International Journal of E-Health and Medical Communications
Volume 15 • Issue 1 • January-December 2024

Comprehensive Analysis of Blockchain Technology in the Healthcare Sector and Its Security Implications

Yelezhanova Shynar
https://orcid.org/0000-0001-9815-9594
Atyrau University Named After H. Dosmukhamedov, Kazakhstan

Altynbek Seitenov
https://orcid.org/0000-0001-5777-4363
L.N. Gumilyov Eurasian National University, Kazakhstan

Aizhan Kenzhegarina
https://orcid.org/0009-0008-0200-5098
Astana IT University, Kazakhstan

Amir Kenzhetayev
https://orcid.org/0009-0001-9825-197X
Boston University, USA

Ayan Kemel
https://orcid.org/0009-0008-2074-0942
Astana IT University, Kazakhstan

Nurzhan Ualiyev
https://orcid.org/0000-0001-8854-3525
Zhetysu University Named After I. Zhansugurov, Kazakhstan

Alua Myrzakerimova
https://orcid.org/0000-0002-8500-1672
Astana IT University, Kazakhstan

Gulzhan Mursakimova
https://orcid.org/0000-0001-8608-3561
Zhetysu University Named After I. Zhansugurov, Kazakhstan

Alibek Orynbek
https://orcid.org/0009-0007-2102-1977
Astana IT University, Kazakhstan

Aivar Sakhipov
https://orcid.org/0000-0003-1045-4199
Astana IT University, Kazakhstan

ABSTRACT

Blockchain technology presents a promising solution for healthcare, addressing key challenges like data breaches, patient control, and interoperability. This paper analyzes blockchain applications in three areas: electronic health records, pharmaceutical supply chain traceability, and clinical trials. The authors explore security concerns, regulatory compliance, and smart contract vulnerabilities, proposing solutions like advanced cryptography and improved consensus mechanisms. Real-world examples, such as Medicalchain and Chronicled's MediLedger, demonstrate enhanced transparency and security. However, adoption faces barriers like scalability, computational costs, and regulatory complexities. The study also highlights ethical issues around data ownership and suggests future research into improving interoperability and integrating technologies like artificial intelligence and internet of medical things for better healthcare outcomes.

KEYWORDS

Blockchain, Medical Data, Data Privacy, Smart Contracts, EHR, Decentralization, Healthcare, Interoperability

INTRODUCTION

The healthcare sector is undergoing a significant transformation driven by the digitization of medical records, telemedicine adoption, and growing concerns about patient data security. As healthcare organizations navigate the challenges of protecting sensitive patient information while ensuring efficient communication among providers, traditional centralized database systems have proven inadequate. These systems often fail to meet stringent requirements for secure medical

DOI: 10.4018/IJEHMC.372423

communication, privacy, and seamless interoperability. Consequently, innovative technologies that can address these challenges while improving patient outcomes have garnered significant attention. Blockchain technology, with its decentralized and immutable ledger system, offers a transformative approach to enhancing healthcare data security and real-time communication between stakeholders. By enabling secure and transparent transactions, blockchain facilitates confidential patient-provider interactions, encrypted telehealth consultations, and tamper-proof electronic health record (EHR) exchanges. These capabilities are particularly critical in ensuring trust in medical communication and reducing risks associated with centralized data management.

This paper argues that blockchain technology has the potential to revolutionize healthcare by addressing critical challenges related to data security, privacy, and interoperability while also enabling innovative applications such as artificial intelligence (AI)-driven diagnostics and secure internet of medical things (IoMT) integration. To support this argument, the paper will first explore the fundamental principles of blockchain technology and its relevance to healthcare. It will then examine specific applications, including patient-centric EHRs, supply chain transparency, and smart contracts for insurance settlements. Finally, the paper will discuss the challenges and security implications of implementing blockchain in healthcare; this will be supported by case studies and a forward-looking perspective on its integration with emerging technologies.

Characterized by its decentralized and immutable ledger system, blockchain enables secure and transparent transactions that are crucial in an industry where data integrity is paramount. At its core, blockchain operates on fundamental principles such as decentralization, cryptographic security, and consensus mechanisms. These principles collectively ensure data integrity and prevent unauthorized alterations (Agbo et al., 2019; Moosavi & Taherdoost, 2023). In blockchain, each transaction is meticulously recorded in a block linked to previous blocks, forming a chain that is resistant to tampering, as seen in Figure 1. This unique structure not only enhances data security, but also fosters trust among participants by eliminating the need for a central authority (Mayer et al., 2019).

In the healthcare sector, the relevance of blockchain technology is particularly pronounced as it addresses critical challenges related to data security, privacy, and interoperability. Traditional healthcare systems often suffer from fragmented data storage, leading to inefficiencies and increased risks of medical errors (Kamangar et al., 2023; Khezr et al., 2019). Blockchain's capability to provide a secure, decentralized platform for managing EHRs can significantly enhance data sharing and coordination among healthcare providers, ultimately improving patient care (Umrao et al., 2022). Furthermore, the technology's inherent features—such as traceability and transparency—can bolster trust in medical supply chains, ensuring the authenticity of pharmaceuticals and medical devices (Agbo et al., 2019; Alnssayan et al., 2021).

