



**Politécnico
de Viseu**

Escola Superior
de Tecnologia
e Gestão de Viseu

Healthcare Data Management Through Blockchain Technology

Pedro Miguel Pereira Melo

Dissertação

Mestrado em Engenharia Informática - Sistemas de Informação

Trabalho efetuado sob a orientação de
Professor Doutor Carlos Augusto da Silva Cunha

Março de 2025



**Politécnico
de Viseu**

Escola Superior
de Tecnologia
e Gestão de Viseu

Healthcare Data Management Through Blockchain Technology

Pedro Miguel Pereira Melo

Dissertação

Mestrado em Engenharia Informática - Sistemas de Informação

Trabalho efetuado sob a orientação de

Professor Doutor Carlos Augusto da Silva Cunha

Março de 2025

Abstract

The healthcare industry struggles with significant data management challenges, primarily around interoperability, security, and transparency. Even with impressive technological progress, the continued use of closed, proprietary medical systems blocks the path toward truly effective and accessible healthcare solutions. These obstacles harm patient care quality, decrease operational efficiency, and challenge ethical standards, creating an urgent need for fresh solutions to these technological and systemic barriers.

Inspired by how modern technologies could transform healthcare delivery, this project examines blockchain technology's potential to tackle these persistent problems by strengthening security, ethics, and efficiency in health data management. We have established six critical goals: enhancing data compatibility between systems, strengthening data security and privacy protections, putting more control in patients' hands, bringing greater efficiency and transparency to clinical trials, improving medication tracking throughout supply chains, and discovering productive connections with emerging technologies like *Artificial Intelligence* (AI) and *Internet of Things* (IoT).

With careful attention to privacy concerns, transparency requirements, and ethical data practices, we connect technological capabilities with healthcare needs, building stronger trust and accountability frameworks for handling sensitive patient information. Our research followed a carefully structured two-phase approach, beginning with a broad scientometric analysis to identify research trends, followed by an in-depth systematic review examining real-world implementations and their results.

Findings demonstrate that blockchain's decentralized architecture and cryptographic practices significantly enhance data interoperability and privacy. The use of smart contracts enables granular access control settings that empower patients to govern their own health records. Blockchain's properties also increase efficiency in clinical trials and supply chain management. Moreover, the integration with AI, IoT and big data analytics amplifies blockchain's impact in the healthcare industry, enhancing predictive diagnostic practices, enabling gradual blockchain implementation and supporting real-time monitoring.

In conclusion, this research contributes a comprehensive evaluation of blockchain's benefits and limitations in healthcare, highlighting its potential to

foster a secure, patient-centric, and efficient data ecosystem. It underscores the necessity for collaborative efforts among healthcare stakeholders, technologists, and regulators to address technical and organizational hurdles, paving the way for blockchain's practical integration into global healthcare systems.

Keywords: Blockchain; Healthcare; Data Management; Interoperability; Data Security; Data Privacy

Resumo

O sector da saúde enfrenta desafios significativos relativos à gestão de dados, principalmente em torno da interoperabilidade, segurança e transparência da informação. Mesmo com progressos tecnológicos impressionantes, a utilização contínua de sistemas médicos fechados e proprietários impede o avanço para soluções de cuidados de saúde verdadeiramente eficazes e acessíveis. Estes obstáculos prejudicam a qualidade dos cuidados de saúde prestados aos doentes, diminuem a eficiência operacional e desafiam as normas éticas, criando uma necessidade urgente de novas soluções para estas barreiras tecnológicas e sistémicas.

Inspirado na forma como as tecnologias modernas podem transformar a prestação de cuidados de saúde, este projeto examina o potencial da *blockchain* para resolver estes problemas persistentes, reforçando a segurança, a ética e a eficiência na gestão dos dados de saúde. Foram estabelecidos seis objetivos: melhorar a compatibilidade de dados entre sistemas, reforçar a segurança dos dados e a proteção da privacidade, mover o controlo dos dados para os pacientes, aumentar a eficiência e transparência aos ensaios clínicos, melhorar o rastreio de medicamentos e descobrir interligações com tecnologias emergentes como *Artificial Intelligence* (AI) e *Internet of Things* (IoT).

Com especial preocupação em práticas de privacidade, requisitos de transparência e às práticas éticas, são estudadas as capacidades tecnológicas associadas às necessidades dos cuidados de saúde, de modo a criar estruturas confiáveis e de responsabilidade mais fortes para o tratamento de informações sensíveis dos doentes. Esta pesquisa seguiu uma abordagem cuidadosamente estruturada em duas fases, começando com uma ampla análise para identificar tendências de pesquisa, seguida por uma revisão sistemática aprofundada onde foram examinadas implementações no mundo real e analisados os respetivos resultados.

As conclusões demonstram que a arquitetura descentralizada da *blockchain* e as práticas criptográficas melhoram significativamente a interoperabilidade e a privacidade dos dados. A utilização de *smart contracts* permite definições de controlo de acesso granular que permitem aos pacientes gerir os seus próprios registos de saúde. As propriedades da *blockchain* também aumentam a eficiência nos ensaios clínicos e na gestão da cadeia de abastecimento de medicamentos. Além disso, a integração com AI, IoT e a análise de grandes volumes de dados amplifica o impacto da *blockchain* no sector da saúde, melhorando as práticas de diagnóstico preditivo e

permitindo a implementação gradual da *blockchain*.

Em conclusão, esta investigação contribui para uma avaliação abrangente dos benefícios e limitações da *blockchain* nos cuidados de saúde, destacando o seu potencial para promover um ecossistema de dados seguro, centrado no doente e eficiente. Sublinha a necessidade de esforços de colaboração entre as diferentes partes interessadas para resolver os obstáculos técnicos e organizacionais.

Palavras-Chave: Saúde; Gestão de Dados; Interoperabilidade; Segurança de Dados; Privacidade

Contents

List of Tables	vii
List of Figures	ix
List of Acronyms	xi
1 Introduction	1
1.1 Research Questions	2
1.2 Contributions	3
2 Related Work And Background	5
2.1 Background	5
2.1.1 Core Architecture and Transaction Processing	6
2.1.2 Consensus Mechanisms	6
2.1.3 Types of Blockchain	7
2.1.4 Smart Contracts	8
2.1.5 Healthcare Stakeholders and Workflows	8
2.1.6 Privacy, Security and Regulation in Healthcare	9
2.1.7 Healthcare Data Management and Information Systems	9
2.2 Related Work	10
3 Problem Definition and Methodology	15
3.1 <i>Problem Definition</i>	15
3.2 <i>Methodology</i>	17
3.2.1 <i>Stage 1: Scientometric Search</i>	17
3.2.2 <i>Stage 2: Systematic Literature Review</i>	19
Inclusion and Exclusion Criteria	19
3.2.3 Screening and Selection	19
3.3 Research Objectives Definition	20
3.3.1 O1: Improving data interoperability and reducing fragmentation in healthcare systems	20
3.3.2 O2: Evaluating Blockchain’s Capacity To Improve Data Security And Privacy While Maintaining Accessibility For Healthcare Providers	22

3.3.3	O3: Empowering patients with greater control over their health data	23
3.3.4	O4: Improving the Efficiency and Transparency of Clinical Trials and Research	23
3.3.5	O5: Enhancing Drug Traceability and Supply Chain Management	24
3.3.6	O6: Synergies Between Blockchain and Other Technologies	24
4	Results	27
4.1	Research Areas	28
4.2	Answering Research Objectives	29
4.2.1	O1: Improving data interoperability and reducing fragmentation in healthcare systems	29
4.2.2	O2: Evaluating blockchain’s capacity to improve data security and privacy while maintaining accessibility for healthcare providers	30
4.2.3	O3: Empowering patients with greater control over their health data	31
4.2.4	O4: Improving the efficiency and transparency of clinical trials and research	31
4.2.5	O5: Enhancing drug traceability and supply chain management	32
4.2.6	O6: Synergies between blockchain and other technologies	32
4.3	Limitations Of Blockchain In Healthcare	33
5	Discussion	35
5.1	Research Objectives Analysis	35
5.1.1	Improving data interoperability and reducing fragmentation in healthcare systems (O1)	35
5.1.2	Improving data security and privacy and control over health (O2, O3)	37
5.1.3	Improving efficiency and transparency, enhancing traceability and supply chain management (O4, O5)	38
5.1.4	Synergies between blockchain and other technologies (O6)	39
5.2	Blockchain’s Main Adversities	39
	System Complexity	39
	Maintenance Costs and Expertise	40
6	Conclusion	41
6.1	Future work	42
	References	44

List of Tables

4.1	Summary of Challenges of Blockchain Technology in Healthcare. . .	34
-----	---	----

List of Figures

2.1	Representation of block connections in blockchain	6
3.1	Initial search result	18
3.2	Distribution of document types	18
3.3	Distribution of publishing year	19
3.4	Distribution of publishing year	20
3.5	PRISMA chart	21
4.1	Research Categories Distribution	28

List of Acronyms

AI	<i>Artificial Intelligence</i>
EHR	<i>Electronic Health Records</i>
IoT	<i>Internet of Things</i>
PBFT	<i>Practical Byzantine Fault Tolerance</i>
PoA	<i>Proof of Authority</i>
PoS	<i>Proof of Stake</i>
PoW	<i>Proof of Work</i>

Chapter 1

Introduction

The healthcare sector currently occupies a precarious position amid our technological revolution. Medical science continues its advancements, yet the administrative and technological backbone supporting these advances remains surprisingly antiquated. Many institutions still wrestle with disconnected databases that create information silos [Peiris et al., 2024]. Patient data frequently exists in fragmented states across multiple systems, while legitimate privacy concerns often impede the seamless exchange of critical information between providers. These structural inefficiencies persist despite the availability of solutions. This dichotomy represents one of healthcare’s most pressing contemporary challenges. As treatments evolve, the systems managing healthcare delivery must similarly transform.

Blockchain originated within cryptocurrency frameworks but has since expanded considerably beyond these financial beginnings. The technology functions as distributed ledger architecture maintaining transparency, immutability, and transactional security [Anik et al., 2023, Bazel et al., 2021, Firouzi et al., 2023]. Such characteristics correspond directly with healthcare’s fundamental requirements, where maintaining data accuracy, safeguarding patient information, and facilitating proper information transfer remain essential considerations.

Healthcare applications for blockchain extend across numerous domains with transformative potential. These include strengthening electronic medical record systems, enhancing research trial methodology, improving medication tracking processes, and developing more robust health information exchanges. In this regard, blockchain’s convergence with *Artificial Intelligence* (AI), *Internet of Things* (IoT),

and big data analytics creates promising opportunities [Firouzi et al., 2023]. These technological combinations potentially enable significant advances in individualized treatment approaches, distance-based patient assessment systems, and anticipatory healthcare interventions, as these are heavily impacted by the quantity and the quality of available data [Abbate et al., 2023].

Despite growing enthusiasm surrounding healthcare blockchain adoption, a measured evaluation remains imperative. Each potential advantage necessitates careful consideration against practical limitations, ethical implications, and regulatory requirements. Enhanced data protection capabilities must be evaluated alongside implementation difficulties and adoption barriers. Efficiency improvements require balanced assessment against information privacy concerns and preservation of patient autonomy.

This study aims to provide a comprehensive, nuanced examination of blockchain technology's role in reshaping the healthcare landscape. By analyzing current implementations, exploring potential future applications, and critically assessing both opportunities and obstacles, this work seeks to contribute valuable insights to this rapidly evolving field.

1.1 Research Questions

This research is guided by several key questions that will guide the research process:

1. What specific advantages does blockchain technology offer to the healthcare industry, and why are these benefits significant for the future of medical practice and patient care?
2. What potential challenges or drawbacks could arise from implementing blockchain in healthcare settings, and how can these obstacles be effectively addressed?
3. How can the insights from these advantages and challenges inform the future integration of blockchain-based technology within the global healthcare system?
4. What opportunities arise from integrating blockchain with other emerging technologies (such as AI, IoT, or big data analytics) in the healthcare context, and how can these technologies together transform medical practices and health outcomes?

