REPUBLIC OF TÜRKİYE

ALTINBAŞ UNIVERSITY

Institute of Graduate Studies

COMPUTER ENGINEERING AND INFORMATION TECHNOLOGY

BLOCKCHAIN INTEGRATION IN HEALTH CARE INFORMATION SYSTEM: A SECURE AND EFFICIENT APPROACH

Taiye MUKTAR

M.Sc. Thesis

Supervisor

Asst. Professor Timur İNAN

Istanbul, 2024

BLOCKCHAIN INTEGRATION IN HEALTHCARE INFORMATION SYSTEM: A SECURE AND EFFICIENT APPROACH

Taiye MUKTAR

Computer Engineering and Information Technology Department

Master of Science Thesis

Altinbas University

2024

The thesis titled BLOCKCHAIN INTEGRATION IN HEALTHCARE INFORMATION SYSTEM: A SECURE AND EFFICIENT APPROACH prepared by TAIYE MUKTAR and submitted on 10/06/2024 has been **accepted unanimously** for the degree of Master of Science in Informatıon Technologies.

Asst. Prof. Dr. Timur İNAN
Supervisor

Thesis Defense Committee Members:

Asst. Prof. Dr. Timur İNAN	Department of Computer Engineering, Marmara University	____________
Assoc. Prof. Dr. Oğuz ATA	Department of Software Engineering, Altınbaş University	____________
Assoc. Prof. Dr. Kazım YILDIZ	Department of Computer Engineering, Marmara University	____________

I hereby declare that this thesis meets all format and submission requirements of a master's thesis.

I hereby attest that all information of this graduation project has been achieved following academic rules and ethics. All copying studies and findings stated have been referenced in the body text and the references listed, and all in-text citations included in the Reference List are cited in the body text.

Taiye MUKTAR

Signature

DEDICATION

I dedicate this thesis to my lovely spouse and amazing son for their patience and understanding during my study period; HAUWA BABA DANJUMA & USMAN MUKTAR.

ABSTRACT

BLOCKCHAIN INTEGRATION IN HEALTHCARE INFORMATION SYSTEM; A SECURE AND EFFICIENT APPROACH

MUKTAR, Taiye
M.Sc., Computer Engineering and Information Technology Department, Altınbaş University,

Supervisor: Asst. Prof. Dr. Timur İNAN

Date: May/2024

Pages: 61

Because a decentralized open healthcare web is involved, blockchain technology presents a sharp approach for reserving medical information, accomplishing medical processes, and improving confidence for medical information sharing and interaction. Despite the recent significant interest regarding the service of blockchain in the healthcare enterprise, the privacy and security of blockchain technologies are the main issues that are focused in the literature for blockchain-based medical data sharing and transactions. To the best of my knowledge and by covering the literature from 2018 through 2023, I critically evaluate the state of the art in this field with a focus on the works that address the challenges and the applications of blockchain for improved healthcare systems. Our review serves to guide future research areas and improvements by critically appraising and summarizing the literature.

Keywords: Technology in blockchain, Safety and Privacy, Medical Industry, IT

TABLE OF CONTENTS

LIST OF TABLES

Pages

LIST OF FIGURES

Pages

ABBREVIATIONS

PoW	:	Proof-of-Work
PoS	:	Proof of Stake
IoT	:	Internet of Things
PBFT	:	Practical Byzantine Fault Tolerance
EHR	:	Electronic Health Record

1. INTRODUCTION

1.1 BACKGROUND OF THE STUDY

1.1.1 Overview

The blockchain revolution has revolutionized the way we exchange, store, and secure data globally, across all sectors. In healthcare, protecting the privacy of patient statements is critical. This project will explore the role of blockchain technology in improving the security, integrity, and interoperability of healthcare IT systems. In addition to the improved management of health information, we will critically assess the importance and disadvantages of integrating blockchain with existing healthcare IT architectures. The advent of Bitcoin in 2008 showcased the capabilities of blockchain, highlighting features such as decentralization, transparency, and anonymity [1]. Bitcoin's success has sparked interest in the application of blockchain across other data-centric fields, including healthcare [2].

Healthcare services, known for their critical need for timeliness, security, and reliability, often rely on centralized server architectures. These systems limit access to medical data to specific network participants [3], potentially causing delays in medical services and risks to data security. Often, patients are unaware of which entities possess or utilize their health information without consent. The current healthcare systems face challenges in providing secure, multi-entity access to medical records within hospital networks [4].

1.1.2 Blockchain

Blockchain is nothing but a public, distributed register that cannot be altered and stores any transactions. It is designed to be used in a trustless setting where parties to a transaction do not necessarily belief each other [6-5]. It is comprised of a chain of blocks, the "blocks" being individual records linked using cryptography. Each block has a connection to the prior block and a link to the subsequent block, once a block is created, recorded and verified [7]. Initially, blockchain allowed for the open reading, writing, and modification of data by any user, facilitating decentralized management and transactions. This openness has garnered significant interest in blockchain for various applications. Moreover, blockchain supports the concept of smart contracts, which are automated agreements executed without intermediaries. Presently, Ethereum is the most prominent platform supporting smart contracts on the blockchain [8].

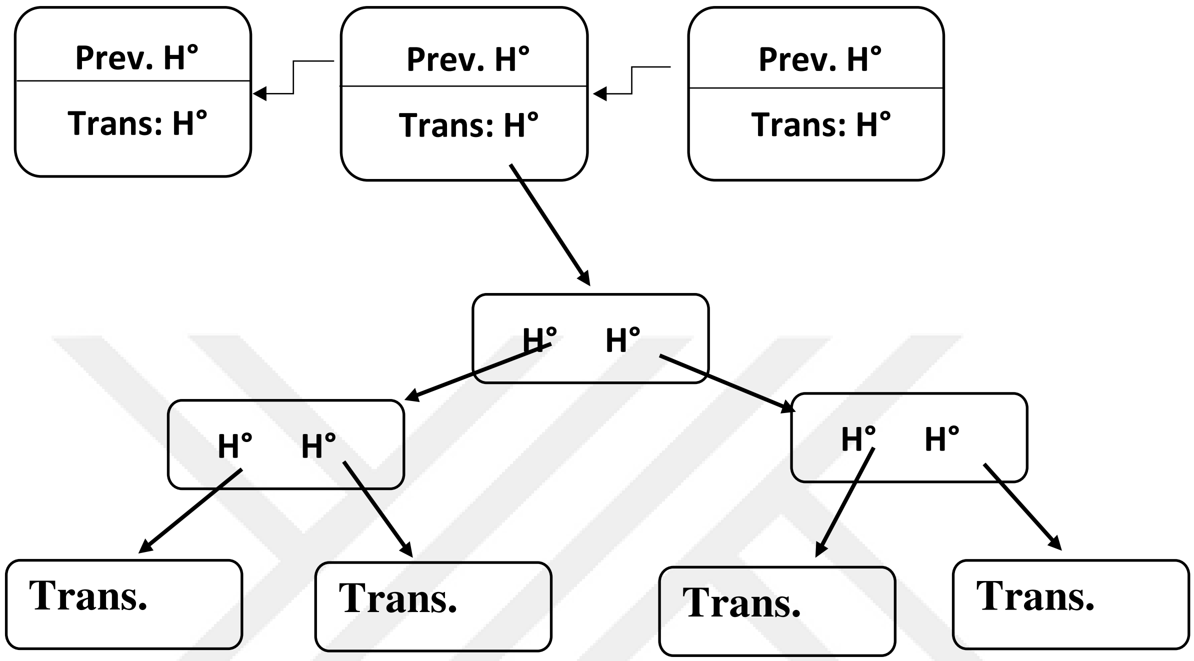

Figure 1.1 Blockchain Structure

1.1.2.1 Key characteristics

Decentralization, or the lack of a single entity controlling the information on the blockchain, is one of the key premises of the technology. Instead, a network of members owning the computing power comes to a consensus as to which entries should be added to the blockchain by applying various consensus mechanisms. Another property is the data permanence or immutability: once an entry is accepted and stored on many nodes of the distributed ledger, it is extremely hard or, ideally speaking, infeasible/almost impossible to alter it or delete it. Also, many blockchains are pseudonymous and/or anonymous and this is often an important feature [9]. A distinguishing and very important feature that makes blockchains such a powerful tool for many applications as well as basic and emergent attributes of others is auditability and traceability. It is achieved through creating a connections of the blocks in a sequential sequence. Each of the block is cryptographically link to the earlier block through the piece of information, called hash. The transactions in the block form an additional structure, called a Merkle tree [10] that allows verifying that the transaction is part of a certain block by only needing the top block stored on the blockchain.

1.1.2.2 Type of blockchains

Blockchains are categorized into 3 primary types: consortium (permissioned by public), private, and public (permissionless), each with distinct levels of access for writing, reading, and data retrieval. Public blockchains allow anyone to participate in consensus and software updates, and to view the data, as seen with major cryptocurrencies like Ethereum and Bitcoin [1], which are public permissionless networks. Consortium blockchains are semi-centralized, granting only a limited number of participants the ability to observe and engage in the consensus process. Private blockchains, while decentralized, often have a centralized aspect, with access limited to specific nodes, typically under the control of a single authority [9]. The precise definition and classification of blockchain varieties remain a topic of discussion, with no consensus on the essential characteristics and consensus mechanisms that define a "blockchain" [11].

Public blockchains allow consensus determination by all miners, offer public read permission, and provide a level of immutability that makes tampering nearly impossible. However, they tend to have low efficiency and are not centralized. The consensus process in public blockchains is permissionless, meaning anyone can participate. Consortium blockchains, on the other hand, have their consensus determined by a selected set of nodes. They can have either public or restricted read permissions and a higher risk of immutability being compromised. They are more efficient than public blockchains and are partially centralized. The consensus process is permissioned, restricted to certain participants.

Private blockchains are controlled by one organization, leading to a centralized consensus determination. Like consortium blockchains, they can have public or restricted read permissions and their immutability could be tampered with. They are efficient and fully centralized, with a permissioned consensus process.

Today's blockchain frameworks and platforms enable the creation of decentralized applications (dapps). Among these, Ethereum stands out as a decentralized platform, while Hyperledger is recognized as a framework [12]. Both platforms provide developers with the instruments to construct new blockchain applications on existing networks and to set up new test networks by leveraging their respective protocols.

Table 1.1: Type of blockchains overview

Property	Public blockchain	Consortium blockchain	Private blockchain
Consensus determination	All miners	Selected set of nodes	One organization
Read permission	Public	Public or restricted	Public or restricted
Immutability	Nearly impossible	Could be tampered	Could be tampered
Efficiency	Low	High	High
Centralized	No	Partial	Yes
Consensus process	Permissionless	Permissioned	Permissioned

1.1.2.3. Consensus mechanisms

An essential element of blockchain technology is the method by which data entries are confirmed and recorded on the ledger through a distributed consensus mechanism. There are several concurrence protocols that have been indicated and enforced [6].

Proof-of-Work (PoW) serves as a consensus protocol closely associated with blockchain, notably utilized in Bitcoin. It entails miners vying to solve a complex computational problem by finding a block hash below a specific threshold. The initial miner to achieve this is rewarded and validates the block's transactions [1]. Despite its prevalence, PoW faces scrutiny for its substantial energy consumption, akin to the electricity usage of a small nation in Bitcoin mining [15].

In distinction, Proof of Stake (PoS) offers an alternative approach, where nodes select validators based on their stake in the blockchain, determined by the amount of cryptocurrency they possess. However, this method may favor wealthier nodes. To address this issue, hybrid PoS models have emerged, incorporating a blend of random selection and stake size. Ethereum, the 2nd cryptocurrency, is poised to shift from PoW to PoS [9].

Practical Byzantine Fault Tolerance (PBFT) relies on a Byzantine agreement protocol and mandates that all nodes be identifiable within the network, limiting its viability in public blockchains. The PBFT consensus process unfolds in three stages: pre-preparation, preparation, and commitment, each necessitating a 2/3rd preponderance vote from all nodes to progress. Hyperledger Fabric presently integrates PBFT [14].

Smart contracts, a feature supported by certain blockchain infrastructures like Ethereum, denote self-executing contractual agreements with homogenized source code. These contracts automatically enforce pre-agreed provisions, functioning without intermediaries. The application of smart contract functionality holds promise, particularly in the domain of healthcare [8].

Table 1.2: Consensus mechanisms comparison

Property	**Proof-of-Work (PoW)**	**Proof of Stake (PoS)**	**Practical Byzantine Fault Tolerance (PBFT)**
Node management	Open	Open	Permissioned
Energy consumption	High	Medium	Low
Tolerated power of adversary	< 25% computing power	< 51% stake	< 33.3% faulty replicas
Example	Bitcoin [1]	Peercoin [13]	Hyperledger Fabric [14]

1.1.3 The Potential of Blockchain in the Health Domain

In healthcare facilities, the proficiency to access, modify, and trust data is fundamental to its overall functioning. This sector is driven by challenges, and it relies heavily on both personnel and data. For optimal health outcomes, a multidisciplinary squad of healthcare specialists must utilize current information, tools, and techniques in patient care, encompassing triage, problem-solving, clinical decision-making, enactment, and evaluation of knowledge-based care. Collaboration with academic institutions is vital for training students, providing them with patient access and learning environments, while educational institutions supply the healthcare industry with trained professionals.

Health institutions must also partner with research and engineering-focused organizations for access to experts, informants, subjects, and samples. Participation in clinical trials requires health facilities to contribute to their design, planning, execution, and reporting, receiving in return the latest knowledge, methods, and tools from research and engineering entities.