The integration of blockchain with AI and the IoMT presents additional opportunities for data-driven healthcare optimization. AI-driven predictive analytics, combined with blockchain's secure infrastructure, enables fraud-resistant insurance claims processing, AI-assisted diagnostic transparency, and real-time IoMT-based patient monitoring. These integrations not only strengthen healthcare security, but also enhance medical communication by ensuring data accuracy, authenticity, and accessibility.

The growing interest in blockchain applications within healthcare is evidenced by a surge in research and pilot projects aimed at exploring its potential benefits. Recent studies indicate that the adoption of blockchain in healthcare is gaining momentum, with numerous organizations investigating its use for secure data sharing, patient monitoring, and clinical trials (Adeghe, 2024; Jamil et al., 2021). Successful pilot projects, such as Estonia's Healthcare System and MediLedger for pharmaceutical traceability, exemplify how blockchain can enhance healthcare operations. For instance, a systematic review highlighted that blockchain could enhance EHR management by making records more accessible and secure (Mayer et al., 2019). Additionally, the COVID-19 pandemic has accelerated the exploration of blockchain solutions for tracking vaccinations and managing health

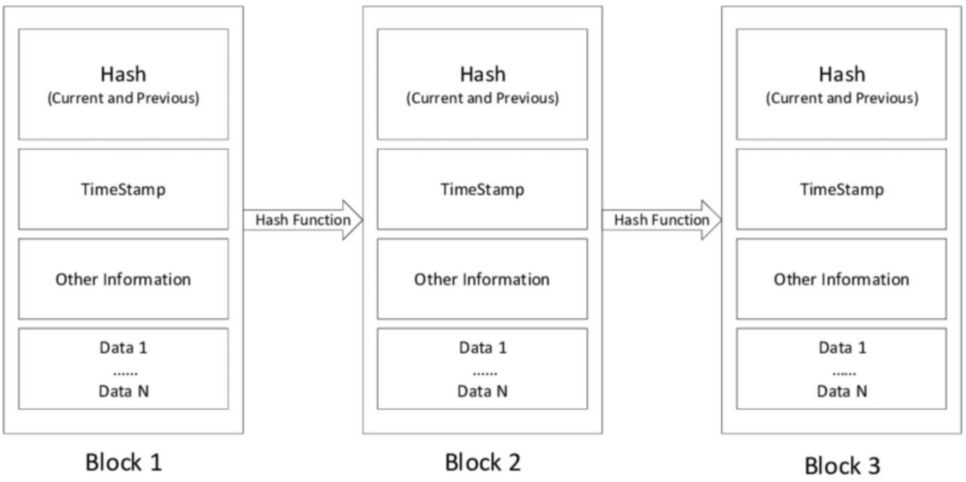
data, further underscoring its relevance in addressing contemporary healthcare challenges (Marbouh et al., 2020; Martínez et al., 2022).

METHODOLOGY

This paper conducts a comparative analysis of blockchain implementations in healthcare, drawing on case studies such as Estonia's blockchain-enabled EHRs, MediLedger for pharmaceutical traceability, and IBM's blockchain pilot for clinical trials. The study evaluates how blockchain addresses data security, patient control, and interoperability challenges while ensuring regulatory compliance with frameworks like the health insurance portability and accountability act (HIPAA) and the general data protection regulation (GDPR). Empirical findings from industry reports and academic studies are incorporated to assess blockchain's real-world impact and feasibility in healthcare systems.

This paper builds upon existing studies by providing a detailed analysis of blockchain's role in healthcare security and is supported by case studies and a forward-looking perspective on its integration with emerging technologies. The subsequent sections will explore specific applications of blockchain in healthcare. These include patient-centric EHRs, supply chain transparency, smart contracts for insurance settlements, and credential verification for medical staff. Additionally, this analysis will discuss the challenges faced by traditional healthcare systems and how blockchain technology can address these issues through enhanced interoperability and security. Finally, the article will examine the security implications of implementing blockchain in healthcare, alongside case studies of successful implementations and future directions for research and development.

Figure 1. Blockchain structure



Challenges in Traditional Healthcare Systems

Blockchain technology holds immense potential for various healthcare applications. In this section, we focus on three key areas: medical records management, pharmaceutical traceability, and clinical trials. Each of these areas faces significant challenges related to security, data integrity, and transparency.

This section outlines the conventional methods used in these areas: the HIPAA and the GDPR; it demonstrates the limitations that blockchain technology seeks to address. Traditional healthcare systems are governed by stringent privacy regulations, such as the HIPAA in the United States and the GDPR in Europe. While these frameworks aim to ensure the confidentiality and security of patient

information, healthcare systems continue to face significant challenges, including data breaches, limited patient control, and interoperability issues. These challenges are compounded by the increasing digitalization of healthcare, where personal health information is stored and transmitted across various systems.