1.2 Contributions

The distinctive aspect of this research resides in its holistic methodology, which makes the following contributions:

- **Analysis of blockchain implementations:** We conduct a critical evaluation of current blockchain applications in healthcare, assessing successes and limitations across diverse use cases to provide a balanced view of the technology's practical impact.
- **Integration with emerging technologies:** We analyze the convergence of blockchain with emerging technologies (*Artificial Intelligence* (AI), *Internet of Things* (IoT), big data analytics) in healthcare, evaluating the potential for enhanced data management, improved diagnosis, and optimized treatment protocols.
- **Data ownership and privacy impact:** We examine blockchain's impact on patient data ownership and privacy, analyzing how the technology could empower patients with greater control over their health information while ensuring data integrity and security.

The remainder of this document is organized as follows. Chapter 2 presents technological specification of blockchain technology and reviews related work. Chapter 3 defines the problem definition and outlines the methodology used in the study. Chapter 4 presents the results and Chapter 5 critically discusses the findings from the analysis process. Finally, Chapter 6 concludes this study by summarizing the analyzed problems, results, and findings and by presenting the future work.

Chapter 2

Related Work And Background

This chapter examines the background and related work that form the backbone of this study. The history, concepts and features of blockchain technology and its applications in the healthcare industry are explored, followed by a review of the state-of-the-art related to this work.

2.1 Background

The blockchain concept first appeared within Nakamoto's 2008 publication detailing decentralized ledger architecture supporting Bitcoin operations [Nakamoto and Bitcoin, 2008]. Though initially conceived for digital currency purposes, core blockchain elements, such as distributed information storage, cryptographic protection methods, and consensus validation mechanisms, have since expanded beyond original applications. Key features including decentralization, unalterable record maintenance, and operational transparency demonstrate value across numerous industrial sectors [Farouk et al., 2020, Angelis and Da Silva, 2019, Ahram et al., 2017]. Within healthcare environments specifically, these attributes address fundamental challenges involving systems integration, information accuracy preservation, and data protection requirements [Angraal et al., 2017], [Goel et al., 2019].

2.1.1 Core Architecture and Transaction Processing

Blockchain functions as distributed information architecture maintaining transparent, permanent data records. Information segments occupy cryptographically connected blocks forming sequential arrangements. This structural linking between successive blocks creates chronological information chains. Figure 2.1 represents this connection between blocks in blockchain. Unlike conventional database systems permitting modification or replacement of existing records, blockchain architecture ensures recorded information remains unalterable without compromising subsequent block integrity within the established sequence.

This design provides a secure, decentralized framework for data storage and verification, making it a robust solution for applications requiring transparency and tamper-proof records. Each transaction in the blockchain is grouped into blocks and, once validated, these blocks are cryptographically linked to the previous ones, creating a chain of information that is secure and immutable. This ensures that no one can change a transaction after it is recorded without altering the entire chain, which everyone on the network would detect.

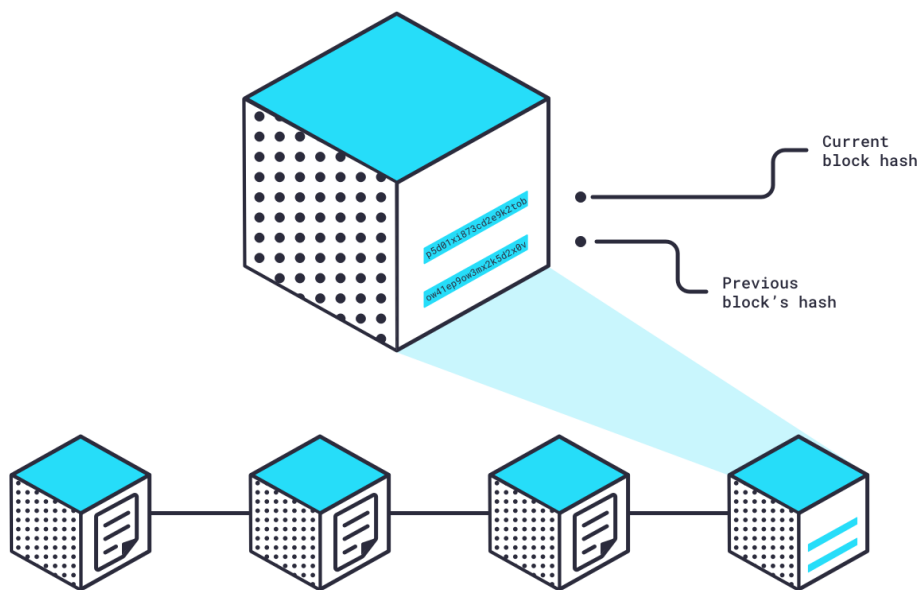


Figure 2.1: Representation of block connections in blockchain

2.1.2 Consensus Mechanisms

Blockchain security fundamentally depends upon transaction validation procedures requiring network-wide participant agreement. These consensus protocols ensure collective verification where network members authenticate transaction validity before permanent chain incorporation occurs [Farouk et al., 2020, McGhin et al., 2019].. Distributed validation methodology

enhances system reliability and security attributes through responsibility allocation across multiple network nodes rather than concentrating verification authority within individual entities.

Proof of Work (PoW) is currently one of the most used consensus mechanisms [Alzoubi and Mishra, 2024, Frikha et al., 2021]. This mechanism requires participants (miners) to solve computationally intensive cryptographic hash problems to validate transactions, making the system secure but energy intensive [Alzoubi and Mishra, 2024, Frikha et al., 2021]. On the other hand, PoS works by selecting validators based on the amount of cryptocurrency they stake in the system, making it more energy efficient and scalable while maintaining security through economic incentives [Asif and Hassan, 2023].

In healthcare contexts, this distributed validation improves data sharing security by creating an auditable trail of access and modifications while enforcing predefined consensus rules for data validation. However, implementing such systems in healthcare requires careful consideration of additional factors such as privacy regulations, access control mechanisms, and healthcare-specific security requirements [Farouk et al., 2020, McGhin et al., 2019].

2.1.3 Types of Blockchain

Blockchain comes in several forms: public, private, consortium, and permissioned blockchains. Public blockchains are open to anyone and rely on decentralized consensus mechanisms. Private blockchains, on the other hand, are restricted to specific participants. Consortium blockchains, a hybrid between public and private, are managed by a group of organizations rather than a single entity, where multiple stakeholders need shared access to sensitive data. Permissioned blockchains combine elements of public blockchains with access controls, allowing only authorized users to participate while still maintaining some level of decentralization [Farouk et al., 2020, Hasselgren et al., 2020].

Each type of blockchain offers unique advantages depending on the use case. In permissioned blockchains, consensus is often achieved through *Practical Byzantine Fault Tolerance* (PBFT), a consensus protocol that operates through a voting system where all validator nodes communicate with each other to agree on the state of the network, enabling the system to tolerate up to one-third of nodes exhibiting malicious or faulty behavior while maintaining system reliability. Another common mechanism is *Proof of Authority* (PoA), where network validators, known as authorities, are explicitly authorized to validate transactions based on their proven reputation and identity, with their real-world identities being at stake as an incentive for honest behavior. These consensus mechanisms are crucial as they ensure that data is securely validated and shared without a central authority [Farouk et al., 2020, McGhin et al., 2019].

The implementation of consensus mechanisms in permissioned blockchains [Farouk et al., 2020, Meghin and Johnson, 2019] provides the technological foundation for executing complex operations in healthcare environments. Within this context, smart contracts emerge as a key technological component that builds upon these consensus protocols to enable automated healthcare processes.

2.1.4 Smart Contracts

Smart contracts are automated programs that execute predefined actions when specific conditions are met without requiring intermediaries. In the context of blockchain, they enhance system functionality by ensuring that all actions are secure, transparent, and immutable. For example, in healthcare, a smart contract can release patient records to authorized doctors only after verifying patient consent, ensuring privacy and compliance. By leveraging the decentralized nature of blockchain, smart contracts reduce fraud, improve trust, and streamline processes like claims management, data sharing, and financial settlements [Angraal et al., 2017, Goel et al., 2019].

As blockchain technology matures, its applications increasingly cross into various domains, including healthcare, supply chain management, and telemedicine. This expansion offers significant opportunities while presenting challenges, particularly in healthcare, where the secure sharing of patient data and the authenticity of medical records are crucial.

The potential of blockchain technology in healthcare go beyond smart contracts and automated execution methods. As healthcare institutions increasingly use blockchain solutions for safe data storage and process automation, the technology's potential to address system-wide issues becomes clear. A particular obstacle is healthcare interoperability.

2.1.5 Healthcare Stakeholders and Workflows

Healthcare systems involve complex interactions between multiple stakeholders, each playing crucial roles in the delivery and management of healthcare services. Primary stakeholders include patients, healthcare providers (physicians, nurses, specialists), healthcare institutions (hospitals, clinics, laboratories), insurance providers, and regulatory bodies. These stakeholders interact through various workflows and data exchange patterns that form the backbone of healthcare delivery [Mackey et al., 2019].

The traditional healthcare workflow typically involves multiple touch points where patient data is created, accessed, and shared. When a patient visits a healthcare provider, the interaction generates clinical data that needs to be securely stored, potentially shared with other providers, and eventually used for insurance claims

processing. These workflows have historically been fragmented, with data siloed within individual institutions, leading to inefficiencies in care delivery and patient experience.

2.1.6 Privacy, Security and Regulation in Healthcare

Healthcare data privacy and security are governed by stringent regulations designed to protect patient information while enabling necessary data sharing for care delivery. These regulations establish frameworks for data protection, patient consent management, and secure information exchange between healthcare stakeholders. Key regulatory frameworks include the Health Insurance Portability and Accountability Act (HIPAA) [Cohen and Mello, 2018, Said et al., 2023] in the United States and the General Data Protection Regulation (GDPR) [Said et al., 2023] in Europe, which set specific requirements for handling protected health information. These regulations mandate strict access controls, audit trails, and patient consent mechanisms for data sharing.

2.1.7 Healthcare Data Management and Information Systems

Healthcare data management encompasses the creation, storage, and exchange of various types of health information through electronic systems. EHR systems serve as digital repositories of patients' medical histories, designed to streamline data access and management in healthcare settings. These systems must handle diverse data types, including clinical notes, laboratory results, imaging studies, and administrative information.

Interoperability remains a critical challenge in healthcare data management. Healthcare information systems must support digital access rules management, data aggregation, identity verification, and immutability of records. The infrastructure must scale to handle clinical transaction volumes while ensuring compliance with privacy regulations and maintaining patient consent management.

Healthcare data standards play a crucial role in enabling interoperability between different systems. Standards such as Health Level Seven (HL7) [Strasberg et al., 2021], Fast Healthcare Interoperability Resources (FHIR) [Kramer and Moesel, 2023], and Digital Imaging and Communications in Medicine (DICOM) [Larobina, 2023] provide frameworks for structured data exchange. The evolution of healthcare information systems has led to the development of specialized applications including Hospital Management Systems (HMS), Clinical Decision Support Systems (CDSS), and telemedicine platforms. These systems must integrate seamlessly while maintaining data integrity, security, and accessibility.

2.2 Related Work

This chapter provides a comprehensive review of existing blockchain-based solutions within the healthcare domain, beginning with systematic reviews exploring blockchain integration in healthcare systems. These reviews highlight recurring challenges, such as data breaches, interoperability issues, and data management inefficiencies, while discussing proposed solutions like decentralized structures and patient-centric frameworks. The chapter then delves into related work, focusing on specific blockchain implementations, their design approaches, and practical applications that aim to reshape healthcare delivery systems.

[Anik et al., 2023] presents a review on integrating blockchain technology into *Electronic Health Records* systems, which are digital repositories of patients' medical histories designed to streamline data access and management in healthcare. The study emphasizes the potential of blockchain to empower patients through enhanced control, access, and transparency over their medical data. The review highlights key challenges in the current EHR systems, including data breaches, incorrect entries, lack of interoperability, and inefficient data management. With its decentralized structure, smart contracts, and immutable ledgers, blockchain offers solutions to these issues by improving data security and transparency while allowing patients to selectively control their health information. This work also discusses the limitations of blockchain, such as scalability concerns, transaction costs, and the need for regulatory frameworks. The authors propose a patient-centric framework based on blockchain that could enhance patient empowerment, while future research should address challenges related to governance, cross-institutional data sharing, and the integration of blockchain with existing healthcare infrastructure.