Thus, entities involved in medical training and biomedical research and engineering are integral to health facility operations (17). Activities necessitate efficient exchange of permissions, patient data, documentation, and reimbursement procedures, which implies transferring data across institutional boundaries. Health institutions are also responsible for safeguarding sensitive patient data.

Preserving patient privacy while sharing data within the healthcare ecosystem needs useful access control, data origin, data integrity, and interoperability. Conventional access management relies on confidence between data lessors and data-storing commodities, which are tasked with setting and enforcing access policies (18). Interoperability enables different information systems, gadgets, or applications to connect and share data to improve personal and population health. Data provenance tracks the narrative and origin of data, enhancing the auditability and trustworthiness of Electronic Health Records (EHR). Data integrity, as defined by Courtney and Ware, concerns meeting or surpassing the anticipated data quality (19).

Healthcare institutions face growing demands for real-world data from enterprise and research bodies (20). Concurrently, public trust in these organizations is eroding due to mishandled data sharing, reported security breaches, and information theft. Trust abuses, such as issues with counterfeit drugs and procedures, represent another challenge. This situation calls for a reevaluation and exploration of alternative strategies. Blockchain technology, with its decentralization, distribution, and data integrity, offers a promising solution for enhancing interoperability, data sharing, access control, provenance, and data integrity, thus fostering a new trust infrastructure without third-party dependence..

1.2 STATEMENT OF THE PROBLEM

Blockchain technology operates as a decentralized and public ledger that documents transactions across multiple computers, ensuring that records cannot be retroactively modified without modifying all subsequent blocks. This system, known as blockchain, creates an extensive chain by validating and linking to the previous block. It provides significant accountability, as each transaction is publicly recorded and verified, rendering the data immutable and authentic. By disseminating data across a web relatively than centralizing it in a single database, blockchain enhances security and mitigates the risk of hacking.

Blockchain presents an outstanding platform for the creation of innovative business models, challenging conventional corporate structures [21]. It is being utilized in varied sectors, including healthcare, to stock and exchange patient information among clinics, laboratories, drugstores, and physicians through a blockchain network. This technology can precisely identify crucial errors in the medical field, thereby enhancing the efficiency, security, and transparency of medical data exchange. Healthcare facilities can harness blockchain to effectively analyze medical data and gain fresh insights.

The healthcare industry is gradually recognizing blockchain's potential to transform healthcare information systems by providing a secure and efficient method. However, there remains a shortage of comprehensive research on the specific challenges and advantages of integrating blockchain into healthcare information systems. The research issue for this thesis topic is to explore the potential benefits and obstacles of integrating blockchain technology into healthcare data systems and to propose a secure and efficient approach that addresses the distinct prerequisites and concerns of the healthcare industry.

1.3 MAIN AIM AND OBJECTIVES OF THE STUDY

1.3.1 Aim

The main aim of this study was to investigate and provide a safe and efficient approach for integrating blockchain technology into healthcare information systems.

1.3.2 Objectives

1. To find out the specific challenges of blockchain integration technology into HealthCare information systems.
2. To explore and evaluate the opportunities to improve the safety and privacy of healthcare data through blockchain, while ensuring data integrity and authenticity.
3. To assess and mitigate the potential uses and risks with the enactment of blockchain in healthcare information systems.
4. To identify & analyze the technical requirements and considerations for integrating blockchain into existing healthcare information systems.
5. To propose strategies and solutions for improving the efficiency and scalability of blockchain solutions to scale the demands of the healthcare facilities.

1.4 RESEARCH QUESTIONS

1. What specific risks and opportunities of blockchain integration technology into healthcare information systems?

2. How can blockchain technology enhance the safety and privacy of healthcare data while confirming data integrity and authenticity?
3. What are the likely benefits and risks in conjunction with implementing blockchain in healthcare information systems, and how can these be mitigated?
4. What are the technical requirements and considerations for integrating blockchain into existing healthcare information systems?
5. How can the efficiency and scalability of blockchain solutions be improved to meet the demands of the healthcare industry?

1.5 JUSTIFICATION OF STUDY

The adoption of healthcare's blockchain information systems could be transformative, enhancing the management, accessibility, and distribution of healthcare data [22]. While interest in this technology is on the rise, there is a noticeable gap in thorough research addressing the specific risks and prospects of blockchain application in healthcare, same as crafting a secure and efficient strategy that meets the sector's distinct needs. Given the sensitive nature of healthcare data, stringent security protocols are essential to maintain patient confidentiality and guard against unauthorized interference [23].

Blockchain's inherent features like decentralized storage, encryption, and permanence can greatly bolster the security and confidentiality of healthcare information systems. It's imperative to delve into these features to confirm the protection of patient's information [23]. The integrity and veracity of healthcare data are critical for precise diagnosis, treatment, and research [24]. Blockchain's structure, which is both decentralized and unalterable, offers a trustworthy method for preserving the integrity and authenticity of healthcare data [23].

Identifying and assessing the potential advantages and drawbacks of blockchain's integration into healthcare is vital. Recognizing the benefits, such as enhanced transparency, interoperability, and data sharing, can guide healthcare organizations in understanding the merits of blockchain adoption. Concurrently, it's important to recognize and address potential risks like scalability constraints, regulatory issues, and technical hurdles.

Technical aspects like system architecture, data standards, interoperability, and scalability must be carefully deemed in the context of blockchain integrations [21]. Exploring technical elements specific to healthcare information systems can offer crucial insights for IT experts and healthcare institutions, aiding in the effective technique and deployment of blockchain solutions. Efficiency and scalability are paramount in the healthcare sector to manage the large volumes of data, ensure prompt access, and facilitate smooth operations. Addressing how to enhance the efficiency and scalability of blockchain within healthcare information systems can help resolve issues related to transaction speeds, energy use, and network capacity, allowing the technology to fulfill the demands of the healthcare field.

1.6 SCOPE AND LIMITATION OF STUDY

The study primarily concentrate on use of blockchain technology in healthcare data strategies, comprising electronic health records, health data trade platforms, and healthcare supply chain administration. It will examine the possibility applications of blockchain technology in these areas and analyze how it can help address the unique requirements and hazard faced by the healthcare industry.

The findings and recommendations of this study may not be universally useful to all healthcare institutions, as the implementation and adoption of blockchain technology can vary depending on factors such as organizational size, resources, and technological infrastructure. Blockchain technology is still evolving, and there may be limitations and technical challenges that need to be considered. The study may not cover all the intricacies and technical facts of implementing blockchain in healthcare information systems.

The analysis is subject to limitations in terms of time, budget, and access to data and resources. These constraints may impact the profundity and capacity of the research, potentially limiting the scope of the study. Blockchain technology in healthcare is a rapidly developing field, and new expansions may occur during or after the study. The study's findings and recommendations may need to be updated or expanded to reflect these emerging trends and advancements.

2. RELATED LITERATURE REVIEW

2.1 INTRODUCTION

Blockchain, a decentralized digital catalog, documents transactions across numerous computers, ensuring that altering any record would necessitate transitions to all subsequent blocks. This process forms a secure chain by validating each of marketing and linking it to previous block. The transparency of blockchain ensures that every transaction is publicly documented and verified, making the data tamper-proof and authentic. By distributing data across a grid relatively than storing it in a single database, blockchain enhances security and reduces hacking risks.

This technology offers a robust platform for developing innovative business models that can rival traditional enterprises [25]. In healthcare, blockchain tracks medical product usage and combats counterfeit drugs by enabling traceability of treatments to their origin. It ensures the confidentiality and immutable recording of patient histories, utilizing a decentralized network that optimizes resources for healthcare research and treatment planning [26].

Blockchain's distributed ledger allows for the addition and removal of entries without centralized control. The importance of each data block is secured by a cryptographic hash, providing a reliable and accessible data source for all network participants. The decentralized nature of blockchain fortifies the system against singular points of attack, enhancing overall security. It streamlines health data management and patient care, offering cost and time savings. Patients can track their medical records stored on the blockchain, ensuring transparency and control [27]. Researchers can access extensive data for population studies, advancing precision medicine. Blockchain also supports real-time health monitoring through technology and the Internet of Things (IoT), aiding physicians in managing high-risk patients and facilitating emergency communication [28].

2.1.1 Blockchain

Blockchain technology, known for its decentralized nature, enables secure transactions without the necessity for a prominent authority, gaining prominence with Bitcoin's success. Let's delve into the core elements of blockchain [29]. Blockchain networks are categorized based on node permissions into:

1. Private blockchain: Governed by access control, this network requires authorization for user participation.

2. Public ledger system: Unlock to all, the populace blockchain allows anyone to join as a node or miner, often for financial gain.

3. Blockchain consortium: A semi-private system, the consortium blockchain is shared among pre-approved organizations, commonly used in business settings.

Key features of blockchain comprise decentralization, which disseminates data across a web of nodes, eradicating single points of loss. Cryptographic hashing secures data integrity by linking each block to its predecessor, making tampering exceedingly difficult [30]. Unanimity mechanisms like proof of stake and proof of work enable new coalition additions, while smart contracts stimulate automated contract enforcement. Blockchain's immutability and public key cryptography ensure secure, transparent transactions [31].

In healthcare, blockchain can revolutionize the industry by enhancing interoperability and patient-centricity. Decentralized storage and cryptographic measures give patients tremendous supervision over their medical data, allowing them to grant or deny entry as they see fit, thus promoting privacy and patient-focused care [32].

Blockchain's transparency is crucial for business applications, as it allows for controlled access in consortium and private networks, ensuring only authorized participants can enter. This technology could be instrumental in resolving healthcare interoperability challenges, improving security, privacy, and patient engagement.

Blockchain applications extend to remote monitoring, mobile apps, and medical data surveillance, empowering patients with access to, sharing of, and ownership over their medical records [33].

2.2 BLOCKCHAIN IN HEALTHCARE

The healthcare facility is rapidly advancing, necessitating the adoption of innovative technologies to improve the quality of healthcare services. Blockchain technology is climacteric in this transformation, offering explanations to longstanding challenges. The enterprise is increasingly adopting a patient-centric method, emphasizing the availability of services and the condition of sufficient medical aids. Blockchain supports healthcare providers in delivering top-notch installations and care.

The cumbersome process of health information exchange, a significant contributor to healthcare costs, can be streamlined with blockchain. This technology enables public engagement in health research and fosters better care through enhanced research and data sharing. Healthcare management typically relies on a unified database [34]. Historically, the main hurdles in population health management have been data sharing, interoperability, and security. Blockchain addresses these concerns by ensuring dependable data management. When implemented actually, it enhances data trade, security, innocence, interoperability, and delivers real-time updates and entry.

Securing data, especially in the context of wearables and personalized medicine, is a critical challenge. Blockchain offers a solution, enabling patients and healthcare professionals to securely record, transmit, and consult data across networks, alleviating security concerns [35].

2.2.1 Security in Healthcare

A variety of methods are employed to bolster the security of healthcare data, drawing from research that integrates technological, administrative, and physical safeguards. Healthcare organizations utilize a spectrum of security practices to enhance the protection of confidential patient data within digital health records [36]. These security measures restrict access to patient data, shielding it from unauthorized individuals, a process managed through operational controls within the entity [37]. Blockchain technology is poised to transform healthcare by securely storing and transferring sensitive patient data [38]. Protecting private patient information, such as test results, prescriptions, and medical histories, is critical in healthcare, as any data breach could have severe repercussions.

Blockchain technology attracts healthcare firms for its secure, decentralized approach to data exchange and storage. It functions as a robust digital ledger, recording transactions in a secure, unalterable fashion [1]. The term "blockchain" signifies the sequential arrangement of data in interconnected blocks. Blockchain's suitability for secure data management in healthcare is due to its key attributes:

1. Decentralized storage: Unlike centralized strategies vulnerable to hacking, blockchain distributes data across a web, significantly decreasing the risk of unauthorized access.

2. Immutability: Data on a blockchain are permanent once added, ensuring integrity and preventing tampering.

3. Encryption: State-of-the-art encryption safeguards data on blockchain, ensuring access is confined to authorized entities.

4. Smart contracts: These automated agreements streamline data exchange and access control, adding a layer of security by allowing only authorized access.

5. Transparency: Blockchain enhances clarity by making data verifiable by all web participants, fostering responsibility and deterring deception.

In implementing blockchain in healthcare, prioritizing protection is paramount scheduled to the sensitive essence of healthcare data [39]. Cryptographic techniques enable data encryption and digital autographs, necessary for conserving confidentiality and virtue [40]. Individuality management and entry control instruments, such as multi-factor authentication (MFA) [42] and role-based access control (RBAC) [41], enable secure user authentication and data entry restriction. Regular safety audits and successive monitoring are vital to promptly catch sight of and address safety threats. Blockchain equips a decentralized, secure forum for control and storing confidential medical data, with the prospect to revolutionize healthcare. Nonetheless, challenges such as the need for standardized protocols, interoperability concerns, and legal and regulatory frameworks must be addressed for its widespread adoption [43].

2.3. PRIVACY IN HEALTHCARE

Blockchain technology is recognized as a promising device for addressing healthcare challenges, notably in improving the safety and confidentiality of patient data [38]. The solitude of medical documents is paramount in healthcare, as they encompass susceptible data that must stay confidential. Unauthorized exposure could negatively influence patients and lead to legal repercussions for providers. Blockchain's disseminated, decentralized catalog technique disperses data across multiple nodes, reducing the risk of centralized breaches or attacks. Additionally, blockchain enables the innovation of smart agreements that automate data sharing while adhering to privacy regulations [44]. Data on the blockchain can be encrypted and pseudonymized, safeguarding personal data while permitting entry to ratified individuals.