One of the most critical areas where these issues manifest is in the management of EHRs. Despite their advantages in digital data storage, EHR systems face significant security vulnerabilities, limitations in patient control, and challenges related to interoperability. Additionally, compliance with the HIPAA and GDPR remains a persistent challenge in safeguarding personal health data. In this section, we explore how EHR systems are affected by these limitations and how blockchain technology has the potential to offer solutions, ensuring better security, control, and seamless data sharing across platforms.

EHR Management

Historically, medical records have been managed through EHRs or electronic medical record (EMR) systems. These systems are designed to digitally store and manage a patient's health information. These systems operate on centralized databases, which are managed either by individual healthcare institutions or by third-party providers.

EMRs encompass a range of data, including a patient's medical history, test results, diagnoses, treatments, prescribed medications, and allergies. These records are typically managed through identity and access management systems that utilize logins and passwords to authenticate authorized users, such as nurses, doctors, and administrative staff. Additionally, EMR systems can be integrated with other medical infrastructures and systems, such as pharmacies, laboratories, and billing systems (Anshari, 2019). While EHR systems have revolutionized healthcare, they continue to face significant challenges related to security, patient control, and interoperability, which are highlighted by several high-profile incidents.

Challenges in EHR Management

Despite the improvements offered by EHR systems, healthcare continues to grapple with substantial data management challenges. These challenges underscore the urgent need for more robust and secure solutions.

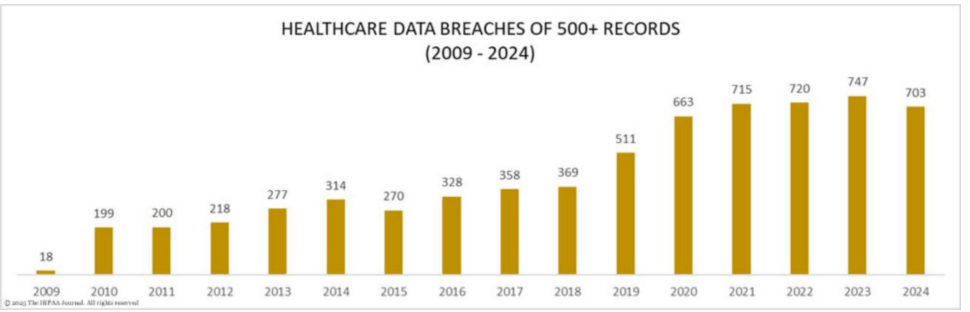
Data Breaches

Data breaches are among the most pressing concerns in EHR management. The largest healthcare data breach of the year occurred at Change Healthcare, which impacted an estimated 100 million individuals—over half of the year's total breached records. This attack was carried out by BlackCat, also known as ALPHV, a sophisticated ransomware-as-a-service (RaaS) group that has become a major cybersecurity threat, particularly in critical sectors like healthcare. BlackCat is known for using a double extortion strategy, where they not only encrypt files but also exfiltrate sensitive data to pressure victims into paying ransoms (Nicho et al., 2023). In this case, the attackers exfiltrated secured health information before encrypting the files, further escalating the impact of the breach. Despite a $22 million ransom payment, the group did not receive the expected funds, and the stolen data was later handed over to the RansomHub group (HIPAA Journal, 2024). Data breaches are not a new phenomenon in healthcare. One of the most notorious attacks in recent history was the 2017 WannaCry ransomware attack, which targeted the British National Health Service. This attack encrypted thousands of patient records and critical healthcare data, highlighting the vulnerabilities inherent in centralized healthcare systems (Kaushik & El Madhoun, 2023). According to recent statistics, healthcare data breaches involving 500 or more records have steadily increased over the years. In 2024, there were 703 reported breaches, reflecting a slight decrease of 5.9% from the 747 breaches recorded in 2023. However, the number of individuals affected has risen dramatically. In

2024 alone, over 184 million healthcare records were compromised, affecting 53% of the American population, underscoring the growing security concerns in the sector.

Additionally, the financial impact of these breaches is substantial. In 2024, the average cost of a healthcare data breach surged to nearly $10 million, highlighting the severe consequences of inadequate cybersecurity measures (HIPAA Journal, 2024; IBM Security, 2024). Figure 2 shows illustrates the increasing trend in healthcare data breaches from 2009 to 2024, highlighting the sharp rise in incidents over the past decade. The graph demonstrates a consistent upward trajectory, with significant spikes in breach occurrences observed after 2018.

Figure 2. Healthcare data breaches of 500+ records (2009–2024)



Lack of Patient Control

In centralized EHR systems, patients often have limited control over their health data. Patients cannot revoke access or limit whoever views their sensitive information. This lack of control can lead to unauthorized access, data misuse, and privacy breaches. According to a survey by the American Medical Association, 92% of patients consider privacy a fundamental right, and 80% want the ability to opt out of data sharing (AMA, 2022).