The work conducted by [Angraal et al., 2017] provides a foundational exploration of blockchain technology's applications in healthcare. The authors systematically reviewed existing literature, analyzing use cases and theoretical frameworks to assess blockchain's potential for addressing critical challenges such as data security, privacy, and interoperability in healthcare systems. Their methodology involved evaluating blockchain's technical capabilities, such as decentralization and immutability, and examining case studies or proposed implementations to highlight opportunities and limitations. Key findings include blockchain's ability to secure patient data and streamline information sharing among healthcare providers while emphasizing challenges such as scalability, regulatory compliance, and integration with existing systems. The study concludes with a call for interdisciplinary research and collaboration to overcome these barriers and realize the full potential of blockchain technology in improving healthcare outcomes.

[Abbate et al., 2023] proposes a blockchain platform tailored for Healthcare 4.0, addressing critical challenges like EHRs and telemedicine services. The study adopts

a hybrid approach, combining a review of existing blockchain-based healthcare platforms with the conceptual design and proposal of a novel framework. Their platform emphasizes decentralization, data immutability, and privacy-preserving mechanisms, while also addressing the integration of telemedicine services and interoperability across healthcare systems. Key characteristics of the proposed framework include the use of smart contracts to automate processes such as patient consent and claims management, and a modular architecture designed to facilitate scalability and adaptability to various healthcare contexts. The authors identified limitations within existing solutions, such as insufficient dissemination of test results among healthcare professionals, which can contribute to medical errors and higher mortality rates. They further highlight the fragmented nature of healthcare data systems and propose their blockchain platform as a potential solution. The paper calls for broader sharing of test results. It emphasizes the need for more randomized controlled trials in telemedicine research to validate the efficacy and implementation of blockchain-based platforms.

Building upon these reviews, specific research has explored the convergence of blockchain with other emerging technologies in healthcare. A study by [Firouzi et al., 2023] provides an in-depth exploration of the convergence of *Internet of Things* (IoT), *Artificial Intelligence* (AI), edge-fog-cloud computing, and blockchain technologies in healthcare¹. This fusion addresses key challenges in IoT, such as security vulnerabilities, latency, and scalability, while enhancing privacy, data management, and operational efficiency. The researchers demonstrate the practical implementation of this convergence through a case study on stress monitoring, using privacy-preserving techniques like federated learning to protect patient data. In the realm of patient-driven interoperability, [Pirtle and Ehrenfeld, 2018] investigated the potential of blockchain technology to facilitate greater patient control over health data. Their study revealed that blockchain could ensure data integrity, mitigate the risk of data loss, and provide a transparent audit trail. However, the shift towards patient-centered interoperability introduces new challenges in security, privacy, technology infrastructure, incentivization, and governance. Both studies highlight persistent challenges in the adoption of blockchain in healthcare. These include scalability issues, privacy and security concerns, patient engagement, and the need for incentives for data sharing. Future research directions identified include addressing requirements for patient-centered interoperability, exploring private vendor-based solutions, advocating for a US national patient identifier, and operationalizing prototyped blockchain solutions for healthcare data sharing.

[Shahnaz et al., 2019] work presents a framework for implementing blockchain technology in healthcare, focusing on *Electronic Health Records* (EHR). The framework employs a permissioned blockchain architecture with smart contracts for access

control, combines symmetric and asymmetric encryption for data security, and utilizes off-chain storage for clinical data while maintaining metadata on-chain. It aims to enhance data security and privacy by implementing granular access rules and off-chain storage to optimize performance. However, the study acknowledges limitations such as confidentiality and scalability when data is stored directly on the blockchain. Further research is needed to assess the feasibility of blockchain adoption in healthcare, address challenges, establish universal standards for data exchange, address privacy and security concerns, and overcome scalability issues.

[Younis et al., 2022] proposes a blockchain-based solution for secure and privacy-preserving data access in healthcare. It allows patients to manage access permissions securely while ensuring healthcare organizations comply with privacy regulations. Sensor data is stored in cloud storage, while access control and session logs are handled in blockchain. A data-driven authentication and secure communication protocol is introduced to mitigate fraud and identity theft. Smart contracts regulate stakeholder interactions. The solution's security properties are analyzed, demonstrating computational efficiency. However, limitations include the need for additional measures, inherent risks of identity theft and fraud, and shortcomings in encryption key management. Research gaps include exploring encryption key limitations, lack of support for key management in cloud storage systems, vulnerabilities in telehealth systems, scalable and resource-efficient data storage solutions, and enhancing flexibility and high-integrity features in conventional cloud-based storage systems.

[Liu and Li, 2022] evaluated a proposed Healthcare IoT system using simulations. It finds that the fixed block size scheme outperforms others in most episodes, with offloading outperforming the fixed block interval scheme. The study also examines the effects of computing tasks, transaction sizes, and block size on system performance. However, security vulnerabilities and limited energy capacity are identified as the main limitations. The study proposes integrating permissioned blockchain and deep reinforcement learning techniques to address these issues. Further research is needed to consider energy efficiency and security concerns in these systems. Field experiments are also needed to validate the system in real-world settings. Future research may focus on practical implementation and unique requirements in complex environments.

[Yongjoh et al., 2021] demonstrated a novel nationwide blockchain implementation addressing critical healthcare information system challenges. By developing a consortium blockchain platform integrated with mobile applications and decentralized access mechanisms, the researchers provided a comprehensive solution to long-standing issues in medical data management. The system's innovative approach utilized software agents installed in hospitals and Raspberry Pi devices, enabling seamless interconnectivity among hospital health information systems through the

MQTT protocol. Key contributions include enhanced information retrieval capabilities, improved data security, and reduced susceptibility to data loss. The research distinguished itself by offering a scalable, practical approach to blockchain deployment across thousands of hospitals, highlighting potential strategies for large-scale healthcare technology integration.

[Chelladurai and Pandian, 2022] presents a blockchain-based healthcare system designed to address critical challenges in health record management by offering a secure, efficient, transparent, consistent, and decentralized alternative to traditional methods. The proposed system leverages blockchain technology and smart contracts to ensure the integrity and immutability of health records while enhancing accessibility for authorized users. To evaluate its efficacy, experiments were conducted to assess the performance of blockchain-based smart contracts under various scenarios, highlighting the system's capability to manage and process health records securely and efficiently. The study identifies key features of the system, such as decentralized data storage, tamper-proof record management, and automated verification through smart contracts. Despite these advancements, several research gaps persist, including the lack of integrated data management systems, challenges in achieving seamless network connectivity, and difficulties in sharing comprehensive patient health histories. The work also emphasizes issues related to fragmented health information and underscores the critical need for secure storage and retrieval mechanisms for EHR. The authors highlight the importance of addressing privacy and security concerns inherent in blockchain-based systems, particularly focusing on implementation challenges in real-world healthcare settings. Additionally, the study notes the absence of standardized protocols to ensure interoperability between blockchain-enabled healthcare applications, as well as the limited exploration of specific use cases and workflows. These findings call for further research to establish robust frameworks and protocols that can enhance the practical applicability and adoption of blockchain technology in the healthcare domain.

[Bazel et al., 2021] introduces a blockchain-based framework for managing healthcare big data, emphasizing its transformative potential akin to the impact of telehealth. The proposed solution leverages distributed ledger technology to optimize healthcare data handling by providing a secure, decentralized, and cost-efficient system. Key features of the framework include real-time access to patient data, enhanced data privacy through patient-controlled permissions, and secure data sharing among authorized parties. Additionally, the system facilitates global connections between patients with similar conditions, fostering improved treatment options and better patient outcomes. The authors outline the methodology underpinning the framework, focusing on how blockchain technology ensures data integrity, immutability, and accessibility. Privacy is reinforced by giving patients direct control over their health records, empowering them to selectively

share data with healthcare providers while safeguarding sensitive information. The study also highlights the role of distributed ledgers in reducing administrative overhead, minimizing costs, and enhancing overall system efficiency. Despite these advancements, the work identifies several technological challenges that must be addressed for widespread adoption. Scalability remains a critical barrier, as blockchain networks often face limitations in handling large volumes of healthcare data. The study also emphasizes implementation barriers, including the complexity of integrating blockchain with existing healthcare IT infrastructure, and the urgent need for standardized protocols to ensure interoperability. The authors recommend that future research explore advanced encryption techniques to bolster data security, develop more efficient consensus mechanisms to improve system performance, and investigate strategies for seamless integration of blockchain into existing healthcare ecosystems.

Previous work has extensively studied the use of blockchain technology in healthcare, as well as the integration between some technologies with the goal to increase security. However, despite these advancements, little attention has been given to the combination of blockchain with standardized interoperability protocols. Additionally, most studies remain theoretical or confined to small-scale pilot projects, with real-world implementation and validation being notably scarce.

Chapter 3

Problem Definition and Methodology

This chapter showcases the definition of the problem of the study and the fundamental challenges within healthcare systems. Specific research objectives that guides this investigation are also defined in this chapter. The methodology chosen to address the research objectives follows.

3.1 *Problem Definition*

The healthcare industry is currently dealing with considerable challenges with data management, security, and interoperability. These concerns have far-reaching ramifications for patient care, research, and the general efficiency of healthcare delivery and processes. A thorough examination of these challenges reveals issues, including:

- **Data Fragmentation:** Patient information is frequently distributed across various healthcare providers, institutions, and systems. This lack of centralized access results in incomplete medical histories, which can compromise the quality of care, delay treatment, and increase the likelihood of medical errors [Angraal et al., 2017];
- **Interoperability Challenges:** The inability of healthcare systems to seamlessly share data hinders effective collaboration among providers.

This limitation affects the timely exchange of information during critical situations, leading to fragmented care and inefficient operations [Goel et al., 2019, Pirtle and Ehrenfeld, 2018];

- **Data Security and Privacy Concerns:** With the increasing digitization of health records, protecting sensitive patient information from unauthorized access and cyber threats has become paramount. Current systems often struggle to balance data accessibility with robust security measures [Meghin and Johnson, 2019];
- **Patient Data Ownership and Control:** Patients frequently lack control over their personal health information and its distribution. This issue raises ethical concerns and can limit patients' ability to make informed decisions about their healthcare [Hasselgren et al., 2020];
- **Inefficiencies in Clinical Trials and Research:** The current infrastructure for conducting clinical trials and medical research is often plagued by data silos, lack of transparency, and difficulties in patient recruitment and data verification [Farouk et al., 2020];
- **Drug Traceability and Supply Chain Management:** The pharmaceutical supply chain faces challenges in ensuring the authenticity of drugs and efficiently tracking their movement from manufacture to patient administration [Angelis and Da Silva, 2019];
- **Integration of Emerging Technologies:** While technologies like AI, IoT, and big data analytics offer immense potential for improving healthcare, integrating them securely and effectively with existing healthcare infrastructure presents significant challenges.

This research aims to explore how blockchain technology can address these multifaceted problems in healthcare data management. Specifically, the objectives of this study are defined as the following:

- **O1:** Improving data interoperability and reducing fragmentation in healthcare systems;
- **O2:** Evaluating blockchain's capacity to improve data security and privacy while maintaining accessibility for healthcare providers;
- **O3:** Empowering patients with greater control over their health data;
- **O4:** Improving the efficiency and transparency of clinical trials and research;
- **O5:** Enhancing drug traceability and supply chain management;

- **O6:** Synergies between blockchain and other technologies.

By addressing these objectives, this research seeks to contribute to the ongoing dialogue about the transformative potential of blockchain in healthcare. It aims to provide insights that can guide future implementations, inform policy decisions, and ultimately contribute to improved patient care and more efficient healthcare systems.

To thoroughly investigate the challenges and opportunities identified in the Section 2.2, this study adopts a structured methodological approach. This approach starts by running a scientometric search based on the most relevant terms that will yield a group of articles to be studied. With this dataset of studies, some of them will be filtered to ensure that only the most relevant and up-to-date are analyzed. Finally, the resulting studies will be individually analyzed, and insights will be extracted to attempt to answer the research objectives defined.

