The Journal of Community Health Management 2024;11(2):71–87

Content available at: https://www.ipinnovative.com/open-access-journals

The Journal of Community Health Management

Journal homepage: https://www.jchm.in/

Review Article

Block chain technology for e-health

Mohammed Sanusi Sadiq[1], **I. P. Singh**[2], **N. Karunakaran**[3]*, **M. M. Ahmad**[4], **B. Maryam**[5]

[1]*Dept. of Agricultural Economics and Extension, FUD,, Dutse, Jigawa, Nigeria*
[2]*Dept. of Agricultural Economics, SKRAU, Bikaner, Rajasthan, India*
[3]*People Institute of Management Studies (PIMS), Kasaragod, Kerala, India*
[4]*Dept. of Agricultural Economics and Extension, BUK, Kano, Nigeria*
[5]*MCA-Google Apps, Suresh Gyan Vihar University, Jaipur, Rajasthan, India*

ARTICLE INFO

Article history:
Received 29-05-2024
Accepted 03-06-2024
Available online 20-07-2024

Keywords:
Information and communication technology (ICT
Evidence-based medicine (EBM)
e-health systems (EHS)

ABSTRACT

There is a dearth of interoperability between apps, data streams, and predictability in the healthcare industry for a significant amount of the data generated by multiple digital ecosystems. Real-time data streams can be derived as meaningful and scalable enough to enable real-time healthcare predictive analytics thanks to the new technology approach in distributed messaging and Blockchain, which has become a fundamental component of many healthcare technology stacks. Additionally, absorbing data streams from multiple sources from patterns of data can enhance models that are hampered by complex and lengthy analyses by raising the level of prediction and accuracy. Improved responses, lowered availability requirements, and unified predictive modeling will speed up healthcare interoperability and, in turn, improve diagnosis accuracy, move evidence-based medicine (EBM) in the right direction, and produce other positive effects on healthcare that improve best results and quality.

1. Introduction

The provision of health services is one of the most important fundamental human rights. In order to provide medical services to people, a variety of health institutions, including hospitals, clinics, and pharmacies, are well-equipped. Information and communication technology (ICT) development has paved the path for the integration of wearable sensors with physical equipment.[1] The efficient and effective collecting, processing, and creation of data over a vast network is made possible by the employment of software and technological devices. Even though there are numerous medical facilities, fatal illnesses, including heart disease, cancer, the flu, and pneumonia, have become much more prevalent and claim a great number of lives.[2] The well-being of patients is regularly monitored and observed by a sizable number of medical professionals, therapists, nurses, and other employees.[3] Chronically ill patients are routinely watched over and evaluated. Various healthcare monitoring systems have been developed over the past few years and are now being used to gather, process, and evaluate data obtained from sensing devices.[4]

One of the best uses of smart technology and networks like the Internet of Things (IoT) is e-health systems (EHS), which offer individuals vital, permanently altering services.[5] People are feeling the effects of these services not just in developed urban areas, but also in rural and, notably, in developing nations. According to statistics, the worldwide e-health market increased tenfold between 2013 and 2018, with patients increasing from roughly 0.35

* *Corresponding author*.
E-mail address: narankarun@gmail.com (N. Karunakaran).

https://doi.org/10.18231/j.jchm.2024.014

million to 7 million, linked devices & services increasing in value from 440.6 million to 4.5 billion, and a compound annual growth rate of 30.8%.[6] By 2025, there will likely be 75.44 billion IoT devices in use worldwide. To cut expenses and boost the standard of care, medical professionals are increasingly using remote communications and monitoring technology.[7] The World Health Organization reports that 87% of nations have already started to implement e-health efforts, and it is anticipated that upcoming 5G technology will further boost this number. The necessity for automated, effective, and unified e-health systems is highlighted by the fact that the skilled workforce (physicians) is not growing at such a rate (Figure 1).

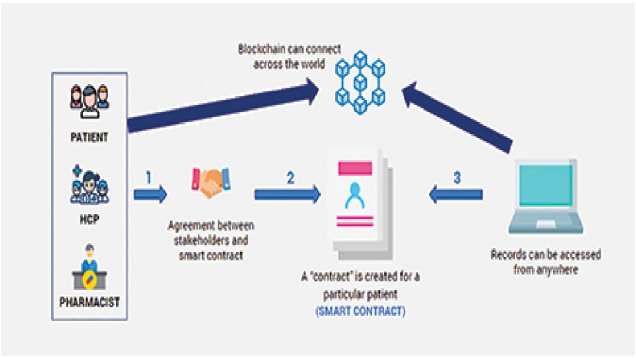

Figure 1: Globalization of blockchain with IoHT

Due to their quick uptake and implementation, Internet of Medical Things (IoMT) devices and networks play a significant role in e-health systems.[8] The majority of the time, healthcare professionals utilize them to monitor patients remotely. IoMT includes body area and body sensor networks, which are made up of diverse devices that produce multidimensional data. A person often uses 2-3 IoT devices in addition to IoMT devices, such as a smartphone with several sensors, a smartwatch, and possibly a smart fitness wearable.[8] Therefore, every patient who uses the EHS makes use of a significant number of IoMT devices, some of which may have been created by different manufacturers and may not adhere to any particular data storage standard. Because of this, the data produced is highly heterogeneous and is typically stored in Relational Databases (RDB) that support Structured Query Language (SQL) on a central server. Additionally, because there are several independent e-health service providers in real-world circumstances, a patient's common history is recorded on numerous different servers, which violates the atomicity of data.[9] The information systems of these health service providers must be consolidated or linked in order to create a national-level (or comparable) health service that can offer superior medical facilities. Data gathering and analysis for illness prediction and prevention on a bigger scale will be improved by doing this since it keeps atomicity while also eliminating data redundancy. Patients will directly benefit from this because all service locations, regardless of who owns them, will have easy access to their medical information. With secure and automated data analysis, blockchain helps build a system that creates and manages content blocks called ledgers.[10] The safe recording and analysis of all health-related data will provide fast updates for medical professionals, healthcare workers, and payers. Incorporating AI algorithms into the blockchain, is advanced.[11] AI has started to learn and think like a clinician in order to understand health trends and patterns. It collects unstructured data from a variety of sources, including the patient, the radiologist, and the pictures (Figure 2).

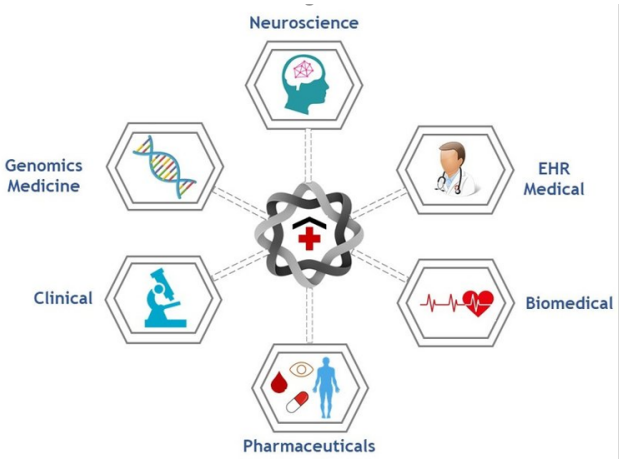

Figure 2: Blockchain applications in healthcare

Building an e-health ecosystem at the national level is fraught with two primary obstacles.[12] The first focuses on the integration and interoperability of current independent healthcare service providers (i.e., hospitals, diagnostic centers, primary health facilities, IoMT applications, insurance providers, etc.). The second relates to the first service provider's system's many internal and external components having secure access to patient digital records.[12] The unified access control measures are made more difficult by the high size and amount of this data. The major goal of the entire national healthcare ecosystem is to make it possible for different service providers to exchange medical data, while keeping the technological and administrative specifics of each process and treatment.[13] Furthermore, a gradual transition towards interoperability is the only viable option rather than completely replacing the current systems. The format of digital assets, the structure of stored data, the application interfaces of information management systems, the types of users, and centralized/distributed networks, to name a few, are just a few of the concerns that must be taken into account during the unification and integration at the national level or even corporate level.[14] In the event that such unification takes place in a situation where a centralized system

links various EHS and permits the exchange of patient records (digital assets) among them, asset security and privacy become crucial. All users (such as patients and doctors) might register on a separate system, and the role-based access control (RBAC) method could be used to set access control policies.[14] However, under a unified system, the same patient might go to another hospital whose doctor might not be known to the first service provider. Access control consequently becomes quite challenging in such circumstances. Similar to this, various users may have varied access privileges to data. For instance, a doctor may have full access while a nurse may only be able to view information on prescribed medications.[15] Additionally, the incorporation of unaffiliated IoMT devices, like smartwatches and health monitors, uploads the data to each server's server. Passive privacy attacks can compromise patient information in a number of ways, starting with device-level permissions, wireless access, and server interaction with the ecosystem.[16] The centralized structure of this approach will also always result in a single point of failure and scalability problems for massive data and storage/access.