A significant concern with centralized systems is that healthcare providers and tech companies hold full control over patient data. A 2022 lawsuit against Meta highlights this issue, where the company was accused of gathering sensitive patient data without consent via the Meta Pixel tool embedded in healthcare websites. This tool tracked patients' health activities and used the data for targeted advertising, raising serious privacy and ethical concerns (HIPAA Journal, 2022; Kahn, 2022).

Blockchain technology, by contrast, gives patients more control over their data, ensuring better privacy and security while reducing the risk of unauthorized access.

Interoperability Issues

Healthcare data is often fragmented across various systems and providers, hindering the efficient sharing of patient information. This fragmentation can lead to delays in diagnosis and treatment, ultimately affecting the quality of care. Many healthcare providers struggle to access complete medical histories due to challenges in data exchange(Bataineh et al., 2022).

A study by Lubin and Shah (2022) revealed that 41.5% of transfer-of-care (TOC) forms were missing during data transfer between Emergency Medical Services (EMS) and Emergency Departments (ED). Critical details such as chief complaints, medications, and allergies were often absent or inconsistent, increasing the risk of misdiagnosis and incorrect treatment. Additionally, a survey by Propeller Insights for Carta Healthcare (2023) found that 60% of consumers lack adequate access to their health data, underscoring the need for improved interoperability.

Regulatory Barriers

In addition to technical barriers, regulatory frameworks such as the GDPR in the European Union introduce further complexities to healthcare data interoperability. While the GDPR was designed to enhance data privacy and security, it has inadvertently created obstacles to the free exchange of patient data between healthcare entities, particularly in cross-border contexts (European Commission, 2022). One of the most significant regulatory challenges imposed by the GDPR is its requirement for strict data access controls and patient consent mechanisms. Under Article 17 of the GDPR, patients have the "right to be forgotten," meaning they can request the deletion of their personal data at any time. (Regulation (EU) 2016/679, Article 17). However, this conflicts with the legal and ethical requirements of healthcare providers to maintain accurate medical histories for patient safety, insurance claims, and medico-legal accountability (Shabani & Marelli, 2019). The contradiction between the GDPR's data deletion rights and the healthcare sector's need for long-term record retention has created uncertainty in how EHR systems should be designed to accommodate both compliance and patient safety requirements.

Another critical GDPR-related challenge involves restrictions on cross-border data sharing. Article 44 of the GDPR mandates that healthcare data cannot be transferred outside the European Union unless the receiving country ensures equivalent levels of data protection. This has had significant implications for multinational healthcare organizations and international clinical trials that rely on collaborative data-sharing frameworks. A study conducted as part of the *Joint Action InfAct* project found that GDPR was perceived as a barrier to the secondary use of health data by one-third of the experts surveyed, with challenges including delays in data sharing, increased administrative workload, and inconsistencies in GDPR implementation across EU member states (Vukovic et al., 2022). Differences in national interpretations of GDPR have further complicated cross-border data exchange, leading some countries to stop sharing health data due to concerns over potential violations of data protection laws. These delays and regulatory inconsistencies negatively affect time-sensitive medical research, including drug development, epidemiological studies, and the coordination of multinational healthcare initiatives

Moreover, the GDPR's lack of standardized implementation across European Union member states further exacerbates interoperability challenges. While the GDPR provides a broad regulatory framework, each country interprets and enforces compliance requirements differently, leading to inconsistencies in how healthcare data are stored, shared, and processed. For example, a comparative analysis of data protection legislation across eight EU countries revealed significant differences in national laws, policies, and practices, despite the harmonizing intent of the GDPR (Custers et al., 2017). These discrepancies create additional burdens for healthcare providers operating across multiple jurisdictions, as they must navigate differing compliance requirements that add complexity to data interoperability solutions.

Moreover, the GDPR's lack of standardized implementation across European Union member states further exacerbates interoperability challenges. While the GDPR provides a broad regulatory framework, each country interprets and enforces compliance requirements differently, leading to inconsistencies in how healthcare data are stored, shared, and processed. For example, a comparative analysis conducted by the European Medicines Agency (2023) found that while Germany required explicit patient consent for nearly all health data exchanges, France had implemented a more flexible approach that allowed automated anonymized data-sharing protocols for research purposes. These discrepancies create additional burdens for healthcare providers operating across multiple jurisdictions, as they must navigate differing compliance requirements that add complexity to data interoperability solutions.

Additionally, the bureaucratic nature of GDPR compliance procedures has introduced inefficiencies in healthcare data exchange. Many hospitals and clinics require manual verification before patient data can be transferred, adding administrative overhead and delaying critical treatment decisions. A study by Staunton et al. (2019) found that while GDPR aims to harmonize data

privacy laws across the EU, its implementation has led to significant complexities in data-sharing practices, resulting in inefficiencies in health research and medical data processing. These delays are particularly pronounced in cases involving specialist referrals and cross-border healthcare services, where legal reviews and additional patient consent procedures often take extended periods to complete. Such inefficiencies not only burden healthcare providers but also negatively impact patient outcomes, as timely access to medical history is crucial for accurate diagnosis and treatment planning.

