International Journal of Intelligent Communication and Computer Science
Vol. 2, No. 3, 2024, Pages 18-37.

Blockchain-Enabled E-Health Care Medical Systems: Overview and Review

Ajai Pratap Singh[1] and Rohitashwa Pandey[2]

[1]Research Scholar, Department of Computer Science and Engineering, Bansal Institute of Engineering and Technology, Lucknow, Affiliated to AKTU, Lucknow
[2]Department of Computer Science and Engineering Bansal Institute of Engineering and Technology, Lucknow,, Affiliated to AKTU, Lucknow

Review Paper

Email: pratap1984ajay@gmail.com
Received: 18 May 2024, Revised: 8 Oct. 2024, Accepted: 30 Oct 2024

Abstract:

Blockchain technology, initially popularized by cryptocurrencies, has emerged as a powerful tool for addressing key challenges in the healthcare sector. This paper provides an in-depth review of blockchain-enabled medical systems, exploring its potential to enhance security, interoperability, data privacy, and operational efficiency in healthcare. It examines how blockchain can improve the integrity of patient data, foster trust in medical records, enable secure sharing of sensitive health information, and facilitate the integration of diverse healthcare services. Key use cases, benefits, limitations, and challenges to adoption are discussed, with particular focus on scalability, regulatory compliance, and integration with existing healthcare infrastructures. The paper concludes by outlining future research directions and practical implementation strategies for blockchain in healthcare, highlighting the need for cross-disciplinary collaboration and the development of pilot projects to test and refine blockchain applications in real-world healthcare environments. Ultimately, the paper asserts that while blockchain holds transformative potential, overcoming technical, legal, and organizational barriers will be essential for its successful integration into healthcare systems worldwide.

Keywords: Blockchain, HER, Digital health

1. Introduction

The healthcare industry, despite its critical importance to society, faces a multitude of challenges that hinder its ability to provide efficient, secure, and high-quality services. Among the most pressing challenges are issues related to data security, patient privacy, interoperability, and the efficiency of medical systems [1]. Traditional healthcare systems predominantly rely on centralized databases to store patient information, which, while effective in some ways, introduces significant vulnerabilities. Centralized systems are inherently prone to data breaches, fraud, and unauthorized access, as they create a single point of failure that can be targeted by malicious actors. When sensitive medical data, such as patient health records, is stored in one central location, it becomes a prime target for cyberattacks, and a breach can expose vast amounts of personal information at once, leading to identity theft, fraud, or even physical harm [2].
Additionally, the issue of patient privacy is of utmost concern in the healthcare sector. Patients trust healthcare providers with some of the most sensitive aspects of their lives, and any mishandling of this information can lead to significant legal and reputational damage. Current systems often struggle with ensuring that privacy regulations, such as HIPAA (Health Insurance Portability and Accountability Act) [3] in the United States, are

properly adhered to, particularly in systems where access control and auditing mechanisms are not sufficiently robust.

Another major challenge is the interoperability of healthcare systems. Medical data is often fragmented across multiple healthcare providers, insurance companies, and specialist centers. Each institution may use different electronic health record (EHR) [4] systems or proprietary databases, which leads to inconsistent or incomplete patient histories. When medical records are siloed, it becomes difficult for healthcare providers to access and share crucial information in a timely manner, particularly in emergency situations. This fragmentation can result in misdiagnosis, delayed treatments, and suboptimal care, as healthcare professionals may not have the full picture of a patient's medical history or the most recent diagnostic data.

Moreover, the efficiency of medical systems remains a critical concern. Healthcare institutions are often burdened with bureaucratic processes and administrative overhead, including complex billing systems, paperwork, and slow insurance claim processes. These inefficiencies can slow down patient care, increase operational costs, and contribute to the fragmentation of healthcare delivery, resulting in poor outcomes for patients and increased stress on the healthcare workforce.

Figure 1 illustrates a blockchain-enabled healthcare ecosystem where key stakeholders—patients, doctors, medical institutions, cloud services, and blockchain—interact to create a secure, efficient, and interoperable system. Patients control access to their medical records through blockchain, ensuring privacy and data integrity. Doctors and medical institutions access and update patient data stored on the blockchain, fostering trust and reducing errors. Cloud services provide scalability and additional functionalities, such as data analytics and telemedicine, while seamlessly integrating with blockchain. This decentralized approach ensures transparency, secure data sharing, and traceability across healthcare platforms, ultimately improving care coordination and patient outcome

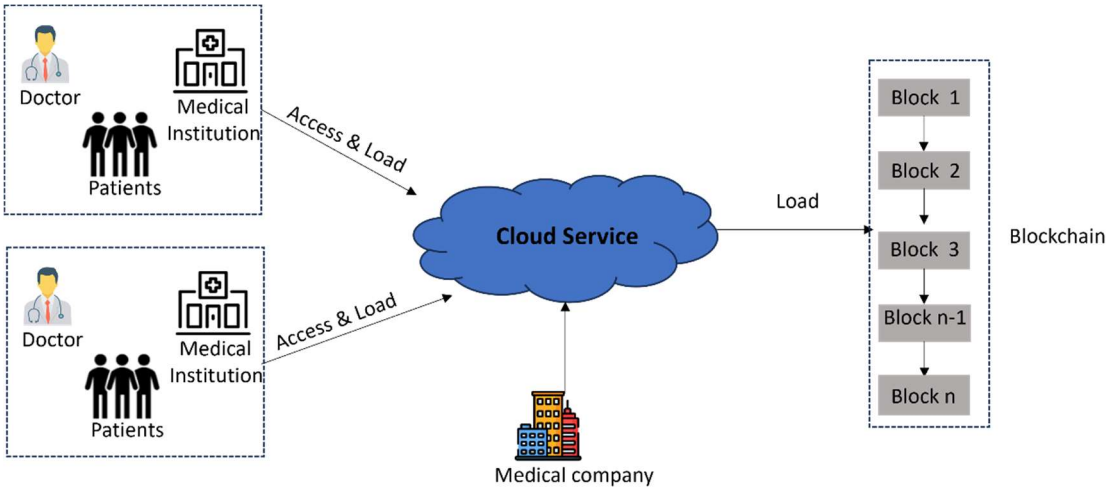

Figure 1: Illustration a blockchain-enabled healthcare ecosystem

Blockchain technology presents a potential solution to these complex issues. At its core, blockchain is a decentralized and immutable ledger system that can securely record transactions across a distributed network. Unlike traditional centralized databases, where a single entity controls access to the data, blockchain operates on a peer-to-peer network. This decentralization eliminates the risk of a single point of failure, making it more resistant to cyberattacks and fraud. Each transaction or data point added to the blockchain is cryptographically secured and linked to the previous one, creating an immutable chain of data. This structure ensures that once data is recorded on the blockchain, it cannot be altered or deleted, thus guaranteeing the integrity and authenticity of medical records.