2. Block Chain Principles

Recent advancements in technology have made blockchain (BC) a contender for systems that can offer unmatched security characteristics.[17] The history of Blockchain technology is attempted to be explained simply by a number of definitions. A distributed system (distributed ledger) organized into blocks and connected by nodes is one of the most often used definitions of a blockchain. In order to distribute encrypted data safely and instantly across the chain of blocks in the blockchain, mathematical models are used.[18] Therefore, in order to comprehend the definition of blockchain, it is first necessary to take into account the following fundamental concepts.

The phrase "distributed system" has been around for a while in computer jargon and refers to an earlier notion of a computer network where each computer operates independently and is dispersed across a region.[19] Messages are passed between computers (referred to as "nodes") in a system of numerous autonomous processes, which is used a lot more frequently today. Decentralized refers to the absence of a central organization or point of control for transactions, identities, and data storage. The Block merely symbolizes a file; it could be a text file (such as a book chapter), a picture, a sample of a movie, a spreadsheet, or any other type of structured data that contains records that are storable and machine-readable. Information transmission is controlled through a chain-like procedure created by the blocks' connections to nodes (hubs).[20]

Information, or data transmission that refers to one block is what transactions are in reality. They operate on the principle of message dissemination. Simply said, a transaction is a single operation performed across a single node, and since nodes can communicate with one another and move data from one node to another over a network, this is possible.[21] Each node serves as a central hub during the transmission process and has the ability to create and digitally sign the transaction. In a peer-to-peer network, each node must independently verify incoming transactions for their legitimacy, compliance, and conflicts with peers. All of them must be digitally signed and tested in order for the transactions that made it through the verification procedure to enter the memory pool, a local list of the nodes that are still tentatively designated as unconfirmed transactions. They are thereafter passed on to their classmates. The orphan pool, which serves as a temporary holding area, is where all rejected transactions are put.

Cryptographic hashing is another principle that ensures a successful data transport or transaction.[22] The header of each data block must be cryptographically hashed using the SHA-256 cryptographic hash technique. The parent block's hash is also included in the header. Each block contains the hash of its parent to complete the linear list of blocks and construct a sequence, forming a chain that goes all the way back to the first block ever made. The genesis block refers to the first block in the chronology. The parent (prior) block of information, including the timestamp (date-time), origin, and originator, is linked to each block in the blockchain. Figure 3 shows a condensed representation of the blockchain.

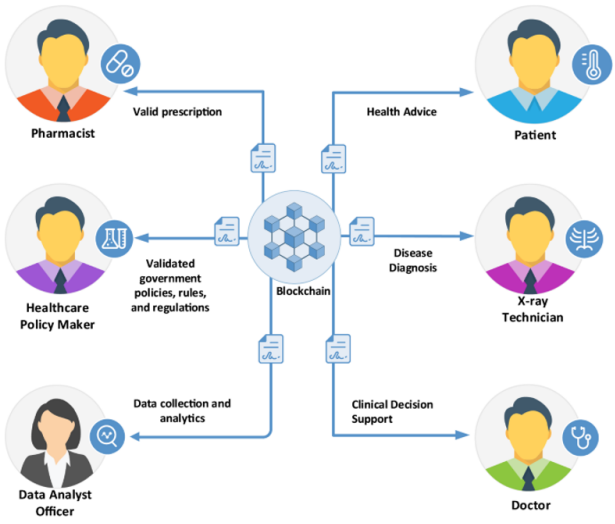

Figure 3: A condensed representation of blockchain

Blockchain has mainly been used for cryptocurrency, but it can also be used in other fields, including IoT, asset monitoring, access control, and corporate operations.[23] Additionally, the qualities of its immutability of ledger,

user anonymization, support for encryption, and validation through multi-peer consensus can be incredibly helpful for e-health systems.[24] A consensus process is used in the peer-to-peer decentralized networking system known as blockchain to authorize any type of transaction. Between two system users, a transaction might be the exchange of information/data, digital assets, or cryptocurrencies. Through a vote procedure among network peers, consensus is the mechanism used to validate and legitimize a transaction so that it can be included in an immutable block. A pre-established smart contract (also known as chaincode) among the users who are transacting serves as the foundation for the validation. The block in which transactional data is stored is connected to the block before it in a chain structure by the hash value.[25] A single point of failure is removed by storing this structure in the ledger, where every peer retains the same data. The potential for malicious change after commit is also removed by the fact that the data contained in blocks is both encrypted and immutable. The majority of blockchain systems currently in use are designed for cryptocurrency exchange or payments; as a result, they are unsuitable for tracking or exchanging digital assets. For complicated commercial applications that require business logic to be included in smart contracts, Ethereum and Hyperledger Projects (Fabric, Sawtooth, Iroha) are more viable alternatives. In the blockchain, the ability to create transactions has an impact on access control. The permissions of the participants to transactions are determined by the smart contract in this predominantly role-based system.[26]

3. Block Chain: Private vs. Public

Blockchain is a shared ledger: blockchain can be either a public or a private network from the perspective of the authority because there are numerous parties involved in transactions exchanging the data that is headed by cryptographic keys.[27] Depending on the technology you require, there is a significant difference. Additionally, it depends on the guiding principle of not allowing anyone to make changes to your blockchain or those of a well-known and thoroughly vetted participant. The initial one, referred to as "public," refers to the connotation that people frequently ascribe to the blockchain when they discuss it.[28] This essentially means that anyone can read or write data without specific authorization from a third party. This one is also referred to as a blockchain with no permissions. Despite the ease with which permission to use blockchain may be regulated, there is a larger chance that security will be compromised. The second, and undoubtedly most well-known, is the private blockchain. It is a blockchain with known participants that operate under permissions. In their industrial group, for instance, they are trusted; therefore, many of the permission methods are not required. Legal contracts are occasionally used to replace them. Another point of worry in the application of this new technology is the question of private versus public blockchain. Critique on top of vulnerability is the first of them. Someone will eventually identify a flaw in the smart contract's coding loop. In June 2016, this already occurred.[29] If a majority of validators abide by the rules and establish a stronger (also less expensive) immutability, such as one produced by using the private blockchain, this or something like that should be overridden. Additionally, the general public will have more access to using a private blockchain. It will be helpful and acceptable as long as both or one achieves the fundamental requirements of data immutability, smart contracts vulnerability preservation, and the preservation of anonymous information during transactions by agreement with authentication.[30]

4. E-Health and the Block Chain

A distributed database using state machine replication, the blockchain ensures the integrity and tamper-resistance of the transaction log through hash linkages between blocks.[1] Atomic database changes, known as transactions, are grouped into blocks. In the context of decentralized electronic currency, the blockchain concept was first introduced for Bitcoin. Because of the success of Bitcoin, blockchain technology can be leveraged to provide secure and reliable transactions across an unreliable network without the need for a third party. On the fundamental building components of the blockchain, there have been numerous reports. Blockchain is a logical collection of blocks that each contain a list of accurate and comprehensive transaction data. A chain is formed by the blocks' relationships (hash values) to one another.[31] The initial block is known as the block of genesis, and the block that comes before a specific block is known as its block header.[15] Blockchain technology has become extremely popular and advanced to distribute safe and stable monitoring of medical records due to a growing interest in a variety of applications, ranging from data storage, financial markets, computer protection, IoT, and nutritional science to the healthcare industry and brain studies. By combining and showing all real-time clinical records of a patient's welfare in a modern, secure healthcare setting, it might be a tool that, in theory, helps with individualized, trustworthy, and safe treatment.[32]

The proposed solution assesses the patient's general state, diagnosis, and recovery system using a blockchain platform that focuses on concurrent execution and artificial intelligence in healthcare networks.[33] Additionally, it explores the pertinent surgical interventions by concurrent operations and computational clinical decision-making studies to evaluate the standard of care for patients and the viability of diagnosis. The suggested technique has been assessed in real-world and simulated healthcare systems. Tagde et al. (2021) reported that Singh and Kim