Given these interoperability and regulatory challenges, healthcare institutions are increasingly exploring technological solutions that enable secure yet compliant data-sharing mechanisms. Blockchain technology has emerged as a promising alternative for managing healthcare data in a way that ensures both interoperability and GDPR compliance.

While EHR systems exemplify the challenges of data security and patient control, these issues extend to other critical healthcare domains, such as pharmaceutical traceability. Inadequate tracking and security in pharmaceutical supply chains further illustrate the systemic vulnerabilities within healthcare data management. This section addresses the key issues in pharmaceutical traceability, focusing on fragmentation, inefficiencies, and security risks.

Pharmaceutical Traceability

Pharmaceutical traceability has long depended on complex supply chains. These systems employ centralized databases to document and monitor the movement of medications at each stage, from production to distribution to the end user. The tracking process typically entails the use of batch numbers and barcodes, which are scanned and recorded at each transfer point (Hammi et al., 2023). This enables the monitoring of pharmaceutical product movement and the management of inventory. Furthermore, traceability systems may incorporate mechanisms for monitoring storage and transportation conditions, such as temperature (Hammi et al., 2023). The data collected is used to ensure regulatory compliance and for product recalls if necessary (Trautmann et al., 2022). Despite efforts to ensure traceability in pharmaceutical supply chains, significant security vulnerabilities remain, including fragmented supply chains, inefficiencies in tracking, and outdated paper-based methods.

Fragmented Supply Chain

The pharmaceutical supply chain faces significant technical challenges due to its fragmented nature and the multitude of stakeholders involved. This lack of a unified traceability system creates gaps in medication monitoring, which increases the risk of counterfeit products infiltrating the market. A notable example is the counterfeit COVID-19 vaccine incidents reported in India in 2021, where individuals were administered saline instead of actual vaccines at various centers. Over 2,000 people in Mumbai were affected, highlighting the grave consequences of fragmented systems. Additionally, in operations across Southern Africa, authorities seized millions of dollars' worth of counterfeit goods, including fake vaccines. In South Africa, authorities dismantled a warehouse containing 400 ampules of counterfeit COVID-19 vaccines, highlighting the challenges posed by inadequate monitoring and traceability systems. These counterfeit medications can be ineffective or even harmful, posing serious public health risks. The World Health Organization (WHO) estimates that counterfeit medicines make up to 10% of the global medicines market, particularly in regions with poor traceability systems (Blais, 2022; Hammi et al., 2023; Kumar et al., 2022; WHO, 2017).

These incidents underscore the critical need for robust traceability systems and regulatory frameworks to combat the infiltration of counterfeit products into the pharmaceutical supply chain and to protect public health.

Inefficiency of Tracking

The current traceability mechanisms employed by the healthcare ecosystem are frequently reliant on paper registers or centralized databases. Consequently, these mechanisms are characterized by a lack of transparency and the inability to conduct real-time tracking. This inefficiency gives rise to

significant challenges in the tracing of the provenance of medicines, particularly in the context of recalls or security incidents. The ability to trace the source and route of pharmaceuticals rapidly and accurately is of paramount importance in ensuring patient safety (Sahoo et al., 2020).

Outdated Methods Such as Paperwork

The continued reliance on paper-based documentation within the healthcare ecosystem, particularly in the pharmaceutical supply chain, poses a considerable risk of human error and falsification. Consequently, such errors and manipulations can result in inaccurate information within the supply chain, thereby compromising patient security. Additionally, given their susceptibility to alteration, paper documents are not an optimal medium in high-stakes domains such as healthcare and the pharmaceutical industry, where reliability and security are of paramount importance (Trautmann et al., 2022).

Counterfeit antimalarial medicines in Africa exemplify the significant technical and regulatory challenges associated with drug safety. The WHO has reported that counterfeiters frequently utilize unregulated facilities to produce substandard or dangerous medications, which may contain incorrect ingredients or improper dosages.

These counterfeit products are often distributed through illicit channels, including unregulated online sales and parallel trade, which disrupt legitimate supply chains.

The lack of effective monitoring and quality control in many African countries, where regulatory systems are often under-resourced and lack sufficient technical expertise, exacerbates this issue. The public health risks associated with counterfeit medicines include therapeutic failures, drug resistance, and direct harm to patients (WHO, 2017, 2023).

Moreover, detecting and combating counterfeit activities poses significant challenges that require international cooperation, advanced testing technologies, and robust legal frameworks to effectively track down offenders. Beyond the immediate health risks, counterfeit medicines also have considerable economic and social consequences. They undermine confidence in healthcare systems, lead to financial losses for legitimate manufacturers, and can potentially fund other illicit activities (WHO, 2010, 2017). The challenges of data integrity and security are also deeply felt in clinical trials, where accurate data collection, consent management, and secure sharing of information are essential.