Blockchain's cryptographic security mechanisms and consensus protocols further ensure the privacy and protection of sensitive medical data. In a blockchain system, participants must validate transactions using consensus algorithms (such as Proof of Work [5] or Proof of Stake [5]) before they are recorded on the ledger, ensuring that only authorized parties can modify the data. This makes blockchain highly suited for applications in healthcare, where privacy, accuracy, and trust are paramount. Furthermore, blockchain can enable patients

to have more control over their data by allowing them to grant or revoke access to their medical records, ensuring patient autonomy and fostering trust between patients and healthcare providers.
In addition to ensuring security and privacy, blockchain can address the issue of interoperability. By using a decentralized, standardized protocol, blockchain can enable healthcare providers across different institutions to securely exchange medical records, regardless of the systems or technologies they are using. This would create a unified, comprehensive medical history that follows the patient, facilitating timely and coordinated care across multiple providers. Furthermore, blockchain-based smart contracts could automate and streamline many administrative tasks, such as insurance claims, billing, and payment processing, reducing fraud and increasing operational efficiency. The transparency of blockchain systems could also improve accountability in healthcare operations, as all transactions are recorded on an immutable ledger accessible by authorized parties.
Despite these promising benefits, the integration of blockchain into healthcare is not without challenges. Scalability is a significant concern, as blockchain systems, particularly those using proof-of-work consensus algorithms, are often limited by transaction speed and throughput. For blockchain to handle the vast amounts of data generated in healthcare, particularly in real-time applications like IoT devices and telemedicine, scalable solutions will need to be developed.
Another challenge is the regulatory landscape. Healthcare systems are highly regulated, and integrating blockchain into these systems will require navigating a complex web of laws and regulations regarding data privacy, security, and governance. Data governance in decentralized systems is also a topic that requires careful consideration, particularly when it comes to ensuring that sensitive medical data is appropriately accessed and shared, and that it complies with regulations such as the General Data Protection Regulation (GDPR) [6] in the EU or HIPAA in the U.S. There are also legal implications regarding data ownership and the potential conflict between blockchain's immutable records and patients' rights to delete or update their medical information.
This paper aims to provide a comprehensive review of the current landscape of blockchain-enabled medical systems, examining how blockchain can address the challenges faced by the healthcare industry. The paper will evaluate the potential benefits of blockchain in healthcare, including improvements in data security, patient privacy, interoperability, and efficiency, and will also explore its drawbacks and limitations, such as scalability issues, regulatory concerns, and technical challenges. Finally, the paper will discuss the path forward for integrating blockchain into healthcare solutions, identifying key research areas and development opportunities that could accelerate the adoption of blockchain in the healthcare industry.
By examining the current state of blockchain in healthcare, this paper aims to provide valuable insights into how this transformative technology could reshape the way medical data is managed, shared, and protected, ultimately improving the quality of care and operational efficiency in healthcare systems globally.

2. Blockchain Fundamentals

Blockchain is a distributed ledger technology (DLT) [7] that allows data to be stored across a network of decentralized nodes or computers, ensuring that there is no single point of control or failure. This design contrasts sharply with traditional databases, which typically rely on a centralized system controlled by one entity (such as a bank, hospital, or government) to store and manage data. Instead, blockchain provides a system where multiple participants, called nodes, independently store copies of the same data, making it distributed, secure, and resilient to manipulation or attack [8].

2.1 Key Features

The key features of blockchain that distinguish it from traditional databases are [9]:

Decentralization
In a decentralized blockchain system, there is no central authority controlling or managing the data. Instead, the blockchain operates on a peer-to-peer network where all participants (or nodes) have equal access to the same data. Every participant maintains a copy of the blockchain's record, which is synchronized across the entire network. This decentralization ensures that no single point of failure exists, making the system more robust and less vulnerable to cyberattacks or fraudulent activities that could occur in a centralized system. The distributed nature of blockchain also eliminates the need for intermediaries or trusted third parties, which are typically required to facilitate transactions in centralized systems. This decentralization promotes

transparency, as every participant can independently verify transactions on the network, and it ensures that no single entity has control over the data, which significantly reduces the risks of manipulation or fraud.

Immutability
One of the most significant characteristics of blockchain is its immutability, meaning that once a transaction is recorded on the blockchain, it cannot be altered or deleted. This is achieved through the cryptographic hash functions that ensure each new block of data is linked to the previous one. This chain of blocks creates a historical record that is permanent and tamper-resistant. If an individual or entity tries to alter a block of data, they would have to modify every subsequent block in the entire chain, which would require an enormous amount of computational power and would be immediately detectable by the network. This feature ensures the integrity and permanence of data, making blockchain particularly suited for applications where accuracy and reliability are essential, such as financial transactions, medical records, and supply chain tracking. For instance, in the context of healthcare, once patient data (such as medical records or prescriptions) is recorded on the blockchain, it cannot be tampered with, which builds trust between patients and healthcare providers and ensures that the data remains unaltered.

Transparency
Blockchain systems are inherently transparent, meaning that the records stored on the blockchain are visible to all participants in the network. This visibility fosters a level of trust and accountability, as everyone involved can independently view and verify transactions. Transparency in blockchain is particularly valuable in industries like supply chain management, finance, and healthcare, where it is crucial for all stakeholders to have access to accurate, real-time information. While transparency allows for public verification, it's important to note that blockchain can be designed to preserve privacy. For example, sensitive information can be encrypted, ensuring that only authorized individuals can view certain aspects of the data. This approach balances the need for transparency and security, providing stakeholders with assurance that the data has not been tampered with while maintaining confidentiality.

Security
The security of data on the blockchain is one of its most compelling features. Data is stored in an encrypted format, meaning that it is unintelligible to anyone without the proper decryption keys. Blockchain uses a combination of public and private cryptographic keys to control access to the data, ensuring that only authorized parties can view or modify it. This cryptographic security ensures that blockchain transactions are resistant to hacking, fraud, and identity theft. Furthermore, each block of data is connected to the previous block through a cryptographic hash function, creating a secure chain of blocks that cannot be modified without altering all subsequent blocks. This makes the blockchain tamper-resistant, as any changes to a single block would be immediately noticeable by the network. For applications in healthcare, cryptographic security guarantees that patient records remain private and protected from unauthorized access, while still enabling patients to control who can access their medical data.

Consensus Mechanisms
Blockchain networks rely on consensus mechanisms to validate and agree upon the state of the blockchain. These algorithms ensure that all participants in the network agree on the validity of transactions before they are recorded in the ledger. Consensus mechanisms are crucial because they maintain the integrity of the blockchain by preventing fraudulent transactions or double-spending.
The two most common consensus algorithms are Proof of Work (PoW) [5] and Proof of Stake (PoS) [5], although other mechanisms, such as Delegated Proof of Stake (DPoS) [10] and Practical Byzantine Fault Tolerance (PBFT) [11], are also used in some blockchains.

Proof of Work (PoW): This algorithm requires participants (called miners) to solve complex mathematical puzzles in order to validate and add new transactions to the blockchain. Once a puzzle is solved, the miner is rewarded with cryptocurrency (in the case of Bitcoin, for example). PoW is highly secure but can be energy-intensive due to the computational power required to solve the puzzles.

Proof of Stake (PoS): In contrast to PoW, PoS allows participants (called validators) to create new blocks and validate transactions based on the number of coins they hold (their "stake"). The greater the stake, the more

likely a participant is to be chosen to validate a transaction. PoS is more energy-efficient than PoW and is becoming increasingly popular in blockchain networks.

Consensus mechanisms play a critical role in ensuring that transactions are valid and that all participants in the network agree on the state of the ledger. These mechanisms help to prevent fraud, double-spending, and other types of malicious behavior, ensuring the reliability and trustworthiness of the blockchain network.

2.2 Related Works

A central theme in many studies is the use of blockchain for improving security and privacy of electronic health records (EHRs) (Table 1). In their survey, Shi et al. (2020) [12] explore blockchain's role in safeguarding EHRs by ensuring data integrity, preventing unauthorized alterations, and enabling secure data sharing among healthcare providers. The authors highlight that blockchain's immutability and decentralized nature make it an ideal candidate for enhancing the security and privacy of healthcare data, which is often vulnerable to breaches due to centralized storage systems (Shi et al., 2020). Similarly, Keshta and Odeh (2021) [13] discuss the growing concerns around EHR security and privacy and emphasize the need for new frameworks that address these issues using blockchain technology (Keshta & Odeh, 2021).
Further emphasizing security, Saeed et al. (2022) [14] provide a comprehensive review of blockchain applications in healthcare and its capacity to ensure secure and transparent access to medical records, effectively preventing unauthorized access (Saeed et al., 2022). This is particularly important in light of regulations like the Health Insurance Portability and Accountability Act (HIPAA), which require robust mechanisms to ensure patient privacy (Act, 1996).

