transfer the pharmaceuticals to the distributor, who will then engage in an equal economic venture with the pharmacy. The basic layout of a blockchain-based pharmaceutical chain control is shown in Figure 11.

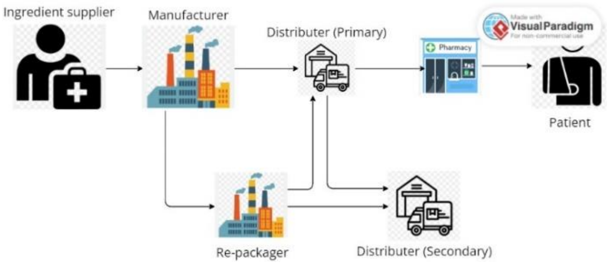

Figure 11. Blockchain-based pharmaceutical supply chain management system

3.6 Counterfeit pills discovery and delivery chain

Blockchain technology and paperless systems offer a stable, decentralized system for thwarting fraud [36]. Smart contracts have been defined as blockchain-based systems that enable the importation of traceable non-modifiable data along the entire drug supply chain, from the producer to the end user [37]. Two of blockchain's unique characteristics are its compatibility with numerous technologies and its real-time accessibility across the whole pharmaceutical distribution chain. The pharmaceutical supply chain can benefit from a decentralized distribution system with the chance of inexpensive statistics storage, which gives smart contract stakeholders accessibility, dependability, and integrity [38]. Utilizing RFID tags, clever contracts can give someone access to tune false returns to the manufacturer and supplier [39, 40]. Patients and sponsors can both have real-time access to information about their clinical trials, which lowers the cost of the studies. Smart contracts can handle security-demanding scenarios by addressing common security concerns, making use of contemporary technology, offering permission-based blockchains, stopping unauthorized and additional drug purchases, monitoring the distribution of vaccines, and storing and validating data both on- and off-chain.

Due to the open structure of the delivery chain, smart contracts were suggested as a solution to combat theft, loss, and fraud problems by providing stakeholders with security and transparency [40]. The integration of smart contracts into blockchain networks is currently gaining traction thanks to recent developments in the blockchain age. Many advantages result from this approach, including the elimination of intermediaries, self-execution, changelessness, and self-checking [41]. To preserve patient privacy, permission-based complete blockchains provide access to authenticated individuals [42]. With the help of QR code-enabled prescriptions, clever contracts written in the solidity language to operate on the Ethereum platform may be used to stop patients from buying excess medication that isn't prescribed to them to avert death [43]. The same study illustrates the use of multiple validation syntaxes to prevent reapplication attacks if the off-chain and on-chain do not match in terms of the write depend [44].

But for healthcare programs, using smart contracts might come with extra costs and hazards. A comparison of MultiChain, Hyperledger Fabric, and Ethereum finds that MultiChain may be the most user-friendly blockchain platform, Hyperledger Fabric is the most secure due to its layers of security, and Ethereum has the most developer support [45]. Similar benefits accrue to the pharmaceutical industry from Ethereum-based smart contracts built in the solidity language, including speed, cost savings, accuracy, and the ability to use backup [43].

Table 4. Main contributions and gaps identified in counterfeit pills discovery and delivery chain

Ref.	Main Contributions	Gaps Identified
[36]	The implementation of a BCT-enabled healthcare sustainable supply chain is the main goal of this research to enhance HSCP. Based on the findings, it was discovered that BCT had a beneficial impact on HSSCP practices and stakeholder involvement (SI). Together, they have a favourable effect on HSCP's performance. According to this study, using BCT made healthcare sustainable supply chains more effective in fending off COVID-19 outbreaks.	The three BCT features—transparency, immutability of data, and monitoring work—are the only ones included in this study; although, many other parameters might be taken into account to enhance it.
[37]	They offer a thorough analysis of the research on the use of blockchain technology in the pharmaceutical sector. We gathered, examined, categorised, and talked about research that we had retrieved from seven databases.	The lack of smart contracts in the suggested approach does not eliminate the middleman between the patient and the manufacturer.
[38]	This study provides an Ethereum blockchain-based track-and-trace system for the health care supply chain that makes use of data immutability and smart contracts. Data is kept in a publicly distributed ledger by hash functions. This discloses and safeguards data. Because smart contracts automate agreement execution, there is no need for a middleman or delay informing parties of the outcome. It also described the application architecture and algorithms for the decentralised healthcare supply chain. In order to solve the traditional supply chains' lack of tracking and openness, this paper suggests a solution. This study proposes a blockchain-based approach that utilises Solidity smart contracts. The results are shown as an average petrol cost for a given capability. The system's algorithms and methodologies are tested against a range of inputs.	Every nation that wants to employ blockchain technology in its healthcare supply chain should educate its citizens about it and encourage them to do so. To address issues like market players' concern of losing competency, there must be a public conversation about technology. Every nation ought to legalise safe, encrypted online payments. The technology can also be integrated with Internet of Things devices for better outcomes.
[39]	They have demonstrated how to create and put into practice a blockchain-based strategy that guarantees trustworthy supply chain management for goods shipped in smart containers. Our developed solution uses smart contract characteristics of the Ethereum blockchain to manage the sender-receiver interactions. Internet of Things (IoT)-enabled sensors in smart containers are used to monitor transportation conditions and verify predetermined shipping requirements. Ethereum smart contracts are used to verify receivers, automate payments, and issue reimbursements when predetermined criteria aren't met.	-
[40]	To address supply chain issues in a secure and effective manner, this research suggests a blockchain-based supply chain framework (SESCF). First, the supply chain system's information symmetry is guaranteed by the usage of smart contracts and blockchain. Secondly, real-time quality monitoring is aided by the unique identity that radio frequency identification (RFID) gives goods. Furthermore, tracking the provenance of items is made possible by the blockchain's distributed storage and immutability. Third, the issue of payment defaults is resolved by using the effective payment channel.	We combine several transaction types into a single chain in this paper. This could make the search less effective. We will think about placing various transaction types on various side chains in the future because it is an intriguing problem to extend our framework into a multichain structure. By doing this, the system throughput will increase along with the search efficiency.
[41]	By dumping the massive amount of medical data into the InterPlanetary File System (IPFS) storage and building an enforced cryptographic authorisation and access control method for outsourced encrypted medical data, this work closes the gap between PHRs and blockchain technology. The smart contract-based attribute-based searchable encryption (SC-ABSE), a novel lightweight cryptographic idea, serves as the foundation for the access control mechanism.	First off, authorised users can decrypt patient medical data stored in IPFS using standard access control. On-site first-aid medical staff are unable to access the patient's prior medical records, which makes it more difficult to provide first-aid when the patient's life is in danger. Second, in order to upgrade or revoke a user's attribute within the system, revocation methods for both users and attributes are required throughout (BC-ABSE).
[42]	They suggest a unique approach to managing safe drug supply chain records by utilising Hyperledger Fabric, a blockchain-based platform. By executing drug record transactions on a blockchain to build a smart healthcare ecosystem with a drug supply chain, the suggested method addresses this issue. To provide time-limited access to patient electronic health information and electronic medication records, a smart contract is launched.	Expanding the network size and then testing the system's viability and performance in an actual setting could be possible future directions.
[43]	Drug tracking got more challenging with the centralised architecture. A significant problem in the centralised network is avoiding counterfeit or duplicate medications made by dishonest producers. Real patients purchase medications without a prescription, which leads to numerous issues in daily life. Thus, with the use of a QR Code scanner connected to the prescription	Use Oracle Time Services to track the expiration date, steer clear of expired medications, and deploy the complete application as a mobile app that can be scanned with a QR code. to learn more about this technology's latency and throughput.