Despite its potential to bolster patient privacy, blockchain faces hurdles such as platform incompatibility, where healthcare providers may operate on disjointed systems [45]. The complexity of blockchain implementation, requiring resources and expertise not universally available, poses another challenge. Blockchain incorporates various privacy-enhancing technologies to secure sensitive patient data. Encryption authorizes for the secure transfer and repository of healthcare data, with entry limited to approved people with decryption keys. Smart contracts facilitate permission management, aligning data management with patient intentions [46]. Zero-knowledge evidence on the blockchain enhance data confidentiality by verifying information without exposing the actual data [47]. Off-chain data storage is important for highly susceptible data, storing critical data off the blockchain and only keeping a cryptographic braise reference, minimizing exposure risks [48].

Blockchain also increases anonymity by using cryptographic addresses for transactions instead of real identities, enhancing patient privacy [49]. It improves accountability and transparency in healthcare data management through automated permission and access rights, providing an auditable route and ensuring regulatory compliance [50]. In summary, blockchain technology bids a decentralized and secure framework for managing patient data, but general adoption in healthcare will require overcoming several challenges.

2.4 DATA INTEROPERABILITY AND STANDARDS IN HEALTHCARE BLOCKCHAIN

Interoperability stands as the principal technological challenge in integrating blockchain technology within the healthcare sector. The varied nature of healthcare systems, each with its own electronic health record (EHR) systems and medical devices featuring distinct data formats and standards, complicates the seamless exchange of healthcare data. Integrating these disparate systems into a blockchain network requires meticulous planning and data translation, a task further complicated by legacy systems that may not be readily compatible with blockchain technology [51].

To solve these interoperability issues and open blockchain's full potential in healthcare, many solutions and approaches are proposed. One adequate strategy is to establish uniform data formats and criteria for healthcare information within blockchain networks. These would provide a consistent framework for test results, prescription details, patient records, and more, facilitating a common language across various systems [52].

Middleware is another essential element, acting as a bridge between existing systems and blockchain networks, simplifying data translation and format conversion. Achieving a consensus on data standards is also vital. Collaborative efforts among healthcare organizations, regulatory bodies, and technology providers are necessary to develop these standards and build the foundation for sufficient data exchange and interoperability [53]. Blockchain-based identity management systems can enrich both data safety and interoperability. These systems securely manage patient individualities and access rights, streamlining the integration process by mapping and translating data from multiple sources into a standardized format suitable for blockchain [54].

2.5 DIFFERENT CAPABILITIES OF BLOCKCHAIN TECHNOLOGY TO SUPPORT THE HEALTHCARE CULTURE GLOBALLY

Blockchain technology conforms to numerous roles in healthcare, from overseeing the drug resource chain to facilitating the secure trade of patient documents, thus aiding investigators in genetic finding. Its advanced characteristics, such as cryptocurrency protection, data management, and digital tracking, contribute to its growing prominence in healthcare [55]. Blockchain introduces translucency throughout the medication method, from production to diffusion, and coupled with the Internet of Things, it enables efficient logistics planning to prevent drug shortages [56].

Blockchain technology's immutable and distributed ledger is ideal for the protection of health records, ensuring confidentiality while maintaining openness. It facilitates the prompt and safe exchange of medical details among healthcare professionals, patients, and insurers. Blockchain technology fosters a patient-centric approach to data interoperability, bolstering confidentiality and granting individuals more authority over their health information [57].

The integration of blockchain in the healthcare sector is gaining momentum, with pioneers receiving it favorably. To revolutionize healthcare, blockchain must tackle existing system limitations, ensuring data accessibility for all involved parties. Medical institutions are investigating how blockchain can be applied to manage health records, streamline payments, and distribute patient histories, confirming its vital position in conjunction with different technologies like artificial intelligence and machine learning [58].

With the ability to house extensive patient health records, encompassing diagnoses, laboratory outcomes, therapeutic strategies, and readings from medical devices, blockchain provides a unified system for storing data. This grants doctors access to a patient's full medical background, leading to precise diagnostic and therapeutic guidance. Blockchain also protects network infrastructures from external dangers, reducing hazards such as cyber-attacks and equipment malfunctions [59].

2.6 ENABLERS OF BLOCKCHAIN TECHNOLOGY FOR REVIVING HEALTHCARE SERVICES

Blockchain technology is gaining traction in healthcare, supported by various industrial and medical stakeholders who have contributed to its research and application [60]. Companies like BurstIQ, Guardtime, Robomed, Simply Vital, Encrypgen, Chronicled, and Tieion are at the forefront, facilitating blockchain's real-world implementation. This technology addresses the redundancy and time wastage in updating medical records. It ensures that each participant in the supply chain has appropriate access rights, and securely links medical details through cryptographic hashes. When patients visit new clinics, blockchain can streamline the creation and integration of their medical cards, consolidating records from various caregivers into a comprehensive and accessible format [62].

Blockchain's role extends to clinical trials, where it can record and verify data, enhancing the trustworthiness of results for researchers, pharmaceutical firms, and regulators. It promises greater accountability and transparency in clinical research. The technology's record-keeping capabilities are particularly beneficial in healthcare, as it allows both patients and physicians to access medical information while addressing privacy concerns. Blockchain's application in supply chains translates well to the pharmaceutical sector, improving drug traceability and management [63].

Blockchain simplifies consent management and data acquisition in healthcare, promoting efficiency and reducing procedural delays. It supports clinical guidance, personalized treatments, and health research. As blockchain becomes more prevalent, it is poised to transform healthcare into a reliable online directory, addressing challenges like prescription traceability, patient data management, and clinical trial processes [64].

Blockchain empowers the healthcare ecosystem to make informed decisions, track fraud, reduce costs, ensure reliable task execution, eliminate redundant work, and foster transparency. It stores key assets like decentralization, immutability, and trust, enhancing the credibility of clinical trials and patient consent processes. Patients benefit from increased security of their medical histories and improved care prospects [65].

Patients are gaining more control over their health records with blockchain, which allows secure data exchange and enhances privacy. The technology's potential is vast, enabling different networks to collaborate and provide valuable treatment insights. A nationwide blockchain network for electronic medical records is expected to increase efficiency and improve patient outcomes. Blockchain acts as a digital ledger, creating an unalterable record of transactions linked together, which can be instrumental in tracking medical supplies and ensuring the integrity of medical data during transit [66].

2.7 COOPERATIVE WORK-FLOW PROCESS OF BLOCKCHAIN TECHNOLOGY REALIZATION IN HEALTHCARE AMENITIES

Blockchain technology brings a host of benefits to healthcare, such as enhancing the master patient index, refining medical supply chain management, and bolstering interoperability and data collection. It initiates a digital and interactive workflow that prioritizes quality and innovation in healthcare services [67]. Blockchain's continuous growth adapts to industry needs, offering a robust monitoring system that updates results instantly.

It safeguards against record tampering and financial discrepancies, ensuring the integrity of clinical trial data, which reduces fraud and errors [68]. Blockchain's role extends beyond healthcare, fostering trust across various sectors. It could revolutionize consent processes, allowing for shared clinical data and benefits for participants, and streamline consent management [69]. Authorized blockchain networks facilitate secure data transmission within and across organizational boundaries, with each transaction forming a permanent record [70].

Blockchain-driven supply chains guarantee the security and timeliness of pharmaceutical deliveries, complying with regulatory standards. It also enables medical devices to charge accurately and share data anonymously with stakeholders [71]. Blockchain's transparent and decentralized nature offers a stable platform for confidential medical data, simplifying complex billing processes and allowing secure patient data access [72]. This technology is set to transform health information sharing, improving the efficiency, dependability, and protection of electronic medical documents.

2.8 BLOCKCHAIN APPLICATIONS FOR HEALTHCARE

Blockchain is a rising technology that is discovering imaginative applications in healthcare, facilitating the smooth flow of data among key stakeholders and enabling the development of cost-effective, cutting-edge treatments. This technology is poised to drive growth in healthcare by offering solutions that enhance logistics, a sector where digital innovation directly affects the quality of life. Already prevalent in finance, blockchain presents healthcare with numerous opportunities, from research to enhancing the patient-care provider relationship [73].

Blockchain's decentralized ledger system marks a departure from traditional healthcare management, streamlining administrative tasks with its precision and cost-effectiveness. It addresses one of healthcare's major challenges: the leakage of sensitive data, and ensuring secure access to present, accurate patient records. This capability positions blockchain as a promising tool for healthcare, connecting various services within the network for uniform information access. Its adoption in healthcare promises advancements across clinical rehearsals, medical study, patient data management, supply chain integrity, and pharmaceutical safety [75].

Storing medical patient data securely and efficiently on a blockchain involves several steps and considerations. Below is a simplified example of how this can be achieved using a smart contract on the Ethereum blockchain. This example is written in Solidity, a programming language for writing smart contracts.

solidity

```solidity
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract MedicalRecords {

    // Define a structure to hold patient data
    struct Patient {
        string name;
        uint age;
        string medicalCondition;
        address patientAddress;
    }

    // Mapping from patient address to their data
    mapping(address => Patient) private patients;

    // Address of the hospital or administrator
    address public hospital;
```

```solidity
    address public hospital;

    // Event to log new patient data
    event NewPatient(address indexed patientAddress, string name, uint ag

    // Event to log updated patient data
    event UpdatePatient(address indexed patientAddress, string name, uint

    // Modifier to restrict access to hospital only
    modifier onlyHospital() {
        require(msg.sender == hospital, "Access restricted to hospital on
        _;
    }

    // Constructor to set the hospital address
    constructor() {
        hospital = msg.sender;
    }

    // Function to add new patient data
    function addPatient(address _patientAddress, string memory _name, uin
```

```solidity
ess, string name, uint age, string medicalCondition);


ddress, string name, uint age, string medicalCondition);

nly

restricted to hospital only");









 string memory _name, uint _age, string memory _medicalCondition) public only
'Invalid patient address");
annot be empty");
han zero");
```

```solidity
    function updatePatient(address _patientAddress, string memory _name, u
        require(_patientAddress != address(0), "Invalid patient address");
        require(bytes(_name).length > 0, "Name cannot be empty");
        require(_age > 0, "Age must be greater than zero");
        require(bytes(_medicalCondition).length > 0, "Medical condition ca

        Patient storage patient = patients[_patientAddress];
        patient.name = _name;
        patient.age = _age;
        patient.medicalCondition = _medicalCondition;

        emit UpdatePatient(_patientAddress, _name, _age, _medicalCondition
    }

    // Function to retrieve patient data (restricted to hospital only)
    function getPatient(address _patientAddress) public view onlyHospital
        require(_patientAddress != address(0), "Invalid patient address");

        Patient memory patient = patients[_patientAddress];
        return (patient.name, patient.age, patient.medicalCondition);
    }
```

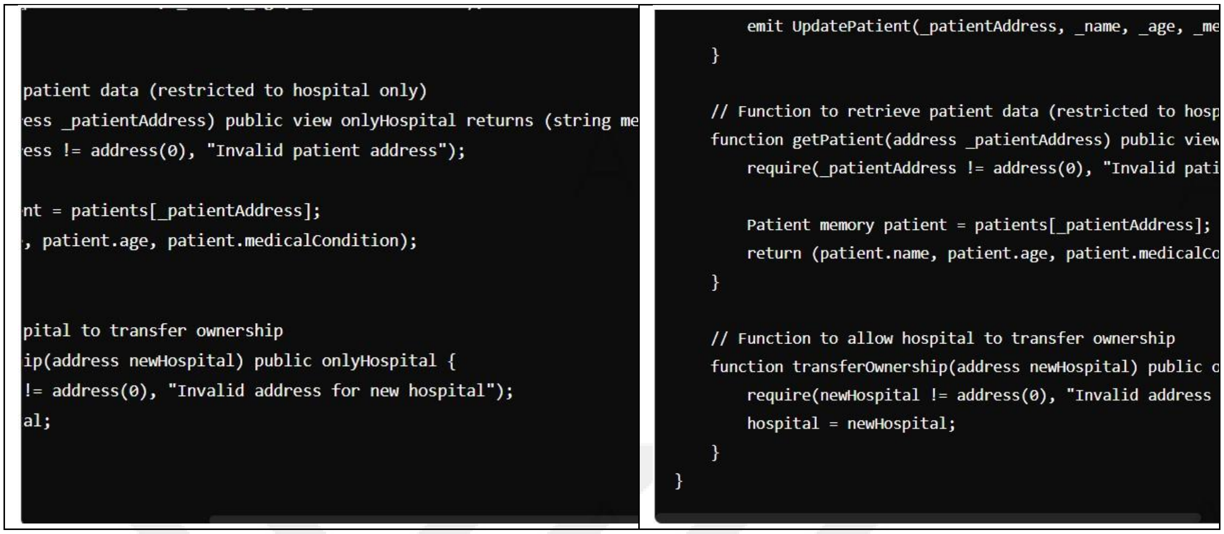

Figure 2.1 Solidity Smart Contract for Medical Patient Data

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract MedicalRecords {
    // Define a structure to hold patient data
    struct Patient {
        string name;
        uint age;
        string medicalCondition;
        address patientAddress;
    }
    // Mapping from patient address to their data
    mapping(address => Patient) private patients;
    // Address of the hospital or administrator
    address public hospital;
    // Event to log new patient data
    event NewPatient(address indexed patientAddress, string name, uint age, string medicalCondition);
    // Event to log updated patient data
```