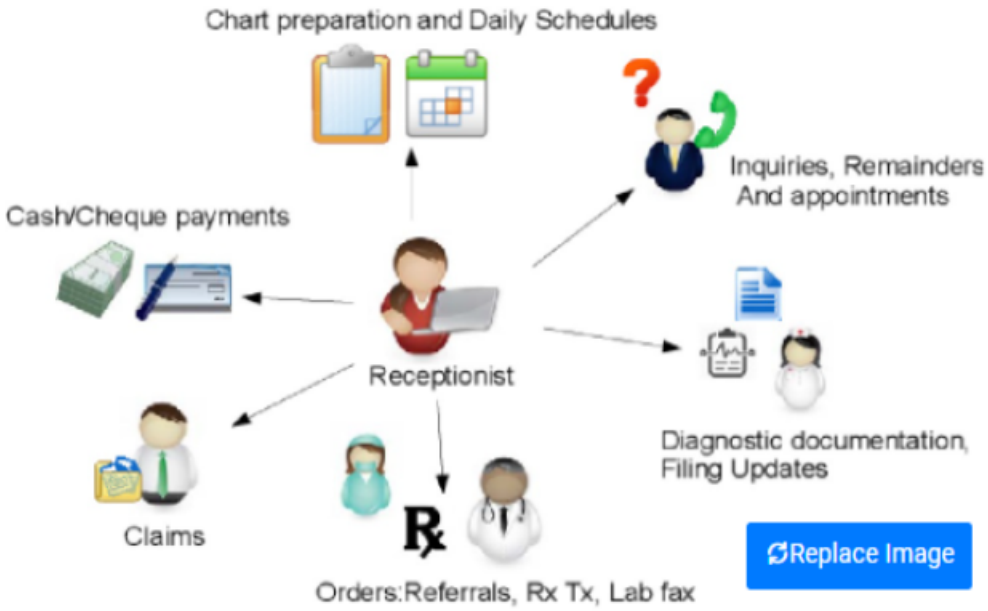

Figure 4: Health record management through blockchain technology

(2018) developed CHIE, a particular blockchain-oriented healthcare knowledge-sharing network. The proposed platform assesses the requirements for the exchange of health care data, particularly for personal health data and electronic medical reports, and discusses a variety of other data types by integrating blockchains within different sources. To ensure that the application met good criteria for validity and privacy, they coupled it with on-chain and off-chain authentication mechanisms. The use of blockchain technology to exchange medical records and provide clinical staff, healthcare organizations, and patients with anonymity and protection can be considerably increased.[34] An analogous technique adopted by Cryan suggested a methodical and inventive architecture utilizing blockchain technologies to secure private patient records, address fundamental data protection issues, and launch a blockchain software framework for use across hospitals. Blockchain technology has also shown enormous promise in the medicinal and therapeutic fields. Even prior to starting a clinical study or test, it may be able to store all clinical approvals, schedules, and protocols on a blockchain through the practical implementation of blockchain technologies.[35] This will improve the accuracy, security, timeliness, and transparency of crucial clinical trial-related information (Figure 4).

5. The E-Health Solutions

5.1. E-health security measures that are customary

The majority of contributions focus on effective security and privacy assurance by incorporating additional processes into the current centralized architecture because it processes everything at a single location in the centralized architecture (Sultanaet al., 2020). A three-factor authentication technique employing both asymmetric and symmetric crypto-systems was proposed as a way to meet most security requirements. The majority of these contributions are key-based access control solutions (public/private keys, biometric keys, etc.). The limits of three-factor key authentication-which is vulnerable to insider attacks-are discussed, and a novel three-factor system based on the discrete logarithm issue for elliptic curves is suggested. To propose a new system, which is more expensive than the previous one, the authors also included other discoveries such as meaningless user identification, no session key, no mutual authentication, and impersonation assaults. One person serves as both the data owner and the data retriever in the system that Jeetand Kang (2020) presented, taking user-centric security concerns into consideration. To access or submit transactions, this scheme employs authentication key agreement mechanisms. Numerous service providers in an EHS frequently have access to the patient's data. In light of the problem, Ghazalet al.(2022) present multi-user Searchable Encryption Schemes (SES), which are capable of preventing data leaking. The strict consideration of data

encryption or storage security is not given, despite the authors' main focus being on multi-user access control on cloud-based servers. The authors of (Abdellatifet al., 2021) suggest a SES-based EHS that supports encryption, reoccurring data storage on the cloud, and multi-user access keys. Additionally, it is asserted that the monitoring of distant patients and support for interoperability in intra-EHS services. Abdellatifet al.(2020) addresses the difficulties that such centralized e-health systems encounter. Interoperability makes it possible for EHSs to interchange data in a flexible manner, but it also raises issues with privacy leaks. The authors of (Velliyangiri et al., 2022) provide a hash-based dynamic privacy protection technique for biometric authentication. All transactional and authentication data are kept anonymous, yet they are all kept on a single server. The cloud-based access control system that is immune to inference attacks is discussed by the authors (Kondepogu and Andrew, 2022). For precise access control, they provide a two-layer encryption system, and to assure anonymity, they suggest a blind data retrieving protocol. A smart card and password-authentication based system has been presented in (Radjenovic, 2020) to mitigate the denial of service (DoS) attack. Due to centralized storage, it tackles DoS difficulties; however, a multi-user authentication-based approach is not feasible. The single point of failure and interoperability with various EHS remain problems for all of the key-based security and privacy solutions mentioned here for a centralized e-health system. E-health solutions built on the blockchain: Research on the subject of blockchain and e-health has been conducted, mainly with the goal of enhancing security capabilities inside centralized e-health systems. The research in (Kondepogu and Andrew, 2022) suggests a pairing technique for data sharing in EHS utilizing BC, but it does not outline the whole architecture for IoMT integration or unification at the federal level. Similar to Kayasthaet al. (2021), Chelladurai and Pandian(2022) give ideas about HoT devices and BC integration while Kadam and Motwani(2022) propose a BC-based continuous patient monitoring & data management. Core integration issues, digital asset management, access control to digital assets, and transaction/block size restrictions are not taken into account in these works (such as 1MB in Bitcoin.

5.2. E-health solutions built on the blockchain

Research on the subject of the blockchain and e-health has been conducted, mainly with the goal of enhancing security capabilities inside centralized e-health systems. The research in (Kondepogu and Andrew, 2022) suggests a pairing technique for data sharing in EHS utilizing BC, but it does not outline the whole architecture for IoMT integration or unification at the federal level. Similar to Kayastha et al. (2021), Chelladurai and Pandian (2022) gives ideas about HoT devices and BC integration while Kadam and Motwani (2022) proposes a BC-based continuous patient monitoring & data management. Core integration issues, digital asset management, access control to digital assets, and transaction/block size restrictions are not taken into account in these works (such as 1MB in Bitcoin).

5.3. Access control with blockchain

Access control has been provided in a variety of domains to some extent using BC. Meisami et al. (2021) describe a distributed key management architecture based on BC for cross-domain access that satisfies IoT access control and fine-grained auditability. It suggests a key management security access manager that is comparable to the peer of a general blockchain. The authors of Meisami et al. (2021) provide a decentralized design for IoT application access control, and BC is utilized for decentralization security. They make use of a delegation of permissions system, in which a set of permissions is assigned to IoT users or devices and continually verified. Only permission delegation services based on the smart contract of the device owner are used by BC. However, because there may be millions of IoT devices with various access requirements, making a smart contract for everyone would be expensive and inefficient.

5.4. Access control in EHS using blockchain technology

Certain specialized studies have concentrated on using BC to provide access control in EHS. Kadam and Motwani (2022) put forth a BC-based electronic health record (EHR) system that, by utilizing a collective authority, enables interoperability and integrity of data records. The abrupt changes in permits (and hence the use of smart contracts), many EHS for the same patient, and massive amounts of medical picture data are not taken into account. Additionally, a private or consortium blockchain does not require the usage of incentives for block creation. For safe access to patient medical histories, authors in Mukherjee et al. (2021) use BC. It demonstrates how doctors can access patient information and perform mutual authentication among patients with common conditions. Using a keyword search & encrypted answer-based access control mechanism, Mukherjee et al. (2021) proposes a BC based privacy-preserving EHR sharing protocol. But each of these answers only deals with a single problem and offers a fairly straightforward solution.

6. E-Health Block Chain Use Cases in Healthcare

6.1. Transparency in the supply chain

Healthcare, like many other industries, places a premium on the guarantee of medicinal commodities' origins to establish their legitimacy.[36] Using a blockchain-based

system, consumers can monitor products from the point of manufacture to every stage of the supply chain, providing them with complete visibility and transparency over the items they are purchasing.[36] This is a major issue for the sector, particularly in developing nations where fake prescription pharmaceuticals result in tens of thousands of fatalities each year. Additionally, as more telehealth monitoring is installed, its importance for medical equipment is increasing quickly, piqued the curiosity of dishonest actors. A well-known blockchain platform called MediLedger enables companies in the prescription drug supply chain to verify the legitimacy of medications, as well as their expiration dates and other important details.

6.2. Smart contracts

To preserve transparency across all phases of a medical study, smart contracts may also be used, repeated, and then enforced. A blockchain, in the traditional sense, is used to process a smart contract, which is a script.[19] It was found that malignant cells can be found and managed via a blockchain-based telemonitoring healthcare system for far-off patients. The proposed approach includes smart contracts and blockchains, which are commonly utilized to ensure the confidentiality and authenticity of patient data in highly developed hospitals and outpatient facilities. In a different study, a blockchain-based system called Dermonet was offered as a way for patients to receive online dermatological consultations and teledermatology monitoring.[37]

On the other hand, a blockchain-based network called proactive aging encourages older individuals to lead active lives. Recall that chronic diseases (like cancer), surgical operations, and aging may all benefit from the use of blockchain technology as an effective and well-suited solution. Additionally, it might be possible for pharmaceutical businesses, medication manufacturers, and biomedical researchers to employ DNA knowledge stored on blockchains to undertake enhanced global analysis at the genomic level. The blockchain should incorporate smart contracts to make transactions between various parties considerably faster and more effective.[8] The concept was first presented by Nick Szabo in 1994.[1] In his proposal, he defined a smart contract as "a process that enables computers to communicate and implement the terms of a contract" and suggested converting contract clauses into code to eliminate the need for counterparties to coordinate amongst groups. A smart contract has a destination identification on a blockchain, as reported by Tagde et al. (2021). By providing the blockchain address, a smart contract can be rapidly generated for use in trade. Depending on the information in the transaction, it is manually executed on each network node separately.[38]

6.3. Electronic health records that focus on the patient

Healthcare experts, hospitals, and healthcare equipment have been the primary drivers of the need for a sharp increase in digital technology of medical health data over the past few years.[39] This is because digital technology of this knowledge enables more accessible communication and control and serves as the basis for better and quicker decision-making. Electronic medical records currently use blockchain technology in healthcare in the highest numbers.[40] However, individuals leave their data fragmented across multiple institutions when life circumstances isolate them from the data of one provider through another, and as a result, they lose simple access to historical data. Electronic health records (EHRs) are never generated between numerous organizations to maintain everlasting information. Since there is a critical need for a novel approach to handling EHRs that enables patients to share their current and traditional health data, several researchers have raised the issue of blockchain application verification to protect the EHRs. A "MedRec" prototype makes use of unique blockchain benefits to handle security, honesty, and quick data sharing. It offers patients a full, permanent background and works on a decentralized basis to retain data and claims. It also gives patients quick and simple access to their own clinical records across numerous providers and care facilities.[1] Medical papers would not be preserved by "MedRec" or cause an adaptation period to start. It notifies the patient who is responsible for where the form will go and stores a record label on a blockchain.