3.2 Methodology

To address the research objectives, this study employs a two-stage methodological framework. This comprehensive approach is designed to provide a detailed analysis of the underlying theoretical concepts while rigorously examining the challenges and opportunities associated with blockchain implementations in healthcare.

In the first stage, a scientometric analysis is used to capture broad patterns and sentiments in blockchain and healthcare research. In the second stage, a systematic literature review is conducted to explore specific implementations, challenges, and opportunities in depth. The second stage of this methodology involved a systematic literature review specifically designed to address the core research objectives identified in Section 3.1. This phase also analyzes solutions and validates their effectiveness in addressing healthcare data management challenges.

3.2.1 Stage 1: Scientometric Search

The first stage involved conducting a scientometric search using the Scopus platform. The initial search criteria were "blockchain" AND ("health" OR "healthcare" OR "clinical" OR "medical").

To ensure that the findings are as current as possible, only documents published from 2020 onward were included. The initial search criteria returned 9022 documents (represented by Figure 3.1). As this search returned work accepted but still not published, those papers were filtered from the search.

A comprehensive investigation of the remaining 170 papers found that most papers are articles (around 92%), while approximately 4% are reviews. Another 3%

Status	Quantity
Published	170
Accepted for publishing	8852
Total	9022

Figure 3.1: Initial search result

relate to erratum, while the minority (about 1%) are Notes. Figure 3.2 displays the proportions of various types of documents.

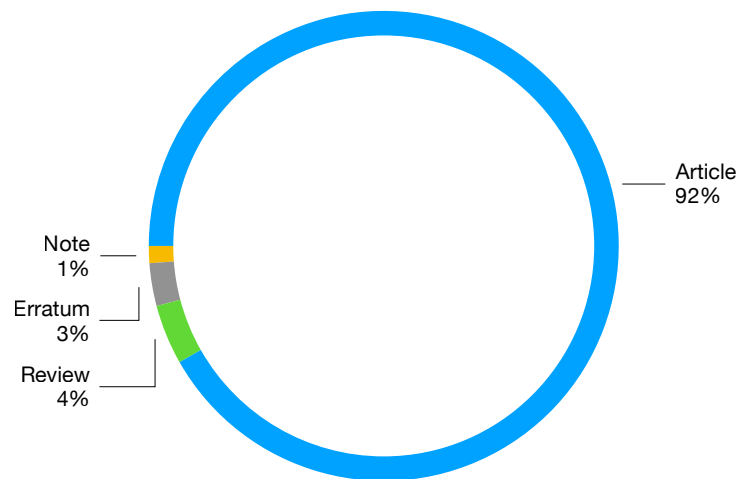


Figure 3.2: Distribution of document types

Figure 3.3 shows that there has been a significant growth in interest in this topic over the previous five years, as evidenced by the increase in the number of studies in the field. Most papers were published in 2024 (129 published papers corresponding to 76%). The remaining work is distributed in the following manner: 29 studies published in 2023 (about 17%), 6 published in 2022 (about 4%), while 4 studies were published in 2021 and only 2 were published in 2020 (about 2% a 1%, respectively).

Figure 3.4 compares the proportion of different outcomes across the years.

Year	Quantity
2020	2
2021	4
2022	6
2023	29
2024	129

Figure 3.3: Distribution of publishing year

3.2.2 Stage 2: Systematic Literature Review

The second phase of the study further filtered the retrieved papers with the objective of retaining only the most up-to-date and relevant results. To ensure the precision and relevance of these findings, specific selection criteria were implemented, focusing on publication timeframes and research titles. Additionally, a thorough manual screening process was incorporated to validate the selected literature's academic rigor and topical alignment.

Inclusion and Exclusion Criteria

The titles of the inclusion criteria included the terms "Blockchain", "health", "healthcare", "clinical", and "medical". We excluded publications published before 2021 that lacked citations to provide the most current and accurate results.

The selection process was based on the PRISMA guidelines ([Page et al., 2021]), as represented in figure 3.5.

3.2.3 Screening and Selection

The initial search resulted in 170 studies in total. The use of filters and conditions allowed for a more targeted pool. From the original 170 studies, 102 did not meet the research title criteria (the study title did not contain "health", "healthcare", clinical and "medical"). Furthermore, 43 studies were removed since those have not been cited in other studies. Lastly, the selected results were limited between 2022 and 2024 to ensure the most up-to-date research, removing 3 studies. No duplicates were ever retrieved.

The quantity of studies that needed to be analyzed was significantly reduced by these inclusion/exclusion filters, from 170 to 22 studies. Subsequently, 6 other studies were removed due to inaccessibility through available academic databases and institutional repositories, as can be viewed in Figure 3.5.

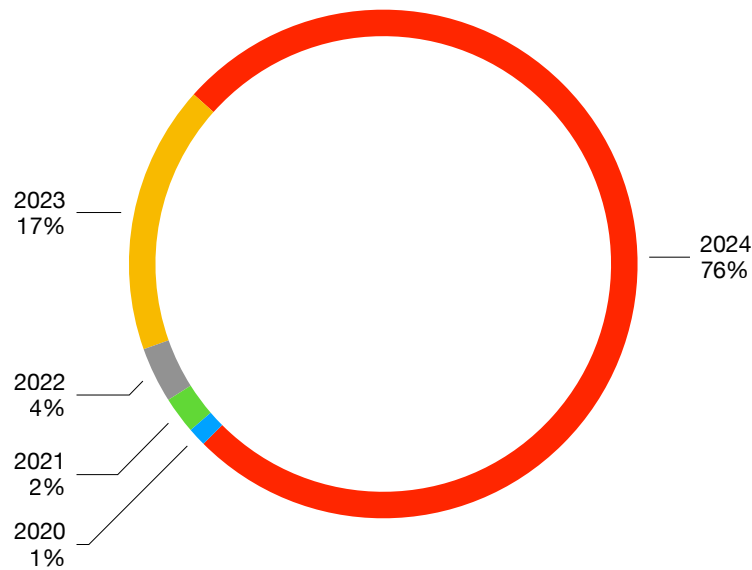


Figure 3.4: Distribution of publishing year

3.3 Research Objectives Definition

This section provides a detailed explanation of the research objectives established for this study.

3.3.1 O1: Improving data interoperability and reducing fragmentation in healthcare systems

In order to answer the first research objective, a targeted literature analysis was carried out in the 16 studies that resulted from the screening process. Among the studies, [Dbesan et al., 2023, Chaurasia, 2024] emerged as the most relevant and comprehensive in addressing the specific focus of this objective.

[Dbesan et al., 2023] adopted a comprehensive mixed-method approach. The authors designed semi-structured interviews and surveys targeted at healthcare professionals, IT experts, and policy makers that allowed them to explore the practical challenges and perceived benefits of blockchain technology. Data collected from interviews were systematically coded and analyzed using content analysis techniques to identify recurring themes, which were then statistically validated against the survey responses. This combination of qualitative insights and quantitative rigor allowed the researchers to both theorize and empirically test a blockchain-based knowledge-sharing model aimed at reducing data fragmentation.

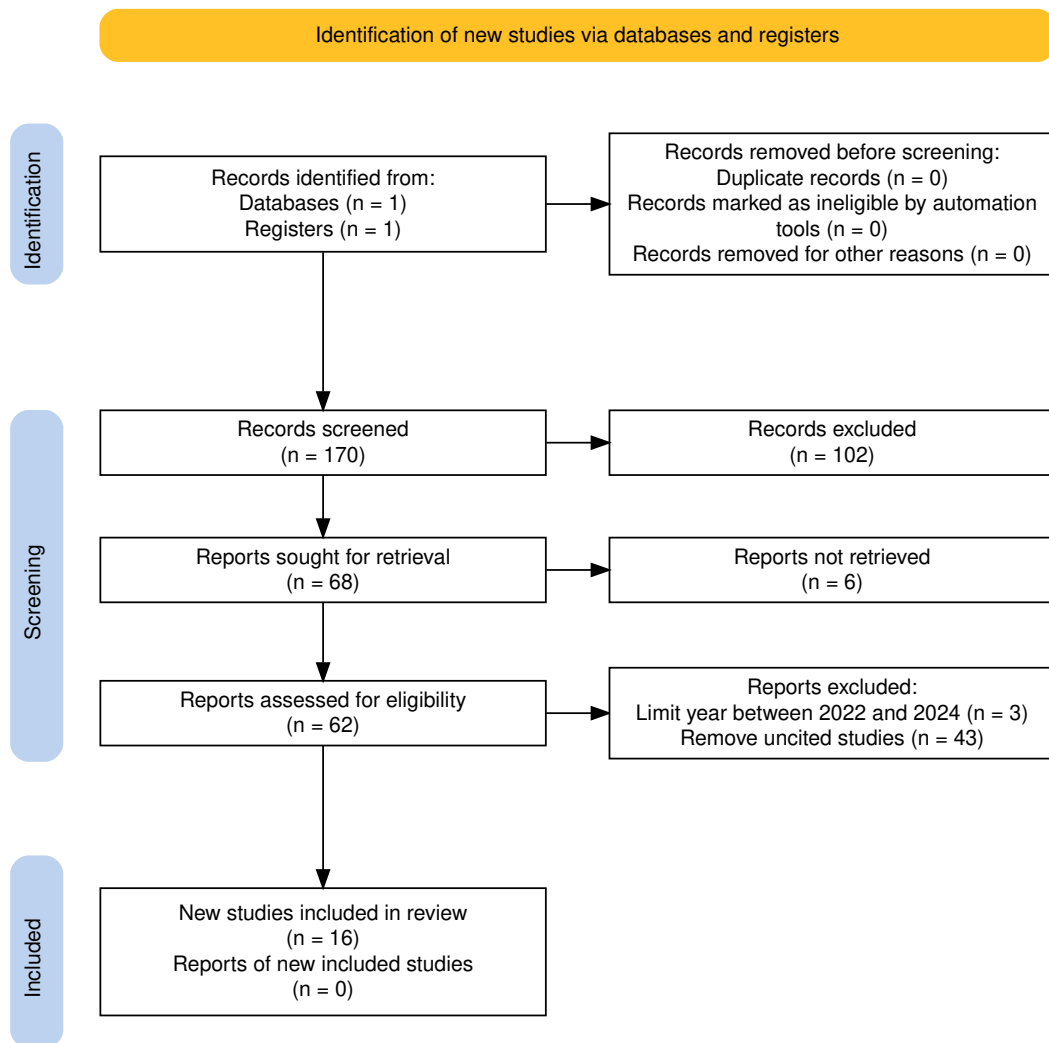


Figure 3.5: PRISMA chart

[Chaurasia, 2024] employed a design science framework to develop and test a prototype system called MediVault. Initially, the authors gathered system requirements by conducting stakeholder interviews and reviewing existing healthcare data management practices. This groundwork informed the design of a decentralized repository that leverages blockchain’s immutability and security features. The authors then built a proof-of-concept implementation using established blockchain protocols. The prototype was subjected to a series of controlled experiments that measured key performance indicators such as transaction throughput, latency, and scalability under simulated healthcare data loads. Additionally, comprehensive security assessments were conducted to evaluate the system’s resistance to cyber threats. This methodical development and evaluation process clearly demonstrated how a blockchain-enabled MediVault could unify disparate data sources and address fragmentation.

3.3.2 O2: Evaluating Blockchain's Capacity To Improve Data Security And Privacy While Maintaining Accessibility For Healthcare Providers

To address the second research objective, we selected six key studies [Chaurasia, 2024, Kumari et al., 2024, Jakhar et al., 2024, Awan et al., 2024, Saha et al., 2024] that focus on the interplay between data security, privacy, and accessibility in healthcare settings.

[Chaurasia, 2024] adopt a decentralized architecture integrating Ethereum smart contracts with Interplanetary File System storage and Firebase cloud infrastructure, ensuring both immutability and scalable access. By anchoring encrypted medical records to the blockchain via cryptographic hashes and leveraging asymmetric encryption for data confidentiality, the framework establishes a secure, patient-centric model. Performance validation and encryption speed metrics further underscores the practical feasibility of maintaining real-time accessibility without compromising security, illustrating blockchain's capacity to harmonize these priorities in operational settings.