```
event UpdatePatient(address indexed patientAddress, string name, uint age, string medicalCondition);
// Modifier to restrict access to hospital only
modifier onlyHospital() {
    require(msg.sender == hospital, "Access restricted to hospital only");
    _;
}
// Constructor to set the hospital address
constructor() {
    hospital = msg.sender;
}
// Function to add new patient data
function addPatient(address _patientAddress, string memory _name, uint _age, string memory _medicalCondition) public onlyHospital {
    require(_patientAddress != address(0), "Invalid patient address");
    require(bytes(_name).length > 0, "Name cannot be empty");
    require(_age > 0, "Age must be greater than zero");
    require(bytes(_medicalCondition).length > 0, "Medical condition cannot be empty");
    patients[_patientAddress] = Patient({
        name: _name,
        age: _age,
        medicalCondition: _medicalCondition,
        patientAddress: _patientAddress
    });
    emit NewPatient(_patientAddress, _name, _age, _medicalCondition);
}
// Function to update existing patient data
function updatePatient(address _patientAddress, string memory _name, uint _age, string memory _medicalCondition) public onlyHospital {
    require(_patientAddress != address(0), "Invalid patient address");
```

```
        require(bytes(_name).length > 0, "Name cannot be empty");
        require(_age > 0, "Age must be greater than zero");
        require(bytes(_medicalCondition).length > 0, "Medical condition cannot be empty");
        Patient storage patient = patients[_patientAddress];
        patient.name = _name;
        patient.age = _age;
        patient.medicalCondition = _medicalCondition;
        emit UpdatePatient(_patientAddress, _name, _age, _medicalCondition);
    }
    // Function to retrieve patient data (restricted to hospital only)
    function getPatient(address _patientAddress) public view onlyHospital returns (string memory, uint, string memory) {
        require(_patientAddress != address(0), "Invalid patient address");
        Patient memory patient = patients[_patientAddress];
        return (patient.name, patient.age, patient.medicalCondition);
    }
    // Function to allow hospital to transfer ownership
    function transferOwnership(address newHospital) public onlyHospital {
        require(newHospital != address(0), "Invalid address for new hospital");
        hospital = newHospital;
    }
}
```

Explanation:

1. **Data Structure**: The Patient struct holds the patient's name, age, medical condition, and address.
2. **Mapping**: The patients mapping stores the patient data, using the patient's address as the key.
3. **Access Control**: The onlyHospital modifier ensures that only the hospital (the address that deployed the contract) can add or update patient data.

4. **Events**: The contract emits events (NewPatient and UpdatePatient) to log actions, which can be useful for tracking changes.
5. **Functions**:
    i. addPatient: Adds a new patient's data.
    ii. updatePatient: Updates existing patient data.
    iii. getPatient: Retrieves patient data; restricted to hospital access only.
    iv. transferOwnership: Transfers contract ownership to a new hospital address.

Deployment and Usage:

(a) Deploy this contract on an Ethereum network.
(b) The hospital will interact with this contract using a web interface or another application to add, update, and retrieve patient data.

Considerations:

i. **Security**: Ensure the smart contract and any off-chain applications interacting with it are secure.
ii. **Privacy**: Patient data stored on the blockchain should be encrypted to protect privacy. This example stores data in plaintext for simplicity, but encryption should be implemented for real-world use.
iii. **Scalability**: Consider the scalability of the blockchain and the potential need for off-chain storage solutions (e.g., IPFS) for large medical records.

This example provides a basic framework. Real-world applications would need additional features and optimizations for performance, security, and compliance with healthcare regulations.

Additional Considerations and Features

a. **Data Encryption**: To protect patient privacy, it's crucial to encrypt sensitive data before storing it on the blockchain. Here's a basic approach using client-side encryption. Patient data is encrypted on the client side before being sent to the blockchain.

b. **Off-Chain Storage**: For larger files like medical images or detailed records, using a decentralized storage solution like IPFS (InterPlanetary File System) can be more efficient. The blockchain can store the hash of the file for integrity verification, while the actual data is stored off-chain.

c. **Role-Based Access Control**: To ensure that only authorized personnel can access or modify patient data, implement role-based access control. This can be done by expanding the smart contract to manage roles and permissions.

Example: Encrypting Data Before Storing

Here's an extended example with a simple encryption mechanism using a hash function. In practice, use more robust encryption methods.

solidity

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract MedicalRecords {

    struct Patient {
        string name;
        uint age;
        string medicalCondition;
        address patientAddress;
        string encryptedData; // Encrypted medical data
    }

    mapping(address => Patient) private patients;

    address public hospital;
```

```
    event NewPatient(address indexed patientAddress, string name, uint
    event UpdatePatient(address indexed patientAddress, string name, ui

    modifier onlyHospital() {
        require(msg.sender == hospital, "Access restricted to hospital
        _;
    }

    constructor() {
        hospital = msg.sender;
    }

    function addPatient(address _patientAddress, string memory _name, u
        require(_patientAddress != address(0), "Invalid patient address
        require(bytes(_name).length > 0, "Name cannot be empty");
        require(_age > 0, "Age must be greater than zero");
        require(bytes(_medicalCondition).length > 0, "Medical conditio
        require(bytes(_encryptedData).length > 0, "Encrypted data canno

        patients[_patientAddress] = Pati  ({
            name: _name,
```

```
atient) private patients;

al;

ess indexed patientAddress, string name, uint age, string medicalCondition);
ddress indexed patientAddress, string name, uint age, string medicalConditio

l() {
er == hospital, "Access restricted to hospital only");



ender;


ddress _patientAddress, string memory _name, uint _age, string memory _medica
ddress != address(0), "Invalid patient address");
me).length > 0, "Name cannot be empty");
 "Age must be greater than zero");
dicalCondition).length > 0, "Medical condition cannot be empty");
```

```
_age, string memory _medicalCondition, string memory _encryptedData) public o


 be empty");
pty");



rns (string memory, uint, string memory, string memory) {


ncryptedData);
```

```
function addPatient(address _patientAddress, string memory _name, uint _age,
    require(_patientAddress != address(0), "Invalid patient address");
    require(bytes(_name).length > 0, "Name cannot be empty");
    require(_age > 0, "Age must be greater than zero");
    require(bytes(_medicalCondition).length > 0, "Medical condition cannot b
    require(bytes(_encryptedData).length > 0, "Encrypted data cannot be empt

    patients[_patientAddress] = Patient({
        name: _name,
        age: _age,
        medicalCondition: _medicalCondition,
        patientAddress: _patientAddress,
        encryptedData: _encryptedData
    });

    emit NewPatient(_patientAddress, _name, _age, _medicalCondition);
}

function updatePatient(address _patientAddress, string memory _name, uint _
    require(_patientAddress != address(0, "Invalid patient address");
    require(bytes(_name).length > 0, "Name cannot be empty");
```

```
e, string memory _medicalCondition, string memory _encryptedData) public onlyHo


 be empty");
pty");



_age, string memory _medicalCondition, string memory _encryptedData) public onl
```

```
        Patient storage patient = patients[_patientAddress];
        patient.name = _name;
        patient.age = _age;
        patient.medicalCondition = _medicalCondition;
        patient.encryptedData = _encryptedData;

        emit UpdatePatient(_patientAddress, _name, _age, _medicalCondition);
    }

    function getPatient(address _patientAddress) public view onlyHospital returns (string
        require(_patientAddress != address(0), "Invalid patient address");

        Patient memory patient = patients[_patientAddress];
        return (patient.name, patient.age, patient.medicalCondition, patient.encryptedData
    }

    function transferOwnership(address newHospital) public onlyHospital {
        require(newHospital != address(0), "Invalid address for new hospital");
        hospital = newHospital;
    }
}
```

Figure 2.2 Encrypting Data Before Storing

```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;
contract MedicalRecords {
    struct Patient {
        string name;
        uint age;
        string medicalCondition;
        address patientAddress;
        string encryptedData; // Encrypted medical data
    }
    mapping(address => Patient) private patients;
    address public hospital;
    event NewPatient(address indexed patientAddress, string name, uint age, string medicalCondition);
    event UpdatePatient(address indexed patientAddress, string name, uint age, string medicalCondition);
    modifier onlyHospital() {
        require(msg.sender == hospital, "Access restricted to hospital only");
        _;
    }
    constructor() {
        hospital = msg.sender;
    }
    function addPatient(address _patientAddress, string memory _name, uint _age, string memory _medicalCondition, string memory _encryptedData) public onlyHospital {
        require(_patientAddress != address(0), "Invalid patient address");
        require(bytes(_name).length > 0, "Name cannot be empty");
        require(_age > 0, "Age must be greater than zero");
        require(bytes(_medicalCondition).length > 0, "Medical condition cannot be empty");
        require(bytes(_encryptedData).length > 0, "Encrypted data cannot be empty");
```

```
    patients[_patientAddress] = Patient({
        name: _name,
        age: _age,
        medicalCondition: _medicalCondition,
        patientAddress: _patientAddress,
        encryptedData: _encryptedData
    });
    emit NewPatient(_patientAddress, _name, _age, _medicalCondition);
}
function updatePatient(address _patientAddress, string memory _name, uint _age, string memory _medicalCondition, string memory _encryptedData) public onlyHospital {
    require(_patientAddress != address(0), "Invalid patient address");
    require(bytes(_name).length > 0, "Name cannot be empty");
    require(_age > 0, "Age must be greater than zero");
    require(bytes(_medicalCondition).length > 0, "Medical condition cannot be empty");
    require(bytes(_encryptedData).length > 0, "Encrypted data cannot be empty");
    Patient storage patient = patients[_patientAddress];
    patient.name = _name;
    patient.age = _age;
    patient.medicalCondition = _medicalCondition;
    patient.encryptedData = _encryptedData;
    emit UpdatePatient(_patientAddress, _name, _age, _medicalCondition);
}
function getPatient(address _patientAddress) public view onlyHospital returns (string memory, uint, string memory, string memory) {
    require(_patientAddress != address(0), "Invalid patient address");
    Patient memory patient = patients[_patientAddress];
    return (patient.name, patient.age, patient.medicalCondition, patient.encryptedData);
}
function transferOwnership(address newHospital) public onlyHospital {
```

require(newHospital != address(0), "Invalid address for new hospital");

hospital = newHospital;

}

}

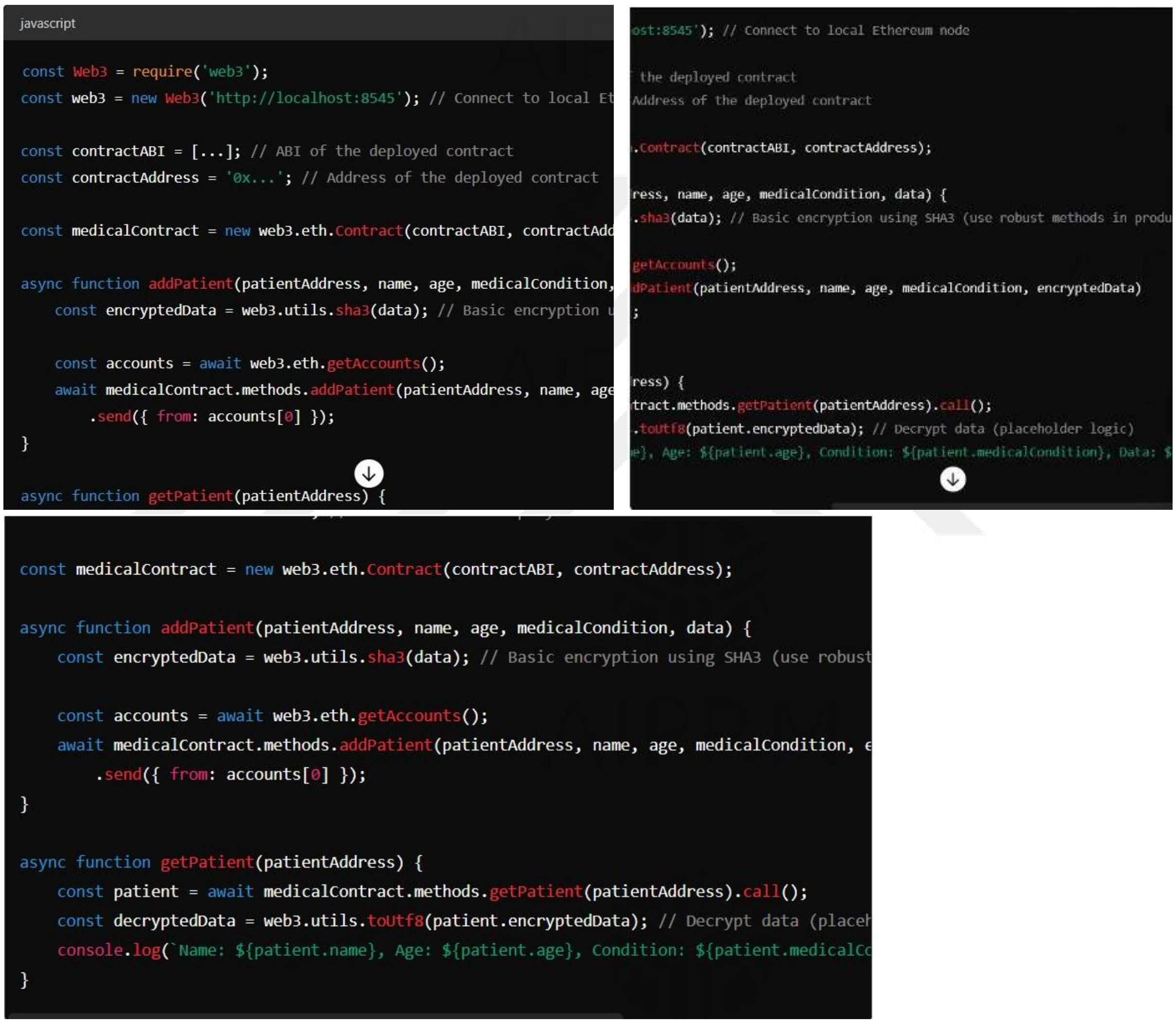

Figure 2.3 Front-End Integration (JavaScript Example)

```
const Web3 = require('web3');

const web3 = new Web3('http://localhost:8545'); // Connect to local Ethereum node

const contractABI = [...]; // ABI of the deployed contract

const contractAddress = '0x...'; // Address of the deployed contract

const medicalContract = new web3.eth.Contract(contractABI, contractAddress);
```

```
async function addPatient(patientAddress, name, age, medicalCondition, data) {
  const encryptedData = web3.utils.sha3(data); // Basic encryption using SHA3 (use robust methods in production)
    const accounts = await web3.eth.getAccounts();
  await medicalContract.methods.addPatient(patientAddress, name, age, medicalCondition, encryptedData)
    .send({ from: accounts[0] });
}
async function getPatient(patientAddress) {
  const patient = await medicalContract.methods.getPatient(patientAddress).call();
  const decryptedData = web3.utils.toUtf8(patient.encryptedData); // Decrypt data (placeholder logic)
  console.log(`Name: ${patient.name}, Age: ${patient.age}, Condition: ${patient.medicalCondition}, Data: ${decryptedData}`);
}
```