Inadequate control over data, data provenance, monitoring, and safety monitoring of medical information throughout the deployment of EHR are just a few of the serious problems associated with medical data exchange during the implementation of EHR. MeD Share has been made available as a safe blockchain framework for exchanging medical data between unreliable parties while keeping in mind some restrictions. MeD Share can be used by cloud service providers, doctors, and healthcare research organizations to share medical data and keep electronic health records with high information authenticity, tailored audit authority, and minimal possible dangers to data protection and privacy. EHR typically contains extremely private and crucial patient information that is shared for effective diagnosis and treatment by doctors, neurosurgeons, healthcare providers, and scientists.[7] The majority of professionals with the patient seem to notice things right away when a hospital visit starts. Without the requirement for laborious forms of pharmacological compromise, medication errors, hypersensitivities, and medication solutions may be reasonably readily accommodated across blockchain records by useful patient-caring algorithms. Therefore, the application of blockchain innovation would support better patient access to care, oversight of medical records, faster validation of clinical knowledge, improved

surveillance, and more efficient care organization.

6.4. Verifying the credentials of medical staff

Similar to how they can be used to trace the origins of a medical good, cryptographic method can be used to track the experience of medical personnel. Credentials of staff members can be logged by reputable medical facilities and healthcare organizations, which streamline the employment procedure for those organizations. Using the R3 Corda blockchain protocol, ProCredEx, a company based in the USA, has developed a system for verifying medical credentials.[1] According to Tagde et al. (2021), the blockchain system has the following primary benefits:

1. Healthcare firms will be able to obtain credentials more rapidly during the hiring procedure.
2. A possibility for healthcare organizations, insurers, and medical institutions to make money off of the credentials information they already have on former and present personnel.
3. Openness and guarantee for partners, such as businesses that subcontract locum tenens or those involved in developing virtual health care models, to inform patients of the qualifications of medical staff.

The gathering, distribution, and dissemination of this highly personal patient information to several entities could have an impact on the patient's care and carry serious dangers to the patient's welfare and background information.[8] Due to a lengthy history of pre- and post-treatment, obey, and recovery, the incidence of such hazards may rise in patients with chronic illnesses (such as leukemia and HIV). Maintaining a current medical background has, therefore, been very important. When Estonia pioneered the idea of keeping millions of medical records private while making them accessible to insurance companies and medical professionals at the same time in 2016, it established itself as the world leader in blockchain technology.[1] The express promise that patients can use this technology to create their own records may be the reason for the growth of blockchain technology in medicine globally. Any attempt at access or modification may be clearly identified and remembered in the blockchain. This protects patient confidentiality and reveals any criminal activity, such as large-scale fraud or record tampering.

6.5. Remote monitoring with IoT security

One of the biggest advancements in digital health is the usage of remote monitoring technologies, in which all types of sensors detecting patients' vital signs are used to help give healthcare practitioners improved visibility into patients' health, enabling more proactive and preventative care.[20] Health IoT security is a key worry, though, as it must be kept secure and private while also guarding against data manipulation to produce false results. It is equally important that the supporting systems are extremely resilient to attacks that disrupt service in some scenarios where a connected device may be relied upon in an emergency, such as warning an old person's career that they have fallen or had a heart attack. In the field, IoT devices could be more securely monitored with the help of blockchain technology because:

1. Using a unique hash function, personal information is preserved on the blockchain, and blockchain cryptography ensures that only people with the proper permissions can access it. Any modification to the source data will result in a new hash function, which can only be decoded into the original data by a user who is in possession of a specified set of cryptographic keys.
2. Because doing so would require having access to all stored copies, altering patient data once it has been recorded on the blockchain ledger (as a hash function) is practically impossible.

6.6. Tracking drugs and clinical trials

1. A medical strategy used to identify and prevent disease is clinical trials. To prevent and identify diseases, numerous systems have been developed in recent years.[17] Data integrity, record-sharing, data privacy, and patient enrollment are some of the weaknesses in existing systems, which blockchain technology can address. The clinical healthcare systems listed below offer data integrity and privacy. Healthcare is a token-based system for tracking data on, among other things, insurance providers, hospital staff, physicians, and health plans. Using smart contracts, the FHIRChain smart health system enables the interchange of clinical healthcare data.
2. The blockchain-based record-sharing tool Connecting Care is similar and is available in numerous English cities.[1] Connecting Care is used in a diverse healthcare organization to safeguard information about hospitals and other medical record data. In order to guarantee that only those with permission can use the clinical system, it offers an access control list. The implementation of blockchain smart contract functionality uses an Ethereum-based framework. The Healthcare system uses an enrolling approach to sign up a patient. The patient can enter their personal information into the system and the authorities have access to their medical records.[23] Blockchain-based clinical settings will surely create new scientific potential for the advancement of medical research. On the other hand, the dependable, secure, and scalable gathering, storing, and retrieval of these medical studies in applications for precision medicine can help create attractive potential for the diagnosis and

treatment of illnesses. An online database could be used for cognitive systems. Blockchain technology may be used to process a digitized brain, and neurotechnologies are still in the experimental phase. Few companies have even announced a position for blockchain technology.

7. Block Chain for the Healthcare Sector

Although the technology has been in use since 2009 and is one of the key elements utilized to exchange the digital currency Bitcoin, blockchain was a big topic in 2016.[24] The system receives significant funding and attention from the National Health Information Technology Manager due to its potential to solve numerous fundamental healthcare issues. With the constantly evolving technological landscape, it would be possible to govern and transfer electronic health records while maintaining confidentiality, interoperability, a standardized shared infrastructure, and international standards.[27] IT executives understand that their objective is to implement the right health IT trends and technologies as healthcare continues to advance relentlessly. To avoid becoming early adopters of cutting-edge technology that jeopardizes a patient's health, health IT administrators must exercise caution. One of the global industries with the quickest growth is the pharmaceutical sector. It is a key factor in patient outcomes and helps get cutting-edge, possibly helpful therapies to market. It upholds the standard and effectiveness of medical products sold under prescription to the general population.[32] Additionally, it facilitates the diagnosis and processing of sterile drugs, hastening the recuperation of patients. The majority of the time, drug manufacturers struggle to quickly monitor their products, which may offer serious hazards by encouraging counterfeit goods to undermine manufacturing or penetrate the system for counterfeit pharmaceuticals. Its manufacture and dissemination, as a result, pose a serious threat to global health, particularly in industrialized nations. For testing, monitoring, and ensuring the manufacturing procedures of possible medications during their manufacture and research and development (R&D), blockchain technology may be the ideal option.[34] In this context, a long-term option for preventing illicit substances could be an automated drug management system (DDCS). Sanofi, Pfizer, and Amgen, three major pharmaceutical corporations, launched a joint pilot initiative to examine and evaluate investigational drugs utilizing a blockchain-based DDCS (Figure 5).[1]

Blockchain, which may be configured to record online financial transactions in a safe and unchangeable manner, is essentially a distributed ledger (database).[33] Each transaction on the blockchain is digitally signed by participants to guarantee its security and legitimacy. Consensus rules the distributed ledger's operation (smart contracts). Each transaction will be recorded in a block and validated by both parties in the ledger before being added

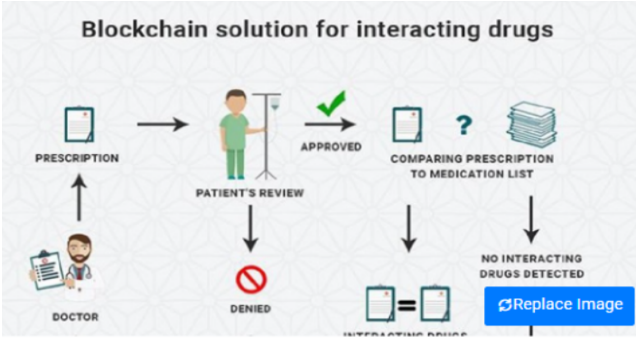

Figure 5: Blockchain solution for interacting with drugs

to a chain. Each block includes information and data.[1] Last but not the least, the chain is secured by encryption techniques, making it impossible to alter or modify. Due to the decentralized nature of blockchain technology and the several copies that exist on various servers, no one is able to change transaction data. Cybercrime is a threat to data resources kept on centralized systems. As opposed to this, blockchain stores data in decentralized locations to guarantee its security and anonymity.[41] Blockchain technology's market worth significantly expanded during the last few years. In comparison to all previous record-keeping methods, blockchain technology is more reliable and secure. All nodes in the network share the same documents in this distributed ledger. By using blockchain technology to automate the conventional procedure, it is also used to boost efficiency and speed. Because it does not necessitate the purchase and sale of goods through intermediaries, it also lowers expenses.