[Kumari et al., 2024] extend this evaluation through a hybrid consensus mechanism combining PoW and [?]. The authors' embeds IoT-generated health data into the blockchain via gateway nodes, applying multi-layered security measures such as device authentication, end-to-end encryption, and continuous integrity verification. By simulating networks, the study quantifies latency and throughput trade-offs, providing empirical evidence that blockchain can sustain performance standards required for critical healthcare applications. This approach directly correlates consensus design choices with both security robustness and system responsiveness, emphasizing the technology's role in balancing adversarial resistance with provider usability.

[Jakhar et al., 2024] propose a blockchain-based framework for electronic health records management that prioritizes privacy preservation and granular access control. Their methodology leverages Hyperledger Fabric's private channels to implement role-based access, complemented by Attribute-Based Encryption for fine-grained data control. The integration of zero-knowledge proofs for identity verification and off-chain storage with blockchain-anchored hashes addresses both privacy concerns and scalability challenges.

[Awan et al., 2024] further push the boundaries of blockchain application in healthcare by introducing MediTwin, a Web 3.0-integrated digital twin concept for patient-centric care in the metaverse. Their methodology combines blockchain's immutable ledger with virtual reality interfaces, creating a secure yet highly accessible platform for remote patient monitoring and tele-medicine.

[Saha et al., 2024] address the intersection of blockchain, 6G networks, and IoT in healthcare cyber-physical systems. Their smart contract-based access control

scheme leverages the high-bandwidth, low-latency capabilities of 6G to enhance real-time data processing while maintaining strict security protocols.

3.3.3 O3: Empowering patients with greater control over their health data

Regarding the topic of patient empowerment, two of the resulting studies approach this topic [Dbesan et al., 2023, Dhingra et al., 2024].

[Dbesan et al., 2023] employed a multi-methods approach, combining a survey-based quantitative analysis with structural equation modeling to investigate the behavioral intention of doctors in the adoption of blockchain-driven knowledge-sharing systems in government hospitals. The data collection involved survey to 322 participants and analysis for preliminary data exploration. This methodology allowed for the validation of trust, knowledge sharing, and behavioral intention, providing a robust framework for evaluating blockchain adoption in healthcare.

[Dhingra et al., 2024] utilized a conceptual model grounded in the Technology-Organization-Environment framework and Organizational Information Processing Theory. Data was collected through a structured survey targeting experts in the Indian healthcare sector familiar with blockchain technology. The analysis was conducted using AMOS 19 to perform structural equation modeling, enabling the authors to test hypotheses related to factors influencing blockchain adoption and its mediating role in improving healthcare supply chain performance.

In summary, [Dbesan et al., 2023] demonstrates the application of structural equation modeling to explore behavioral factors influencing blockchain adoption, while [Dhingra et al., 2024] highlights the use of theoretical frameworks to evaluate blockchain's impact on organizational performance within healthcare supply chains.

3.3.4 O4: Improving the Efficiency and Transparency of Clinical Trials and Research

From the resulting studies, only one addresses blockchain applications in healthcare procurement systems [Dhingra et al., 2024]. This study researched the impact of transparency and efficiency relevant to medical research infrastructure.

The authors conducted an in-depth qualitative study focusing on the potential of blockchain technology in enhancing drug traceability and supply chain management within the healthcare sector. The methodology involved interviews with a diverse group of stakeholders, complemented by manual in-person validation to enrich the data collection process. The study also explored the various domains of impact affected by the implementation of blockchain technology in healthcare industry.

3.3.5 O5: Enhancing Drug Traceability and Supply Chain Management

For the purpose of answering the fifth research objective, the focus turned to two articles resulting from the screening process [Bak et al., 2025, Dhingra et al., 2023, Dhingra et al., 2024]. These articles discuss how blockchain technology can be used in supply chain management. On one hand, [Bak et al., 2025] proposes a framework for blockchain-enabled drug traceability while [Dhingra et al., 2024] explores the obstacles and potential for adopting blockchain in supply chain management.

Both papers were critically studied to extract thematic aspects about blockchain's promise for maintaining data transparency, decreasing counterfeiting threats, and optimizing the supply chain process. [Bak et al., 2025] conducted a case study that involved in-depth interviews with various stakeholders, such as medical consultants, doctors and nurses with diverse responsibilities; and data collection through observation in meetings, interviews, and taking notes during focus group discussions.

[Dhingra et al., 2023] employs a hybrid Multi-Criteria Decision Making (MCDM) approach, integrating the Best-Worst Method (BWM) and the Decision-Making Trial and Evaluation Laboratory (DEMATEL), to systematically address challenges and opportunities in blockchain adoption. Although the study targets waste management, the methodology and findings are adaptable to enhancing drug traceability and supply chain management in the pharmaceutical sector.

Regarding [Dhingra et al., 2024], the authors explored the transformative potential of blockchain technology in improving drug traceability and supply chain management using a conceptual model grounded in the Organizational Information Processing Theory and the Technology-Organization-Environment framework. The researchers employed structural equation modeling to analyze data collected from 304 Indian healthcare professionals via a survey.

3.3.6 O6: Synergies Between Blockchain and Other Technologies

In order to answer the sixth research objective, a targeted analysis was carried out on the eight studies that emerged from the screening process [Dbesan et al., 2023, Awan et al., 2024, Saha et al., 2024, Chaurasia, 2024, Bhatia, 2024, Nath et al., 2023, Vishwakarma et al., 2023, Ogbuke et al., 2023]. These studies were selected as they directly study the integration of blockchain with complementary technologies.

The integration of blockchain with AI has garnered attention due to its potential to enhance data integrity and knowledge-sharing efficacy. [Dbesan et al., 2023] utilized partial least squares structural equation modeling to validate a theoretical framework that links blockchain's data integrity to AI-driven knowledge-sharing,

surveying 322 clinicians across healthcare institutions in India. This approach demonstrates how blockchain can improve the trustworthiness of data, enhancing AI's effectiveness in clinical environments.

[Awan et al., 2024] advanced this integration by adopting a Web 3.0-integrated digital twin architecture that leverages AI, smart contracts and cryptography to address challenges related to data synchronization and security.

[Vishwakarma et al., 2023] studied the integration of blockchain technology with IoT devices. In this regard, the authors captured data by using IoT devices, and relay these records between multiple networks depending on data classification. This framework connects a blockchain system to cloud servers and ensures secure connection and efficient data processing.

[Chaurasia, 2024] studied the integration of blockchain technology with NFT generation and secure access through the use of vaults. The authors were also able to analyze the integration with storage systems, either decentralized file systems such as IPFS (Inter Planetary File System) and centralized systems such as Google Firebase. Similarly, [Bhatia, 2024] investigated the integration of IoT, AI, and cloud technologies. Sensory information was collected using wearable devices and processed/fused using ML. These records were then sent to online databases hosted in the cloud.

[Nath et al., 2023] addressed this challenge by employing IBM Hyperledger to create a health data-sharing framework that integrates with edge computing devices, on an IoT layer, that perform local data processing instead of relying on the chain itself. This platform also employs symmetric encryption to protect sensory information.

[Saha et al., 2024] studied the integration of blockchain with 6G, IoT and big data analytics, using smart contracts as an access control system. In this regard, the IoT layer was used mainly for real-time patient data collection, while the 6G layer was used for low-latency communication. Finally, big data analytics enabled AI/ML techniques to gather predictive insights.

[Ogbuke et al., 2023] contextualize these technical evaluations within pandemic-driven healthcare demands, analyzing blockchain's interplay with broader data-driven technologies during COVID-19. The authors conducted a study to investigate the role of data-driven technologies (big data, AI, IoT and 3D printing) in global healthcare practices. The methodology employed by the authors highlights the technology's ability to ensure data integrity and facilitate secure information sharing in healthcare systems during the COVID-19 pandemic.

Chapter 4

Results

This chapter presents the findings from the systematic investigation conducted. This analysis reveals key patterns, trends, and insights found in the articles. The results are organized thematically to provide a clear understanding of how blockchain technology is currently being utilized and conceptualized within healthcare frameworks.

Three distinct categories of research approaches in blockchain healthcare studies were identified and represented in picture 4.1:

1. **Application-focused:** 11 articles (50%)
2. **Systematic Reviews:** 7 articles (32%)
3. **Combination of Reviews and Application:** 4 articles (18%)

The literature was found to be dominated by application-focused studies, which represented about 50% (11 articles) of the reviewed publications. These studies were primarily concentrated on specific technological implementations and solutions. Systematic reviews were identified in 31,8% (7 articles) of the literature, where patterns similar to those observed in blockchain education studies were noted. These review papers typically examined advantages, challenges, and implementation prospects within healthcare contexts. The remaining 18,2% (4 articles) were constituted by hybrid studies, combining theoretical review and practical applications. This distribution pattern can be aligned with observations in related fields, where comprehensive understanding through reviews is shown to support and guide practical

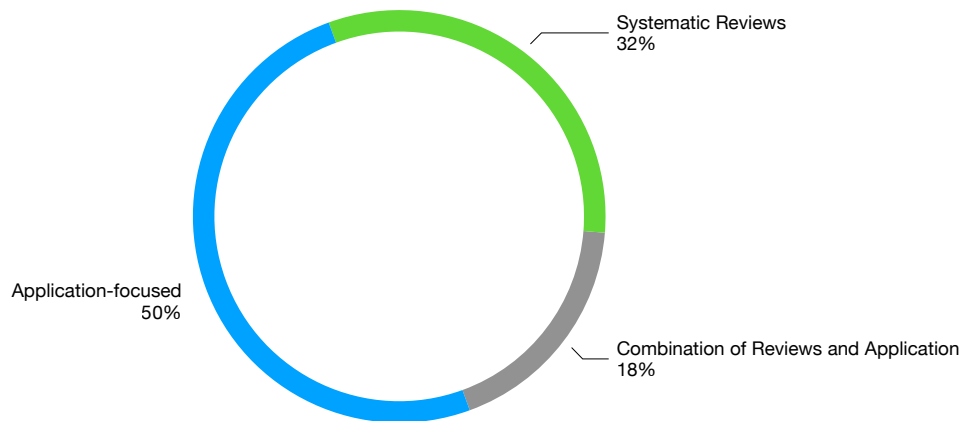


Figure 4.1: Research Categories Distribution

implementations while a strong focus on practical applications and solutions is maintained.

4.1 Research Areas

Based on this research, the themes *Security and Privacy Solutions*, *IoT and Infrastructure Integration*, *Supply Chain and Resource Management*, *Implementation Studies and Adoption Analysis* and *Data Management and Healthcare Systems* were identified. *Security and Privacy Solutions*, *IoT and Infrastructure Integration*, and *Supply Chain and Resource Management* both appear 23% of the total articles analyzed in the study, while *Implementation Studies and Adoption Analysis* appeared in 18% of the results. Finally, *Data Management and Healthcare Systems* accounted for the remaining 13%. This distribution highlights the diverse applications of blockchain technology in the healthcare sector, underscoring its multifaceted potential.

The balanced focus across *Security and Privacy Solutions*, *IoT and Infrastructure Integration*, and *Supply Chain and Resource Management* (each comprising 23% of the total studies) indicates that researchers are addressing current challenges and future technological advancements in healthcare. This uniform distribution between the researched applications reflects a mature and comprehensive approach to leveraging blockchain for enhancing security protocols, integrating next-generation technologies, and optimizing healthcare logistics. The notable proportion of studies dedicated to *Implementation Studies and Adoption Analysis* (18%) suggests that the field is at a pivotal stage where the theoretical benefits of blockchain are being rigorously tested against real-world challenges.

Finally, the focus on *Data Management and Healthcare Systems* (13%) highlights the strategic use of blockchain for improving data integrity and system efficiency in healthcare.

4.2 Answering Research Objectives

This section presents the comprehensive conclusions derived from addressing the research questions initially outlined in Section 3.3. The following subsections will methodically unpack the findings from the analyzed studies, demonstrating evidence to answer each research question.

4.2.1 O1: Improving data interoperability and reducing fragmentation in healthcare systems

Blockchain technology addresses healthcare data interoperability challenges by establishing decentralized, standardized frameworks for secure data exchange across disparate systems.