	that will be applied via a mobile application, patients cannot purchase pharmaceuticals without verified doctor's prescriptions, nor can they purchase excess drugs that could endanger someone's life. The smart contract, which operates on a public Ethereum network and is written in Solidity, is used to overcome these issues.	
[44]	This article provides a thorough analysis to highlight the blockchain technology's importance for the healthcare industry from both an application and a technological standpoint. The benefits and applications of blockchain technology in several fields are covered in the article, along with interoperability in the healthcare industry. The blockchain's intricate operation and consensus mechanisms are explained within the framework of healthcare. To select the best blockchain platform for healthcare applications, an overview of the architecture, platforms, and classifications is covered.	-
[45]	By (1) comparing the technical features of platforms, (2) choosing three platforms, (3) building blockchain networks, (4) testing the blockchains, and (5) summarising the experience and time used for implementation by students, we addressed practical considerations while building a healthcare blockchain and smart contract system. Our study's conclusions can hasten the adoption of blockchain technology in the biomedical and healthcare fields while lowering associated risks.	There may be limitations to the scope because they only compared three platforms. Our findings enable an informatics researcher, IT specialist, or technical leader in the hospital or other institution to evaluate the platforms' many practical characteristics, including setup/learning time and special technical features.
[46]	The "why" and "how" of BC-IoT systems are investigated inductively in this research using a systematic literature review of 120 peer-reviewed studies. Our proposal involved the application of a multi-perspective framework to examine the current systems in order to fully capture the heterogeneous nature of BC-IoT integration. We looked at the technical issues and improvement goals that drive BC integration to understand their motives. In terms of design, we documented BC's role in IoT systems as well as the content and tasks that IoT systems delegate to BC.	-
[47]	The purpose of this project is to create a blockchain-based pharmacosurveillance system and evaluate its performance in a mock network.	The following are some limitations of the study design: • The suggested approach will only be able to identify medication movements that correspond with official distribution chains that are recognised by the regulatory body. The suggested system will be developed and tested in a controlled simulated network; consequently, results obtained from this study may not be reflective of actual performance when deployed in a real-world setting. • It is unable to track counterfeit drugs that are distributed through routes outside of authorised distribution chains.
[48]	They offer a general framework to automate procedures and information transmission, utilising decentralised storage systems and Ethereum smart contracts. They also include intricate algorithms that record the relationships between supply chain participants. The Remix environment was used to develop and test the smart contract code.	In order to fully automate the PPE supply chain process for all supply chain stakeholders, it is suggested that decentralised applications be designed and developed.
[49]	The objective of this work was to create a methodology that, by monitoring the stakeholder business process, improves the safety of blockchain-based supply-chain workflow against a variety of internal (like Stuxnet) and external (like a local data breach of a stakeholder) cyber threats. Because our methodology shields the stakeholder's local process against assaults that take advantage of process knowledge that isn't protected by smart contracts, it works in tandem with the blockchain-based solution.	We intend to only permit legitimate and safe limitations that don't add any new or unsafe behaviours. Furthermore, if a constraint necessitates communication with external components for verification, the monitor's real-time performance may also be jeopardised.
[50]	Electronic medical record administration, pharmaceutical supply chain management, biomedical research and education, remote patient monitoring, processing health insurance claims, and health data analytics are key domains for blockchain applications in the health care industry.	Further research will focus on creating more blockchain-based healthcare proofs of concept to gain a better grasp of the systems' advantages and disadvantages. Additionally, more study needs to be done to create solid answers for the problems that have been identified. Ultimately, the amalgamation of blockchain technology with cutting-edge artificial intelligence (AI) technologies, such as deep learning, will guarantee our healthcare systems' enhanced ability to collaborate in a highly safe and confidential setting.

Table 5. Main contributions and gaps identified under medical health insurance enterprise

Ref.	Main Contributions	Gaps Identified
[51]	Since January 2016, survey articles offering IoT security solutions have been published in English. Among the many observations we make is that there aren't enough publicly accessible IoT datasets that the academic and practitioner groups can utilise. The development of a standard for sharing IoT datasets within the practitioner and academic communities, as well as other pertinent stakeholders, is necessary due to the potentially sensitive nature of these datasets.	Future studies will look into how additional IoT and related systems might be secured using blockchain technology as a collaborative security foundation.
[52]	In order to illustrate the capabilities of the blockchain-based transaction processing system (TPS) in real-time accounting, continuous monitoring, and fraud detection, this paper offers a design for the system and constructs a prototype. We compare and analyse the computing performance of a blockchain-based TPS with relational databases.	BB-CASs, which are made up of a sequence of smart contracts that can be programmed to deliver messages automatically when trigger conditions are satisfied and to continually monitor transaction activity, are being developed.22 While blockchain still has a significant computational overhead when compared to relational databases, it is anticipated that advancements in technology will lead to cost reductions, making blockchain an infrastructure that is widely used for enterprise information systems and continuous monitoring systems.

Clever contracts help to deliver chain transparency by reducing the supply of fake capsules, reducing the financial burden of fake and inferior tablets, streamlining global options by exchanging product-related statistics, managing dynamic changes in cross-border distribution channels, and offering real-time cargo tracking. The selling of counterfeit medications can potentially be restricted by smart contracts. A sizeable chunk of the massive Asian counterfeit drug market is represented by the 30% of tested capsules in pharmacies in the Philippines that are fakes [46]. By utilizing a blockchain-based pharmacy surveillance technology to spot phoney and inferior drugs in the supply chain, this financial suffering could be mitigated [47]. Smart contracts are essential to the advancement of logistics and global trade.

It is difficult to detect fake goods because of the intricacy of distribution networks. Although one looks suggests a framework for the use of distributed ledgers and smart contracts to address this issue in the medication supply chain [42]. In this approved blockchain community, a transaction proposal is transmitted across the blockchain network. This transaction proposal is made possible by permitting all CRUD (create, review, update, and delete) operations on the data.

Smart contracts can enhance transparency and encourage thoughtfulness among supply chain actors [48]. All stakeholders are protected by the so-called end-to-quit protection and privacy across a blockchain, which offers benefits like enhancing chain auditing, identifying and mitigating the impact of incidents, and bringing transparency to the entire organization rather than just those who specialize in transactions [49]. Table 4 highlights the main contributions and gaps identified in counterfeit pills discovery and delivery chain. Clever contracts can help fitness-care applications—complex blockchain programs—create guidelines for health record users' use and foster a sense of agreement among users that data is immutable [50].

3.7 Blockchain and the medical health insurance enterprise

In this paper, we have a look at the feasibility and implications of these use cases in terms of ways blockchain may want to, directly and indirectly, enhance an insurer's fundamental techniques and business models. The instances deal with upgrades in an insurance corporation's operational capabilities in addition to dealings with vendors, intermediaries, and policyholders, thereby improving the purchaser experience, improving product cost. Table 5 highlights the main contributions and gaps identified under medical health insurance enterprise.

- Transferring towards interoperable, comprehensive health facts.
- Assisting administrative and strategic imperatives with clever contracts.
- Detecting fraud efficiently.
- Enhancing provider listing accuracy.
- Simplifying the application system with the aid of making it extra client-centric
- Facilitating a dynamic insurer/customer courting.