7.1. *Immutability*

The time stamping of a ledger, its connection to other ledgers, and its access to earlier documents form the foundation of the blockchain data structure. Due to its decentralized nature, the blockchain can be used to store any type of record in industries where legitimacy, authenticity, and auditability are crucial, including healthcare, banking, and supply chains.[42]

7.2. *Decentralized agreement*

A blockchain's resilience comes from its decentralization. The two factors that prevent the blockchain from being tampered with are encryption and immutability. However, it is a decentralized agreement that puts it into action. This company will alter a blockchain where all networks are controlled by a single entity or company. Just the blockchain nodes who want to approve the activity are required.[43] Due to the fact that several parties with conflicting motives must agree by means of decentralized consensus as to what

counts as a legal transaction, it is far more difficult to undermine the consistency of the blockchain. Because it is highly unlikely that far more than 50 percent of the nodes would knowingly agree to corrupt the blockchain data in this situation, numerous businesses running a few nodes each is the most effective strategy.

Integrated incentives

An individual member of the network must perform specific tasks, such as preserving data and validating transactions, in order for a blockchain to transform networks into markets at a high level. The node is a distributed ledger system that offers a secure, decentralized, distributed information repository that is tamper-proofed, and it generates some profit in proportion to the effort done to make up for that task. A community of untrusting people can work together and conduct business without the involvement of outside parties, thanks to the trustless method provided by blockchain. Additionally, it offers a shared data archive in place of hierarchical records management for transaction processing, allowing each peer in the network to have a copy of mirrored data. Any consensus process is handled by the network for data replication, exchange, and synchronization between peers. The digital currency is built on a set of communication protocols that allow for the shared management of transactions among numerous computing devices that are spread out geographically.[44]

Since its introduction in 2000, the term "blockchain e-health" has become widely used in the healthcare sector to refer to information and communication technologies (ICT). Through the Internet and related technologies, it can provide innovative solutions for the medical industry, including those for applications like medical informatics, patient healthcare, healthcare practitioners, healthcare staff, medicine, etc., related to clinical insurance and health information. Patients can obtain their medical history and information about care if knowledge or data are easily accessible through increased software, applications, and mobile devices.[45]

8. Data Efficiency and E-Health System Security

To maintain the integrity, confidentiality, and dependability of health records and health reports that include all wearable sensor results and patient treatment records from service facilities, the storage and management of medical details require a uniform notion of access control, validation, and immutability of data.[46] Role-based permission should be required for data upload and processing due to the sensitivity of the data and the privacy and confidentiality involved in maintaining medical records. The requests can be recorded and documented, and access can be gained to the tracked data, using auditing mechanisms. Blockchain provides an effective framework for creating a private/public network with a secure information access management system for multi-party organizations. Recently, researchers have looked into the potential of blockchain to create a reliable, decentralized network for data sharing. To encourage clients to keep their medical information up to date, a solution for doing so using a private blockchain and the launch of the Healthcare Data Gateway (HDG) has been found. Individual healthcare information system was proposed by Casado-Vara et al. (2018) as cited by Tagde et al. (2021) to be integrated into the distributed digital blockchain, where patient records are authenticated and stored openly. However, there are several drawbacks to blockchain technology in terms of where blockchain data is stored.[47] So far, there haven't been many attempts to leverage blockchain as a catalyst for reliable healthcare networks. They employed digital currency and blockchain to support the processing or governance of the knowledge but rejected blockchain as a data layer. Monitoring and managing encrypted off-chain data was to be done using blockchain-based decentralized user authentication. In the absence of precise clinical data in the blockchain, FHIRChain is a healthcare utilization paradigm, and a health data-sharing mechanism managed through a smart contract. Scalability, limited interoperability, a lack of blockchain developers, inadequate standards, high energy consumption, and a lack of regulatory certainty are some of the issues the technology faces that have delayed development.[13] Along with the difficulties in using blockchain technology that have been described as follows, there are fundamental priorities in installing secure blockchain-based EHR systems. Adoption of blockchain is facing difficulties, and deploying safe blockchain-based EHR systems is a top priority (Figure 6).

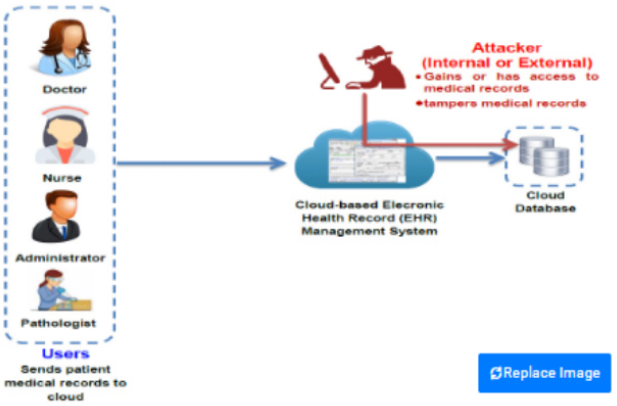

Figure 6: Security risks in conventional cloud-based electronic medical records

8.1. Security challenge

8.1.1. System bugs

1. Security weaknesses can be exploited by malicious software to build decentralized applications based on the established blockchain.
2. In order to facilitate other crimes like identity theft and data theft, these malicious assaults take advantage of security holes in the implementation of smart contracts.

8.1.2. Secure blockchain deployment's top priorities

The following three objectives must be met:

1. Privacy: The data is only accessible to authorized users.
2. Dignity: Information must be accurate while in transit and cannot be altered by an unauthorized organization.
3. Accessibility: Services and information are not unjustly withheld from legitimate users.

8.2. Confidentiality challenge

8.2.1. System bugs

Presenting a framework for data privacy and integrity on a blockchain-based EHR that makes use of cryptographic techniques is the key difficulty in ensuring patient data privacy.

1. By using his current account number, it is impossible to identify a specific patient thanks to this function. The shortcomings in the safeguarding of patient data in any system like that should be fixed.
2. Since using blockchain-based frameworks within EHR requires a lot of computing power and takes a while to complete each task, patients ought to first be able to interchange their data with ease.
3. Second, new patients must add a new node to the blockchain network, which calls for a number of steps to confirm the patient's reliability.

9. A Secure Block Chain Deployment's Top Priorities

For public blockchain privacy protection in healthcare applications, the following conditions must be satisfied:

1. No links between transactions should be visible or accessible.
2. Only the parties involved in the transactions should be given access to their information. To meet the criteria for data security, a healthcare application built on a private or consortium blockchain can put up an access control policy.
3. In a public blockchain environment, the privacy protection of transactions is a "double-edged sword." On the one hand, a well-behaved patient wants to maintain the privacy of his identity and behavior.
4. However, a rival party might utilize the privacy protection system to carry out a criminal transaction. The security of blockchain transactions in healthcare applications may be restricted from the perspectives of legal traceability and accountability, ensuring the authority's reliability.
5. The best way to keep track of a specific user and gather all of his messages while maintaining the user's sensitive information's privacy is something that researchers should investigate.
6. From a development perspective, one interesting research issue is how to increase privacy in a blockchain with unreliable underlying assumptions and cheap processing costs.
7. A potential method for permitting an unreliable third party to compute on patient data without violating their privacy is secure multiparty computing.

9.1. Scalability challenge

9.1.1. System bugs

1. Another issue with IoMT devices is their increased overhead or processing resources due to their lack of scalability.
2. This difficulty could lead to an increase in the overall processing demands on the blockchain infrastructure.
3. The issue becomes even more difficult when there are many smart devices or sensors present because their computing power is inferior to that of a standard computer.
4. Data latency and high processing power are caused by the computationally intensive and high overhead bandwidth IoT devices in the blockchain network.
5. These devices might not have the processing power necessary to use blockchain features, requiring them to operate at subpar or even excessive speeds, preventing them from running both their original software and blockchain software at once.

9.1.2. A secure blockchain deployment's top priorities

Studies are being conducted on the scalability of blockchain in healthcare applications as the volume of medical data increases.

9.2. Interoperability challenge

9.2.1. System bugs

1. Blockchain interoperability is the ability to send data, conduct analyses, and handle allocations across several blockchain networks without the use of a middleman or central authority. The lack of interoperability may make mass adoption all but impossible.
2. Blockchain technology is decentralized and cloud-based, in contrast to the centralized local databases and offline architecture used by current EHR solutions.