Final Considerations:

1. **Encryption**: Use robust encryption libraries like crypto-js for JavaScript or equivalent libraries for other languages.
2. **Off-Chain Storage**: Integrate with IPFS or another decentralized storage for storing large files, saving the file hash on the blockchain.
3. **Role Management**: Expand the contract to manage different roles (e.g., doctors, nurses) with appropriate permissions.
4. **Compliance**: Ensure the implementation complies with relevant healthcare regulations (e.g., HIPAA in the U.S., GDPR in the EU).

By implementing these additional features and considerations, the blockchain solution can be robust, secure, and practical for storing medical patient data in a real-world hospital setting.

3. METHODOLOGY

3.1 SEARCH STRATEGY

Aided by a medical research librarian, a systematic search was conducted across various bibliographic databases. The investigation strategy encountered challenges in retrieving free-text terms associated with "blockchain" within health-related databases. The Boolean operator AND was utilized to combine "health" and "blockchain" in other databases, while OR was used to link variations and related terms within these concepts. The snowballing method, involving both backward and forward searches, was employed to comprehensively review relevant literature. This process continued until no extra relevant articles were established. The publications search was concluded on December 11, 2023. All references were compiled into EndNote (version x9.1) to eliminate duplicates and facilitate the final review.

3.2 SELECTION PROCESS

The selection process for relevant literature involved a reviewer applying inclusion and exclusion criteria to sift through titles, abstracts, and full texts. Publications that met the inclusion criteria or were uncertain were further assessed by a supervisor. Any controversies were resolved through dialogue/conversation the supervisor and the reviewer. Initially, 110 articles were found, from which 96 non-duplicate articles were identified. After pertaining to the inclusion/exclusion criteria, 46 articles were screened, and ultimately, 22 articles were selected for an in-depth critical review based on their title, abstract, and keywords

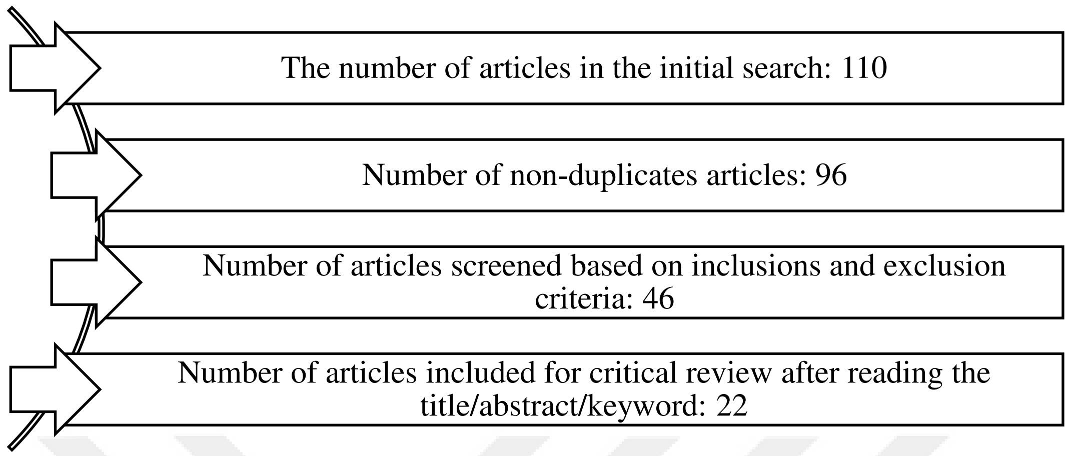

Figure 3.1: Selection Process

3.3 INCLUSION & EXCLUSION CRITERIA

3.3.1 Inclusion criteria

I. Analyses was cast between 2018 and 2023.

II. The journal attends to as the only realm of the research.

III. Both "blockchain" and "healthcare" should be the central topics of research.

IV. Articles that suggested a system, model, or framework.

3.3.2 Exclusion criteria

I. The reduction of articles in the press.

II. Non-English-language essays.

III. Exclusion of book branches, dissertations, monographs, symposia, studies, and works based on interviews.

IV. Case studies

3.4 DATA EXTRACTION

Data for the initial development matrix were sourced from selected studies. The primary reviewer conducted the initial data extraction, which was subsequently reviewed for accuracy by a supervisor. Once extracted, the data were systematically arranged into a matrix format and then presented as tables and graphs for clarity. To facilitate collaboration within the research team, the matrix was initially created in Google Sheets before being transferred to Microsoft Excel 2023 for finalization.

3.5 DATA ANALYSIS

The gathered quantitative data from the studies were compiled and analyzed using Microsoft Excel 2023. The mean, denoted by ±, and the SD were computed where applicable. All values were rounded to the nearest whole number, and categorical data were presented as percentages unless stated otherwise.

3.6 QUALITY ASSESSMENT

A thorough evaluation of the included publications' quality was carried out as a crucial step in the review process. It was necessary to design a specific tool for this aim because there are currently no documented and tested methods for evaluating the various methodologies of the included papers. In order to do this, certain elements of the Hölbl et al. technique were applied and adjusted as necessary [76]. The technique of evaluating the quality did not omit any publications.

Table 3.1: Quality assessment tool adapted from *Hölbl et al [6]*

Quality Assessment Query	Indicator (0–2)
Q1 Is the health domain problem described?	No-Moderately-YES
Q2 Are the research objectives clearly outlined?	No-Moderately-YES
Q3 Are the main contributions well described?	No-Moderately-YES
Q4 How appropriate is the problem-solution fit?	Scarcely-Moderately-Adequately

Q5 Are the proposed solutions feasible (scalable, economical, and implementable)?	No-Moderately-YES

4. RESULTS AND DISCUSSION

Blockchain technology is increasingly existing utilized to improve data security, privacy, and virtue within the healthcare sector. The preliminary aim of this research is to address ongoing security and solitude challenges. The results illustrate how blockchain can securely organize and limit entry to medical data, protecting the confidentiality of patients and healthcare specialists. The protocols formulated are cost-effective in terms of computation and transmission and meet the essential security norms.

In the analysis by Kumar et al., federated education combined with blockchain introduces a fiction approach for swapping medical imaging data across a decentralized web [77]. The off-chain health data storage architecture, leveraging the InterPlanetary File Systems and, ensures patient solitude while offering high levels of protection, scalability, and robustness. The outcomes suggest that incorporating data into the blockchain-primarily influences execution time and computational action [78–82].

Several studies propose explanations that authorize patients to control access to their medical records [83–88], facilitating submission with privacy restrictions for healthcare providers. These solutions also secure payment processes, allowing reliable transactions for diagnostic and storage services. Security analyses and thorough testing indicate that these techniques are resilient against various attacks, including impersonation, conspiracy, and man-in-the-middle invasions. The solutions demonstrate substantial defense tools, efficient storage allocation, and exceptional encryption rendition, enhancing the preservation and transfer of health data. Bespoke smart contracts and progressive cryptographic methods are employed to assure safe searches, privacy care, and personalized access management in Internet of Medical Things (IoMT) scenarios. Some studies have optimized their methodologies to address the space constraints of IoT sensor nodes [89].

Yugha et al.'s research [89] presents a strategy that ensures the secure and efficient transmission of IoT medical data while maintaining patient solitude. The forenamed research underscores the potential of blockchain technologies for the secure, confidential, and efficient exchange of healthcare data and access management. The proposed methods meet the anticipated security requirements and are viable for IoMT applications due to their competitive computational and communication costs. These technologies offer practical solutions to the enduring privacy and safety issues in healthcare. The consequence of these studies on healthcare security and privacy is summarized in Figure 4.0.

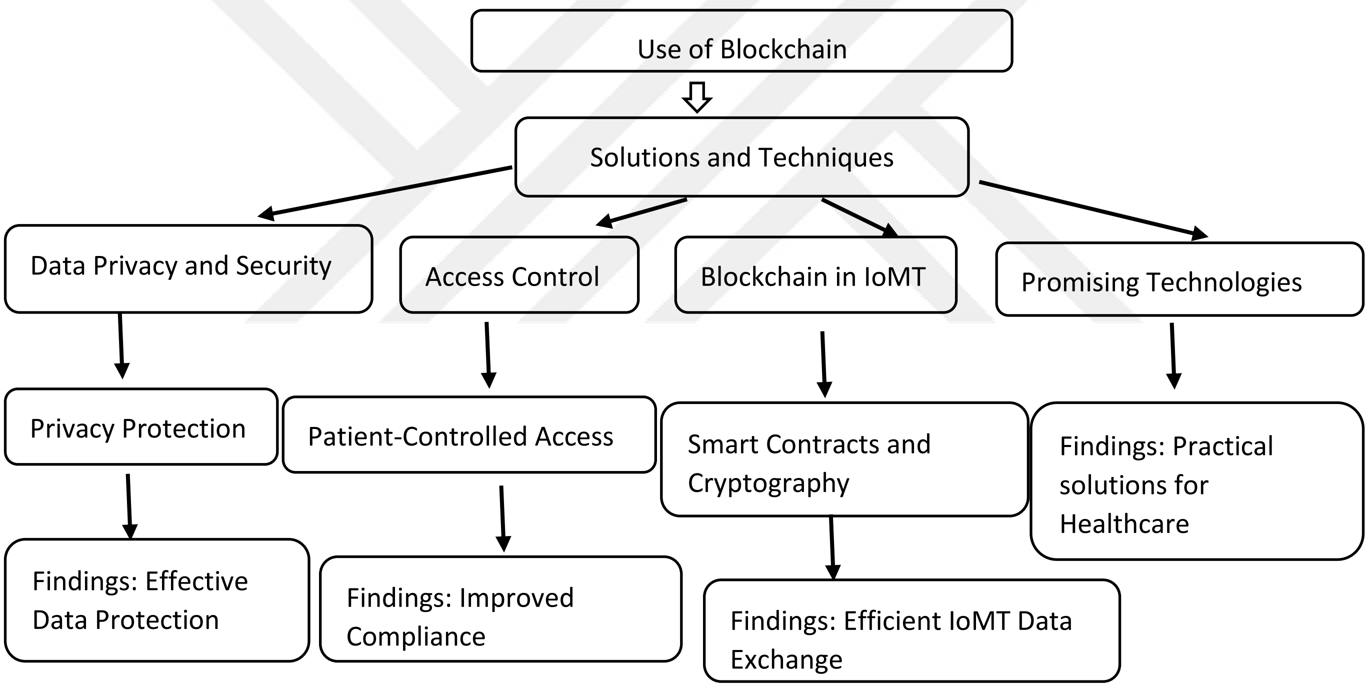

Figure 4.1: Privacy and safety in healthcare with blockchain and cryptography

Study question 1: What healthcare-related blockchain applications for security and privacy are there?

In the healthcare industry, patient privacy and security are crucial concerns. Electronic health records (EHRs) are repositories of confidential patient information that require robust security measures to uphold patient privacy and prevent unauthorized access. Protecting the privacy of patient information is a significant challenge within the healthcare sector. EHR systems powered by blockchain technology could provide a fortified, impenetrable framework for the safe exchange and storage of patient data. Smart contracts and digital currency transactions can be employed to restrict data access exclusively to verified users, while blockchain's decentralized nature can thwart data breaches and maintain data accuracy. Patient-directed access control is another feature that empowers patients to manage who can view their data, with the flexibility to grant or deny permissions as needed. Blockchain's approach to access control can further enhance data privacy, allowing patients to selectively permit or restrict access to their information, ensuring it is shared only with approved entities. These mechanisms demonstrate the practical application of smart contracts in safeguarding data privacy.