Table 1: State of the art methods (Security and Privacy Aspects)

Reference	Key Focus	Security and Privacy Aspects
Shi et al. (2020) [12]	Blockchain for safeguarding EHRs	Blockchain's immutability and decentralized nature enhance security and prevent unauthorized alterations
Keshta & Odeh (2021) [13]	Security and privacy of EHR systems	Emphasizes the need for new frameworks to address security gaps
Saeed et al. (2022) [14]	Blockchain applications in healthcare	Blockchain ensures secure data access, preventing unauthorized access

3. Blockchain in Healthcare: Key Use Cases

Several promising use cases for blockchain technology have emerged in the healthcare industry (Figure 2). These include [15]:
The healthcare industry is rapidly evolving, and blockchain technology offers solutions to many of its most pressing challenges, including security, privacy, and efficiency. Several promising use cases for blockchain in healthcare are emerging, and they have the potential to fundamentally transform how healthcare systems operate. These use cases address a wide range of issues, from data management to payment processing, clinical trials, and supply chain management.

3.1. Electronic Health Records (EHRs)

One of the most significant issues in modern healthcare is the management and sharing of Electronic Health Records (EHRs). Healthcare providers often store patient data in isolated silos, and accessing this information across different systems can be time-consuming, inefficient, and prone to errors. Blockchain can serve as a decentralized, immutable repository for EHRs, allowing patients to control access to their data while enabling secure sharing across multiple healthcare providers. By leveraging blockchain, the following benefits can be realized:

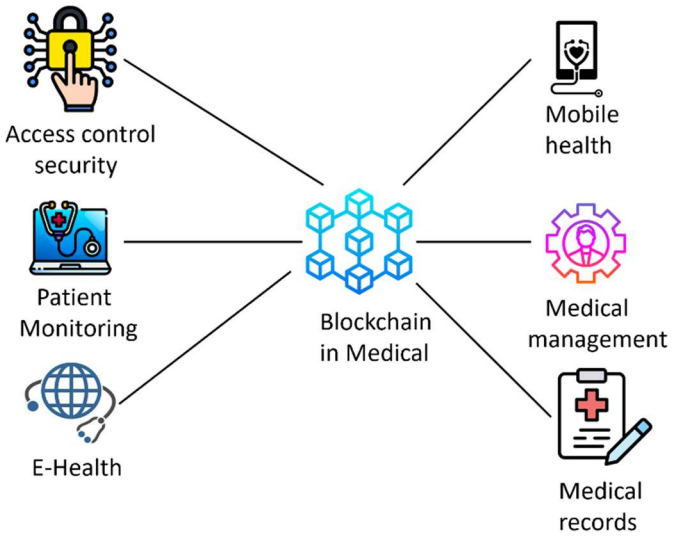

Figure 2: Blockchain enabled e-healthcare system

Data Integrity: Blockchain ensures that EHRs are tamper-proof. Since each record is encrypted and added to the blockchain in a chronologically ordered chain of blocks, any attempt to alter the data would require changing all subsequent blocks—a process that is computationally impractical. This immutability guarantees the integrity of patient data, reducing the risk of fraudulent alterations and ensuring that health records remain accurate and trustworthy.

Patient-Centric Control: One of the most compelling features of blockchain in EHR management is the ability for patients to retain control over their data. Using blockchain, patients can grant or revoke permission for specific healthcare providers to access their health records. This enhances patient autonomy and privacy, as patients can make informed decisions about who can view their data, based on their preferences or treatment needs.

Interoperability: Healthcare systems have long struggled with the issue of interoperability, where different healthcare providers use different software systems that cannot easily communicate with each other. Blockchain's decentralized nature can resolve these interoperability issues by creating a unified, standardized platform where patient data is accessible to all authorized healthcare providers, regardless of the specific technologies they use. This improves the flow of information across institutions and ensures more efficient, coordinated care.

3.2. Medical Supply Chain Management

The medical supply chain is a complex and highly regulated ecosystem, involving various stakeholders such as manufacturers, wholesalers, distributors, healthcare providers, and regulators [16]. Blockchain can improve transparency and traceability in the supply chain, ensuring that pharmaceutical products and medical devices are authentic, securely handled, and properly tracked throughout their lifecycle. Some key benefits of blockchain in medical supply chain management include:

Prevention of Counterfeit Drugs: Counterfeit drugs are a significant global concern, with the World Health Organization (WHO) estimating that up to 10% of the world's medicines are falsified. Blockchain can ensure that pharmaceutical products are traceable from the manufacturer to the end consumer by creating an immutable, transparent record of the product's journey. Each transaction (or transfer of goods) is recorded on

the blockchain, allowing for complete visibility and ensuring that only authentic drugs reach consumers, helping to combat the counterfeit drug market.

Improved Transparency: Blockchain allows for real-time tracking of products throughout the supply chain, ensuring greater transparency for all stakeholders. Manufacturers, wholesalers, distributors, and regulators can access up-to-date information about the status of pharmaceutical products and medical devices. This not only improves the accountability of all parties involved but also helps identify bottlenecks or inefficiencies in the supply chain that could otherwise delay product delivery or increase costs.

3.3. Clinical Trials and Research

Clinical trials are crucial for advancing medical science, but the process of conducting and managing trials often involves issues such as data integrity, lack of transparency, and difficulty sharing results. Blockchain can streamline and secure the process of clinical trials by ensuring the integrity of data and making the results more transparent and accessible. Blockchain's features can enhance clinical trials in the following ways [17]:

Data Integrity: Blockchain's immutable nature ensures that clinical trial data, once recorded, cannot be tampered with or altered. This provides a verifiable and trustworthy record of all trial data, ensuring that results are authentic and that any changes made during the trial process are fully traceable. This significantly reduces the risk of fraud or manipulation of trial results, making the process more reliable and credible.

Transparency: Blockchain can provide greater transparency in clinical trials by allowing participants, researchers, and the public to access trial protocols, progress reports, and results. This openness not only increases trust in the scientific community but also ensures that findings can be scrutinized and validated by independent researchers, promoting accountability and ethics in the research process. Moreover, patients can track the status of trials they are involved in and view results more efficiently.

3.4. Payment and Insurance Processing

The administrative side of healthcare, including billing, insurance claims, and payment processing, is often slow, error-prone, and prone to fraud. Blockchain has the potential to revolutionize these processes by improving efficiency, transparency, and security. Key benefits of blockchain for payment and insurance processing include [18]:

Smart Contracts: Blockchain-based smart contracts can automate many aspects of the insurance reimbursement process. For instance, when a patient receives treatment, a smart contract can automatically trigger the payment to the healthcare provider once the conditions for reimbursement are met (e.g., the treatment is approved by the insurer). This eliminates the need for intermediaries, speeds up processing times, and reduces human error, ensuring that both insurers and healthcare providers are paid promptly and accurately.

Cost Reduction: By eliminating intermediaries (such as billing agents and administrative staff), blockchain can reduce administrative costs in healthcare systems. The automation and streamlined nature of blockchain-based claims processing make it more efficient, reducing the time and cost spent on paperwork, verification, and disputes. Additionally, by improving data accuracy and reducing fraud, blockchain can help insurers offer lower premiums and improve the overall cost-effectiveness of healthcare.