3. The creation of an efficient EHR system capable of creating linkages and interoperability across both medical and scientific communities will be required in order to move healthcare systems in this path and include blockchain technology.

9.2.2. Secure blockchain deployment's top priorities

1. Interoperability efforts to close the gap between various blockchains have increased, according to researchers. Numerous them attempt to connect private networks to public blockchains or the other way around. Prior strategies that focused on open blockchains and cryptocurrency-related tools were ultimately less beneficial to corporate executives.

9.3. Anonymity challenge

9.3.1. System bugs

1. Bitcoin blockchain and Ethereum, which function as public ledgers, need that all transactions be automatically available.

9.3.2. Secure blockchain deployment's top priorities

1. Rather than using usernames or passwords, the Ethereum network offers pseudo-anonymity. For instance, transactions are linked to addresses that are public keys that are generated from user-held private keys.
2. A user can verify a transaction using General Ethereum, also called as zk-SNARKS (zero-knowledge succinct non-interactive proof of knowledge), without seeing the transaction's underlying data or conversing with the user who aired it.
3. Zk-SNARKs, in the setting of a blockchain, enable participants to keep their payments confidential while still validating them in accordance with the network's consensus process.
4. Once implemented, companies will be able to conduct business on the same network as their rivals in complete secrecy while gaining access to the public Ethereum blockchain's security.

9.4. Latency challenge

9.4.1. System bugs

1. Blockchain integration into medical applications that demand real-time responses to situations and data may be problematic because it will take time for consensus to form and transactions to be confirmed. Transaction latency is the amount of time it takes a blockchain to process a transaction.
2. For instance, the network must wait 10 minutes for each transaction to be confirmed on the bitcoin blockchain. It is advised that each transaction be verified in one hour, even though five or six additional blocks must be included in the chain before confirmation. However, the majority of conventional database systems only need a short while to confirm a transaction.

9.4.2. Secure blockchain deployment's top priorities

1. Less latency has been associated with blockchain-based Internet of Things devices, but it can also be used in other blockchain applications.
2. A network with delay is necessary for the IoT network since many devices are communicating with one another simultaneously.
3. The consensus mechanism certifies each block's transaction, greatly reducing delays that would otherwise negatively impact the performance of the application.

10. The Difficulties of Unifying Block Chain and E-Health

The application server, database, password protection, and certification authority are all located in one location due to the centralized architecture of existing independent e-health systems, which leads to a single point of failure.[24] They are typically found on the same subnet, which is vulnerable to attack, even though they are different physical devices. A solitary point of data leaking results from this as well. Transferring information is another crucial element because a patient can eventually visit several different care providers. The previous medical records are frequently unavailable since there is no direct linkage between the various EHS. The cooperation between EHSs must take place at a higher level of management and may be impeded by procedural and administrative concerns, despite the fact that this activity can be automated. Last, but not least, all users have the same access to information because it is defined as a system component and not controlled by the patient. Although this is not a disadvantage, the patient should have full control over their information since they are the owner of it. A blockchain-based e-health system can be built to address these problems. However, this movement faces a number of difficulties, which are outlined below:

1. Design: Resolving network type disparities since different networks differ in their nature and architecture, such as whether they are centralized or decentralized.
2. Synchronization of transactions: While centralized systems handle transactions synchronously, several peers in the BC network handle huge concurrent transactions.
3. Data atomicity: It can be difficult to maintain the atomicity of earlier data. Medical information about a single patient is stored on numerous separate servers

in various ways, with or without timestamps, and this data may contain contradicting information.

4. Data migration: It is not possible to directly migrate all old record to the BC system. Previous records with outdated timestamps cannot be accepted by BC ledger. Each new transaction must include a timestamp that is up to date.
5. Data types: Due to capacity restrictions, which include 1MB for Bitcoin and 8MB for HDAc, adoption of medical photos and documents in the BC block is not possible.[26] However, with an e-health system, substantial medical photos and documentation are always included in the data. Additionally, data can be produced by various devices at various rates, such as an IoMT sensor as opposed to an MRI.
6. User types: Different user types have different needs for access management. A patient receives services from a variety of service providers, including doctors, diagnostic facilities, nurses, and others, and each one may have a different set of access requirements.
7. Access limitation: It's crucial to restrict a patient's access to their current provider. A patient may request that the previous doctor not access new information, and this request may change regularly. Similar to that, anonymization may be necessary before releasing the data. As a result, capabilities for transaction generation must be coupled with role-based access control.

11. IOT Data Sharing, Safeguarding, and Confidentiality E-Health Records Using Block Chain

The use of blockchain technology to advance healthcare and e-health services has recently attracted increasing interest.[27] With its decentralized and reliable nature, blockchain has proven to have enormous potential in a number of e-health industries, including the secure exchange of Electronic Health Records (EHRs) and the management of data access among numerous medical institutions.[42] Consequently, the implementation of blockchain technology can offer potential solutions to simplify healthcare delivery and radically alter the healthcare sector. Electronic health records (EHRs) are increasingly being stored in mobile cloud environments, which merge mobile technology with cloud computing to make it easier for patients and healthcare professionals to share medical data. With the help of this cutting-edge strategy, healthcare services are made available along with EHRs and minimal operational costs.[36] The introduction of cutting-edge technologies like Mobile Cloud Computing (MCC) and the Internet of Medical Things (IoMT) has significantly altered how e-health operations are conducted in the healthcare sector.[48] Patients can now gather their own personal health data at home using mobile devices (such as smartphones and wearable sensors) and share it in cloud environments, which healthcare professionals can instantly access to review patient records and provide prompt medical assistance. This clever e-health service makes it possible for medical professionals to remotely monitor patients by providing ambulatory care while at home, which not only streamlines the delivery of healthcare but also helps patients financially.[49] Additionally, the availability of full EHRs in the cloud aids in tracking patient health and provides appropriate medical services throughout the diagnosis and treatment stages. Despite all these wonderful benefits, the trend toward storing EHRs in the cloud also presents security issues that make it difficult to install e-health apps there.[38] Secure EHR exchange between healthcare providers and patients in mobile cloud environments is one of these security concerns. Without patients' permission, unauthorized parties may get harmful access to EHRs, which has a negative effect on the confidentiality, security, and integrity of cloud-based e-health systems. Additionally, patients can find it challenging to track and manage the cloud-based health records that are shared among healthcare providers. Therefore, it is vital to suggest effective access control measures for systems that share mobile cloud EHRs (Figure 7).

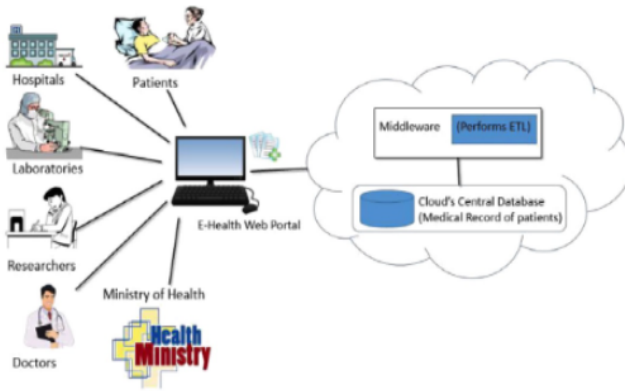

Figure 7: Cloud-based architecture to implement electronic health record (EHR) system

A patient's medical information is preserved in digital form as a medical health record (MHR). Electronic healthcare records are becoming increasingly important in the modern world of data and technology in the medical industry.[37] However, there are issues with patient medical health reports' confidentiality and privacy. By using Ethereum blockchains and cloud-based technologies, which connect patients and doctors everywhere in the globe, we can see that many people are striving to solve these problems. It gives patients complete control over their data access and allows them to authorize others to examine their data. Today, we use our mobile devices to store our photos, videos, emails, and even financial services, but we remain unable to keep our medical information safe because the

healthcare ecosystem is becoming more complex due to the involvement of stakeholders in challenging and crucial data interactions. Privacy, data security, and operational effectiveness may all suffer as a result. Because of this, the problem of information-related health interoperability is still open. When Nakamoto wrote a piece on Bitcoin in 2008, he first mentioned blockchain technology. It is a network of peer-to-peer nodes that communicate with one another.[40] Decentralized networks, distributed databases, enhanced security, and peer-to-peer transactions that can be verified are some of blockchain's key characteristics. As a result, blockchain technology has the capability to safeguard patient information in the healthcare system. Blockchain is an advanced data framework in which expanding records are kept in blocks, each of which has four components: information, the current block hash, the preceding block hash, and the timestamp. As a result, each new block that is added to the blockchain is linked to the one before it. This ensures that the information integrity is maintained across the endpoints without the need for human intervention by using a hash value that renders it immutable, time-stamping all workflow recordings to give them an identity, and distributing replicas to each network node that is a player. The InterPlanetary File System (IPFS) is a peer-to-peer (P2P) bit torrent-like distributed storage technique that intends to connect all digital devices to a single file system of files, making it possible to store enormous amounts of medical records. Just the hash address of the information has to be kept in the blockchain network rather than the patient's medical records.[3] High-integrity digital content that is accessible to everyone is stored using IPFS. There is no one point of failure with IPFS because it is distributed. For maximum bandwidth, IPFS also supports a content-addressed block storage approach. The Internet of Things (IoT) has been growing in popularity in recent years, particularly in the healthcare industry.[6] The development of IoT and wearable devices in the medical industry along with the advancement of technology has enhanced the standard of healthcare. Wearable technology collects patient health information and gives it to hospitals or physicians. Critical and sensitive medical data are produced by wearable IoT devices. Because it is closely tied to a patient's life, this information must be secured with great care. Blockchain is a fantastic way to protect the medical data that these IoT devices produce.