Clinical Trials

In the context of research and clinical trials, data are typically collected, stored, and analyzed using a clinical data management system. These systems collect data from various sources, including direct observations, questionnaires, biological samples, and measuring devices. Subsequently, the data are processed and stored in a centralized database. The process often involves a manual input of data, although electronic data capture devices are increasingly used to enhance efficiency and minimize errors. Then, researchers employ statistical software to analyze the collected data, assessing the efficacy, safety, and potential adverse effects of the treatments under study. Finally, the consent of participants is managed using consent forms, which are often paper based (Nourani et al., 2019). Data manipulation, inefficiencies in consent management, and lack of secure data sharing have created serious vulnerabilities in clinical trials, similar to those seen in other areas of healthcare.

SECURITY VULNERABILITIES IN RESEARCH AND CLINICAL TRIALS

Data Manipulation

In clinical trials, the manipulation of data is a serious concern, as it can distort research results and lead to inaccurate conclusions about the efficacy and safety of new treatments. Manipulated or falsified data compromises the validity of research and can pose direct risks to patient safety (Banerji

et al., 2018). The 2013 research scandal involving GlaxoSmithKline (GSK) in China serves as a prominent example that has severely impacted trust in pharmaceutical research practices.

Investigations revealed multiple irregularities in GSK's clinical trials for cancer treatments, with the primary concern being data manipulation. This manipulation allegedly involved altering or omitting certain data to present more favorable or less risky trial outcomes, thereby misrepresenting the true efficacy and safety of the medicines under investigation. Such unethical actions have raised significant doubts regarding the integrity of pharmaceutical research and the processes used for approving new medicines, not only in China but globally. The public's and healthcare professionals' confidence in the validity of clinical trial results and the approval of new treatments has been seriously undermined.

Ineffective Management of Patients' Consent

Consent management in traditional clinical trials is often inefficient, relying on paper-based forms that are prone to errors or mismanagement. Inadequate consent processes can lead to legal and ethical violations, diminishing public trust in both medical research and healthcare providers. Patients may not fully understand how their data is being used or may be unable to revoke consent once granted (Chen et al., 2023).

Data Sharing

In the absence of robust security protocols used to safeguard the sharing of data between researchers, there is a significant vulnerability that could potentially lead to the exposure of sensitive information. This is a particularly concerning issue, particularly when the data in question is sensitive. In addition, the violation of the confidentiality of patients participating in clinical trials represents a significant threat to the credibility and trustworthiness of medical research (White et al., 2022).

According to a report by the British Medical Journal, GSK faced scrutiny for its lack of transparency and ethical breaches, which highlighted the need for more rigorous oversight in clinical trials (Coombes, 2012). These actions violate fundamental principles of clinical research and compromise patient safety, as patients may rely on falsified data when using these medicines. The fallout from this scandal emphasizes the critical importance of maintaining ethical standards and transparency in clinical trials to restore trust and ensure patient safety.

The challenges faced by traditional healthcare systems can be broadly categorized into three key issues: inadequate data security, limited patient control over health information, and poor interoperability among healthcare providers. These factors not only jeopardize the quality of care, but also undermine trust in the healthcare system. Security concerns, such as data breaches, cyberattacks, and insider threats, represent significant risks to patient privacy and the overall stability of healthcare organizations.

Healthcare data management faces persistent challenges in security, patient control, and interoperability. Traditional centralized systems struggle to utilize medical information effectively and securely. Blockchain technology offers a promising solution by providing a decentralized, immutable, and transparent approach. This technology has the potential to significantly enhance data security, empower patients with greater control over their health data, and improve interoperability across healthcare providers. The following sections will explore how blockchain can address these critical issues.

ADDRESSING HEALTHCARE CHALLENGES WITH BLOCKCHAIN

Technical Overview of Blockchain Technology

Blockchain is a decentralized technology that allows data to be securely stored across a network of computers, rather than in a single location. This decentralized nature makes it highly resistant to fraud, ensuring that the information stored is transparent, traceable, and immutable. It is fundamentally

structured around several key components, including blocks, hashes, cryptographic security, and consensus mechanisms.

A blockchain consists of a series of blocks, each containing a list of transactions. Each block is linked to the previous one through a cryptographic hash, as illustrated in Figure 3. This figure depicts how each block in the chain is structured, with a hash that integrates both its own content and the hash of the preceding block, ensuring the integrity of the data. The hash serves as a unique identifier for the block and ensures the integrity of the data contained within it. The hash is generated using a cryptographic hash function, which transforms input data into a fixed-length output, making it extremely difficult to recover the original data from the hash (Anwar et al., 2021). Any change to the block's data alters the hash, immediately revealing tampering, and this property is crucial for maintaining data integrity (Kiktenko et al., 2018; Sharma et al., 2023). For example, if a patient's HER is stored on a blockchain, any changes would be instantly detected, ensuring data security in sensitive fields like healthcare.