3.5. Medical IoT (Internet of Medical Things) Integration

The Internet of Medical Things (IoMT) refers to the growing network of connected medical devices that collect and transmit health data [19]. These devices, such as wearables, diagnostic tools, and implantables, generate vast amounts of real-time data that can be critical for patient care. Blockchain can be used to securely manage this data, ensuring that it remains tamper-proof and confidential. Key applications of blockchain in IoMT include:

Secure Data Collection: As medical devices and IoT systems gather sensitive patient data, blockchain provides a secure, encrypted method of storing and transmitting this information. Each data point is recorded on the blockchain, ensuring its authenticity and security. This prevents unauthorized access or modification of patient data, making it more difficult for hackers or malicious actors to tamper with IoMT data.

Real-Time Monitoring: Blockchain can also enable real-time updates and monitoring of patient conditions. For example, wearable devices that track heart rate, glucose levels, or blood pressure can send data directly to a blockchain, where it can be securely stored and accessed by authorized healthcare providers. This enables continuous monitoring of patients, particularly in critical care situations, and allows for faster decision-making and more timely interventions.

3.6 Related Works

Another key benefit of blockchain is its potential to enhance interoperability across fragmented healthcare systems, a list of notable papers is given in Table 2. Aceto et al. (2020) [20] discusses how blockchain, alongside other technologies like IoT, big data, and cloud computing, can facilitate Healthcare 4.0 by enabling seamless data exchange between disparate healthcare systems (Aceto et al., 2020). The authors argue that blockchain's decentralized architecture can eliminate barriers between healthcare providers, ensuring that data is readily available to all stakeholders while maintaining privacy and security. This view is supported by Villarreal et al. (2023) [21], who explore how blockchain can be used to improve the interoperability and security of healthcare management systems, addressing the challenges of diverse healthcare platforms and protocols (Villarreal et al., 2023).
Hasselgren et al. (2020) [22] conduct a scoping review on blockchain applications in healthcare, concluding that interoperability is a major area of impact. They suggest that blockchain could act as a universal layer for data integration, allowing different healthcare systems to securely exchange information while ensuring compliance with privacy regulations (Hasselgren et al., 2020).

Table 2: State of the art methods (Interoperability and Data Exchange)

Reference	Key Focus	Interoperability and Data Exchange
Aceto et al. (2020) [20]	Blockchain in Healthcare 4.0	Blockchain enables interoperability by eliminating barriers between healthcare providers
Villarreal et al. (2023) [21]	Blockchain for healthcare management systems	Blockchain enhances interoperability across diverse healthcare platforms and protocols
Hasselgren et al. (2020) [22]	Scoping review on blockchain applications in healthcare	Blockchain facilitates secure data exchange between different systems while ensuring privacy

4. Benefits of Blockchain in Healthcare

The potential of blockchain to revolutionize healthcare lies in its ability to address many long-standing challenges, particularly those surrounding data security, privacy, transparency, and efficiency. Blockchain's unique features—decentralization, immutability, cryptographic security, and consensus-driven validation—provide a range of advantages that can significantly improve healthcare systems. Below are the key benefits of blockchain in healthcare.

4.1. Enhanced Security

One of the most compelling benefits of blockchain in healthcare is its enhanced security. In traditional centralized systems, data is often stored in a single, vulnerable database, which becomes a prime target for

cyber-attacks, hacking, or unauthorized access. Blockchain, on the other hand, offers several features that make healthcare data far more secure:

Cryptographic Security: Data stored on the blockchain is encrypted using advanced cryptographic techniques, making it nearly impossible for unauthorized parties to read or alter it. Each record is secured with a cryptographic hash function that binds it to the previous record in the chain, creating an unbreakable chain of data.

Distributed Ledger: Rather than relying on a single centralized repository, blockchain stores data across a distributed network of nodes (computers). This decentralized architecture makes it highly resistant to attacks. If a hacker attempts to alter data at one node, the changes would need to be replicated across every node on the network, which is a near-impossible task.
Tamper-Proof Data: The immutability of blockchain ensures that once a piece of data is recorded, it cannot be tampered with or deleted. This makes it an ideal solution for securing sensitive healthcare data, such as medical records, prescriptions, or diagnostic results, protecting them from malicious actors or accidental alterations.

These combined features ensure that healthcare data is not only protected from external threats but also from internal risks, such as unauthorized access by medical staff or service providers.

4.2. Improved Patient Privacy and Control

Patient privacy and control over personal health data are among the most pressing concerns in the healthcare industry. Blockchain provides a robust framework for addressing these issues by giving patients full control over their own health records:

Patient-Centric Control: With blockchain, patients can decide who can access their health data, and for how long. This can include granting access to specific healthcare providers, insurers, or researchers, and revoking access at any time. Blockchain facilitates the management of patient consent in a way that is transparent, auditable, and secure.

Granular Access Control: Blockchain allows for fine-grained control over health data, meaning that patients can authorize different levels of access depending on the need. For example, a primary care physician may have access to a patient's full medical history, while a specialist may only be granted access to relevant portions of the record. This granular control ensures that personal health data is shared only with authorized entities for specified purposes.

Reduction in Privacy Concerns: With the growing concern over data breaches in healthcare, patients' ability to maintain control over their health data could reduce privacy concerns and foster greater trust in healthcare systems. Blockchain's transparency ensures that every access request and data sharing action is logged, providing an audit trail that can be used for accountability.

4.3. Increased Transparency

Blockchain's transparency is a key advantage in ensuring trust and accountability in healthcare systems. In a typical healthcare environment, it is difficult for all stakeholders—patients, providers, insurers, and regulators—to access and verify data in real-time. Blockchain solves this problem by offering the following benefits:

Real-Time Data Access: Blockchain provides a real-time view of healthcare data to authorized participants, enabling patients, providers, insurers, and other stakeholders to access and verify medical records, prescriptions, or test results as needed. This increases trust, as all parties have access to the same information and can independently verify its authenticity.

Traceability of Actions: Blockchain's immutable ledger records every transaction or data exchange in a transparent, tamper-resistant manner. This provides an audit trail that stakeholders can follow, ensuring that

all actions, such as prescribing medication, making treatment decisions, or processing insurance claims, are fully traceable and accountable.

Accountability: With transparent records, providers and patients are encouraged to follow ethical practices, knowing that all activities are verifiable. This can reduce instances of fraud, malpractice, or unethical practices in healthcare, while also ensuring compliance with healthcare regulations.

By making healthcare operations more transparent, blockchain enhances trust between patients, healthcare providers, and other stakeholders, improving the overall quality of care and the patient experience.

4.4. Streamlined Processes

Blockchain can streamline numerous processes in healthcare by reducing the need for intermediaries, automating workflows through smart contracts, and eliminating redundancies. These efficiencies translate into significant cost savings, improved patient care, and faster operations:

Reduction of Intermediaries: Blockchain's decentralized nature means that intermediaries (such as data brokers, insurance claim processors, or third-party administrators) can be eliminated or replaced. This reduces administrative costs, eliminates delays, and speeds up healthcare operations. For example, insurance claim processing can be significantly faster and more accurate without the need for multiple intermediaries to verify claims.

Automation with Smart Contracts: Smart contracts are self-executing contracts with the terms of the agreement directly written into code. In healthcare, smart contracts can automate administrative tasks such as billing, insurance claims, and reimbursement. For example, a smart contract could automatically trigger a payment once treatment is confirmed, ensuring timely payment and reducing human error or fraud.

Elimination of Redundancies: Blockchain enables automation and standardization, which reduces duplication of efforts across multiple healthcare providers. For instance, the same patient's data doesn't need to be manually entered multiple times at different hospitals or clinics. Blockchain's shared and transparent nature ensures that data is always up-to-date and accessible, reducing the chances of redundant tests or procedures.

By automating processes and reducing inefficiencies, blockchain can help create a more cost-effective and patient-centric healthcare system, ultimately leading to improved healthcare delivery.