Blockchain technologies were first used in Bitcoin, where each block uses a hash value to link to earlier blocks. It denotes the transactions are unchangeable once they are created. Researchers and scientists are paying close attention to blockchains in the present era for a number of reasons, including wireless network decentralization, access control, data security, and privacy. With the expansion of electronic health data and the regulation of patient data privacy, the healthcare environment is quickly changing as technology advances. New opportunities are also opening up for the management of health data. Additionally, it is practical for patients to consult their medical records. Blockchain is a brand-new, revolutionary technology that may be able to address the issue of digitized data' authenticity. Blockchain, however, is an expensive data storage technology, especially for large amounts of information and digital content. For storing substantial volumes of data and content, we advise adopting an IPFS system files. It is clear from a comparison of HTTP to IPFS that HTTP has many drawbacks, including centralization, inefficiency, and a lack of historical versioning. Thus, IPFS overcomes HTTP's drawbacks. There are issues like inefficiency and bad system adaption since the numerous health record platforms are not created to meet the demands and requirements of patients. Additionally, they contend that the usage of EHRs has had a negative impact on how information is processed. Due to these problems, it makes sense to look for a platform, such as blockchain, that may help transform the healthcare industry into one that is patient-focused.[10] A platform that delivers integrity of data to the patients' health records and is open, secure, and reliable (Figure 8).

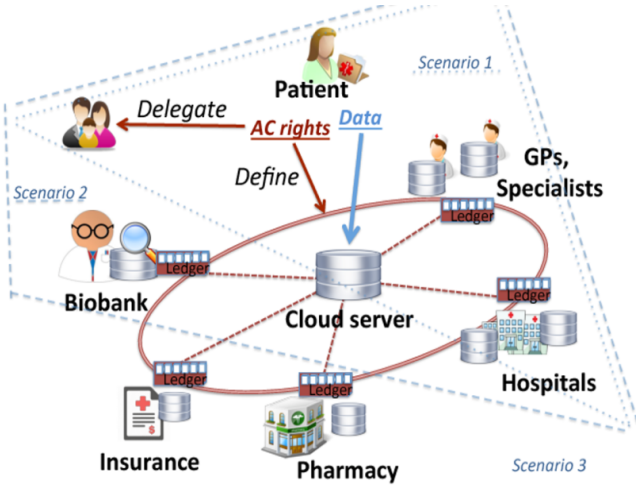

Figure 8: Secure and trustable electronic medical records sharing using blockchain

The information is kept in a cloud with third-party reliance in the earlier EHR models. To secure medical data, a key management system is used. A secret key is used to transfer the data between peers. However, most people just utilize one key to exchange data. Data can, therefore, be hacked or altered if the opponent knows the key. Every workflow in the blockchain is given a time stamp, an identity, and copies that are shared throughout all of the network's nodes. Although blockchain has many benefits, it also has a few limitations that pose some domain-specific difficulties. Scalability, storage, anonymity, customization, and legislation are the four primary problems

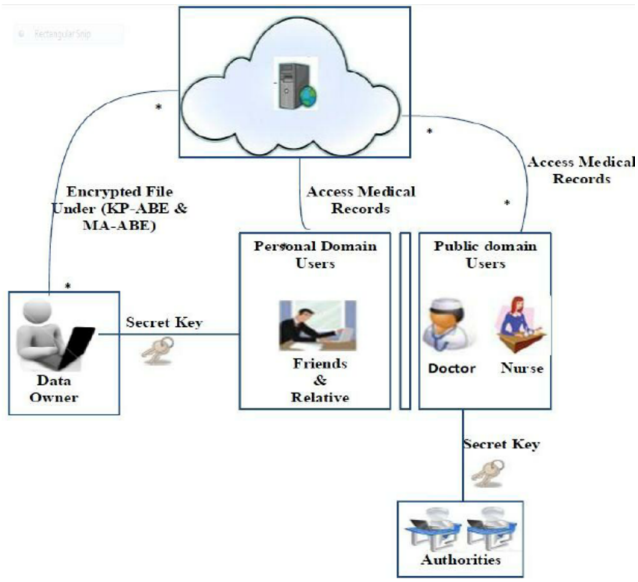

Figure 9: Architecture of patient record sharing

that blockchain systems must overcome. Here are a few answers to the issues mentioned above: Instead of storing personal information on the blockchain, IPFS can be used to store data, and the hash from IPFS will be kept on the blockchain. It keeps a pseudonymous record of personal information. The data is kept in the mentioned local database. Classical databases can be used to store data, but since a single authority is in charge of large volumes of information, one cannot be sure that the data is confidential, authentic, and trustworthy. A growing number of technological building blocks are connected by cryptographic algorithms to form the blockchain. No centralized data repositories exist in this distributed ledger. Ledger technology, which may be used to create distributed smart contracts, eliminates the need for a middleman by instantly defining and enforcing the rules and obligations laid down by the participants in the ledger. IPFS can be used as a peer-to-peer backup system that is widely distributed via hypermedia. It employs a block storage strategy with address links to the Merkle Directed Acyclic Graph's contents (DAG). IPFS has no likelihood of failing because it is distributed. To store medical records, a variety of EHR technologies have been developed, but the current electronic health record architecture has issues with privacy and security. While some of the applications also employed blockchain to address security-related issues, they also featured intricate medical processes for managing a significant amount of medical information. In recent years, various sensors, gadgets, and automobiles have been linked to the Internet. Remote patient monitoring is one of these technologies. These days, treating and taking care of patients in this way is commonplace. These technologies also involve digital data transmission, which creates privacy and security issues, as does the logging of data transfers (Figure 9). Blockchain technology has the potential to be the answer for data privacy and security for health data; each block comprises a Block Header, a Transaction, a Counter, and a Transaction.

12. Conclusion

The cornerstone for digitalization that can touch millions of lives will be blockchain-based technologies. Blockchain enters the communication industry and digital healthcare as a player thanks to its fundamental decentralized information collection and decentralized database, and yet communicating and dispensing information across networks by certified users with the option to add and at the same period avoiding data alteration. From the early hype surrounding healthcare, it has recently emerged as a viable technology that can enter the story of healthcare interoperability. There are many aspirations and visions about how and what exactly this unique technology can do for the interoperability of healthcare data. Our society's nervous system will be an innovative fusion of blockchain, smart contracts, and artificial intelligence, enabling us to live longer, healthier lives. Although it has the potential to close the interoperability gap, blockchain cannot yet do so. In order to be technologically fit, hospitals around the world need to modernize their infrastructure and add additional healthcare personnel. They won't be able to converse in the same language or be functional unless they have that.

13. Source of Funding

None.

14. Conflict of Interest

None.

References

1. Tagde P, Tagde S, Bhattacharya T, Tagde P, Chopra H, Akter R, et al. Blockchain and artificial intelligence technology in e-health. *Environ Sci Pollut Res Int*. 2021;28(38):52810–31.
2. Nagasubramanian G, Sakthivel RK, Patan R, Gandomi AH, Sankayya M, Balusamy B. Securing e-health records using keyless signature infrastructure blockchain technology in the cloud. *Neural Comput Appl*. 2020;32(3):639–47.
3. Neto MM, Marinho CS, Coutinho EF, Moreira LO, Machado JC, Souza JN. Research opportunities for e-health applications with DNA sequence data using blockchain technology. In: 2020 IEEE International Conference on Software Architecture Companion (ICSA-C); 2020. p. 95–102.
4. Biswas S, Sharif K, Li F, Mohanty SP. Blockchain for e-health-care systems: Easier said than done. *Comput*. 2020;53(7):57–67.
5. Benil T, Jasper J. Cloud based security on outsourcing using blockchain in e-health systems. *Comput Netw*. 2020;178(3):107344.
6. Shamshad S, Rana M, Mahmood K, Kumari S, Chen CM. A secure blockchain-based e-health records storage and sharing scheme. *J Inf Secur Appl*. 2020;55:102590.
7. Pandey P, Litoriya R. Securing e-health networks from counterfeit medicine penetration using blockchain. *Wireless Personal Commun*.