In the current device, the coverage claim method is coordinated between the fitness care companies and coverage companies by way of coverage dealers. Coverage dealers might also intentionally or unintentionally leak essential files like patient facts, clinical fitness information, and coverage policy records. The coverage-claiming process is completed manually and consumes lots of time and energy. In a traditional dispensed database, study/write operations are managed through a centralized device. Those statistics can get changed. With the upward thrust of the era and boom in the amount of data, information breaches and file tempering are a danger to the privacy and authentication of records whilst stored on a significant server. As a result, information integrity and getting entry to manipulate are primary issues in healthcare and coverage enterprises. Coverage industries also are facing the issue of declaring fraud. Fake facts can be furnished for the price of false claims through policy holder. Detecting fraud has grown to be a project which could result in losses to the corporation but also growth in the transaction processing time and charge settlement time because the business enterprise may additionally touch extra assets for records.

- Improve integrity and protection by way of providing better management of affected person records.
- Name for a better pleasant of scientific trial information.
- Lessen regulatory and compliance expenses.
- Set up new requirements and practices.
- Optimize interactions between healthcare specialists, insurance businesses, and policyholders.

- Shape partnerships with leading ventures using the blockchain era.

Based on keyword statistics, co-occurrence functions of different key phrases related to blockchain and insurance are taken into account to illustrate the sizable trends in keyword co-incidence. Figure 12 displays the co-prevalence network evaluation, association, and node of the 50 most often occurring terms in published publications on blockchain studies. Figure 12 suggests that the research area was divided into three major clusters. The red cluster was focused on an extremely generalized idea of blockchain that was primarily related to the insurance industry, smart contracts, Ethereum, the internet of things, cryptocurrency, bitcoins, consensus, and blockchain security. The blue cluster, on the other hand, was more focused on the area of medical insurance or healthcare.

Additionally, the unexperienced cluster revealed the keyword's proximity concerning financial insurance tech, generation, chance, and fintech banking. The Blockchain cluster is demonstrated to be of great importance and great interest for the good purpose of revolutionary research.

Blockchain's contribution to the insurance business.

- Blockchain deployments try to cut down on inefficiencies, expensive transaction fees, and protracted claim processing times by creating distributed ledgers. Information and payments are securely recorded, reducing risks, and increasing the amount of insurance on hand. Currently, fraud detection, automatic claim agreement, cash flow document tracking, and self-purchase insurance are the main applications of blockchain in the insurance sector.
- In the past, claims were often processed through KYC (Know Your Customer), however computerized claims have eliminated the need for KYC. Since the year 2000, financial institutions have been using KYC, one of the main methods of identifying often used by business entities around the world. Clients can grant insurance companies access to their identifying records as needed. Once the KYC profile has been reviewed, the consumer can avoid repeat authentication processes and obtain improved identification information before other agencies require it. Disintermediation, transparent transactions, and lack of centralized control are just a few benefits of a fully blockchain-based KYC system.

Many organizations have altered the way statistics are processed using the capabilities of blockchain de-mediation. For instance, Stratumn, a French insurance company with headquarters in Paris, shares verified customer data through blockchain, which reduces the cost and time associated with each request for a statistical analysis to determine whether the customer is eligible for insurance coverage. As a result, customers can purchase insurance on their own. In December 2018, Ant coverage published the "blockchain + declare" challenge, which allowed the use of digital notes as declared notes [51].

The smart contract era, which is entirely dependent on blockchain creation, is frequently used for fraud detection. Smart contracts are specialized protocols created to automate contract validation and compliance. We can conduct traceable, permanent, and comfortable transactions thanks to clever contracts, which eliminate the necessity for one-third of events. If the requirements are met, an intelligent settlement will include all the transaction information and best carry out the subsequent process. Computer systems create intelligent contracts, which makes them distinct from conventional paper contracts. As an illustration, Taikang Online deployed blockchain generation-based total coverage fraud detection for an Anti-Moth assignment. The company's clever contracting system can determine if the buyer is considering coverage and whether they meet the insurance requirements that not only protect privacy but also help to prevent coverage fraud [52].

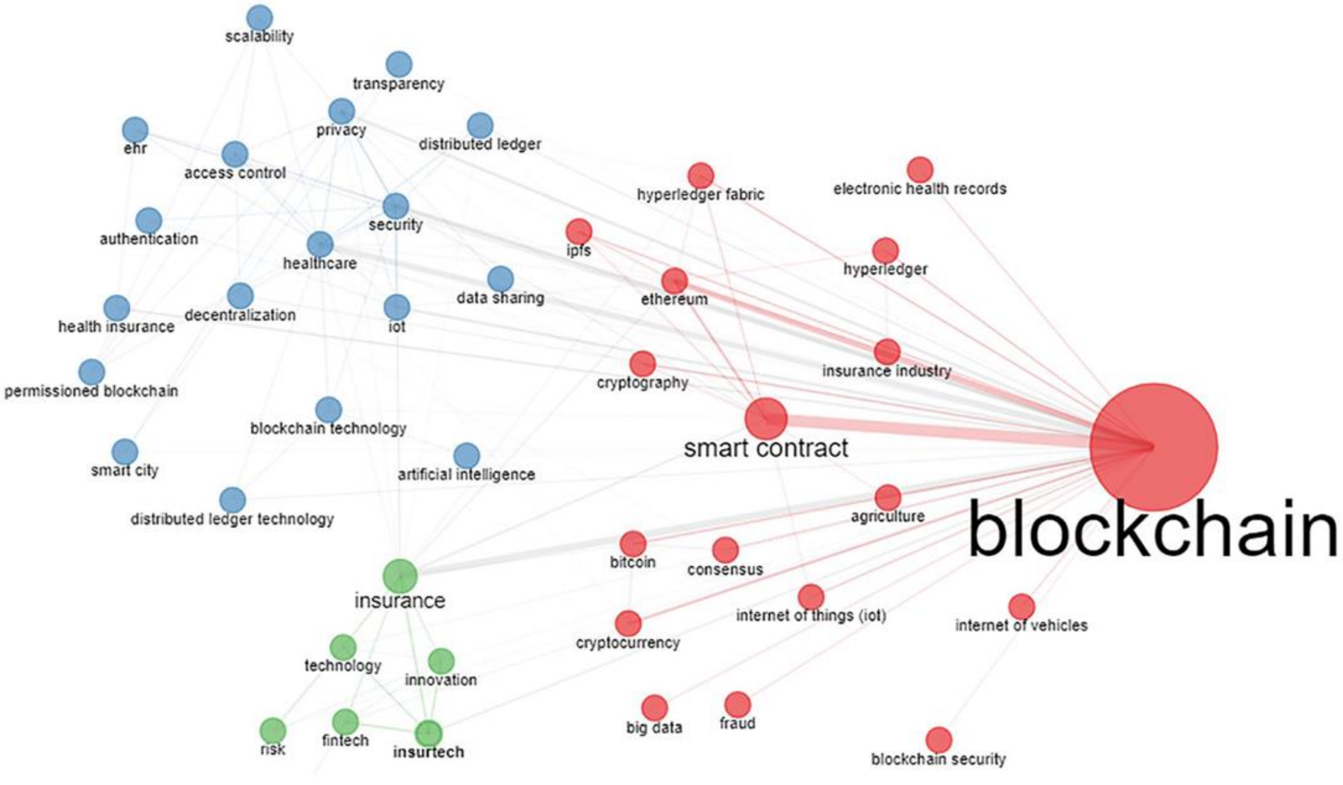

Figure 12. Co-occurrence network analysis

The characteristics of dispersed ledgers make it possible to track historical capital flow statistics. A dispersed ledger is controlled in a decentralized manner, spanning various locations, and does not depend on a third entity (such as a bank or clearinghouse) to maintain the accuracy of the records it maintains. A distributed ledger is a database made up of several independent computers (called nodes), and it is up to the nodes to verify, store, and update data. The ability of the dispersed ledger to serve as a dispersed witness makes it extremely challenging to target and attack the community. In a centralized ledger, it is most efficient for one entity to possess a replica of the ledger. However, in the event of an allocated ledger, every node in the community has a duplicate of the exact ledger. No one entity could alter the ledger without the agreement of all participating nodes because any new changes can be applied to all nodes in a matter of seconds. It uses cryptography to store all the data, and only the key and encrypted signature can be used to unlock it. As a result, the distributed ledger will not only help to explain the lengthy tracking of capital flow statistics, but it will also guarantee the complete security of the data that is being recorded.