4.5. Better Data Accuracy

Data accuracy is critical in healthcare, as errors in medical records, test results, or treatment protocols can lead to misdiagnoses, unnecessary treatments, or even patient harm. Blockchain addresses this issue by ensuring that healthcare data is both accurate and immutable:

Immutability of Records: Once data is entered into the blockchain, it becomes immutable—meaning that it cannot be changed or deleted. This ensures that all healthcare records, including diagnoses, treatments, and patient history, are verifiable and consistent across all participants in the network. Medical records are maintained with a high level of accuracy, reducing the chances of errors due to data manipulation or discrepancies between systems.

Real-Time Data Updates: Blockchain enables real-time updates to patient data, ensuring that healthcare providers have access to the most current and accurate information available. This is especially important in emergency care situations, where up-to-date information about a patient's medical history, allergies, and prior treatments can be life-saving**.**

Error Reduction: By recording data in an immutable ledger, blockchain minimizes the potential for errors that might arise from human intervention, such as typing mistakes or misunderstandings during data entry. It also

ensures that every transaction or change to a record is logged and can be reviewed, further minimizing the risk of inaccurate or fraudulent data.

The accuracy of healthcare data is vital for effective treatment and care coordination. Blockchain provides a robust solution by ensuring that medical records are trustworthy, consistent, and up-to-date.

4.6 Related Works

Several studies have explored how blockchain can be used for efficient and secure healthcare data management and two of them are highlighted in Table 3. Al Mamun et al. (2022) [23] provide a detailed review of blockchain-based solutions for managing electronic health records (EHRs) and propose a comprehensive framework for future research in this area. The authors discuss the potential of blockchain to streamline healthcare data management by creating a secure and decentralized database for medical records, which can be accessed by authorized personnel across multiple institutions (Al Mamun et al., 2022).
Additionally, Zaabar et al. (2021) [24] describe HealthBlock, a secure blockchain-based healthcare data management system that utilizes smart contracts for data access and processing (Zaabar et al., 2021). This approach allows for automated, transparent, and verifiable data transactions, reducing the need for intermediaries and improving overall efficiency in healthcare data management.

Table 3: State of the art methods (Blockchain Application)

Reference	Focus	Blockchain Application
Al Mamun et al. (2022) [23]	Blockchain-based solutions for managing Electronic Health Records (EHRs)	Decentralized database for medical records management, accessible by authorized users across multiple institutions
Zaabar et al. (2021) [24]	HealthBlock: A blockchain-based healthcare data management system using smart contracts	Smart contracts for automated and secure data transactions, enhancing transparency and efficiency in healthcare data management

5. Challenges to the Implementation of Blockchain in Healthcare

Despite the many promising benefits of blockchain technology, its adoption in healthcare is not without significant challenges. These challenges range from technical and regulatory hurdles to issues related to privacy, integration, and environmental impact. Below are some of the primary obstacles that must be addressed for blockchain to be effectively integrated into healthcare systems [25-28].

5.1. Scalability

One of the key challenges facing the adoption of blockchain in healthcare is scalability. Blockchain's decentralized nature, while beneficial for security and trust, can pose difficulties when applied to large-scale systems like healthcare. Some specific scalability concerns include:

Transaction Speed: Blockchain transactions are often slower compared to traditional centralized databases due to the need for consensus mechanisms and the validation of transactions by all nodes in the network. For instance, blockchain platforms using Proof of Work (PoW), such as Bitcoin, can process only a limited number of transactions per second. In a global healthcare system where vast amounts of medical data need to be transferred quickly (e.g., in emergency situations), blockchain could face significant latency issues. Slow transaction processing could result in delays in accessing critical patient information, which is unacceptable in time-sensitive medical environments.

Storage Capacity: Healthcare data, particularly electronic health records (EHRs), are massive and continuously growing. Storing this data on the blockchain, where every transaction is stored permanently, could lead to massive data bloat. As the number of records increases, the blockchain would need an exponentially larger amount of storage, which could make the system inefficient and cost-prohibitive. Although techniques like off-chain storage (where large data is stored outside the blockchain but linked to it) are being explored, scalability remains a concern when dealing with large, complex datasets like medical images, genetic information, and long patient histories.

Network Latency and Throughput: Large-scale healthcare systems would require a high throughput of transactions and low latency to function effectively. Most public blockchains today, such as Bitcoin or Ethereum, are still not optimized for high-volume use cases, like handling millions of healthcare transactions per day. As blockchain networks grow in size, their processing power and capacity may struggle to keep up with the demands of real-world healthcare systems.

Addressing scalability is a priority for blockchain researchers and developers, and solutions such as sharding, layer 2 solutions (e.g., Lightning Network), and consensus algorithm optimization are being explored to make blockchain more suitable for large-scale healthcare applications.

5.2. Regulatory and Legal Issues

Healthcare is one of the most heavily regulated industries globally, and blockchain's introduction into healthcare systems presents significant regulatory challenges. Some of the primary concerns include:

Compliance with Laws: Blockchain-based healthcare systems must comply with existing laws and regulations, such as HIPAA in the U.S., GDPR (General Data Protection Regulation) in the European Union, and similar laws in other countries. These regulations govern data privacy, access control, and security, and they require healthcare providers to maintain strict oversight of patient data. Blockchain, with its decentralized structure, can complicate this oversight, as it does not fit neatly into existing frameworks for data governance.

Data Ownership: A critical legal issue is data ownership. In a blockchain-based system, multiple parties (e.g., patients, healthcare providers, insurers) have access to the same data, raising questions about who truly owns the medical data. The patient may have control over access, but it is unclear how that control aligns with existing ownership concepts in healthcare data laws. The complexity of defining data ownership in a decentralized, immutable system makes it difficult to apply conventional legal frameworks, leading to legal ambiguity.

Right to be Forgotten: One of the most significant challenges blockchain poses to healthcare compliance is the Right to be Forgotten under regulations like the GDPR. The immutability of blockchain means that once data is recorded, it cannot be deleted or altered, even if the patient requests it. This creates a conflict between blockchain's inherent features and privacy laws, as healthcare systems are required to delete personal data when requested by the patient. Resolving this conflict will require new legal interpretations or technological solutions, such as cryptographic techniques that allow for data erasure without compromising the integrity of the blockchain.

Cross-Jurisdictional Compliance: Healthcare data often crosses national borders, and blockchain's decentralized nature could complicate compliance with international data privacy and protection laws. For instance, how can blockchain-based systems comply with both HIPAA in the U.S. and GDPR in Europe if they are dealing with healthcare data across borders? Legal harmonization will be required to allow blockchain technology to scale globally in healthcare.

5.3. Data Privacy

While blockchain offers strong security features, it also presents significant concerns regarding data privacy. Some key issues include:

Immutability vs. Privacy: Blockchain's immutability is one of its most powerful features, but it also creates a challenge for healthcare systems where personal health information might need to be updated or erased. For example, when a patient's information changes, such as a change in medication or diagnosis, blockchain records are permanent and cannot be altered. This can be problematic when healthcare systems need to update or delete outdated information to ensure that data remains accurate.

Personal Data Exposure: Although blockchain can encrypt data and provide access controls, the transparency of public blockchains can still expose too much personal information to unauthorized parties. Even if health data is encrypted, the very nature of blockchain allows for anyone on the network to view the data's history, creating privacy concerns around who can access what information. Sensitive data such as diagnostic results, treatments, or personal health identifiers could be exposed to individuals or entities who are not authorized to view them, leading to privacy violations.

Permissioned vs. Permissionless Blockchains: The type of blockchain (permissioned vs. permissionless) used in healthcare could influence privacy concerns. While permissioned blockchains provide more control over who can access data, they still face challenges with privacy if the systems are not properly designed. In contrast, permissionless blockchains, which are more open and decentralized, are harder to regulate, which could create significant privacy risks in a sector as sensitive as healthcare.