By replacing centralized structures with distributed ledgers, blockchain ensures secure multi-party data sharing without single-point vulnerabilities [Dbesan et al., 2023]. Integration of multi-party data depends on reliable security mechanisms. The adoption of fine-grained access controls through cryptographic signatures enables complex data management demands with high transaction throughput and robust security against cyber threats [Chaurasia, 2024].

To further increase interoperability in the healthcare industry, and to smooth the curve of technological adoption, multiple networks can be implemented. This allows the connection between multiple systems, either through the use of test settings, or to use as a transition window. By having systems running in parallel and having interfaces that allow effective and efficient communication between these systems, interoperability is enhanced. However, in addition to being a technical change, the move from conventional, centralized systems to decentralized architectures also represents an organizational challenge. Many of the stakeholders involved in this transition are deeply rooted in legacy systems and practices, requiring extensive coordination [Dbesan et al., 2023]. This also affects behavioral and social domains, as healthcare professionals require training, time, resources and incentives to adopt new platforms.

Finally, blockchain enables uniform data structures through smart contracts that automate compliance, allowing systems to interpret shared clinical data consistently. This eliminates the need for custom interfaces between institutions while maintaining semantic consistency in lab results, imaging reports, and treatment histories; [Dbesan et al., 2023, Chaurasia, 2024].

4.2.2 O2: Evaluating blockchain's capacity to improve data security and privacy while maintaining accessibility for healthcare providers

The use of a decentralized architecture combined with immutable data greatly contributes to the security of the data present in blockchain systems. Furthermore, the use of encryption and identity management systems allows for secure sharing of records while privacy and security are ensured by encryption mechanisms.

The work of [Chaurasia, 2024] validated the use of advanced cryptographic techniques that maintain data confidentiality without compromising system performance, directly addressing challenges of data privacy and secure access. [Kumari et al., 2024] found that their Hybrid Consensus Mechanism (HCM) that integrates multiple consensus models, such as PoA, PoS and PoW, is able to achieve higher throughput than traditional models. The system also lowers processing time by efficiently handling block creation and validation. The use of Merkle trees for transaction tracking further streamlines operations, ensuring faster access to patient records without compromising security.

[Jakhar et al., 2024] validated the use of advanced cryptographic techniques that maintain data confidentiality without compromising system performance, directly addressing challenges of data privacy and secure access. According to the author, even doctors are only able to visualize information that patients specifically consented to share.

[Awan et al., 2024]' system employs blockchain's immutable ledger to prevent unauthorized tampering and ensure data integrity, while Web 3.0 features enable secure, decentralized access controls that align with privacy regulations. This approach addresses vulnerabilities by encrypting health records and restricting access to authorized entities through distributed consensus mechanisms. The authors report better performance than other methods in metrics such as latency, throughput and response time, resource utilization and scalability.

[Saha et al., 2024] demonstrated that the proposed system called SACS provides enhanced security and augmented functional capabilities. They also highlighted that SACS reduced communication costs compared to other relevant schemes.

These findings collectively demonstrate blockchain's capacity to significantly enhance healthcare data management, providing robust security measures while maintaining the accessibility necessary for effective healthcare delivery.

4.2.3 O3: Empowering patients with greater control over their health data

As stated previously, the use of identity management systems allows for secure sharing of records while ensuring privacy and security. Extending these systems allow for granular permission controls that enable patients to only share health records with the entities they want. This enables granular consent management, enforced by the usage of smart contracts or context-aware consent triggers for emergency situations. This system also enables transparent data governance, as patients can track who accessed their records and for what purpose.

In [Dbesan et al., 2023], the authors were able to emphasize that blockchain-based systems can grant patients more autonomy over personal health information by enabling real-time access and consent-based data sharing. The enhanced control fosters trust in healthcare providers and enhances patient engagement. The authors indicate that when patients use a blockchain-based platform to manage their health records, they report a stronger sense of ownership and control over their personal information. The study highlights measurable increases in patient trust and satisfaction, largely attributed to transparent data transactions and consent-driven sharing. The authors also note that this enhanced control can bolster patient engagement in health decision-making, as patients can directly grant or revoke access to their records, thus actively participating in the data life cycle.

On the other hand, in [Dhingra et al., 2024], while the main analysis centers on benchmarking blockchain's operational efficiency in healthcare, the authors do report secondary outcomes relevant to patient empowerment. Specifically, they observe that when healthcare providers adopt standardized blockchain protocols, patients benefit from more efficient data retrieval and sharing processes, resulting in quicker access to their own health information. The results suggest that even in a performance-focused context, patients gain indirect but tangible benefits such as fewer administrative barriers and clearer pathways to control who can view or modify their data. These findings imply that performance gains and patient empowerment are not mutually exclusive but can be complementary outcomes of blockchain adoption in healthcare.

4.2.4 O4: Improving the efficiency and transparency of clinical trials and research

Blockchain technology can significantly enhance the efficiency and transparency of clinical trials and research by creating an immutable, auditable record of all research activities. By providing a decentralized and tamper-proof ledger, blockchain ensures the integrity of clinical trial data, preventing selective reporting and reducing the risk of data manipulation. The technology's cryptographic security allows for

secure, privacy-preserving data exchange, facilitating easier collaboration and reproducibility. Additionally, blockchain can streamline participant recruitment, consent management, and provide a comprehensive, chronological record of all research activities.

Furthermore, [Dhingra et al., 2024] noted increased efficiency provided by the use of smart contracts. With smart contracts, processes, such as payments between patients and healthcare providers, can be streamlined and automated, reducing margin for manual errors at the same time. Cryptographic practices also help keep information secure and making sure only authorized authors can access and update health records.

As a result, trust is strengthened among researchers, regulatory bodies, and participants, with every trial step being transparently tracked and verifiable.

4.2.5 O5: Enhancing drug traceability and supply chain management

The fundamental concepts of blockchain technology also help to enhance drug traceability and supply chain management. The use of an immutable ledger, a decentralized architecture, and smart contracts to ensure permission over existing data ensures a transparent, secure, and efficient flow of information.

[Dhingra et al., 2024] concludes that when blockchain is adopted, it enhances transparency, data immutability, and real-time record keeping. In their study, healthcare supply chain factors emerged as the most influential in driving blockchain technology adoption, highlighting its potential to streamline drug traceability alongside broader supply chain management improvements.

[Bak et al., 2025] contributes to these findings by confirming that blockchain's decentralized and secure data sharing capabilities can establish a robust framework for tracking drugs and managing supply chain operations. The authors also stated that in order for a successful blockchain implementation in supply chain management, blockchain's behavior must be aligned with the behavior of the systems currently in use. This includes the implementation of processes that address grey areas or corner cases, and can include the integration with non-integrated tools.

4.2.6 O6: Synergies between blockchain and other technologies

Regarding the synergies between blockchain and other technologies in healthcare, studies reveal that blockchain's immutable ledger systems enhance AI-driven analytics by providing auditable data provenance for predictive diagnostics, as seen in [Awan et al., 2024] and in [Saha et al., 2024].

The integration of blockchain with complementary technologies such as AI, IoT, and big data further improve interoperability, data security and decision-making

[Nath et al., 2023, Chaurasia, 2024, Vishwakarma et al., 2023, Bhatia, 2024, Ogbuke et al., 2023, Dbesan et al., 2023].

By combining IoT devices with blockchain technology, more secure layers are added to the architecture, allowing systems to reach a higher degree of data privacy, security, quality, scalability, and accuracy [Nath et al., 2023, Chaurasia, 2024, Vishwakarma et al., 2023].

The work of [Chaurasia, 2024] demonstrated that the integration of blockchain technology with IPFS and Firebase was able to increase performance by presenting reduced latency and delays when interacting with records, while maintaining a higher level of data evaluation, privacy and, consequently, trust.

Pioneering architectures like those in [Bhatia, 2024] combine multiple networks, including IoT edge networks with blockchain to reduce IoT latency congestion and cost. The work of [Ogbuke et al., 2023] also presented that IoT can help telemedicine by using networking sensors that facilitate tele-screening. This is specially critical for patients who are elderly or with chronic conditions as it should reduce the required number of visits to hospital and clinics. In this regard, big data also allows the increase of applicability of drug prescriptions across the healthcare industry.

4.3 Limitations Of Blockchain In Healthcare

Analysis of the research papers reveals several significant challenges and limitations in blockchain healthcare implementation that span technical, organizational, and regulatory domains. These challenges that can potentially impact widespread adoption are categorized and examined as follows, and summarized in Table 4.1:

- **Technical Challenges:** Studies highlight significant concerns regarding scalability and performance issues when handling large volumes of healthcare data. The computational requirements for consensus mechanisms and data processing can lead to slower transaction speeds and increased energy consumption. Integration with legacy healthcare systems presents additional technical hurdles.
- **Security and Privacy Concerns:** Despite blockchain's security features, researchers identify vulnerabilities in smart contracts and potential risks in private key management. Healthcare organizations face challenges in ensuring HIPAA compliance while maintaining blockchain's transparency. The immutable nature of blockchain poses challenges for implementing the right to be forgotten.
- **Implementation Costs:** The financial burden of blockchain adoption includes substantial initial infrastructure investments, ongoing maintenance costs, and staff training expenses. Healthcare organizations, particularly in

developing regions, face difficulties justifying these costs against immediate operational needs.

- **Regulatory Compliance:** Organizations struggle with varying international healthcare data protection regulations and standards. The lack of standardized blockchain protocols in healthcare creates interoperability issues between different blockchain implementations.
- **Organizational Resistance:** Studies indicate significant resistance from healthcare professionals and administrators due to blockchain's complexity. The requirement for fundamental changes in existing workflows and procedures creates adoption barriers. Limited technical expertise among healthcare staff further complicates implementation.

Table 4.1: Summary of Challenges of Blockchain Technology in Healthcare.

Context	Challenge
Technical Implementation	Scalability issues, high computational requirements, integration complexity with legacy systems
Security and Privacy	Smart contract vulnerabilities, private key management risks, HIPAA compliance challenges
Resource Requirements	High infrastructure costs, ongoing maintenance expenses, training requirements
Regulatory Compliance	Data protection regulations, lack of standardization, interoperability issues
Organizational Barriers	Professional resistance, workflow disruption, limited technical expertise

Chapter 5

Discussion

This chapter discusses the research findings derived from a comprehensive analysis of blockchain applications in healthcare. Furthermore, the conclusions gathered from the defined research objectives are discussed and the main current adversities for transversal blockchain implementation are highlighted.

5.1 Research Objectives Analysis

This section critically discusses the research objectives stated for this work. They evaluate the potential contributions of blockchain technologies to healthcare applications. For that reason, we evaluated prior applications and assessed their usefulness in dealing with known healthcare challenges.

5.1.1 Improving data interoperability and reducing fragmentation in healthcare systems (O1)

Blockchain properties, such as decentralization, eliminate single-point dependencies that often lead to data silos in traditional healthcare systems. By distributing data across multiple nodes that should spread through multiple geographies, the technology enables uniform access protocols, ensuring that all stakeholders, from hospitals to individual clinics, operate on a shared and consistent data structure. This fundamental shift allows healthcare providers to overcome the fragmentation that typically obstructs timely diagnosis and coordinated care.

Unlike traditional systems where disparate electronic health record platforms use varying formats and protocols, blockchain establishes standardized rules for data access and updates. For example, smart contracts can automate compliance with data-sharing agreements, ensuring that clinical data like lab results or treatment histories is interpreted consistently across systems. This reduces the need for custom interfaces, streamlining workflows, and enabling timely diagnosis and coordinated care. The immutability of blockchain records also adds a layer of trust and reliability, ensuring that all stakeholders work with tamper-proof, up-to-date information.

Blockchain's potential is amplified by integration with technologies like smart contracts and cryptographic practices. Smart contracts automate data-sharing rules, ensuring compliance while reducing administrative overhead. Cryptography further secures data, allowing granular access controls where only specific portions of a record are shared with designated parties. This allows only specific portions of a record to be shared with designated parties. These integrations not only bolster interoperability but also address privacy concerns inherent in traditional systems, creating a more patient-centric ecosystem.