3.8 Fraudulent medical health insurance claims

Due to the rapid advancement of clinical information technology, hospitals' record-keeping systems have amassed enormous amounts of data, prompting the scientific community to develop the technology of big facts. The discipline of science has greatly benefited from the introduction of medical big data, which has garnered interest from both academia and business [53]. An important area of research in scientific big statistics is the regulation of scientific cost. The traditional medical health insurance system pays for medical expenses based mostly on clinical provider items, which leads to too intensive medical procedures and rising medical costs. The single disease charge, which is entirely based on diagnosis-related agencies (DRGs), has been extensively researched and implemented to overcome the issues in the item-based fee system [53]. The single-disorder payment approach could be used for fraudulent health insurance. To take advantage of additional money from medical health insurance organizations, the healthcare provider, when assigning the diagnostic code for an inpatient, could swap out the genuine low-cost illness code for another high-fee disease code. The cost of manually reviewing each inpatient's medical statistics is incredibly high due to the enormous variety of inpatients. Since there are over 15 million inpatients in the Jiangsu province of China each year, it is impossible to personally audit each discharge diagnostic. As a result, the single illness price mechanism now faces an urgent problem how to successfully uncover plausible fraud.

3.9 Health information tracking, anonymizing records, and information encryption

In the study of Su et al. [54], the attribute-based signature technique was developed to secure the confidentiality of clinical stakeholders. Keys are known as master keys were introduced on this layout to indicate attributes connected to positive nodes and replace keys to authenticate users. In this plan, a few of the parties involved in the Blockchain community (which included doctors) were noted as having positive characteristics, such as "Hospital A. Department of Oncology. Senior Physician." These characteristics are removed from the affected person by an algorithm known as KUNodes after researching their background information.

In the study of Jeet et al. [55] they created a Blockchain-based system for collecting IoT data. In this system, wearables and sensors were used to gather and update patient statistics every second. As a result, brand-new signs of infection and sensitivity to pills might be immediately logged inside the Blockchain. This framework utilized SHA-256 encryption, and the techniques employed in this study shorten the encryption time. Table 6 shows the main contributions and gaps identified under health information tracking, anonymizing records, and information Encryption.

In the research of Rajasekaran et al. [56] they offered a method for the healthcare Blockchain's cooperating parties to be authenticated. The anonymity of participating events within the healthcare Blockchain is supported by this lightweight authentication system. In this system, clinicians are permitted to share statistics about patients with other doctors without jeopardizing patient confidentiality or record security. Only authorized users can read the information about the healthcare topic using this scheme's authentication method.

Zhang et al. [57] proposed a Blockchain-based plan for secure medical data storage and sharing. A solution to the issue of information dispersion within the healthcare subject has been provided, and the authentication of all events involved in the healthcare system has been rigorously examined in this study.

In the study of Al Omar [58], they suggested MediBchain, a blockchain-based healthcare network where private data is encrypted using a public key encryption method (i.e. Elliptic Curve Cryptography (ECC)) across a secured channel. Additionally, Yang et al. [60] suggested that sensor data might be uploaded to the blockchain network using an exact pair of personal and public keys to protect the confidentiality and privacy of biometric records.

Zheng et al. [59] suggested using a threshold encryption technique along with a symmetric key scheme, such as Rijndael AES, to encrypt data before uploading it to cloud servers. Shamir's mystery-sharing approach can be used to divide the symmetric key into a few stocks that are distributed among several key keepers. The statistics requestor can only decipher the ciphertext if he obtains sufficient key stocks. Information leaking might no longer occur if a small number of key personnel (far less than the threshold) are compromised.

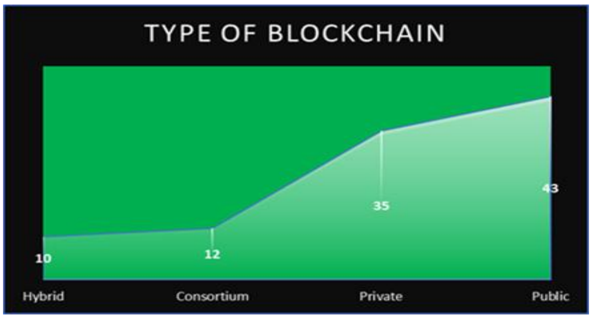

Figure 13. The typical percentage of blockchain utilized in the publications that were reviewed

3.10 What sort of Blockchain became used within the present studies?

Figure 13, which shows the percentage of the Blockchain kind used in each study, illustrates the various types of

Blockchains utilised in each paper. In the poll, private blockchain was used by 35% of respondents, hybrid blockchain by 10%, public blockchain by 43%, and consortium blockchain by 12%.

Table 6. Main contributions and gaps identified under health information tracking, anonymizing records, and information encryption

Ref.	Main Contributions	Gaps Identified
[53]	Describe deep learning approaches for the medical field, with a focus on computer vision, natural language processing, reinforcement learning, and generalised methodologies. We discuss the potential applications of these computational methods in several important medical domains and investigate the development of end-to-end systems. We describe the application of natural language processing to areas such as electronic health record data, and our discussion of computer vision is mostly focused on medical imaging. In a similar vein, generalised deep learning techniques for genomics are examined and reinforcement learning is explored in relation to robotically assisted surgery.	-
[54]	To safeguard user privacy in HS-BC, they suggest an attribute-based signing method with attribute revocation. If attributes serve as a means of user identification and identity protection, the user computes the attribute signing key by combining the attribute master-key and the attribute update-key. The master-key is associated with the user's identity and attribute set, while the update-key is associated with attribute revocation. The KUNodes technique can be used to efficiently accomplish attribute revocation. The developed attribute-based signature system doesn't rely on a central authority and only needs a small number of pairing operations.	-
[55]	The goal of this research paper is to present a block-based data encoding security framework for the healthcare industry that can encrypt sensitive information transferred over cloud servers. To support the SHA-256 hashing technique, a 128-bit AES key is produced in the suggested method. To prevent unwanted access, each user's data is separated into blocks and encrypted. The intended model's practical applicability in the healthcare industry is intended to be presented through an interface-based system. Lastly, the MATLAB software is used to validate the efficacy of the suggested method in terms of MAE, RMSE, MSE, encryption time, and decryption time.	-
[56]	An innovative privacy-preserving authentication strategy based on blockchain is suggested as a way to accomplish patient verification effectively without requiring the assistance of a reliable third party. Additionally, a secure hand-over authentication mechanism is designed to guarantee that patients in multi-doctor communication scenarios do not re-authenticate, and to revoke any potential malicious misbehaviour on the part of medical professionals during IoHT patient communications.	One of the potential future applications of this research effort will be the location privacy of wireless BAN users. When a user is moving and accessing the wireless body area network from different locations, location privacy and security should be maintained. Additionally, an automated billing system for the prescription drugs that the physician provides in order to access patient data can be integrated into IoHT networks, and this is a topic of interest for research. Lastly, future research can expand into other application domains like government agencies, supply chain management, education, and even automobile ad hoc networks.
[57]	They suggested PTBM, a privacy-preserving contact tracing system for blockchain-based medical applications that are integrated with 5G. Everybody can perform location checking with their smartphones or even wearable devices connected to the 5G network to see if they have been in possible contact with a diagnosed patient without having their privacy violated. This is made possible using the 5G-integrated network as the underlying infrastructure in PTBM. A reliable hospital can locate patients and the related close relations with ease.	In the event of a worldwide pandemic, we plan to use this blockchain-based system for more thorough patient management, vaccination schedules, and secure information sharing with international organisations. Another promising area of research is how to combine the newly developed 5G technology with other pertinent medical applications that require low latency and great communication reliability.
[58]	Blockchain technology makes use of distributed or decentralised processes to guarantee the integrity and accountability of its application. This study provides a blockchain-based patient-centric healthcare data management system that achieves anonymity through storage. Utilising cryptographic mechanisms to safeguard patient data ensures pseudonymity.	Deploy this whole system.
[59]	Put out a local reference-based consortium blockchain plan together with the proof-of-familiarity (PoF) consensus-gathering technique. Through PoF, stakeholders establish a medical decision that is both transparent and tenable, hence increasing collaborators'	Creating a complete real-time application, making effective use of past choices, and observing and absorbing information from the surroundings. We will take into account the weighting considerations among entities during collaborative decision-