5.4. Integration with Legacy Systems

Healthcare systems are often built on legacy infrastructures, many of which rely on centralized databases and older technologies. Integrating blockchain into these systems can be complex and costly for several reasons:

Technical Compatibility: Most healthcare organizations use established IT systems that are not designed to work with blockchain technology. These systems may store data in proprietary formats or rely on outdated protocols, creating challenges in interoperability with blockchain. The integration process could involve significant re-engineering of legacy systems to ensure seamless communication with blockchain solutions.

High Implementation Costs: Transitioning to a blockchain-based system often requires substantial investment in new technologies and training. Healthcare providers would need to invest in both the blockchain infrastructure itself (servers, nodes, consensus mechanisms) and the integration of blockchain with existing software solutions (EHR systems, hospital management software, etc.). For many institutions, particularly small or medium-sized providers, these costs may be prohibitively high.

Data Migration: Migrating historical healthcare data from existing centralized systems to a blockchain-based system could be a time-consuming and error-prone process. Data must be cleansed, standardized, and converted into a format that can be stored on the blockchain, and this process must be done carefully to ensure that no critical information is lost or corrupted in the transition.

To overcome these hurdles, healthcare organizations may need to adopt a phased approach to blockchain adoption, starting with smaller, less critical applications (such as supply chain management or clinical trial data) before rolling out blockchain across the entire system.

5.5. Energy Consumption

Blockchain networks, especially those that use Proof of Work (PoW) consensus mechanisms, are known for their high energy consumption. This is a significant concern for widespread adoption in industries like healthcare, where sustainability and environmental considerations are increasingly important. Some key concerns include:

High Energy Demands: Proof of Work, the consensus mechanism used by blockchains like Bitcoin, requires enormous computational resources and energy to validate transactions and secure the network. This could be a major issue in the context of healthcare, as energy consumption can result in higher operational costs and environmental impact.

Cost Implications: The energy-intensive nature of some blockchain networks could significantly increase the costs of using blockchain in healthcare applications. These added costs could be passed on to healthcare providers, insurers, or patients, making blockchain-based solutions less attractive from an economic standpoint.

Environmental Impact: The environmental impact of blockchain, particularly PoW-based networks, has drawn significant criticism due to their carbon footprint. As the healthcare industry moves toward more sustainable practices, blockchain's environmental impact could pose a significant barrier to its adoption unless more energy-efficient consensus mechanisms, such as Proof of Stake (PoS), are used.

To address these concerns, the blockchain industry is increasingly exploring more energy-efficient alternatives, including PoS and other consensus mechanisms that require less computational power.

5.6 Related Works

While blockchain offers numerous benefits, its adoption in healthcare is not without challenges. Issues related to scalability, regulatory compliance, and integration with existing healthcare infrastructure are frequently mentioned in the literature (Table 4). Tandon et al. (2020) discuss these challenges and propose a framework to guide the adoption of blockchain in healthcare systems. The authors highlight that regulatory hurdle, such as the need to comply with health data privacy laws like HIPAA, could slow the implementation of blockchain technologies (Tandon et al., 2020).
Similarly, Arbabi et al. (2022) identifies several technical challenges in adopting blockchain for healthcare, including issues with blockchain's energy consumption and its lack of scalability for handling large volumes of medical data. These challenges must be addressed through innovations in blockchain architecture, such as lightweight blockchain solutions, which are explored by Ismail et al. (2019) as a way to improve blockchain's efficiency in healthcare contexts (Ismail et al., 2019).

Table 4: State of the art methods (Blockchain Challenges)

Reference	Focus	Blockchain Challenges
Tandon et al. (2020) [29]	Discussing the regulatory challenges in adopting blockchain in healthcare	Regulatory hurdles, particularly compliance with HIPAA and other privacy laws
Arbabi et al. (2022) [30]	Identifying technical challenges in adopting blockchain for healthcare	Energy consumption, scalability issues when handling large medical datasets
Ismail et al. (2019) [31]	Exploring lightweight blockchain solutions for improving blockchain efficiency in healthcare	Inefficiency and scalability problems with traditional blockchain solutions

6. Future Directions and Research

Blockchain technology has the potential to transform healthcare, offering significant improvements in security, privacy, transparency, and efficiency. However, the full adoption and integration of blockchain into healthcare systems face several challenges, as outlined in earlier sections. Moving forward, focused research and development efforts will be critical to overcoming these barriers and realizing the true potential of blockchain in healthcare. Below are some key areas where future research should be concentrated to ensure blockchain can be effectively and sustainably implemented in healthcare systems.

6.1. Improved Consensus Mechanisms

Consensus mechanisms are central to the operation of any blockchain network. They ensure that all participants in the network agree on the validity of transactions and the state of the ledger. However, current

consensus algorithms, such as Proof of Work (PoW), have inherent issues related to energy consumption, scalability, and transaction speed—issues that are particularly problematic in healthcare. Therefore, one of the most important areas of future research should be the development of energy-efficient consensus algorithms that can handle the high-volume transactions typical of healthcare data while minimizing their environmental impact. Key research directions include:

Proof of Stake (PoS): PoS is often touted as a more energy-efficient alternative to PoW. Unlike PoW, which requires participants to solve complex mathematical problems, PoS selects validators based on the amount of cryptocurrency they "stake" in the network. PoS could offer faster and more energy-efficient transaction validation, which would be crucial for large-scale healthcare applications.

Hybrid Consensus Models: Hybrid models, such as delegated PoS (DPoS) or Practical Byzantine Fault Tolerance (PBFT), combine multiple consensus mechanisms to strike a balance between efficiency, scalability, and decentralization. Research into these hybrid models could offer a more robust solution that meets the specific needs of healthcare systems.

Scalability Optimizations: Consensus mechanisms also need to be optimized for high transaction throughput. Healthcare data systems often involve large datasets that require quick access, especially in real-time healthcare applications. New mechanisms that reduce latency and improve throughput will be essential for the widespread use of blockchain in clinical environments, emergency care, and large-scale health monitoring systems.

Security and Privacy: In addition to efficiency, consensus mechanisms must continue to prioritize the security and privacy of patient data. Research should explore ways to maintain the integrity of blockchain while simultaneously providing advanced encryption and privacy-preserving features (e.g., zero-knowledge proofs).

6.2. Interoperability Standards

One of the significant barriers to blockchain adoption in healthcare is the lack of interoperability between blockchain-based systems and existing healthcare infrastructures, many of which are based on centralized, legacy systems. For blockchain to become a mainstream technology in healthcare, standards for blockchain integration with existing healthcare data systems, such as Electronic Health Records (EHRs) and Electronic Medical Records (EMRs), must be developed.

Standardization of Data Formats: Healthcare data is often stored in proprietary formats that make it difficult to share across platforms. Blockchain adoption in healthcare will require the development of open standards for data formats to enable seamless data sharing between blockchain and non-blockchain systems. For example, standardized data formats for clinical records, diagnostic images, and medical claims could ensure compatibility across different healthcare providers and jurisdictions.

Cross-System Compatibility: Different healthcare providers may use different systems to store patient data. Blockchain should be designed to interact with a variety of health information exchanges (HIEs), hospital management systems, and insurance claim processing systems. Research should focus on creating protocols that allow blockchain networks to securely exchange data with these systems without compromising patient privacy or data integrity.

Integration with IoT Devices: With the rise of the Internet of Medical Things (IoMT), which connects medical devices to the internet to gather real-time health data, ensuring that these devices can securely communicate with blockchain systems will be crucial. Research could explore interoperability standards that facilitate seamless integration of blockchain with medical devices like wearables, diagnostic tools, and remote patient monitoring systems.