2020;117(1):7–25.
8. Ktari J, Frikha T, Amor NB, Louraidh L, Elmannai H, Hamdi M. IoMT-based platform for E-health monitoring based on the blockchain. *Electron*. 2022;11(15):2314.
9. Xiang X, Wang M, Fan W. A permissioned blockchain-based identity management and user authentication scheme for e-health systems. *IEEE Access*. 2020;8:171771–83.
10. Gadekallu TR, Manoj MK, Krishnan S, Kumar N, Hakak S, Bhattacharya S. Blockchain-based attack detection on machine learning algorithms for IoT-based e-health applications. *IEEE Internet Things Mag*. 2021;4(3):30–3.
11. DAAC: Digital asset access control in a unified blockchain based e-health system;Available from: https://www.smohanty.org/Publications_Journals/2021/Mohanty_IEEE-TBD_2021_DAAC-Blockchain.pdf.
12. Chelladurai MU, Pandian DS, Ramasamy DK. A blockchain based patient centric electronic health record storage and integrity management for e-health systems. *Health Policy Technol*. 2021;10(10):100513.
13. Agbo CC, Mahmoud QH. Design and implementation of a blockchain-based e-health consent management framework. In: 2020 IEEE International Conference on Systems, Man, and Cybernetics (SMC); 2020. p. 812–17.
14. Phapale PA, Patil P, Goswami S, Kendre S. Interoperability and synchronization management of blockchain-based decentralized e-health system. *Int J Sci Res Scie Technol*. 2021;8(2):515–19.
15. Zhang G, Yang Z, Liu W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. *Comput Netw*. 2022;203:108586.
16. Arunkumar B, Kousalya G. Blockchain-based decentralized and secure lightweight e-health system for electronic health records. In: Intelligent Systems, Technologies and Applications . Springer; 2020. p. 273–89.
17. Hussien HM, Yasin SM, Udzir NI, Ninggal MI, Salman S. Blockchain technology in the healthcare industry: Trends and opportunities. *J Ind Inf Integr*. 2021;22:100217.
18. Maseleno A, Hashim W, Perumal E, Ilayaraja M, Shankar K. Access control and classifier-based blockchain technology in e-healthcare applications. In: Intelligent Data Security Solutions for e-Health Applications; 2020. p. 151–67.
19. Xiang X, Zhao X. Blockchain-assisted searchable attribute-based encryption for e-health systems. *J Syst Architecture*. 2022;124:102417.
20. Samuel O, Omojo AB, Mohsin SM, Tiwari P, Gupta D, Band SS. An anonymous IoT-based e-health monitoring system using blockchain technology. *IEEE Syst J*. 2023;17(2).
21. Seitz J, Wickramasinghe N. Opportunities for using blockchain technology in e-Health: E-Prescribing in Germany. In: Delivering Superior Health and Wellness Management with IoT and Analytics. Springer; 2020. p. 299–316.
22. Goncalves JP, Resende HC, Municio E, Villaça R, Marquez-Barja JM. Securing E-Health Networks by applying Network Slicing and Blockchain Techniques. In: 2021 IEEE 18th Annual Consumer Communications & Networking Conference (CCNC). IEEE; 2021. p. 1–2.
23. Sabu S, Ramalingam HM, Vishaka M, Swapna HR, Hegde S. Implementation of a secure and privacy-aware e-health record and IoT data sharing using blockchain. *Glob Transitions Proc*. 2021;2(2).
24. Xiang X, Cao J, Fan W. Decentralized authentication and access control protocol for blockchain-based e-health systems. *J Netw Comput Appl*. 2022;207:103512.
25. Marinho SC, Filho JC, Moreira LO, Machado JC. Using a hybrid approach to data management in relational database and blockchain: A case study on the E-health domain. In: 2020 IEEE International Conference on Software Architecture Companion (ICSA-C), Salvador, Brazil. IEEE; 2020. p. 114–21.
26. Coutinho EF, Neto MM, Abreu AW, Moreira LO, Bezerra CI, Paillard G, et al. Modeling blockchain e-health systems. In: EATIS '20: Proceedings of the 10th Euro-American Conference on Telematics and Information Systems; 2020. p. 1–8.
27. Hossain CA, Mohamed MA, Zishan MS, Ahasan R, Sharun SM. Enhancing the security of e-health services in Bangladesh using blockchain technology. *Int J Inf Technol*. 2022;14(3):1179–85.
28. Chenthara S, Ahmed K, Wang H, Whittaker F, Chen Z. Healthchain: A novel framework on privacy preservation of electronic health records using blockchain technology. *PLoS One*. 2020;15(12):e0243043.
29. Fekih RB, Lahami M. Application of blockchain technology in healthcare: A comprehensive study. In: The Impact of Digital Technologies on Public Health in Developed and Developing Countries; 2020. p. 268–76.
30. Radjenovic Z. The cost-saving role of blockchain technology as a data integrity tool: e-health scenario. *KnE Social Sciences*. 2020;p. 339–52.
31. Lin C, He D, Huang X, Khan K, Choo KK. DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain. *IEEE Trans Inform Forensics Secur*. 2020;15:2440–52.
32. Frikha T, Chaari A, Chaabane F, Cheikhrouhou O, Zaguia A. Healthcare and fitness data management using the iot-based blockchain platform. *J Healthc Eng*. 2021;p. 9978863.
33. Mallikarjuna B, Kiranmayee D, Saritha V, Krishna PV. Development of efficient e-health records using IoT and blockchain technology. In: ICC 2021 - IEEE International Conference on Communications, Montreal, Canada. IEEE; 2021.
34. Singh AK, Lv Z, Ko H. Introduction to the special issue on recent trends in medical data security for e-health applications. *ACM Trans Multimedia Comput Commun Appl*. 2021;17(2s):1–3.
35. Hasselgren A, Kralevska K, Gligoroski D, Pedersen SA, Faxvaag A. Blockchain in healthcare and health sciences-A scoping review. *Int J Med Inform*. 2020;134:104040.
36. Bali V, Khanna T, Soni P, Gupta S, Chauhan S, Gupta S. Combating drug counterfeiting by tracing ownership transfer using blockchain technology. *Int J E Health Med Commun*. 2022;13(1):1–21.
37. Al-Marridi AZ, Mohamed A, Erbad A. Reinforcement learning approaches for efficient and secure blockchain-powered smart health systems. *Comput Netw*. 2021;197(1):108279.
38. Naghizadeh R. Policy factors affecting the technological catch-up of electronic health services in Iran through blockchain technology. *J Inf Technol Manag*. 2022;p. 24–35.
39. Alonso SG, Arambarri J, López-Coronado M, de la Torre Díez I. Proposing new blockchain challenges in ehealth. *J Med Syst*. 2019;43(3):64.
40. Sivan R, Zukarnain ZA. Security and privacy in cloud-based e-health system. *Symmetry*. 2021;13(5):742.
41. Abdellatif AA, Samara L, Mohamed A, Erbad A, Chiasserini CF, Guizani M, et al. MEdge-Chain: Leveraging edge computing and blockchain for efficient medical data exchange. *IEEE Internet Things J*. 2021;8(21):15762–75.
42. Ghazal TM, Hasan MK, Abdullah SN, Bakar KA, Hamadi HA. Private blockchain-based encryption framework using computational intelligence approach. *Egypt Inform J*. 2022;23(2):69–75.
43. Velliyangiri G, Krishnamoorthy V, Inbaraj C, Venkatachalam A, Rahim R, Ramachandran M. Blockchain and artificial intelligent for internet of things in e-health. In: The Convergence of Artificial Intelligence and Blockchain Technologies; 2022. p. 23–42.
44. Kondepogu MD, Andrew J. Secure e-health record sharing using blockchain: A comparative analysis study. In: 2022 6th International Conference on Intelligent Computing and Control Systems (ICICCS); 2022. p. 861–68.
45. Chelladurai U, Pandian S. A novel blockchain based electronic health record automation system for healthcare. *J Ambient Intell Hum Comput*. 2022;13(2):693–703.
46. Meisami S, Beheshti-Atashgah M, Aref MR. Using blockchain to achieve decentralized privacy in IoT healthcare. *Int J Cybernetics Inform*. 2023;12(2):97–108.
47. Kadam S, Motwani D. Protected Admittance E-Health Record System Using Blockchain Technology. In: Computer Networks and Inventive Communication Technologies. Springer; 2022. p. 723–39.
48. Kayastha M, Karim S, Sandu R, Gide E. Ethereum Blockchain and Inter-Planetary File System (IPFS) based Application Model to

Record and Share Patient Health Information: An Exemplary Case Study for e-Health Education in Nepal. In: 2021 19th International Conference on Information Technology Based Higher Education and Training (ITHET). IEEE; 2021.
49. Mukherjee P, Barik LB, Pradhan C, Patra SS, Barik RK. hQChain: Leveraging towards blockchain and queueing model for secure smart connected health. *Int J E Health Med Commun*. 2021;12(6):1–20.

Author biography

Mohammed Sanusi Sadiq, Professor https://orcid.org/0000-0003-4336-5723

I. P. Singh, Professor https://orcid.org/0000-0002-1886-5956

N. Karunakaran, Principal https://orcid.org/0000-0002-7213-2841

M. M. Ahmad, Professor https://orcid.org/0000-0003-4565-5683

B. Maryam, Research scholar https://orcid.org/0009-0004-4782-4032

Cite this article: Sadiq MS, Singh IP, Karunakaran N, Ahmad MM, Maryam B. Block chain technology for e-health. *J Community Health Manag* 2024;11(2):71-87.