Table 4.1: Health Records Applications

Use case	Ref.
Blockchain for Electronic Health Records (EHRs) is being explored to enhance data management systems	[90]
Blockchain in Personal Health Record (PHR) management and sharing is improving the way health data is handled and distributed.	[78]
Blockchain for EHR management is being developed to streamline healthcare data processes.	[79]
Innovations in EHR with blockchain technology are being investigated for their potential to secure health information.	[91]
Enhancing EHR privacy through blockchain is a focus to protect sensitive patient data.	[92]
Integrating service automation into EHRs using blockchain is being considered to increase efficiency.	[93]

Smart contract and cryptocurrency payment systems in EHRs are being designed to secure transactions and access.	[94]
Blockchain applications in PHR systems are being created to provide patients additional control over their health records.	[95]
Blockchain for EHR sharing is being utilized to facilitate the safe exchange of medical information.	[96]
Patient record management through blockchain is being optimized for better data security and accessibility.	[97]

The management and sharing of Personal Health Records necessitate stringent security and privacy protocols. PHRs contain critical health information, including diagnoses, test results, and medical histories. Blockchain technology can secure data exchanges, ensuring that simply ratified parties have access to sensitive patient data (Table 4.2). Executing privacy-preserving K-nearest neighbors (K-NN) algorithms for IoT data can further bolster the security and solitude of healthcare data, contributing to the protected exchange of Electronic Health Records [98,99]. Blockchain's potential in healthcare lies in its capacity to equip a secure and tamper-proof forum for swapping and storing medical data, upholding both the virtue and confidentiality of the data (Table 4.3). More security and privacy measures on the blockchain, such as powerful authentication and approval systems, ensure that healthcare data is convenient only to verified individuals (Table 4.4). Study papers dedicated to progressing security protocols are summarized in Table 4.5, while Table 4.6 details the separate applications and their respective uses.

Table 4.2: Data Management

Use case	Ref
Health IoT data sharing is being enhanced through blockchain technology for better security and efficiency.	[83]
Secure data communication within the healthcare sector is being strengthened by blockchain solutions.	[84]
Medical data sharing is being facilitated by blockchain to ensure privacy and integrity.	[100]
Blockchain-assisted data sharing is being adopted for its robust security measures in healthcare.	[101]
IoT-enabled privacy-preserving healthcare data transfer is being developed to protect sensitive health information.	[81]
Health information exchange is being secured through blockchain to prevent unauthorized access.	[104]
Secure sharing of medical data between substantial entities is being enabled by blockchain's decentralized nature.	[105]
Medical data sharing and privacy-preserving strategies are being implemented to safeguard patient data.	[106]
Healthcare data management is being optimized with blockchain for better coordination and control.	[107]
Collaborative medical decision-making is being supported by blockchain for shared access to accurate data.	[108]
Healthcare big data management is leveraging blockchain for scalable and secure data handling.	[109]
Protected health information (PHI) sharing is being secured through blockchain to maintain confidentiality.	[110]
Data transmission in healthcare is being made more secure with blockchain technology.	[111]
Healthcare information management is being streamlined with blockchain for improved data governance.	[112]
Data storage solutions are being bolstered by blockchain to prevent data breaches.	[79]
Blockchain-enabled medical record protection is being utilized to keep health records safe during the pandemic.	[80]
Blockchain and AI-enabled medical data transmission is being explored for enhanced security and intelligent processing.	[113]
Blockchain's application in healthcare is being expanded to include various innovative use cases.	[114]

Table 4.3: Privacy Enhancement

Use Case	Ref.
Privacy preservation in healthcare is being advanced with blockchain to safeguard sensitive data.	[115]
Privacy enhancement techniques are being integrated into e-health systems for stronger data protection.	[116]
Privacy-preserving e-health systems are utilizing blockchain to maintain confidentiality of health records.	[117]
Privacy-preserving data sharing is being facilitated by blockchain, ensuring secure exchange of medical information.	[118]
Privacy protection measures are being strengthened in healthcare through blockchain's secure architecture.	[119]
Improved privacy-preserving location sharing in healthcare is being developed to protect location data.	[120]
Medical-data privacy protection is being bolstered by blockchain to prevent unauthorized access.	[121]
Medical privacy protection is being enhanced with blockchain to defend patient information.	[122]
Privacy-preserving medical data sharing is being achieved through blockchain, allowing controlled access to health data.	[123]
Health data privacy is being prioritized with blockchain to protect personal health information.	[80]
Privacy protection schemes for medical data are being established with blockchain to create secure health ecosystems.	[104]
Healthcare blockchain privacy is being pursued to create a secure and private environment for medical data handling.	[85]
IoT anonymity: Applying blockchain to maintain user anonymity within the Internet of Things.	[128]

Table 4.4: Authentication

Use Case	Ref.
Authentication: Implementing blockchain to verify user identities and secure access.	[124]
PPBA authentication: Utilizing Privacy-Preserving Biometric Authentication to protect sensitive data.	[125]
Machine learning authentication: Integrating machine learning with blockchain for advanced security measures.	[78]
Identity authentication: Employing blockchain for reliable verification of user identities.	[126]
Authentication & authorization for healthcare data on the blockchain: Ensuring secure access to health records.	[127]
IoT anonymity: Applying blockchain to maintain user anonymity within the Internet of Things.	[128]

Table 4.5: Security Enhancement

Use Case	Ref.
Security enhancement: Blockchain is being utilized to strengthen the overall security framework in healthcare.	[129]
Medical data security: Protecting sensitive medical data is being prioritized through blockchain technology.	[130]
Biomedical security: Blockchain is securing biomedical information, ensuring the safety of critical research data.	[131]
Collaborative analysis: Facilitating secure collaborative analysis in healthcare through blockchain's secure environment.	[132]
Blockchain is improving the confidentiality and virtue of patient healthcare systems.	[133]

Table 4.6: Other Applications

Use Case	Ref.
- Contact Tracing: A method for tracking and preventing the spread of diseases, as documented in source.	[134]
- Verifiable Data Classification: The process of categorizing data in a manner that can be validated, referenced in source.	[135]
- Security and Privacy in IoT Healthcare: Measures to protect data integrity and confidentiality in healthcare devices connected to the Internet of Things, as outlined in source.	[89]

Study question 2: What privacy and security challenges does blockchain technology face within the healthcare sector?

In the healthcare industry, the preservation of security and privacy is of utmost importance expected to the highly sensitive nature of medical data and the severe consequences that could arise from data breaches or unauthorized access. Blockchain technology provides a promising solution with its decentralized, secure infrastructure for data management and exchange. It utilizes cryptographic tools for safeguarding searches and enabling granular access controls, while smart contracts bolster data privacy and manage access permissions. The effectiveness, practicality, and security of these blockchain-based solutions have been substantiated through simulations and empirical research, showing that they can meet stringent security requirements while keeping computational and communication overheads competitive. Additionally, innovative methods like certificateless public-key encryption and enhanced attribute-based cryptographic techniques have also emerged as effective means for ensuring privacy and enabling precise access control within healthcare. However, for these solutions to be truly effective and compliant with privacy laws, they must undergo thorough evaluation for practicality and scalability in real-world healthcare applications by organizations and healthcare professionals.

Study question 3: What is the probable for blockchain security & privacy in the medical industry?

Enhancing security and privacy is anticipated to be a continual focus for the healthcare sector. The adoption of blockchain technology for the safeguarding of medical data is on the rise. Smart medical cloud platforms are innovating privacy protection by enabling the utilization of data without the possibility of it being taken. Strategies to bolster data security and privacy include leveraging cutting-edge technologies like edge computing, federated learning, and blockchain. Blockchain, for instance, can offer robust access control and guard against data tampering, while federated learning enables joint data analysis without compromising sensitive details. Edge computing can further mitigate data breach risks by processing data proximate to its origin, avoiding the need for central data transfer. The implementation of more stringent rules and protocols is another measure to protect private health information. With the escalation of data volumes, protecting healthcare data from unauthorized entry and breaches has never been more critical. Legislation like the Health Insurance Portability and Accountability Act, along with the General Data Protection Regulation, aims to safeguard the confidentiality and security of personal health information. Anticipated advancements in future laws and norms are projected to further fortify the perpetual safeguarding of medical data.

5. CONCLUSION

The interplay between blockchain technology and healthcare is generating a wealth of research topics and practical uses. The most pressing issues to address are interoperability and scalability. Researchers are tasked with creating advanced technologies that facilitate blockchain networks to efficiently regulate large amounts of healthcare data and ensure successful integration via various systems, paving the way for broader adoption. This opens up exciting avenues for future research and applications. Prioritizing scalability and interoperability in healthcare blockchain networks is crucial for effective data management and network integration. Blockchain's protection features could enormously enhance the global transfer of healthcare data, especially for global patient care. It has the potential to revolutionize medical supply chain management by ensuring patient safety and drug authenticity. Combining blockchain with artificial intelligence could unlock powerful data analytics while maintaining privacy.

Blockchain technology could provide secure methods for patients to manage access to their medical histories and potentially monetize them. Patient consent and identity management require careful consideration. Blockchain could help healthcare organizations comply with legal data protection standards and improve the safety of Internet of Things medical appliances by protecting the probity of the data they collect.

Enhancing user interfaces and integrating blockchain-based electronic health records and telemedicine systems with existing healthcare infrastructure is feasible. This discussion highlights key research areas and the transformative influence of blockchain on healthcare. It explores the importance of blockchain in addressing longstanding industry challenges, positioning it as an innovative means for storing medical data, facilitating transactions, and facilitating the integration and sharing of medical information within an open, decentralized network. Despite the growing interest in blockchain for healthcare information sharing, privacy and security concerns persist. The paper reviews research on blockchain's privacy and security in healthcare from 2018-2023.

The study aims to assess the recent terrain, with an emphasis on challenges and empirical undertakings. It infers that blockchain can attend to real-world privacy and protection issues in healthcare. Proposing a decentralized, secure forum for transmitting and reserving susceptible patient data, blockchain enhances the privacy and protection of electronic health records & personal health records. With patient-managed authentication, it entrusts patients to regulate managings their data. Healthcare institutions and practitioners must entirely assess blockchain solutions for subordination with privacy laws and practicality in their distinct contexts. Although promising, blockchain may require customization to meet precise needs, as it is not universally useful. Overall, the review offers valuable insights into the current use of blockchain in healthcare and identifies areas requiring additional research and development to broaden its potential applications.

6. RECOMMENDATIONS

To further advance the adoption and enactment of blockchain in healthcare, I recommend the following research directions:

1. Interoperability and Scalability: Address the urgent need to resolve interoperability and scalability challenges in healthcare blockchain networks. Focus on developing innovative solutions that enable efficient data processing and seamless network connectivity across multiple networks. Investigate approaches that can manage the substantial volume of healthcare data while guaranteeing secure and reliable connectivity.

2. International Data Transmission: Explore the benefits of utilizing blockchain's security features in transmitting healthcare data internationally, particularly in the context of treating international patients. Investigate how blockchain can enhance data privacy, integrity, and security in cross-border healthcare transactions.

3. Transforming the Medical Supply Chain: Investigate the prospect of blockchain technology intransforming the management of the medical supply chain. Explore how blockchain can ensure patient safety and verify the legitimacy of medications. Develop practical solutions that integrate blockchain into existing supply chain processes, ensuring transparency, traceability, and accountability.

4. Data Analytics and Privacy Preservation: Investigate the fusion of blockchain technology withartificial intelligence to unleash strong data analytics capabilities while preserving data privacy. Explore how blockchain can enable secure and privacy-preserving data analytics in healthcare. Develop methodologies and algorithms that leverage the strengths of both blockchain and artificial intelligence to take out valuable discernment from healthcare data while protecting patient privacy.

5. Patient-Controlled Data Access and Monetization: Examine secure ways for patients to control entry to their medical data using blockchain technology. Examine mechanisms that certify patients to organize their data permissions and potentially

monetize their medical records. Pay special attention to patient permission and identity management to ensure privacy and data protection.

6. Legal Compliance and Data Protection: Explore how blockchain technology can assist healthcare organizations in adhering to legal requirements, especially those related to data protection. Investigate the prospect of blockchain to provide a decentralized and tamper-proof platform for storing and managing patient data, ensuring compliance with privacy restrictions. Develop frameworks and approaches for healthcare institutions to evaluate the appropriateness of blockchain solutions in their specific contexts.

7. REFERENCES

1. Nakamoto A. Bitcoin: a Peer-to-Peer Electronic Cash System. 2008.
2. Mettler M. Blockchain technology in healthcare: the revolution starts here. In: Proceedings of the 2022 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom). IEEE; 2022.
3. Amato F, De Pietro G, Esposito M, Mazzocca N. An integrated framework for securing semistructured health records. Knowledge-Based Systems. 2022;79:99-117.
4. Amato F, Mazzocca N, Moscato F. Model driven design and evaluation of security level in orchestrated cloud services. Journal of Network and Computer Applications. 2018;106:78-

   89.
5. IBM. Health rallies for blockchains: Keeping patients at the center. 2022 [cited 02.11. 2023].

   Available from: https://www.ibm.com/downloads/cas/BBRQK3WY.
6. Frost & Sullivan. Global Blockchain Technology Market in the Healthcare Industry 2018-2022.

   2023;4847375.
7. Raikwar M, Gligoroski D, Kralevska K. SoK of used cryptography in blockchain. IEEE Access.

   2019;7:148550-148575.
8. Buterin VJwp. A Next-generation Smart Contract and Decentralized Application Platform. 2019.

9. Zheng Z, Xie S, Dai H, Chen X, Wang H. An overview of blockchain technology: architecture, consensus, and future trends. In: Proceedings of the 2017 IEEE International Congress on Big Data (BigData Congress). IEEE; 2017.

10. Merkle RC. A Certified Digital Signature. In: Proceedings of the Conference on the Theory and Application of Cryptology. Springer; 1989.