6.3. Regulatory Frameworks

Healthcare is a highly regulated industry, and the use of blockchain in healthcare systems introduces new legal and ethical considerations. Future research must involve close collaboration between blockchain developers, healthcare providers, and policymakers to establish regulatory frameworks that govern blockchain applications while ensuring patient privacy and compliance with existing laws. Key areas for regulatory research include:

Data Privacy and Security Regulations: One of the most pressing issues is how blockchain can comply with privacy regulations such as HIPAA (Health Insurance Portability and Accountability Act) in the U.S. and GDPR (General Data Protection Regulation) in the EU. Blockchain's immutable and transparent nature could conflict with the right to be forgotten, where patients are entitled to request the deletion of their personal data. Research should aim to develop regulatory guidelines that allow for compliance with these laws while leveraging the benefits of blockchain technology.

Data Ownership and Consent: Defining data ownership and establishing robust patient consent mechanisms are essential in a blockchain-based healthcare system. While blockchain allows patients to control access to their own health data, the legal frameworks must clarify the rights of patients in a decentralized system, including their ability to revoke consent and manage who has access to their health data. Research should focus on clear legal definitions of ownership and the mechanisms for recording patient consent on the blockchain in a legally enforceable manner.

Cross-Jurisdictional Challenges: Since healthcare data often crosses national borders, research into cross-jurisdictional compliance is needed to ensure that blockchain networks comply with multiple, often conflicting, data protection laws. International collaboration will be key to resolving these regulatory issues and ensuring that blockchain can be used globally in healthcare.

Liability and Accountability: Research should also focus on clarifying the legal liability in blockchain healthcare networks. For instance, in the event of a medical error or data breach, it must be clear who is legally responsible—the healthcare provider, the blockchain network operator, or the patient. Establishing clear accountability frameworks will be vital to the widespread acceptance and legal integration of blockchain in healthcare.

6.4. Pilot Projects and Real-World Applications

Finally, one of the most critical areas of future research is the implementation of pilot projects and real-world use cases to demonstrate the practical viability and scalability of blockchain in healthcare. Pilot projects can help uncover the practical challenges of blockchain adoption and provide valuable insights into how blockchain can be integrated into complex healthcare systems. Future research should prioritize:

Proof-of-Concept Projects: Healthcare providers, technology firms, and blockchain developers should collaborate on pilot programs to test blockchain applications in specific healthcare domains, such as Electronic Health Records (EHRs), supply chain management for pharmaceuticals, or medical billing and insurance claims. These pilots can help validate the technology's efficacy, scalability, and usability in real-world healthcare settings.

Testing in High-Stakes Environments: Conducting blockchain pilots in critical healthcare environments, such as emergency departments or during clinical trials, can test how well blockchain performs in high-pressure situations where real-time data and rapid decision-making are required.

Long-Term Evaluation: Blockchain systems are still relatively new, and long-term studies will be essential to understanding their sustainability in healthcare. Research should focus on evaluating the long-term effects of blockchain adoption on patient care, data integrity, security, and costs, as well as the economic impact on healthcare systems.

User Experience and Adoption: A critical factor in the success of blockchain in healthcare is the user experience for healthcare providers and patients. Research should focus on understanding how doctors, nurses, and patients interact with blockchain-based systems, as well as addressing usability challenges. Ensuring that blockchain solutions are easy to use and understand will be key to widespread adoption.

6.5 Related Works

Finally, there is growing interest in using blockchain for health data analytics (Table 5). Dash et al. (2019) [32] explore the integration of big data, machine learning, and blockchain for predictive analytics in healthcare, showing how blockchain can provide secure data storage and sharing capabilities for large-scale health datasets (Dash et al., 2019). Chen et al. (2021) [33] also explore the use of blockchain for diabetes detection by providing a secure platform for exchanging health data that can be analyzed for early detection and intervention (Chen et al., 2021).

Looking ahead, several authors highlight the need for further research in areas such as blockchain scalability, integration with IoT, and advanced cryptographic techniques to enhance the privacy and security of healthcare data (Saeed et al., 2022 [34]; Yaqoob et al., 2022 [35]). The future of blockchain in healthcare will depend on overcoming these challenges and developing practical, scalable solutions that can be widely adopted across the healthcare ecosystem.

Table 5: State of the art methods (Blockchain Application)

Reference	Focus	Blockchain Application
Dash et al. (2019) [32]	Integration of big data, machine learning, and blockchain for predictive analytics	Blockchain for secure storage and sharing of large-scale health datasets to enable predictive analytics in healthcare
Chen et al. (2021) [33]	Use of blockchain for diabetes detection and early intervention	Blockchain as a secure platform for exchanging health data to facilitate early detection and intervention for diabetes
Saeed et al. (2022) [34]	Future research directions in blockchain scalability, IoT integration, and advanced cryptographic techniques	Blockchain research focused on overcoming challenges related to scalability, security, and data privacy
Yaqoob et al. (2022) [35]	Identifying future research needs in scalability and privacy enhancement for healthcare data	Emphasizes the development of practical, scalable blockchain solutions for broader adoption in healthcare systems

7. Conclusion

In conclusion, blockchain technology holds significant promise for transforming healthcare systems, particularly in the management of electronic health records (EHRs), enhancing data security, ensuring patient privacy, and fostering interoperability. As a decentralized and immutable system, blockchain offers a robust solution to many of the challenges facing the healthcare sector today, including unauthorized access to sensitive health data, fragmented healthcare infrastructures, and inefficiencies in data sharing.

This review highlights the diverse applications of blockchain in healthcare, from securing EHRs and enabling privacy-preserving data exchanges to improving the transparency and efficiency of healthcare operations through smart contracts and decentralized applications. Furthermore, blockchain's potential to facilitate secure collaboration among multiple stakeholders—patients, doctors, medical institutions, and third-party service providers—paves the way for more integrated, patient-centered healthcare systems.

However, despite its many advantages, the widespread adoption of blockchain in healthcare is not without challenges. Issues such as regulatory compliance, scalability, integration with existing healthcare infrastructure, and energy consumption of blockchain networks need to be addressed before blockchain can be fully integrated into mainstream healthcare systems. Moreover, further research is needed to develop

lightweight blockchain solutions that can handle the large volume of data generated in healthcare environments without compromising performance or security.

The future of blockchain in healthcare looks promising, with ongoing advancements in cryptography, scalability, and the integration of blockchain with emerging technologies such as the Internet of Things (IoT) and artificial intelligence (AI). To realize the full potential of blockchain-enabled healthcare systems, it is essential for researchers, healthcare providers, regulators, and technology developers to collaborate in overcoming the technical, regulatory, and operational challenges that remain.

Ultimately, blockchain has the potential to revolutionize healthcare by ensuring secure, transparent, and efficient management of medical data, leading to improved patient outcomes and a more resilient healthcare ecosystem. The path to blockchain adoption in healthcare requires continued innovation, rigorous testing, and comprehensive policy development to ensure that its benefits are fully realized while safeguarding patient privacy and maintaining regulatory compliance.