In addition to hash functions, blockchain leverages digital signatures to authenticate transactions. Each transaction is signed by the sender using a private key, resulting in a unique digital signature. This signature is then verified by the recipient using the sender's corresponding public key. This process ensures transaction authenticity and prevents the sender from denying their involvement, fostering trust within the blockchain network. These cryptographic techniques safeguard data integrity, preventing unauthorized modifications and securing the entire blockchain database (Anwar et al., 2021; Guru et al., 2023). For instance, when a healthcare provider accesses a patient’s data, a private key generates a digital signature, ensuring only authorized access. This guarantees both authentication and non-repudiation, reinforcing trust within the system.

Since blockchain is decentralized, it does not rely on a central authority to validate transactions. Instead, it uses consensus mechanisms to ensure that all participants agree on the state of the data. As illustrated in Figure 3, nodes are individual participants in the blockchain network that interact with blocks and play a pivotal role in maintaining the network's security and consistency. Each node holds a copy of the blockchain and collaborates to validate transactions and propagate updates.

The interaction between nodes and blocks ensures all validated transactions are added to the blockchain only when most nodes reach a consensus. This distributed validation process secures the network and prevents unauthorized modifications to the blockchain.

Consensus mechanisms play a crucial role in maintaining the integrity and security of the blockchain network (Du et al., 2022). Common mechanisms include proof of work (PoW, Lasla et al., 2022), proof of stake (PoS, Feng et al., 2022), delegated proof of stake (DPoS, Liu et al., 2019), and practical Byzantine fault tolerance (PBFT, Liu et al., 2023). Each of these mechanisms has distinct characteristics that impact scalability, efficiency, and energy consumption, particularly in the context of healthcare applications.

PoW is a consensus mechanism widely used in blockchain networks, including Bitcoin, to ensure the security and integrity of the system. It operates by requiring participants, called “miners,” to solve computationally intensive mathematical problems. The first miner to solve the problem earns the right to add a new block of transactions to the blockchain and receives a reward in cryptocurrency. Although highly secure, this approach requires significant computational power and energy, making it less environmentally friendly and slower compared to newer mechanisms (Bard et al., 2021). For example, PoW consumes approximately 707.6 kWh per transaction, producing 380 grams of CO2 emissions. This makes it unsuitable for healthcare systems, which require energy-efficient and scalable solutions that align with sustainability goals, as seen in Table 1.

PoS is an alternative consensus mechanism designed to address the high energy demands of PoW. In PoS, individuals, referred to as “validators,” are chosen to create new blocks and verify transactions based on the amount of cryptocurrency they “stake” as collateral. This system reduces energy consumption significantly and enables faster transaction processing. For instance, PoS requires only 0.002 kWh per transaction, producing 0.8 grams of CO2 emissions. Its efficiency

makes it a promising option for applications like healthcare systems, where speed and environmental considerations are critical (Yang et al., 2019).

DPoS builds on the principles of PoS by introducing a voting system. Participants in the network use their staked cryptocurrency to elect a limited number of trusted representatives, called "delegates," who are responsible for validating transactions and maintaining the blockchain. This reduces the number of active participants in the consensus process, enabling faster block generation and higher transaction throughput. With an energy consumption of only 0.0015 kWh per transaction and CO2 emissions of 0.05 grams, DPoS is often regarded as a highly scalable and sustainable consensus mechanism. These attributes make it particularly suitable for private healthcare blockchains or networks requiring real-time data processing, such as IoMT data integration (Li & Palanisamy, 2020; Li et al., 2023).

Proof of authority (PoA) is another energy-efficient consensus mechanism that achieves extremely low energy consumption (0.00022 kWh per transaction) and minimal CO2 emissions (0.03 grams). PoA relies on a limited number of pre-approved validators, who take turns proposing and validating blocks. This mechanism offers high scalability and sustainability, making it ideal for private healthcare networks that require fast and efficient processing with lower operational costs. However, its reliance on a limited set of validators introduces risks of centralization and internal attacks, which must be mitigated through careful governance and design.

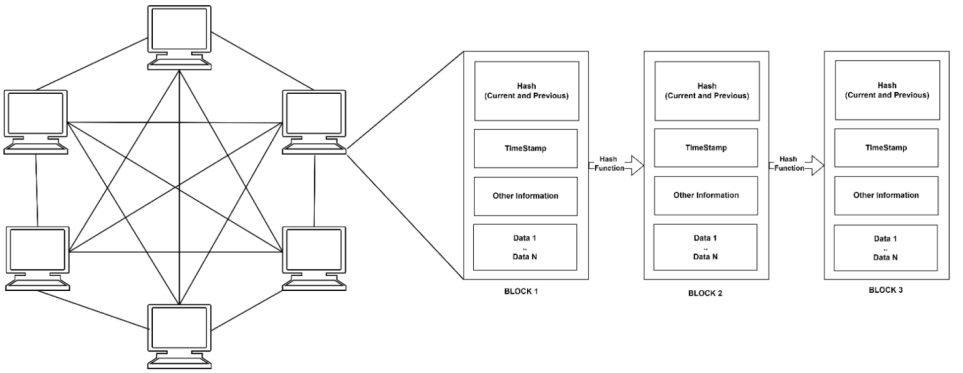
PBFT is a consensus mechanism designed to ensure the reliability and integrity of distributed systems, even when some participants act maliciously. PBFT operates under the assumption that up to one-third of the nodes in the system can be faulty or compromised without affecting the overall system's functionality. The mechanism involves nodes exchanging messages to reach a consensus on the validity of transactions, prioritizing consistency and security. This makes PBFT particularly suitable for private blockchain networks where trust among participants is limited. Its robustness in maintaining system integrity under adversarial conditions positions it as a viable option for healthcare applications that require high reliability and fault tolerance (Xu et al., 2022)