	interoperability. PoF prototype is tested using multichain 2.0, a framework for constructing blockchains. Moreover, two-layer storage, encryption, and a timestamp storing mechanism protect the privacy of identities, EMRs, and judgements.	making in a later version of this study. This will therefore make it possible for the system to be more accurately and widely employed in the commercial sector.
[60]	An extensive analysis of blockchain technology. This paper presents the taxonomy of blockchain technology, describes common consensus algorithms for blockchains, examines various blockchain applications, and addresses both technical obstacles and the latest developments in addressing them. Additionally, this report identifies the directions that blockchain technology will take in the future.	The field of smart contracts is expanding quickly, and numerous applications have been suggested. However, many novel applications are now difficult to execute since smart contract languages still have a lot of flaws and limitations. In the future, we intend to conduct a thorough analysis on smart contracts.

4. OPEN PROBLEMS AND FUTURE DIRECTIONS

4.1 Enhancing the scalability of blockchain based healthcare

Enhancing the scalability of blockchain-based healthcare systems is crucial for widespread adoption and efficient processing of healthcare transactions. Here are several strategies to address scalability challenges in blockchain-based healthcare. Choose or design a consensus mechanism that balances security and scalability. Traditional proof-of-work (PoW) can be resource-intensive, while newer consensus mechanisms like proof-of-stake (PoS) or practical Byzantine fault tolerance (PBFT) may offer better scalability. Table 7 represents the open problems and research directions.

Sharding: Implement sharding, a technique where the blockchain is divided into smaller, more manageable segments (shards). Each shard processes its transactions independently, improving overall network throughput.

4.1.1 Off-chain scaling solutions

To execute transactions off the primary blockchain, use off-chain solutions like state channels or sidechains. This can increase scalability and lessen the strain on the main chain.

4.1.2 Lightning networks

Explore the use of lightning networks, which enable faster and more cost-effective transactions by creating off-chain payment channels.

4.1.3 Smart contract efficiency

Optimize smart contracts to reduce complexity and execution time. Efficient coding practices can contribute to faster transaction processing.

4.1.4 Parallel processing

Enable parallel processing of transactions to allow multiple transactions to be validated simultaneously, enhancing overall throughput.

Table 7. Open Problems and research directions

Open Problems	Current Limitations	Research Direction
Scalability and Performance	Blockchain networks can face scalability issues, especially when dealing with a large volume of healthcare data transactions.	Investigate and develop scalable blockchain solutions, such as sharding and off-chain protocols, to handle the increasing demands of healthcare data while maintaining performance.
Interoperability	Healthcare systems often use diverse data formats and standards, making interoperability a challenge for blockchain integration.	Explore standardization efforts and interoperable frameworks that allow different healthcare systems to seamlessly share and access data on a blockchain while adhering to privacy and security standards.
Data Privacy and Consent Management	Ensuring patient consent and managing privacy on a blockchain while still allowing data sharing for treatment purposes is complex.	Develop privacy-preserving mechanisms, such as zero-knowledge proofs or homomorphic encryption, to enable secure and private sharing of healthcare data on a blockchain, while still maintaining patient consent and control.
Regulatory Compliance	Healthcare is subject to strict regulations, and blockchain applications need to comply with these regulations.	Investigate regulatory frameworks and propose blockchain architectures that align with healthcare regulations, ensuring data security and privacy compliance.
Identity Management	Establishing and managing patient identities securely on a blockchain without compromising privacy can be challenging.	Explore decentralized identity solutions on the blockchain, such as self-sovereign identity (SSI), to provide a secure and privacy-preserving way of managing patient identities and permissions.
Smart Contracts for Healthcare Workflow	Designing and implementing smart contracts that handle complex healthcare workflows while ensuring privacy and security.	Develop smart contract frameworks tailored for healthcare scenarios, incorporating privacy features and mechanisms for handling sensitive healthcare data.
Integration with Legacy Systems	Many healthcare systems use legacy infrastructure, making the integration of blockchain solutions challenging.	Explore methods and tools for seamless integration of blockchain with existing healthcare systems, allowing for a gradual transition and minimizing disruptions.
User Education and Adoption	Ensuring that healthcare professionals and patients understand the benefits and risks of blockchain technology.	Investigate strategies for educating and promoting the adoption of blockchain technology in healthcare, addressing concerns and providing training for users.

Consider using consortium or private blockchains for specific use cases within the healthcare industry. These may offer increased scalability compared to public blockchains.

4.1.5 Consortium blockchains

Some potential methods that could help improve scalability are utilizing Private chains, segmenting data, altering consensus algorithms, and batching transactions. Private chains can help reduce the amount of data that is stored in the blockchain, by whitelisting specific participants that can interact with the chain. Segmenting data helps reduce the amount of data that is stored on the chain by only making specific pieces of data available to certain nodes. By altering consensus algorithms, the number of nodes that are needed to approve each transaction can be adjusted to a lower number. Lastly, by batching transactions, it reduces the overhead cost of those transactions by grouping multiple operations, instead of processing them as individual transactions. By investigating and utilizing these methods to improve the scalability of Blockchain networks, healthcare networks may be able to support an ever-growing number of users and data without sacrificing the security of the network.

4.2 Use more efficient cryptographic techniques

One of the best ways to study the development of new encryption strategies for healthcare transactions is through quantum cryptography. Quantum cryptography uses complex algorithms and codes that use qubits (quantum bits) to allow for the secure transmission of information. This type of encryption is very secure as it relies on the laws of quantum mechanics. It is also significantly more difficult for attackers to intercept the data as the transmission of data is encrypted at the qubit level. Another approach to secure healthcare transactions is to use blockchain technology. Blockchain technology can be used to securely store, access, and transfer patient and medical information between different organizations. It is secure because it makes use of cryptography to store and access data. The data is securely stored in a blockchain, and access requires the appropriate credentials. This makes it difficult for attackers to access the data as they would need to have the credentials as well as the correct cryptographic keys.

In addition, the use of biometric authentication is recommended for healthcare transactions. Biometric authentication requires the use of physical biometric features such as fingerprints, iris scans, and facial recognition. This type of authentication is difficult to bypass and makes it much harder for attackers to gain access to data.

4.2.1 Elliptic Curve Cryptography (ECC)

ECC provides the same level of security as traditional cryptographic systems but with significantly shorter key lengths. This results in faster transaction processing and reduces computational overhead.