References

1. Haddad, Alaa, Mohamed Hadi Habaebi, Md Rafiqul Islam, Nurul Fadzlin Hasbullah, and Suriza Ahmad Zabidi. "Systematic review on ai-blockchain based e-healthcare records management systems." *IEEE Access* 10 (2022): 94583-94615.
2. Rahman, Md Shafiur, Md Amirul Islam, Md Ashraf Uddin, and Giovanni Stea. "A survey of blockchain-based IoT eHealthcare: Applications, research issues, and challenges." *Internet of Things* 19 (2022): 100551.
3. Act, Accountability. "Health insurance portability and accountability act of 1996." *Public law* 104 (1996): 191.
4. Menachemi, Nir, and Taleah H. Collum. "Benefits and drawbacks of electronic health record systems." *Risk management and healthcare policy* (2011): 47-55.
5. Rahman, Md Zia Ur, Sumalatha Akunuri, D. Nagabhushana Babu, M. V. S. Ramprasad, Sk Mohammed Shareef, and Masreshaw D. Bayleyegn. "Proof of trust and expertise (PoTE): A novel consensus mechanism for enhanced security and scalability in electronic health record management." *IEEE Access* (2024).
6. GDPR, General Data Protection Regulation. "General data protection regulation." *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC* (2016).
7. Panwar, Arvind, and Vishal Bhatnagar. "Distributed ledger technology (DLT): The beginning of a technological revolution for blockchain." In *2nd International Conference on Data, Engineering and Applications (IDEA)*, pp. 1-5. IEEE, 2020.
8. Mandapuram, Mounika. "Applications of Blockchain and Distributed Ledger Technology (DLT) in Commercial Settings." *Asian Accounting and Auditing Advancement* 7, no. 1 (2016): 50-57.
9. Rico-Pena, Juan Jesus, Raquel Arguedas-Sanz, and Carmen Lopez-Martin. "Models used to characterise blockchain features. A systematic literature review and bibliometric analysis." *Technovation* 123 (2023): 102711.
10. Saad, Sheikh Munir Skh, and Raja Zahilah Raja Mohd Radzi. "Comparative review of the blockchain consensus algorithm between proof of stake (pos) and delegated proof of stake (dpos)." *International Journal of Innovative Computing* 10, no. 2 (2020).
11. Castro, Miguel, and Barbara Liskov. "Practical byzantine fault tolerance." In *OsDI*, vol. 99, no. 1999, pp. 173-186. 1999.
12. Shi, Shuyun, Debiao He, Li Li, Neeraj Kumar, Muhammad Khurram Khan, and Kim-Kwang Raymond Choo. "Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey." *Computers & security* 97 (2020): 101966.
13. Keshta, Ismail, and Ammar Odeh. "Security and privacy of electronic health records: Concerns and challenges." *Egyptian Informatics Journal* 22, no. 2 (2021): 177-183.

14. Saeed, Huma, Hassaan Malik, Umair Bashir, Aiesha Ahmad, Shafia Riaz, Maheen Ilyas, Wajahat Anwaar Bukhari, and Muhammad Imran Ali Khan. "Blockchain technology in healthcare: A systematic review." *PLOS One* 17, no. 4 (2022): e0266462.
15. Zhang, Peng, Douglas C. Schmidt, Jules White, and Gunther Lenz. "Blockchain technology use cases in healthcare." In *Advances in computers*, vol. 111, pp. 1-41. Elsevier, 2018.
16. Nanda, Saroj Kumar, Sandeep Kumar Panda, and Madhabananda Dash. "Medical supply chain integrated with blockchain and IoT to track the logistics of medical products." *Multimedia Tools and Applications* 82, no. 21 (2023): 32917-32939.
17. Omar, Ilhaam A., Raja Jayaraman, Khaled Salah, Ibrar Yaqoob, and Samer Ellahham. "Applications of blockchain technology in clinical trials: review and open challenges." *Arabian Journal for Science and Engineering* 46, no. 4 (2021): 3001-3015.
18. Hassan, Abid, MD Iftekhar Ali, Rifat Ahammed, Mohammad Monirujjaman Khan, Nawal Alsufyani, and Abdulmajeed Alsufyani. "Secured insurance framework using blockchain and smart contract." *Scientific Programming* 2021, no. 1 (2021): 6787406.
19. Hao, Aiyu, and Ling Wang. "Medical device integration model based on the internet of things." *The Open Biomedical Engineering Journal* 9 (2015): 256.
20. Aceto, Giuseppe, Valerio Persico, and Antonio Pescapé. "Industry 4.0 and health: Internet of things, big data, and cloud computing for healthcare 4.0." *Journal of Industrial Information Integration* 18 (2020): 100129.
21. Villarreal, Edgar R. Dulce, Jose García-Alonso, Enrique Moguel, and Julio Ariel Hurtado Alegría. "Blockchain for healthcare management systems: A survey on interoperability and security." *IEEE Access* 11 (2023): 5629-5652.
22. Hasselgren, Anton, Katina Kralevska, Danilo Gligoroski, Sindre A. Pedersen, and Arild Faxvaag. "Blockchain in healthcare and health sciences—A scoping review." *International Journal of Medical Informatics* 134 (2020): 104040.
23. Al Mamun, Abdullah, Sami Azam, and Clementine Gritti. "Blockchain-based electronic health records management: a comprehensive review and future research direction." *IEEE Access* 10 (2022): 5768-5789.
24. Zaabar, Bessem, Omar Cheikhrouhou, Faisal Jamil, Meryem Ammi, and Mohamed Abid. "HealthBlock: A secure blockchain-based healthcare data management system." *Computer Networks* 200 (2021): 108500.
25. Attaran, Mohsen. "Blockchain technology in healthcare: Challenges and opportunities." *International Journal of Healthcare Management* 15, no. 1 (2022): 70-83.
26. Pandey, Prateek, and Ratnesh Litoriya. "Implementing healthcare services on a large scale: challenges and remedies based on blockchain technology." *Health Policy and Technology* 9, no. 1 (2020): 69-78.
27. Gökalp, Ebru, Mert Onuralp Gökalp, Selin Çoban, and P. Erhan Eren. "Analysing opportunities and challenges of integrated blockchain technologies in healthcare." *Information Systems: Research, Development, Applications, Education: 11th SIGSAND/PLAIS EuroSymposium 2018, Gdansk, Poland, September 20, 2018, Proceedings 11* (2018): 174-183.
28. McGhin, Thomas, Kim-Kwang Raymond Choo, Charles Zhechao Liu, and Debiao He. "Blockchain in healthcare applications: Research challenges and opportunities." *Journal of network and computer applications* 135 (2019): 62-75.
29. Tandon, Anushree, Amandeep Dhir, AKM Najmul Islam, and Matti Mäntymäki. "Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda." *Computers in Industry* 122 (2020): 103290.
30. Arbabi, Mohammad Salar, Chhagan Lal, Narasimha Raghavan Veeraragavan, Dusica Marijan, Jan F. Nygård, and Roman Vitenberg. "A survey on blockchain for healthcare: Challenges, benefits, and future directions." *IEEE Communications Surveys & Tutorials* 25, no. 1 (2022): 386-424.
31. Ismail, Leila, Huned Materwala, and Sherali Zeadally. "Lightweight blockchain for healthcare." *IEEE Access* 7 (2019): 149935-149951.
32. Dash, Sabyasachi, Sushil Kumar Shakyawar, Mohit Sharma, and Sandeep Kaushik. "Big data in healthcare: management, analysis and future prospects." *Journal of big data* 6, no. 1 (2019): 1-25.

33. Chen, Mengji, Taj Malook, Ateeq Ur Rehman, Yar Muhammad, Mohammad Dahman Alshehri, Aamir Akbar, Muhammad Bilal, and Muazzam A. Khan. "Blockchain-Enabled healthcare system for detection of diabetes." *Journal of Information Security and Applications* 58 (2021): 102771.
34. Saeed, Huma, Hassaan Malik, Umair Bashir, Aiesha Ahmad, Shafia Riaz, Maheen Ilyas, Wajahat Anwaar Bukhari, and Muhammad Imran Ali Khan. "Blockchain technology in healthcare: A systematic review." *PLOS One* 17, no. 4 (2022): e0266462.
35. Yaqoob, Ibrar, Khaled Salah, Raja Jayaraman, and Yousof Al-Hammadi. "Blockchain for healthcare data management: opportunities, challenges, and future recommendations." *Neural Computing and Applications* (2022): 1-16.