Previous work has shown that blockchain implementation in healthcare care is primarily constrained by organizational transitions rather than technical restrictions. Current blockchain architectures, technologies, and protocols can cover the requirements needed to successfully use blockchain as the cornerstone of healthcare. Moreover, traditional systems rely on centralized authorities, such as hospital IT departments or third-party vendors, making them vulnerable to single points of failure. Blockchain's distributed nature eliminates this risk, enhancing resilience and security.

To address this, efforts should focus on gradual integration rather than wholesale replacement. A hybrid approach, where blockchain is initially deployed for specific use cases while legacy systems continue handling other functions, could maintain operability during the transition. Developing interoperability layers that bridge legacy databases with blockchain networks is also a solution worth exploring, allowing institutions to adopt blockchain incrementally without disrupting critical services.

In the absence of blockchain, traditional healthcare systems suffer from persistent data silos and limited interoperability, creating inefficiencies and risks for patient care. A patient's medical history might be fragmented across multiple providers, each inaccessible to the others without manual requests or incompatible data formats. This fragmentation can lead to delayed diagnoses, redundant testing, or medical errors.

5.1.2 Improving data security and privacy and control over health (O2, O3)

Smart contracts expand blockchain's functionalities and properties. They serve as technological enforcers of predetermined security policies, ensuring that only properly authenticated and authorized healthcare providers can access or modify patient records. These mechanisms enable granular access control through role-based permissions that can be tailored to specific provider roles, departments, and individual patient preferences.

The transformative potential of smart contracts extends beyond mere technical implementation. They represent a paradigm shift in establishing a new, higher level of trust in the patient-provider relationship. By embedding consent, privacy policies, and access controls directly into immutable code, smart contracts create transparent systems that significantly reduce information asymmetry between patients and providers. This technological foundation enables patients to maintain greater sovereignty over their health information while simultaneously allowing providers appropriate access to deliver quality care.

The impact of the change in this trust relationship requires thorough examination. Its implications touch on various dimensions of healthcare delivery, including clinical workflow efficiency, regulatory compliance, patient engagement, data sharing for research purposes, and the economic aspects of healthcare information exchange. Understanding these implications is crucial for healthcare institutions contemplating blockchain implementation and for policymakers developing governance frameworks for digital health information systems.

Previous work also showed a natural connection between the use of smart contracts and cryptographic techniques. In this regard, smart contracts are extended by the use of cryptography, enabling the platform to reach new standards in security practices. Although these technologies act as layers on top of blockchain technology, previous work concluded that these protection layers do not affect performance in an impactful way.

In the absence of these mechanisms, the healthcare industry faces significant challenges in establishing clear control over the ownership of medical records. This lack of clarity affects both healthcare providers and patients in a variety of ways. On one hand, it leads to inefficiencies, such as the unnecessary repetition of exams and consultations, which not only waste valuable resources but also increase the burden on patients. On the other hand, the more serious consequences of poor data management can result in critical gaps in medical history, where missing or incomplete health records prevent healthcare professionals from making informed decisions. This can compromise patient care, lead to misdiagnoses, and hinder timely interventions.

5.1.3 Improving efficiency and transparency, enhancing traceability and supply chain management (O4, O5)

Blockchain offers a unified solution to enhance operational efficiency and transparency across diverse healthcare applications. Its decentralized ledger, immutable record-keeping, and smart contract capabilities provide a robust framework applicable to both clinical research and pharmaceutical supply chains. Although the underlying technology remains consistent, each domain faces distinct challenges and opportunities.

In clinical trials, blockchain's real-time, tamper-proof ledger ensures that every phase, from patient recruitment to outcome reporting, is securely documented. This comprehensive audit trail minimizes risks associated with data manipulation or selective reporting, strengthening regulatory compliance and research integrity.

Similarly, in supply chain management, blockchain introduces end-to-end traceability of pharmaceutical products. Each transaction, from manufacturing through distribution to final delivery, is immutably recorded, creating a transparent audit trail crucial for combating counterfeit medications and ensuring regulatory compliance.

Beyond secure record-keeping, smart contracts further streamline processes in both domains. In clinical trials, they automate tasks such as participant consent, data submissions, and milestone-triggered payments. In supply chain logistics, they facilitate order validation and shipment tracking, reducing human error and delays.

Research has already demonstrated the efficiency gains achieved through the adoption of smart contracts alongside cryptographic practices. However, while these advancements are promising, integrating blockchain into existing clinical trial management systems presents challenges, including operational inertia and the need for interoperability with traditional platforms. Rather than merely implementing blockchain as a core technology, it is essential to ensure that system behavior aligns seamlessly with existing workflows. This includes addressing corner cases and ambiguous scenarios to maintain reliability and compliance.

Compared to conventional implementations reliant on centralized systems and paper-based documentation, blockchain offers a transformative shift toward efficiency and reliability. In clinical trials, a decentralized ledger enhances transparency and accelerates data verification, directly addressing inefficiencies and risks of manipulation inherent in traditional systems. In supply chain management, a single, immutable record reduces costs, improves traceability, and mitigates fraud risks that plague conventional methods.

5.1.4 Synergies between blockchain and other technologies (O6)

Blockchain's potential is significantly enhanced when integrated with complementary technologies such as AI, IoT, and big data analytics. Together, these technologies form synergistic ecosystems that strengthen healthcare data integrity, drive predictive insights, and enable real-time decision-making.

The integration of blockchain with AI facilitates the development of robust predictive models. Blockchain's immutable ledger ensures that the data feeding into AI systems is both reliable and traceable, mitigating risks associated with data tampering. This combination enhances the accuracy of predictive diagnostics and supports the creation of personalized treatment protocols. Similarly, the convergence of blockchain and IoT allows for secure, real-time data capture from connected medical devices. By ensuring that transmitted data is encrypted and verifiable, blockchain enhances continuous patient monitoring and enables rapid response in critical care settings.

Big data analytics further strengthens this ecosystem by processing vast amounts of healthcare data stored on blockchain networks. Advanced analytical tools can extract meaningful patterns and correlations from these secure datasets, informing clinical decision-making and driving operational improvements.

Beyond these individual benefits, previous research has demonstrated that such integrations act as additional layers on top of an already highly secure foundation, further improving both security and performance. The synergy between blockchain and emerging technologies such as IoT, AI, and big data results in increased processing efficiency, reduced latency, and minimized delays, all while preserving essential features like data privacy, security, and system resilience. By combining blockchain's decentralized architecture with real-time data processing and intelligent automation, this convergence enables more scalable, reliable, and impactful healthcare solutions.

5.2 Blockchain's Main Adversities

Despite the positive points mentioned in the previous sections, several significant challenges must be addressed for successful implementation.

System Complexity

The inherent complexity of blockchain infrastructures presents substantial implementation hurdles. Healthcare organizations must navigate difficult technical architectures that combine distributed ledger technology with existing health information systems, often requiring a complete redesign of established workflows. This complexity extends beyond the technical domain into operational, regulatory, and governance frameworks that must adapt to accommodate decentralized data

management. Healthcare stakeholders frequently lack the specialized knowledge required to evaluate blockchain solutions, leading to resistance among practitioners and administrators who must alter familiar processes. Furthermore, the integration complexity across disparate systems and institutions creates interoperability challenges that can undermine the very connectivity blockchain promises to enhance.

Maintenance Costs and Expertise

The long-term viability of blockchain implementations depends heavily on sustainable maintenance approaches. Healthcare organizations face significant financial burdens associated with ongoing system maintenance, including computational resources, network infrastructure, and regular security updates. These costs are compounded by the scarcity of qualified blockchain specialists with healthcare domain knowledge, creating a competitive talent market with premium compensation requirements. The rapidly evolving nature of blockchain technology necessitates continuous education and system upgrades, introducing additional operational expenses. Many healthcare institutions, particularly smaller practices and rural facilities with limited resources, find these combined financial and expertise requirements prohibitively challenging, potentially widening the technological divide in healthcare delivery.

Chapter 6

Conclusion

This dissertation has systematically investigated the role of blockchain technology in transforming healthcare data management, with a focus on enhancing security, ethics, and efficiency. Through an in-depth systematic analysis of existing literature, empirical findings, and critical discussions, this study provides a comprehensive assessment of blockchain's potential to address longstanding challenges in the healthcare sector. This concluding chapter summarizes the main findings from each chapter, reflects on their significance, and outlines directions for future research and implementation.

The research highlights blockchain's capacity to tackle critical healthcare challenges through its decentralized architecture, immutability, and smart contract capabilities. Specifically, it discusses solutions to data fragmentation by enabling secure, unified data records across disparate systems, reducing the silos that slow healthcare data management. It also addresses interoperability issues through structured architectures that facilitate data sharing between healthcare providers, improving coordination and care delivery. Additionally, privacy concerns are mitigated via cryptographic techniques that ensure data confidentiality, safeguarding sensitive patient information. Beyond these technical benefits, blockchain empowers patients by giving them greater control over their health records, for instance, through transparent consent management. It also streamlines processes such as clinical trials, by automating participant verification to enhance efficiency and trust, and drug traceability, by tracking pharmaceutical supply chains in real time to combat counterfeiting and ensure safety.

Despite its promise, the research identifies significant technological and practical limitations that hinder blockchain's immediate applicability. Scalability constraints are a major concern, as platforms struggle with transaction speeds and data storage capacities, with growing ledger sizes overwhelming smaller systems. High costs also pose a barrier, including implementation expenses for hardware and software upgrades and ongoing maintenance costs, particularly for energy-intensive consensus mechanisms like PoW. Furthermore, regulatory complexities complicate adoption, as compliance with laws, such as GDPR, remains challenging due to unclear legal frameworks for decentralized data governance.

The study also explores how blockchain integrates with emerging technologies, such as AI, IoT, and big data analytics to amplify its impact in healthcare. AI enhances predictive analytics by leveraging blockchain's secure datasets, such as forecasting disease outbreaks with greater accuracy. IoT supplies real-time data from devices like wearable health monitors, which blockchain securely stores and manages to ensure integrity. Big data analytics benefits from blockchain's trustworthy foundation for analyzing vast, decentralized healthcare datasets. This integration positions blockchain as a cornerstone of a more interconnected and responsive healthcare ecosystem.

However, widespread adoption of blockchain in healthcare faces substantial technical and organizational hurdles. Technical challenges include integrating blockchain with legacy systems, such as outdated electronic health record platforms, and addressing compatibility issues across diverse infrastructures. Organizational barriers involve training staff to use blockchain-based systems effectively and shifting organizational culture to embrace decentralized workflows. Successful implementation requires not only technological innovation but also strategic collaboration among healthcare providers, regulators, and technology developers.

6.1 Future work

While this study has explored the technical capabilities of blockchain and their respective applications in the healthcare industry, there remains a significant gap in understanding how patients perceive, engage with, and trust these systems. User adoption and confidence in blockchain-based solutions are critical factors for their widespread implementation, yet research on the social and psychological aspects of patient interaction with such technologies is still underdeveloped. In this regard, future work should analyze the mechanisms of trust formation between the different stakeholders in the healthcare industry and patients. This will allow for more accurate systems development to tailor the experience for the different users.

Additionally, the lack of standards between blockchain and other architecture also emerged as a limitation in current implementations. This interoperability challenge hinders seamless data exchange and integration across healthcare institutions. Future research should focus on analyzing universal data exchange standards for healthcare applications, enabling more efficient, secure, and scalable implementations.