4.2.2 Homomorphic encryption

Computations on encrypted data can be done without having to first decrypt it thanks to homomorphic encryption. This can enhance privacy while enabling certain types of processing to be done off-chain, reducing the computational load on the blockchain.

4.2.3 Zero-knowledge proofs

Zero-knowledge proofs allow one side to demonstrate ownership of information without disclosing it, like in the case of zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge). This lowers the volume of data transferred over the network, which might be helpful for applications that prioritise privacy.

4.2.4 Ring signatures

A group member can sign a message on behalf of the group using ring signatures, keeping the identity of the signer secret. This improves transaction privacy.

4.2.5 Multi-Party Computation (MPC)

With MPC, several parties can work together to jointly compute a function over their private inputs. This can be used for a number of blockchain applications, including safe data aggregation.

4.2.6 Hash functions

Optimizing hash functions, such as adopting more efficient algorithms or utilizing hardware acceleration, can improve the overall performance of blockchain systems.

4.2.7 BLS (Boneh-Lynn-Shacham) signatures

BLS signatures are a type of digital signature that allows for aggregation. This can be particularly useful in reducing the size of transactions in blockchain systems.

4.2.8 Aggregate signatures

Techniques like aggregate signatures allow multiple signatures to be aggregated into a single, more compact signature. This reduces the size of transactions and improves efficiency.

4.3 Globalization of healthcare networks

This would help provide better medical attention and care for those living in remote and/or developing nations. Additionally, this would make records from any country up-to-date and easily available. In turn, healthcare providers would be able to provide much more efficient and accurate treatments. This global medical network would also reduce healthcare costs and offer a level of trustworthiness in the medical system. Blockchain-based networks provide an added layer of data security, which is essential when handling vulnerable patient information. Finally, the digital verification of medical records would significantly reduce administrative paperwork and improve immediate patient care.

4.4 Use of artificial intelligence in Blockchain-based healthcare networks

Integrating artificial intelligence (AI) with blockchain-based healthcare networks can lead to more efficient, secure, and intelligent healthcare systems. Here are several ways AI can be leveraged within blockchain-based healthcare networks.

4.4.1 Data analytics and insights

Utilize AI algorithms to analyze and derive actionable insights from healthcare data stored on the blockchain. This can include identifying patterns, trends, and correlations that may inform treatment strategies, disease prevention, and resource allocation.

4.4.2 Predictive analytics

Implement AI-driven predictive analytics to forecast disease outbreaks, patient admission rates, and other critical healthcare events. By combining blockchain's secure data storage with predictive analytics, healthcare providers can enhance their decision-making processes.

4.4.5 Personalized medicine

Blockchain and AI algorithm integration will enable personalized medicine. AI can offer individualized treatment plans, drugs, and treatments by analyzing patient data, genetic information, and treatment outcomes.

4.4.6 Health monitoring and IoT integration

Connect Internet of Things (IoT) devices for health monitoring to blockchain networks. AI algorithms can process real-time data from these devices to provide timely insights into a patient's health status, facilitating proactive healthcare interventions.

4.4.7 Smart contracts for healthcare automation

Create AI-enabled smart contracts to automate medical procedures. Smart contracts, for instance, can reduce administrative costs by automating the processing of insurance claims, prescription verification, and appointment scheduling.

4.4.8 Fraud detection and security

Use AI algorithms to enhance the security of healthcare data on the blockchain. AI can detect anomalies and patterns indicative of fraudulent activities, ensuring the integrity and confidentiality of patient records.

4.4.9 Natural Language Processing (NLP) for medical records

Apply NLP algorithms to extract valuable information from unstructured medical records stored on the blockchain. This can streamline data retrieval and improve the accuracy of diagnosis and treatment planning.

4.4.10 Clinical Decision Support Systems (CDSS)

To help medical practitioners make wise judgements, incorporate blockchain-based healthcare networks with AI-powered CDSS. CDSS can analyze patient data and medical literature to generate recommendations that are supported by evidence.

4.4.11 Supply chain optimization

Use AI for optimizing pharmaceutical and medical supply chains by predicting demand, improving inventory management, and ensuring the authenticity of medications. Integrating this with blockchain enhances transparency and traceability.

4.4.12 Remote Patient monitoring and AI diagnostics

Combine blockchain with AI for remote patient monitoring and diagnostics. AI algorithms can analyze data from wearable devices and diagnostic images, providing real-time feedback and reducing the need for physical appointments.

4.4.13 Consent management with AI

Develop AI-driven consent management systems on the blockchain. AI can assist in dynamically managing patient consent preferences, ensuring that sensitive healthcare information is shared securely and in compliance with regulations.

4.4.14 Distributed machine learning

Use blockchain networks to deploy distributed machine learning models so that different institutions can train together without exchanging private patient information. In the process, privacy is preserved, and AI model performance is enhanced.

4.4.15 Chronic disease management

Use AI for monitoring and managing chronic diseases through continuous analysis of patient data on the blockchain. AI algorithms can provide insights into disease progression and recommend personalized interventions.

Implementing AI in conjunction with blockchain technology in healthcare networks requires close collaboration between healthcare providers, technology developers, and regulatory bodies. Ensuring compliance with privacy regulations and ethical considerations is paramount to building trust and promoting widespread adoption. Adopting these advanced techniques can contribute to the development of more efficient and secure blockchain systems. It's crucial to remember that the needs and use cases of the blockchain application determine whether cryptography, AI, and machine learning approaches are selected. Additionally, ongoing research in cryptography and Machine learning technique may lead to the development of new and improved techniques over time.

5. CONCLUSIONS

This review briefly discusses blockchain in healthcare and its use in different security issues. This security approach can account for various challenges and blockchain issues that depend on different aspects of security. Transaction Scalability, Availability, Security, and its Benefits. These security structures may be the subject of future research. This article aimed to present blockchain technology as a viable solution to EMR systems' interoperability and security issues in poor nations. Blockchain offers EMR system implementers the opportunity to overcome these challenges. The promise of blockchain is to enable efficient information exchange between stakeholders, protect patient privacy, and ensure data integrity. To date, the introduction of electronic health systems in many developing countries has met with significant resistance from physicians, patients, and regulators due to several legitimate concerns, including the security and privacy of patient records.

This article concludes that blockchain technology can address the current shortcomings of EMR system. The core of an EMR system is to ensure interoperability, privacy, and security of patient records. However, we argue that the adoption of blockchain applications should be gradual with each new technology. Additionally, unresolved issues surrounding the use of blockchain technology, among these are acceptance, rules, and ethics, which need to be taken into account.

ACKNOWLEDGMENT

I want to sincerely thank Dr. Poornima A.S., our supervisor, for her constant assistance and direction during the research process. Her knowledge, perceptions, and support were crucial in enabling us to finish this project. Lastly I would want to thank my family and friends for their love and support

throughout the entire academic process. I could not have finished this study without their inspiration and assistance.