11. Pilkington M. Blockchain technology: principles and applications. In: Research Handbook onDigital Transformations. 2016;225.

12. Cachin C (Ed.). Architecture of the hyperledger blockchain fabric. In: Workshop onDistributed Cryptocurrencies and Consensus Ledgers. 2016.

13. King S, Ppcoin NS. Peer-to-peer Crypto-currency With Proof-of-Stake. Self-published paper.

August 2012;19.

14. Hyperledger. [cited 9.11 2023]. Available from: https://www.hyperledger.org.

15. O'Dwyer KJ, Malone D. Bitcoin Mining and Its Energy Footprint. 2014.

16. Castro M, Liskov B (Eds.). Practical Byzantine Fault Tolerance. OSDI. 1999.

17. Hölbl M, Kompara M, Kamišalić A, Nemec Zlatolas LJS. A Systematic Review of the Use ofBlockchain in Healthcare. 2018;10(10):470.

18. Anderson JP. Computer Security Technology Planning Study. *ESD-TR*-73-51. 1972.

19. Courtney R, Ware W. Some informal comments about integrity and the integrity workshop.In: Ruthberg ZG, Polk WT, editors. Proceedings of the Invitational Workshop on Data Integrity. National Institute of Standards and Technology, *Special Publication*. 1989.

20. Coiera E. Guide to Health Informatics. *CRC Press*. 2019.

21. Khezr S, Moniruzzaman M, Yassine A, Benlamri R. Blockchain technology in healthcare: acomprehensive review and directions for future research. *Appl. Sci*. 2019;9(9):1736.

22. Moona G, Jewariya M, Sharma R. Relevance of dimensional metrology in manufacturingindustries. *MAPAN*. 2019;34:97-104.

23. Kumar T, Ramani V, Ahmad I, Braeken A, Harjula E, Ylianttila M. Blockchain utilisation inhealthcare: key requirements and challenges. In: Proceedings of the 2018 IEEE 20th International Conference on E-Health Networking, Applications and Services (Healthcom). *IEEE*. 2018;1-7.

24. Kassab MH, DeFranco J, Malas T, Destefanis Laplante G, Neto VV. Exploring research in

Blockchain for healthcare and a roadmap for the future. *IEEE Trans. Emerg. Top. Comput.*

2019;1-1.

25. S. Khezr, M. Moniruzzaman, A. Yassine, R. Benlamri, Blockchain technology in healthcare: a comprehensive review and directions for future research, *Appl. Sci*. 9 (9) (2019) 1736.

26. M.H. Kassab, J. DeFranco, T. Malas, Giuseppe Destefanis Laplante, V.V. Neto, Exploring research in Blockchain for healthcare and a roadmap for the future, *IEEE Trans. Emerg. Top. Comput.* (2019), 1-1.

27. U. Chelladurai, S. Pandian, A novel blockchain based electronic health record automation system for healthcare, *J. Ambient Intell. Humanized Comput*. (2021).

28. I. Yaqoob, K. Salah, R. Jayaraman, Y. Al-Hammadi, Blockchain for healthcare data management: opportunities, challenges, and future recommendations, *Neural Comput. App*l. (2021 Jan 7) 1–6.

29. Lin C, He D, Huang X, Khan MK, Choo KK. DCAP: A secure and efficient decentralized conditional anonymous payment system based on blockchain. *IEEE Transactions on Information Forensics and Security*. 2020;15:2440-2452

30. Anwar MR, Apriani D, Adianita IR. Hash Algorithm In Verification Of Certificate Data
Integrity And Security. *Aptisi Transactions on Technopreneurship* (ATT). 2021;3:181188.

31. Javaid M, Haleem A, Singh RP, Suman R, Khan S. A review of Blockchain Technology applications for financial services. *BenchCouncil Transactions on Benchmarks, Standards and Evaluation*. 2022;2:100073.

32. Khatri S, Alzahrani FA, Ansari MTJ, Agrawal A, Kumar R, Khan RA. A systematic analysis on blockchain integration with healthcare domain: Scope and challenges. *IEEE Access.* 2021;9:84666-84687.

33. Chen HS, Jarrell JT, Carpenter KA, Cohen DS, Huang X. Blockchain in healthcare: A patientcentered model. *Biomedical Journal of Scientific & Technical Research*. 2019;20:15017.

34. A. Farouk, A. Alahmadi, S. Ghose, A. Mashatan, Blockchain platform for industrial healthcare: vision and future opportunities, *Comput. Commun*. 154 (2020 Mar 15) 223–235.

35. V. Dhillon, D. Metcalf, M. Hooper, Blockchain in healthcare, in: Blockchainenabled Applications, Apress, Berkeley, CA, 2021, pp. 201–220.

36. Mohanasundaram, S.; Ramirez-Asis, E.; Quispe-Talla, A.; Bhatt, M.W.; Shabaz, M. Experimental replacement of hops by mango in beer: Production and comparison of total phenolics, flavonoids, minerals, carbohydrates, proteins and toxic substances. *Int. J. Syst. Assur. Eng. Manag*. 2022, 13, 132–145.

37. Hassan, N.H.; Ismail, Z. A conceptual model for investigating factors influencing informationsecurity culture in healthcare environment. Procedia-Soc. *Behav. Sci*. 2022, 65, 1007– 1012.

38. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies forbiomedical and health care applications. *J. Am. Med. Inform. Assoc.* 2017, 24, 1211–1220.

39. Keshta, I.; Odeh, A. Security and privacy of electronic health records: Concerns andchallenges. *Egypt. Inform. J*. 2021, 22, 177–183.

40. Das, S.; Namasudra, S. A novel hybrid encryption method to secure healthcare data in IoTenabled healthcare infrastructure. *Comput. Electr. Eng*. 2022, 101, 107991.

41. Rahman, M.U.; Guidi, B.; Baiardi, F.; Ricci, L. Context-aware and dynamic role-based accesscontrol using blockchain. In Proceedings of the Proceedings of the 34th International Conference on Advanced Information Networking and Applications (AINA-2020), Caserta, Italy, 15–17 April 2020; pp. 1449–1460.

42. Almadani, M.S.; Alotaibi, S.; Alsobhi, H.; Hussain, O.K.; Hussain, F.K. Blockchain-basedmulti-factor authentication: A systematic literature review. *Internet Things* 2023, 23, 100844.

43. Zheng, Z.; Xie, S.; Dai, H.-N.; Chen, X.;Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv*. 2018, 14, 352–375.

44. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical dataaccess and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25– 30.

45. Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y. Blockchain for healthcare datamanagement: Opportunities, challenges, and future recommendations. *Neural Comput. Appl.* 2021, 34, 11475–11490.

46. Hewa, T.; Ylianttila, M.; Liyanage, M. Survey on blockchain based smart contracts: Applications, opportunities and challenges. *J. Netw. Comput. Appl*. 2021, 177, 102857.

47. Gabay, D.; Akkaya, K.; Cebe, M. Privacy-preserving authentication scheme for connectedelectric vehicles using blockchain and zero knowledge proofs. *IEEE Trans. Veh. Technol*. 2020, 69, 5760–5772.

48. Miyachi, K.; Mackey, T.K. hOCBS: A privacy-preserving blockchain framework forhealthcare data leveraging an on-chain and off-chain system design. *Inf. Process. Manag*. 2021, 58, 102535.

49. Zhang, R.; Xue, R.; Liu, L. Security and privacy on blockchain. ACM Comput. Surv. (CSUR) 2019, 52, 1–34.

50. Liu, W.; Zhu, S.; Mundie, T.; Krieger, U. Advanced block-chain architecture for e-health systems. In Proceedings of the 2017 IEEE 19th International Conference on e-Health Networking, Applications and Services (Healthcom), Dalian, China, 12–15 October 2017; pp. 1–6.

51. Appelbaum D, Cohen E, Kinory E, Stein Smith S. Impediments to blockchain adoption. *Journal of Emerging Technologies in Accounting*. 2022;19:199-210.

52. Alnafrani M, Acharya S. SecureRx: A blockchain-based framework for an electronic prescription system with opioids tracking. *Health Policy and Technology*. 2021;10:100510.

53. Hasan MR, Deng S, Sultana N, Hossain MZ. The applicability of blockchain technology in healthcare contexts to contain COVID-19 challenges. *Library Hi Tech*. 2021;39:814-833.

54. Shae Z, Tsai J. Transform blockchain into distributed parallel computing architecture for precision medicine. In: Proceedings of the 2018 IEEE 38th International Conference on Distributed Computing Systems (ICDCS*). IEEE*; 2018; pp. 1290-1299.

55. J. Chanchaichujit, A. Tan, F. Meng, S. Eaimkhong, Blockchain technology in healthcare, in: healthcare 4.0, Palgrave Pivot, Singapore, 2019, pp. 37–62.

56. G. Srivastava, R.M. Parizi, A. Dehghantanha, The future of blockchain technology in healthcare internet of things security, Blockchain Cybersecurity, Trust and Privacy (2020) 161–184.

57. M. Bhavin, S. Tanwar, N. Sharma, S. Tyagi, N. Kumar, Blockchain and quantum blind signature-based hybrid scheme for healthcare 5.0 applications, Journal of Information Security and Applications 56 (2021 Feb 1) 102673.

58. E. Chukwu, L. Garg, A systematic review of Blockchain in healthcare: frameworks, prototypes, and implementations, IEEE Access 8 (2020 Jan 28) 21196–21214.

59. E.M. Abou-Nassar, A.M. Iliyasu, P.M. El-Kafrawy, O.Y. Song, A.K. Bashir, A.A. Abd ElLatif, DITrust chain: towards blockchain-based trust models for sustainable healthcare IoT systems, IEEE Access 8 (2020 Jun 2) 111223–111238.

60. R. Kumar, N. Marchang, R. Tripathi, Distributed off-chain storage of patient diagnostic reports in healthcare system using IPFS and Blockchain, in: In2020 International Conference on COMmunication Systems & NETworkS (COMSNETS), IEEE, 2020 Jan 7, pp. 1–5.

61. K. Miyachi, T.K. Mackey, hOCBS: a privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design, Inf. Process. Manag. 58 (3) (2021 May 1) 102535.

62. K. Miyachi, T.K. Mackey, hOCBS: a privacy-preserving blockchain framework for healthcaredata leveraging an on-chain and off-chain system design, Inf. Process. Manag. 58 (3) (2021 May 1) 102535.

63. C. Esposito, A. De Santis, G. Tortora, H. Chang, K.K. Choo, Blockchain: a panacea forhealthcare cloud-based data security and privacy? IEEE Cloud Computing 5 (1) (2018 Mar 28) 31–37.

64. I.A. Omar, R. Jayaraman, M.S. Debe, K. Salah, I. Yaqoob, M. Omar, Automating procurementcontracts in the healthcare supply chain using blockchain smart contracts*, IEEE Access* 9 (2021 Feb 26) 37397–37409.

65. P. Pandey, R. Litoriya, Securing and authenticating healthcare records through blockchaintechnology, *Cryptologia* 44 (4) (2020 Jul 3) 341–356.

66. R. Abujamra, D. Randall, Blockchain applications in healthcare and the opportunities and theadvancements due to the new information technology framework, in: Advances in Computers, vol. 115, *Elsevier*, 2019 Jan 1, pp. 141–154.

67. A. Sharma, S. Bahl, A.K. Bagha, M. Javaid, D.K. Shukla, A. Haleem, Blockchain technologyand its applications to combat COVID-19 pandemic, *Research on Biomedical Engineering* (2020 Oct 22) 1–8.

68. R. Kumar, W. Wang, J. Kumar, T. Yang, A. Khan, W. Ali, I. Ali, An integration of blockchainand AI for secure data sharing and detection of CT images for the hospitals, *Comput. Med. Imag. Graph.* 87 (2021 Jan 1) 101812.

69. R. Kumar, R. Tripathi, Scalable and secure access control policy for healthcare system usingBlockchain and enhanced Bell–LaPadula model, J*ournal of Ambient Intelligence and Humanized Computing* 12 (2) (2021 Feb) 2321–2338.

70. R. Jayaraman, K. Salah, N. King, Improving opportunities in healthcare supply chain processesvia the internet of things and blockchain technology, in: *International Journal of Healthcare Information Systems and Informatics (IJHISI)*, vol. 14, 2019 Apr 1, pp. 49–65, 2.

71. S. Balasubramanian, V. Shukla, J.S. Sethi, N. Islam, R. Saloum, A readiness assessmentframework for Blockchain adoption: a healthcare case study, *Technol. Forecast. Soc. Change* 165 (2021 Apr 1) 120536.

72. D.K. Aswal, Quality infrastructure of India and its importance for inclusive national growth,*MAPAN* 35 (2020) 139–150, https://doi.org/10.1007/s12647-020-00376-3.

73. K.P. Satamraju, Proof of concept of scalable integration of internet of things and Blockchainin healthcare, *Sensors* 20 (5) (2020 Jan) 1389.

74. N. Kshetri, Blockchain and electronic healthcare records [cybertrust*], Computer* 51 (12) (2018) 59–63.

75. M. Javaid, A. Haleem, R.P. Singh, S. Khan, R. Suman, Blockchain technology applications forIndustry 4.0: a literature-based review, BLOCK: *Research and Applications* (2021 Aug 12) 100027.

76. Hölbl, M., Kompara, A., Kamišalić, L.J.S. and Nemec Zlatolas, A Systematic Review of the Use of Blockchain in Healthcare, (2018), p. 470 10 (10).