References

- [Abbate et al., 2023] Abbate, S., Centobelli, P., Cerchione, R., Oropallo, E., and Riccio, E. (2023). Blockchain technology for embracing healthcare 4.0. *IEEE Transactions on Engineering Management*, 70(8):2998–3009. [Cited on pages 2 and 10]
- [Ahram et al., 2017] Ahram, T., Sargolzaei, A., Sargolzaei, S., Daniels, J., and Amaba, B. (2017). Blockchain technology innovations. In *2017 IEEE Technology Engineering Management Conference (TEMSCON)*, pages 137–141. [Cited on page 5]
- [Alzoubi and Mishra, 2024] Alzoubi, Y. I. and Mishra, A. (2024). Blockchain consensus mechanisms comparison in fog computing: A systematic review. *ICT Express*, 10(2):342–373. [Cited on page 7]
- [Angelis and Da Silva, 2019] Angelis, J. and Da Silva, E. R. (2019). Blockchain adoption: A value driver perspective. *Business Horizons*, 62(3):307–314. [Cited on pages 5 and 16]
- [Angraal et al., 2017] Angraal, S., Krumholz, H. M., and Schulz, W. L. (2017). Blockchain technology: Applications in health care. *Circulation: Cardiovascular Quality and Outcomes*, 10(9). [Cited on pages 5, 8, 10, and 15]
- [Anik et al., 2023] Anik, F. I., Sakib, N., Shahriar, H., Xie, Y., Nahiyani, H. A., and Ahamed, S. I. (2023). Unraveling a blockchain-based framework towards patient empowerment: A scoping review envisioning future smart health technologies. *Smart Health*, 29:100401. [Cited on pages 1 and 10]
- [Asif and Hassan, 2023] Asif, R. and Hassan, S. R. (2023). Shaping the future of ethereum: Exploring energy consumption in proof-of-work and proof-of-stake consensus. *Frontiers in Blockchain*, 6:1151724. [Cited on page 7]
- [Awan et al., 2024] Awan, K. A., Din, I. U., Almogren, A., and Rodrigues, J. J. (2024). Meditwin: A web 3.0-integrated digital twin for secure patient-centric healthcare in the metaverse. *IEEE Transactions on Consumer Electronics*. [Cited on pages 22, 24, 25, 30, and 32]
- [Bak et al., 2025] Bak, O., Braganza, A., and Chen, W. (2025). Exploring blockchain implementation challenges in the context of healthcare supply chain

- (hpsc). *International Journal of Production Research*, 63(2):687–702. [Cited on pages 24 and 32]
- [Bazel et al., 2021] Bazel, M. A., Mohammed, F., and Ahmed, M. (2021). Blockchain technology in healthcare big data management: Benefits, applications and challenges. In *2021 1st International Conference on Emerging Smart Technologies and Applications (eSmarTA)*, pages 1–8. [Cited on pages 1 and 13]
- [Bhatia, 2024] Bhatia, M. (2024). Iot-inspired secure healthcare framework for adult: Blockchain perspective. *Mobile Networks and Applications*, 29(2):460–476. [Cited on pages 24, 25, and 33]
- [Chaurasia, 2024] Chaurasia, B. K. (2024). Blockchain enabled medivault for healthcare system. *Multimedia Tools and Applications*, pages 1–21. [Cited on pages 20, 21, 22, 24, 25, 29, 30, and 33]
- [Chelladurai and Pandian, 2022] Chelladurai, U. and Pandian, S. (2022). A novel blockchain based electronic health record automation system for healthcare. *Journal of Ambient Intelligence and Humanized Computing*, 13(1):693–703. [Cited on page 13]
- [Cohen and Mello, 2018] Cohen, I. G. and Mello, M. M. (2018). Hipaa and protecting health information in the 21st century. *Jama*, 320(3):231–232. [Cited on page 9]
- [Dbesan et al., 2023] Dbesan, A. H., Abdulmuhsin, A. A., and Alkhwalidi, A. F. (2023). Adopting knowledge-sharing-driven blockchain technology in healthcare: a developing country’s perspective. *VINE Journal of Information and Knowledge Management Systems*, (ahead-of-print). [Cited on pages 20, 23, 24, 29, 31, and 33]
- [Dhingra et al., 2024] Dhingra, S., Raut, R., Kumar, M., and Naik, B. K. R. (2024). Factors impacting indian healthcare supply chain performance and influence in the public and private sector: the mediating role of blockchain technology adoption. *Benchmarking: An International Journal*. [Cited on pages 23, 24, 31, and 32]
- [Dhingra et al., 2023] Dhingra, S., Raut, R. D., Yadav, V. S., Cheikhrouhou, N., and Naik, B. K. R. (2023). Blockchain adoption challenges in the healthcare sector: a waste management perspective. *Operations management research*, pages 1–19. [Cited on page 24]
- [Farouk et al., 2020] Farouk, A., Alahmadi, A., Ghose, S., and Mashatan, A. (2020). Blockchain platform for industrial healthcare: Vision and future opportunities. *Computer Communications*, 154:223–235. [Cited on pages 5, 6, 7, 8, and 16]

- [Firouzi et al., 2023] Firouzi, F., Jiang, S., Chakrabarty, K., Farahani, B., Daneshmand, M., Song, J., and Mankodiya, K. (2023). Fusion of iot, ai, edge–fog–cloud, and blockchain: Challenges, solutions, and a case study in healthcare and medicine. *IEEE Internet of Things Journal*, 10(5):3686–3705. [Cited on pages 1, 2, and 11]
- [Frikha et al., 2021] Frikha, T., Chaabane, F., Aouinti, N., Cheikhrouhou, O., Ben Amor, N., and Kerrouche, A. (2021). Implementation of blockchain consensus algorithm on embedded architecture. *Security and Communication Networks*, 2021(1):9918697. [Cited on page 7]
- [Goel et al., 2019] Goel, U., Ruhl, R., and Zavorsky, P. (2019). Using healthcare authority and patient blockchains to develop a tamper-proof record tracking system. In *2019 IEEE 5th intl conference on big data security on cloud (BigDataSecurity), IEEE Intl conference on high performance and smart computing, (HPSC) and IEEE Intl conference on intelligent data and security (IDS)*, pages 25–30. IEEE. [Cited on pages 5, 8, and 16]
- [Hasselgren et al., 2020] Hasselgren, A., Krlevska, K., Gligoroski, D., Pedersen, S. A., and Faxvaag, A. (2020). Blockchain in healthcare and health sciences—a scoping review. *International Journal of Medical Informatics*, 134:104040. [Cited on pages 7 and 16]
- [Jakhar et al., 2024] Jakhar, A. K., Singh, M., Sharma, R., Viriyasitavat, W., Dhimman, G., and Goel, S. (2024). A blockchain-based privacy-preserving and access-control framework for electronic health records management. *Multimedia Tools and Applications*, pages 1–35. [Cited on pages 22 and 30]
- [Kramer and Moesel, 2023] Kramer, M. A. and Moesel, C. (2023). Interoperability with multiple fast healthcare interoperability resources (fhir®) profiles and versions. *JAMIA open*, 6(1):ooad001. [Cited on page 9]
- [Kumari et al., 2024] Kumari, T., Kumar, R., and Dwivedi, R. K. (2024). Blockchain-based secure and smart healthcare iot system using hybrid consensus mechanism with an honest block. *Health Services and Outcomes Research Methodology*, pages 1–39. [Cited on pages 22 and 30]
- [Larobina, 2023] Larobina, M. (2023). Thirty years of the dicom standard. *Tomography*, 9(5):1829–1838. [Cited on page 9]
- [Liu and Li, 2022] Liu, L. and Li, Z. (2022). Permissioned blockchain and deep reinforcement learning enabled security and energy efficient healthcare internet of things. *IEEE Access*, 10:53640â53651. [Cited on page 12]

- [Mackey et al., 2019] Mackey, T. K., Kuo, T.-T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., Obbad, K., Barkovich, R., and Palombini, M. (2019). ‘fit-for-purpose?’—challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC medicine*, 17:1–17. [Cited on page 8]
- [McGhin et al., 2019] McGhin, T., Choo, K.-K. R., Liu, C. Z., and He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of network and computer applications*, 135:62–75. [Cited on pages 6 and 7]
- [Meghin and Johnson, 2019] Meghin, S. and Johnson, D. (2019). Blockchain technology in healthcare: A comprehensive review of consensus mechanisms and implementation challenges. *Journal of Healthcare Informatics Research*, 3(2):114–135. [Cited on pages 8 and 16]
- [Nakamoto and Bitcoin, 2008] Nakamoto, S. and Bitcoin, A. (2008). A peer-to-peer electronic cash system. *Bitcoin*.—URL: <https://bitcoin.org/bitcoin.pdf>, 4(2):15. [Cited on page 5]
- [Nath et al., 2023] Nath, S. S., Sadagopan, S., Babu, D. V., Kumar, R. D., Jonnala, P., and Murthy, M. Y. B. (2023). Block chain-based security and privacy framework for point of care health care iot devices. *Soft Computing*, pages 1–13. [Cited on pages 24, 25, and 33]
- [Ogbuke et al., 2023] Ogbuke, N., Yusuf, Y. Y., Gunasekaran, A., Colton, N., and Kovvuri, D. (2023). Data-driven technologies for global healthcare practices and covid-19: opportunities and challenges. *Annals of Operations Research*, pages 1–36. [Cited on pages 24, 25, and 33]
- [Page et al., 2021] Page, M. J., McKenzie, J. E., Bossuyt, P. M., Boutron, I., Hoffmann, T. C., Mulrow, C. D., Shamseer, L., Tetzlaff, J. M., Akl, E. A., Brennan, S. E., Chou, R., Glanville, J., Grimshaw, J. M., Hróbjartsson, A., Lalu, M. M., Li, T., Loder, E. W., Mayo-Wilson, E., McDonald, S., McGuinness, L. A., Stewart, L. A., Thomas, J., Tricco, A. C., Welch, V. A., Whiting, P., and Moher, D. (2021). The prisma 2020 statement: an updated guideline for reporting systematic reviews. *BMJ*, 372. [Cited on page 19]
- [Peiris et al., 2024] Peiris, D., Feyer, A.-M., Barnard, J., Billot, L., Bouckley, T., Campaign, A., Cordery, D., de Souza, A., Downey, L., Elshaug, A. G., et al. (2024). Overcoming silos in health care systems through meso-level organisations—a case study of health reforms in new south wales, australia. *The Lancet Regional Health—Western Pacific*, 44. [Cited on page 1]
- [Pirtle and Ehrenfeld, 2018] Pirtle, C. and Ehrenfeld, J. (2018). Blockchain for healthcare: The next generation of medical records? *Journal of Medical Systems*, 42(9):172. [Cited on pages 11 and 16]

- [Saha et al., 2024] Saha, S., Das, A. K., Wazid, M., Park, Y., Garg, S., and Al-rashoud, M. (2024). Smart contract-based access control scheme for blockchain assisted 6g-enabled iot-based big data driven healthcare cyber physical systems. *IEEE Transactions on Consumer Electronics*. [Cited on pages 22, 24, 25, 30, and 32]
- [Said et al., 2023] Said, A., Yahyaoui, A., and Abdellatif, T. (2023). Hipaa and gdpr compliance in iot healthcare systems. In *International conference on model and data engineering*, pages 198–209. Springer. [Cited on page 9]
- [Shahnaz et al., 2019] Shahnaz, A., Qamar, U., and Khalid, A. (2019). Using blockchain for electronic health records. *IEEE access*, 7:147782–147795. [Cited on page 11]
- [Strasberg et al., 2021] Strasberg, H. R., Rhodes, B., Del Fiol, G., Jenders, R. A., Haug, P. J., and Kawamoto, K. (2021). Contemporary clinical decision support standards using health level seven international fast healthcare interoperability resources. *Journal of the American Medical Informatics Association*, 28(8):1796–1806. [Cited on page 9]
- [Vishwakarma et al., 2023] Vishwakarma, S., Goswami, R. S., Nayudu, P. P., Sekhar, K. R., Arnepalli, P. R. R., Thatikonda, R., and Abdel-Rehim, W. M. (2023). Secure federated learning architecture for fuzzy classifier in healthcare environment. *Soft Computing*, pages 1–12. [Cited on pages 24, 25, and 33]
- [Yongjoh et al., 2021] Yongjoh, S., So-In, C., Kompunt, P., Muneesawang, P., and Morien, R. I. (2021). Development of an internet-of-healthcare system using blockchain. *IEEE Access*, 9:113017–113031. [Cited on page 12]
- [Younis et al., 2022] Younis, M., Lalouani, W., Lasla, N., Emokpae, L., and Abdallah, M. (2022). Blockchain-enabled and data-driven smart healthcare solution for secure and privacy-preserving data access. *IEEE Systems Journal*, 16(3):3746–3757. [Cited on page 12]