REFERENCES

[1] Kassab, M., Defranco, J., Malas, T., Laplante, P., Destefanis, G., Neto, V.V.G. (2021). Exploring research in blockchain for healthcare and a roadmap for the future. IEEE Transactions on Emerging Topics in Computing, 9(4): 1835-1852. https://doi.org/10.1109/TETC.2019.2936881

[2] Shen, B., Guo, J., Yang, Y. (2019). MedChain: Efficient healthcare data sharing via blockchain. Applied sciences, 9(6): 1207. https://doi.org/10.3390/app9061207

[3] Chelladurai, U., Pandian, S. (2022). A novel blockchain-based electronic health record automation system for healthcare. Journal of Ambient Intelligence and Humanized Computing, 13(1): 693-703. https://doi.org/10.1007/s12652-021-03163-3

[4] Parlakkılıç, A. (2021). Blockchain use cases in healthcare. Blockchain technology in Healthcare: Opportunities and Challenges, Hershey, PA: IGI Global, 85-104. https://doi.org/10.4018/978-1-7998-8493-4.ch004

[5] Yaqoob, I., Salah, K., Jayaraman, R., Al-Hammadi, Y. (2022). Blockchain for healthcare data management: Opportunities, challenges, and future recommendations. Neural Computing and Applications, 34(14): 11475-11490. https://doi.org/10.1007/s00521-020-05519-w

[6] Liang, X., Zhao, J., Shetty, S., Liu, J., Li, D. (2017). Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In 2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC), Montreal, QC, Canada, pp. 1-5. https://doi.org/10.1109/PIMRC.2017.8292361

[7] Kiania, K., Jameii, S.M., Rahmani, A.M. (2023). Blockchain-based privacy and security preserving in electronic health: a systematic review. Multimed Tools Appl, 82: 28493–28519. https://doi.org/10.1007/s11042-023-14488-w

[8] Tandon, A., Dhir, A., Islam, A.N., Mäntymäki, M. (2020). Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122: 103290. https://doi.org/10.1016/j.compind.2020.103290

[9] Gaynor, M., Tuttle-Newhall, J., Parker, J., Patel, A., Tang, C. (2020). Adoption of blockchain in health care. Journal of Medical Internet Research, 22(9), 1-10. https://doi.org/10.2196/17423

[10] Agbo, C.C., Mahmoud, Q.H., Eklund, J.M. (2019). Blockchain technology in healthcare: A systematic review. In Healthcare, 7(2): 56. https://doi.org/10.3390/healthcare7020056

[11] Cheikhrouhou, O., Mershad, K., Jamil, F., Mahmud, R., Koubaa, A., Moosavi, S.R. (2023). A lightweight blockchain and fog-enabled secure remote patient monitoring system. Internet of Things, 22: 100691. https://doi.org/10.1016/j.iot.2023.100691

[12] Liu, H., Wang, X., Liu, S. (2004). Feasible direction algorithm for solving the SDP relaxations of quadratic {-1, 1} programming problems. Optimization Methods & Software, 19(2): 125-136. https://doi.org/10.1080/10556780410001647203

[13] Azaria, A., Ekblaw, A., Vieira, T., Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. In 2016 2nd international conference on open and big data (OBD), Vienna, Austria, pp. 25-30. https://doi.org/10.1109/OBD.2016.11

[14] Ekblaw, A., Azaria, A. (2019). MedRec: Medical Data Management on the Blockchain. Viral Communications. https://viral.media.mit.edu/pub/medrec.

[15] Faruk, M.J.H., Shahriar, H., Valero, M., Sneha, S., Ahamed, S.I., Rahman, M. (2021). Towards blockchain-based secure data management for remote patient monitoring. In 2021 IEEE international conference on digital health (ICDH), Chicago, IL, USA, pp. 299-308. https://doi.org/10.1109/ICDH52753.2021.00054

[16] Leeming, G., Cunningham, J., Ainsworth, J. (2019). A ledger of me: personalizing healthcare using blockchain technology. Frontiers in medicine, 6: 171. https://doi.org/10.3389/fmed.2019.00171

[17] Kumar, M., Chand, S. (2021). MedHypChain: A patient-centered interoperability hyperledger-based medical healthcare system: Regulation in COVID-19 pandemic. Journal of Network and Computer Applications, 179: 102975. https://doi.org/10.1016/j.jnca.2021.102975

[18] Haleem, A., Javaid, M., Singh, R.P., Suman, R., Rab, S. (2021). Blockchain technology applications in healthcare: An overview. International Journal of Intelligent Networks, 2: 130-139. https://doi.org/10.1016/j.ijin.2021.09.005

[19] Mettler, M. (2016). Blockchain technology in healthcare: The revolution starts here. In 2016 IEEE 18th international conference on e-health networking, applications and services (Healthcom), Munich, Germany, pp. 1-3. https://doi.org/10.1109/HealthCom.2016.7749510

[20] Houtan, B., Hafid, A.S., Makrakis, D. (2020). A Survey on blockchain-based self-sovereign patient identity in healthcare. IEEE Access, 8: 90478-90494. https://doi.org/10.1109/ACCESS.2020.2994090

[21] Rejeb, A., Bell, L. (2019). Potentials of blockchain for healthcare: case of tunisia. SSRN Electronic Journal, 136: 173-193. https://doi.org/10.2139/ssrn.3475246

[22] Chukwu, E., Garg, L. (2020). A systematic review of blockchain in healthcare: Frameworks, prototypes, and implementations. IEEE Access, 8: 21196-21214. https://doi.org/10.1109/ACCESS.2020.2969881

[23] Abou-Nassar, E. M., Iliyasu, A.M., El-Kafrawy, P.M., Song, O.Y., Bashir, A.K., El-Latif, A.A.A. (2020). DITrust Chain: Towards blockchain-based trust models for sustainable healthcare IoT systems. IEEE Access, 8: 111223-111238. https://doi.org/10.1109/ACCESS.2020.2999468

[24] Paranjape, K., Parker, M., Houlding, D., Car, J. (2019). Implementation considerations for blockchain in healthcare institutions. Blockchain in Healthcare Today, 2: 1-9. https://doi.org/10.30953/bhty.v2.114

[25] Shi, S., He, D., Li, L., Kumar, N., Khan, M.K., Choo, K.K.R. (2020). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. Computers & Security, 97: 101966. https://doi.org/10.1016/j.cose.2020.101966

[26] Le Nguyen, T. (2018, August). Blockchain in healthcare: A new technology benefit for both patients and doctors.

In 2018 Portland International Conference on Management of Engineering and Technology (PICMET), Honolulu, HI, USA, pp. 1-6. https://doi.org/10.23919/PICMET.2018.8481969

[27] Nguyen, D.C., Pathirana, P.N., Ding, M., Seneviratne, A. (2019). Blockchain for secure EHRs sharing of mobile cloud based e-health systems. IEEE Access, 7: 66792-66806. https://doi.org/10.1109/ACCESS.2019.2917555

[28] Yue, X., Wang, H., Jin, D., Li, M., Jiang, W. (2016). Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. Journal of Medical Systems, 40(10): 1-8. https://doi.org/10.1007/s10916-016-0574-6

[29] Liu, J., Li, X., Ye, L., Zhang, H., Du, X., Guizani, M. (2018). BPDS: A blockchain based privacy-preserving data sharing for electronic medical records. In 2018 IEEE Global Communications Conference (GLOBECOM), Abu Dhabi, United Arab Emirates, pp. 1-6. https://doi.org/10.1109/GLOCOM.2018.8647713

[30] Steinfeld, B.I., Keyes, J.A. (2011). Electronic medical records in a multidisciplinary health care setting: A clinical perspective. Professional Psychology: Research and Practice, 42(6): 426-432. https://doi.org/10.1037/a0025674

[31] Aldughayfiq, B., Sampalli, S. (2021). Digital health in physicians' and pharmacists' office: A comparative study of e-prescription systems' architecture and digital security in eight countries. OMICS: A Journal of Integrative Biology, 25(2): 102-122. https://doi.org/10.1089/omi.2020.0085

[32] Sookhak, M., Jabbarpour, M.R., Safa, N.S., Yu, F.R. (2021). Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. Journal of Network and Computer Applications, 178: 102950. https://doi.org/10.1016/j.jnca.2020.102950

[33] Fu, X., Wang, H., Shi, P. (2021). A survey of Blockchain consensus algorithms: mechanism, design and applications. Science China Information Sciences, 64(2): 1-15. https://doi.org/10.1007/s11432-019-2790-1