77. Kumar, R.; Kumar, J.; Khan, A.A.; Zakria; Ali, H.; Bernard, C.M.; Khan, R.U.; Zeng, S.Blockchain and homomorphic encryption based privacy-preserving model aggregation for medical images. Comput. Med. Imaging Graph. **2022**, 102, 102139.

78. Wang, Y.; Zhang, A.; Zhang, P.; Qu, Y.; Yu, S. Security-Aware and Privacy-PreservingPersonal Health Record Sharing Using Consortium Blockchain. IEEE Internet Things J. **2022**, 9, 12014–12028.

79. Jayabalan, J.; Jeyanthi, N. Scalable blockchain model using off-chain IPFS storage forhealthcare data security and privacy. J. Parallel Distrib. Comput. **2022**, 164, 152–167.

80. Kumar, R.; Tripathi, R. Towards design and implementation of security and privacy frameworkfor Internet of Medical Things (IoMT) by leveraging blockchain and IPFS technology. J. Supercomput. **2021**, 77, 7916–7955.

81. Majdoubi, D.E.; Bakkali, H.E.; Sadki, S. SmartMedChain: A Blockchain-Based PrivacyPreserving Smart Healthcare Framework. J. Healthc. Eng. **2021**, 2021, 4145512.

82. Chenthara, S.; Ahmed, K.;Wang, H.; Whittaker, F.; Chen, Z. Healthchain: A novel frameworkon privacy preservation of electronic health records using blockchain technology. PLoS ONE **2020**, 15, e0243043.

83. Younis, M.; Lalouani, W.; Lasla, N.; Emokpae, L.; Abdallah, M. Blockchain-Enabled andData-Driven Smart Healthcare Solution for Secure and Privacy-Preserving Data Access. IEEE Syst. J. **2022**, 16, 3746–3757.

84. Wu, G.;Wang, S.; Ning, Z.; Li, J. Blockchain-Enabled Privacy-Preserving Access Control forData Publishing and Sharing in the Internet of Medical Things. IEEE Internet Things J. **2022**, 9, 8091–8104.

85. Alzubi, O.A.; Alzubi, J.A.; Shankar, K.; Gupta, D. Blockchain and artificial intelligenceenabled privacy-preserving medical data transmission in Internet of Things. Trans. Emerg. Telecommun. Technol. **2021**, 32, e4360.
86. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving frameworkfor access control and interoperability of electronic health records using blockchain technology. Sustain. Cities Soc. **2018**, 39, 283–297.
87. Yue, X.;Wang, H.; Jin, D.; Li, M.; Jiang,W. Healthcare Data Gateways: Found HealthcareIntelligence on Blockchain with Novel Privacy Risk Control. J. Med. Syst. **2016**, 40, 218.
88. Mohammad Hossein, K.; Esmaeili, M.E.; Dargahi, T.; Khonsari, A.; Conti, M. BCHealth: ANovel Blockchain-based Privacy- Preserving Architecture for IoT Healthcare Applications. Comput. Commun. **2021**, 180, 31–47.
89. Yugha, R.; Chithra, S.; Bhalaji, N.; Karthika, S. Privacy Protected IoT-Blockchain using ZKPfor Healthcare application. Control Eng. Appl. Inform. **2022**, 24, 76–87.
90. Barka, E.; Al Baqari, M.; Kerrache, C.A.; Herrera-Tapia, J. Implementation of a BiometricBased Blockchain System for Preserving Privacy, Security, and Access Control in Healthcare Records. J. Sens. Actuator Netw. **2022**, 11, 85.
91. Boumezbeur, I.; Zarour, K. Privacy Preservation and Access Control for Sharing ElectronicHealth Records Using Blockchain Technology. Acta Inform. Pragensia **2022**, 11, 105–122.
92. Karunakaran, C.; Ganesh, K.; Ansar, S.; Subramani, R. A privacy preserving framework forhealth records using blockchain. Pertanika J. Sci. Technol. **2021**, 29, 3081–3098.
93. Egala, B.S.; Pradhan, A.K.; Badarla, V.; Mohanty, S.P. Fortified-Chain: A Blockchain-BasedFramework for Security and Privacy- Assured Internet of Medical Things with Effective Access Control. IEEE Internet Things J. **2021**, 8, 11717–11731.
94. Shanthashalini, K.; Nithya, M. Blockchain based healthcare system to ensure data integrityand security in green computing environments. J. Green Eng. **2020**, 10, 10244–10260.
95. Thwin, T.T.; Vasupongayya, S. Blockchain-Based Access Control Model to Preserve Privacyfor Personal Health Record Systems. Secur. Commun. Netw. **2019**, 2019, 8315614.
96. Cao, Y.; Sun, Y.; Min, J. Hybrid blockchain–based privacy-preserving electronic medicalrecords sharing scheme across medical information control system. Meas. Control **2020**, 53, 1286–1299.
97. Tith, D.; Lee, J.S.; Suzuki, H.;Wijesundara,W.M.A.B.; Taira, N.; Obi, T.; Ohyama, N.Application of blockchain to maintaining patient records in

electronic health record for enhanced privacy, scalability, and availability. Healthc. Inform. Res. **2020**, 26, 3–12.

98. Ul Haque, R.; Hasan, A.S.M.T.; Jiang, Q.; Qu, Q. Privacy-preserving k-nearest neighborstraining over blockchain-based encrypted health data. Electronics **2020**, 9, 96.
99. Al-Otaibi, Y.D. K-nearest neighbour-based smart contract for internet of medical thingssecurity using blockchain. Comput. Electr. Eng. **2022**, 101, 108129.
100. Zhang, D.; Wang, S.; Zhang, Y.; Zhang, Q.; Zhang, Y. A Secure and Privacy-Preserving Medical Data Sharing via Consortium Blockchain. Secur. Commun. Netw. **2022**, 2022, 2759787.
101. Nie, X.; Zhang, A.; Chen, J.; Qu, Y.; Yu, S. Blockchain-Empowered Secure and PrivacyPreserving Health Data Sharing in Edge-Based IoMT. Secur. Commun. Netw. **2022**, 2022, 8293716.
102. Chen, Z.; Xu, W.; Wang, B.; Yu, H. A blockchain-based preserving and sharing system for medical data privacy. Future Gener. Comput. Syst. **2021**, 124, 338–350.
103. Elhoseny, M.; Haseeb, K.; Shah, A.A.; Ahmad, I.; Jan, Z.; Alghamdi, M.I. Iot solution for aienabled privacy-preserving with bigdata transferring: An application for healthcare using blockchain. Energies **2021**, 14, 5364.
104. Lee, D.; Song, M. MEXchange: A Privacy-Preserving Blockchain-Based Framework for Health Information Exchange Using Ring Signature and Stealth Address. IEEE Access **2021**, 9, 158122–158139.
105. Huang, H.; Zhu, P.; Xiao, F.; Sun, X.; Huang, Q. A blockchain-based scheme for privacypreserving and secure sharing of medical data. Comput. Secur. **2020**, 99, 102010.
106. Zou, R.; Lv, X.; Zhao, J. SPChain: Blockchain-based medical data sharing and privacypreserving eHealth system. Inf. Process. Manag. **2021**, 58, 102604.
107. Omar, A.A.; Bhuiyan, M.Z.A.; Basu, A.; Kiyomoto, S.; Rahman, M.S. Privacy-friendly platform for healthcare data in cloud based on blockchain environment. Future Gener. Comput. Syst. **2019**, 95, 511–521.
108. Yang, J.; Onik, M.M.H.; Lee, N.Y.; Ahmed, M.; Kim, C.S. Proof-of-familiarity: A privacypreserved blockchain scheme for collaborative medical decision-making. Appl. Sci. **2019**, 9, 1370.
109. Dwivedi, A.D.; Srivastava, G.; Dhar, S.; Singh, R. A decentralized privacy-preserving healthcare blockchain for IoT. Sensors **2019**, 19, 326.
110. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. J. Med. Syst. **2018**, 42, 140.

111. Yang, H.; Shen, J.; Lu, J.; Zhou, T.; Xia, X.; Ji, S. A Privacy-Preserving Data Transmission Scheme Based on Oblivious Transfer and Blockchain Technology in the Smart Healthcare. Secur. Commun. Netw. **2021**, 2021, 5781354.
112. Miyachi, K.; Mackey, T.K. hOCBS: A privacy-preserving blockchain framework for healthcare data leveraging an on-chain and off-chain system design. Inf. Process. Manag. **2021**, 58, 102535.
113. Huang, Z.; Guo, Y.; Huang, H.; Duan, R.; Zhao, X. Analysis and Improvement of BlockchainBased Multilevel Privacy-Preserving Location Sharing Scheme for Telecare Medical Information Systems. Secur. Commun. Netw. **2022**, 2022, 1926902.
114 Tan, L.; Yu, K.; Shi, N.; Yang, C.;Wei,W.; Lu, H. Towards Secure and Privacy-Preserving Data Sharing for COVID-19 Medical Records: A Blockchain-Empowered Approach. IEEE Trans. Netw. Sci. Eng. **2022**, 9, 271–281.
115. Zhao, J.;Wang,W.;Wang, D.;Wang, X.; Mu, C. PMHE: A wearable medical sensor assisted framework for health care based on blockchain and privacy computing. J. Cloud Comput. **2022**, 11, 96.
116. de Moraes Rossetto, A.G.; Sega, C.; Leithardt, V.R.Q. An Architecture for Managing Data Privacy in Healthcare with Blockchain. Sensors **2022**, 22, 8292.
117. Zhang, G.; Yang, Z.; Liu,W. Blockchain-based privacy preserving e-health system for healthcare data in cloud. Comput. Netw. **2022**, 203, 108586.
118. Xu, L.; Lin, M.; Feng, Y.; Sun, Y. BPDST: Blockchain-Based Privacy-Preserving Data Sharing on Thin Client for Electronic Medical Records. J. Comput. Inf. Technol. **2022**, 29, 235–250.
119. Upadhyay, S.; Kumar, M.; Kumar, A.; Karnati, R.; Mahommad, G.B.; Althubiti, S.A.;
Alenezi, F.; Polat, K. Feature Extraction Approach for Speaker Verification to Support Healthcare System Using Blockchain Security for Data Privacy. Comput. Math. Methods Med. **2022**, 2022, 8717263.
120. Lee, T.F.; Chang, I.P.; Kung, T.S. Blockchain-based healthcare information preservation using extended chaotic maps for hipaa privacy/security regulations. Appl. Sci. **2021**, 11, 10576.
121. Wang, B.; Li, Z. Healthchain: A privacy protection system for medical data based on blockchain. Future Internet **2021**, 13, 247.
122. Wu, H.; Dwivedi, A.D.; Srivastava, G. Security and Privacy of Patient Information in Medical Systems Based on Blockchain Technology. ACM Trans. Multimed. Comput. Commun. Appl. **2021**, 17, 60.

123. Chen, Y.; Meng, L.; Zhou, H.; Xue, G. A Blockchain-Based Medical Data Sharing Mechanism with Attribute-Based Access Control and Privacy Protection. Wirel. Commun. Mob. Comput. **2021**, 2021, 6685762.
124. Jia, X.; Luo, M.; Wang, H.; Shen, J.; He, D. A Blockchain-Assisted Privacy-Aware Authentication Scheme for Internet of Medical Things. IEEE Internet Things J. **2022**, 9, 21838–21850.
125. Sarier, N.D. Privacy-Preserving Biometric Authentication on the blockchain for smart healthcare. Pervasive Mob. Comput. **2022**, 86, 101683.
126. Wen, H.; Wei, M.; Du, D.; Yin, X. A Blockchain-Based Privacy Preservation Scheme in Mobile Medical. Secure. Commun. Netw. **2022**, 2022, 9889263.
127. Rao, K.R.; Naganjaneyulu, S. Permissioned Healthcare Blockchain System for Securing the EHRs with Privacy Preservation. Ing. Des Syst. Inf. **2021**, 26, 393–402.
128. Luong, D.A.; Park, J.H. Privacy-Preserving Blockchain-Based Healthcare System for IoT Devices Using zk-SNARK. IEEE Access **2022**, 10, 55739–55752.
129. Deshmukh, V.; Pathak, S.; Bothe, S. MobEdge: Mobile blockchain-based privacy-edge scheme for healthcare Internet of Thingsbased ecosystems. Concurr. Comput. Pract. Exp. **2022**, 34, e7210.
130. Ranjith, J.; Mahantesh, K. Blockchain-based Knapsack System for Security and Privacy Preserving to Medical Data. SN Comput. Sci. **2021**, 2, 245.
131. Liu, H.; Crespo, R.G.; Martínez, O.S. Enhancing privacy and data security across healthcare applications using Blockchain and distributed ledger concepts. Healthcare **2020**, 8, 243.
132. Zhou, Z.; Liu, Y. Blockchain-Based Encryption Method for Internal and External Health Privacy Data of University Physical Education Class. J. Environ. Public Health **2022**, 2022, 7506894.
133. Ali, A.; Rahim, H.A.; Pasha, M.F.; Dowsley, R.; Masud, M.; Ali, J.; Baz, M. Security, privacy, and reliability in digital healthcare systems using blockchain. Electronics **2021**, 10, 2034.
134. Zhang, C.; Xu, C.; Sharif, K.; Zhu, L. Privacy-preserving contact tracing in 5G-integrated and blockchain-based medical applications. Comput. Stand. Interfaces **2021**, 77, 103520.
135. Zheng, X.; Zhao, Y.; Li, H.; Chen, R.; Zheng, D. Blockchain-based verifiable privacypreserving data classification protocol for medical data. Comput. Stand. Interfaces **2022**, 82, 103605.