[34] Chan, W. K., Zhang, R., Chan, W.K. (2020). Evaluation of energy consumption in blockchains with proof of work and proof of stake. Journal of Physics: Conference Series, 1584(1): 012023. https://doi.org/10.1088/1742-6596/1584/1/012023

[35] Chiappini, S., Guirguis, A., Corkery, J.M., Schifano, F. (2020). Misuse of prescription and over-the-counter drugs to obtain illicit highs: how pharmacists can prevent abuse. The Pharmaceutical Journal, 305(7943): 1-30. https://doi.org/10.1211/PJ.2020.20208538

[36] Vishwakarma, A., Dangayach, G.S., Meena, M.L., Gupta, S., Luthra, S. (2023). Adoption of blockchain technology enabled healthcare sustainable supply chain to improve healthcare supply chain performance. Management of Environmental Quality: An International Journal, 34(4): 1111-1128. https://doi.org/10.1108/MEQ-02-2022-0025

[37] Zakari, N., Al-Razgan, M., Alsaadi, A., Alshareef, H., Alashaikh, L., Alharbi, M., Alomar, R., Alotaibi, S. (2022). Blockchain technology in the pharmaceutical industry: a systematic review. PeerJ Computer Science, 8: e840. https://doi.org/10.7717/peerj-cs.840

[38] Bandhu, K.C., Litoriya, R., Lowanshi, P., Jindal, M., Chouhan, L., Jain, S. (2023). Making drug supply chain secure traceable and efficient: A Blockchain and smart contract based implementation. Multimedia Tools and Applications, 82(15): 23541-23568. https://doi.org/10.1007/s11042-022-14238-4

[39] Naqvi, F.H., Ali, S., Haseeb, B., Khan, N., Qureshi, S., Sajid, T., Aslam, M.I. (2023). Design and implementation of smart contract in supply chain management using blockchain and internet of things. Engineering Proceedings, 32(1): 15. https://doi.org/10.3390/engproc2023032015

[40] Lou, M., Dong, X., Cao, Z., Shen, J. (2021). SESCF: A secure and efficient supply chain framework via blockchain-based smart contracts. Security and Communication Networks, 2021: 8884478. https://doi.org/10.1155/2021/8884478

[41] Hussien, H.M., Yasin, S.M., Udzir, N.I., Ninggal, M.I.H. (2021). Blockchain-based access control scheme for secure shared personal health records over decentralised storage. Sensors, 21(7): 2462. https://doi.org/10.3390/s21072462

[42] Jamil, F., Hang, L., Kim, K.H., Kim, D.H. (2019). A novel medical blockchain model for drug supply chain integrity management in a smart hospital. Electronics, 8(5): 1-32. https://doi.org/10.3390/electronics8050505

[43] Benita, R., Kumar, G., Murugamantham, B., Murugan, A. (2020). Authentic drug usage and tracking with blockchain using mobile apps. International Journal of Interactive Mobile Technologies, 14(17): 20-32. https://doi.org/10.3991/ijim.v14i17.16561

[44] Andrew, J., Priya, D., Sagayam, K.M., Bhushan, B., Sei, Y., Eunice, J. (2023). Blockchain for healthcare systems: Architecture, security challenges, trends and future directions. Journal of Network and Computer Applications, 215: 103633. https://doi.org/10.1016/j.jnca.2023.103633

[45] Yu, H., Sun, H., Wu, D., Kuo, T.T. (2019). Comparison of smart contract blockchains for healthcare applications. In AMIA Annual Symposium Proceedings, American Medical Informatics Association, 2019: 1266-1275.

[46] Khoi, N., Babar, M.A., Boan, J. (2021). Integrating blockchain and Internet of Things systems: A systematic review on objectives and designs. Journal of Network and Computer Applications, 173: 102844. https://doi.org/10.1016/j.jnca.2020.102844

[47] Sylim, P., Liu, F., Marcelo, A., Fontelo, P. (2018). Blockchain technology for detecting falsified and substandard drugs in the pharmaceuticals distribution system. JMIR research protocols, 7(9): e10163.

[48] Omar, I.A., Debe, M., Jayaraman, R., Salah, K., Omar, M. (2022). Blockchain-based supply chain traceability for COVID-19 personal protective equipment. Computers & Industrial Engineering, 167: 107995. https://doi.org/10.1016/j.cie.2022.107995

[49] Al-Farsi, S., Bensmail, H., Bakiras, S. (2022). Securing blockchain-based supply chain workflow against internal and external attacks. Machines, 10(6): 1-19. https://doi.org/10.3390/machines10060431

[50] Solutions, P. (2020). Blockchain in healthcare. International Journal of Health Information Systems and Informatics, 15(3): 82-97. https://doi.org/10.4018/IJHISI.2020070105

[51] Banerjee, M., Lee, J., Choo, K.R. (2018). A blockchain future for internet of things security: a position paper. Digital Communications and Networks, 4(3): 149-160. https://doi.org/10.1016/j.dcan.2017.10.006

[52] Wang, Y., Kogan, A. (2018). Designing confidentiality-preserving Blockchain-based transaction processing systems. International Journal of Accounting Information Systems, 30: 1-18. https://doi.org/10.1016/j.accinf.2018.06.001

[53] Esteva, A., Robicquet, A., Ramsundar, B., et al. (2019). A guide to deep learning in healthcare. Nature medicine, 25(1): 24-29. https://doi.org/10.1038/s41591-018-0316-z

[54] Su, Q., Zhang, R., Xue, R., Li, P. (2020). Revocable Attribute-Based Signature for Blockchain-Based Healthcare System. IEEE Access, 8: 127884-127896. https://doi.org/10.1109/ACCESS.2020.3007691

[55] Jeet, R., Kang, S.S., Safiul Hoque, S.M., Dugbakie, B.N. (2022). Secure model for IoT healthcare system under encrypted blockchain framework. Security and Communication Networks, 2022. https://doi.org/10.1155/2022/3940849

[56] Rajasekaran, A.S., Maria, A., Rajagopal, M., Lorincz, J. (2022). Blockchain enabled anonymous privacy-preserving authentication scheme for internet of health things. Sensors, 23(1): 240. https://doi.org/10.3390/s23010240

[57] Zhang, C., Xu, C., Sharif, K., Zhu, L. (2021). Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications. Computer Standards & Interfaces, 77: 103520. https://doi.org/10.1016/j.csi.2021.103520

[58] Al Omar, A., Rahman, M. S., Basu, A., & Kiyomoto, S. (2017). Medibchain: A blockchain based privacy preserving platform for healthcare data. In Security, Privacy, and Anonymity in Computation, Communication, and Storage: SpaCCS 2017 International Workshops, Guangzhou, China, December 12-15, 2017, Proceedings 10, Springer International Publishing, pp. 534-543. https://doi.org/10.1007/978-3-319-72395-2

[59] Yang, J., Onik, M.M.H., Lee, N.Y., Ahmed, M., Kim, C.S. (2019). Proof-of-familiarity: A privacy-preserved blockchain scheme for collaborative medical decision-making. Applied Sciences, 9(7): 1370. https://doi.org/10.3390/app9071370

[60] Zheng, Z., Xie, S., Dai, H.N., Chen, X., Wang, H. (2018). Blockchain challenges and opportunities: A survey. International Journal of Web and Grid Services, 14(4): 352-375. https://doi.org/10.1504/IJWGS.2018.095647

NOMENCLATURE

EHR	Electronic Health Record
EMR	Electronic Medical Record
HIE	Health information exchange
MedRec	Personal medical health record
HIPPA	Health insurance portability and accountability act