Table 1 below provides a quantitative comparison of key consensus mechanisms in terms of energy consumption, CO2 emissions, scalability, and sustainability. This analysis highlights the trade-offs between security and efficiency, helping to determine their suitability for various healthcare applications.

Table 1. Comparative analysis of blockchain consensus mechanisms in healthcare applications (Pineda et al., 2024)

Feature	Proof of Work (PoW)	Proof of Stake (PoS)	Delegated Proof of Stake (DPoS)	Proof of Authority (PoA)
Energy Consumption (Qualitative)	Very High	Low	Very Low	Very Low
Energy Consumption per Transaction (kWh)	707.6	0.002	0.0015	0.00022
CO2 Emissions per Transaction (g)	380	0.8	0.05	0.03
Energy Efficiency	Low	High	High	High
Resource Usage	High (Mining)	Low	Low	Low
Security	Very High	High	Medium	Medium
Scalability	Low	Medium	High	High
Sustainability	Low	High	Very High	Very High

Figure 3. Blockchain workflow



In addition to the foundational components of blockchain, smart contracts are an essential feature that enables the automation of processes and transactions within a blockchain network. A smart contract is a self-executing contract with the terms of the agreement directly written into lines of code. It automatically enforces and executes the terms of a contract when predefined conditions are met.

Smart contracts operate on the blockchain's decentralized network, which ensures that once a contract is deployed, it cannot be altered by any single party, fostering transparency, security, and trust. They eliminate the need for intermediaries, reduce the risk of human error, and streamline complex processes.

Blockchain's decentralized nature and smart contract functionality offer solutions to critical healthcare issues like data privacy, interoperability, and fraud prevention. By securing patient records and automating administrative tasks, blockchain enhances efficiency and trust, providing a transformative tool for healthcare systems globally.

Addressing Data Security With Blockchain

The healthcare sector faces unprecedented challenges in safeguarding sensitive patient data, with data breaches, unauthorized access, and cyberattacks becoming increasingly prevalent. Traditional centralized systems, while effective in certain contexts, often fall short in addressing the complex security demands of modern healthcare infrastructures. This section provides a comprehensive examination of blockchain-driven solutions, focusing on zero-knowledge proofs (ZKPs), secure multi-party computation, tokenized access control, and Blockchain-enabled intrusion detection systems. Each solution is critically analyzed in terms of its technical mechanisms, real-world implementations, advantages, limitations, and feasibility for large-scale healthcare adoption.

BLOCKCHAIN-DRIVEN SOLUTIONS TO DATA SECURITY CHALLENGES

ZKPs

ZKPs represent a class of cryptographic protocols that enable one party to prove the validity of a statement without revealing the underlying data. In healthcare, ZKPs are particularly valuable for ensuring privacy-preserving data sharing, enabling secure verification of patient identities, medical credentials, and compliance with regulatory frameworks such as the GDPR and HIPAA.

zk-SNARKs are characterized by their efficiency and compact proof sizes, making them suitable for applications where computational resources are limited. The cryptographic foundation of zk-SNARKs relies on elliptic curve pairings and a trusted setup phase, during which a common reference string is generated. While this setup enhances efficiency, it introduces a potential vulnerability if the common

reference string is compromised. In healthcare, zk-SNARKs have been deployed in projects such as MediLedger, where they are used to verify the authenticity of pharmaceutical products without exposing sensitive supply chain data (MediLedger DSCSA Pilot, 2023). This approach ensures compliance with regulatory requirements while maintaining data privacy. However, the reliance on a trusted setup and the computational overhead associated with zk-SNARKs pose challenges for large-scale healthcare implementations.

The application of ZKPs in healthcare extends beyond data verification to include secure access control and compliance auditing. For instance, ZKPs can be integrated into EHR systems to enable healthcare providers to verify patient eligibility for specific treatments without accessing the full medical history. This approach not only enhances privacy, but also ensures compliance with regulations such as the GDPR's "right to be forgotten." However, the adoption of ZKPs in healthcare is hindered by their computational complexity and the need for specialized expertise, which may limit their feasibility in resource-constrained settings.

In Figure 4 this sequence diagram represents how ZKPs are used to establish a user's identity and eligibility for healthcare services in a blockchain-based system.

The actors and components are:

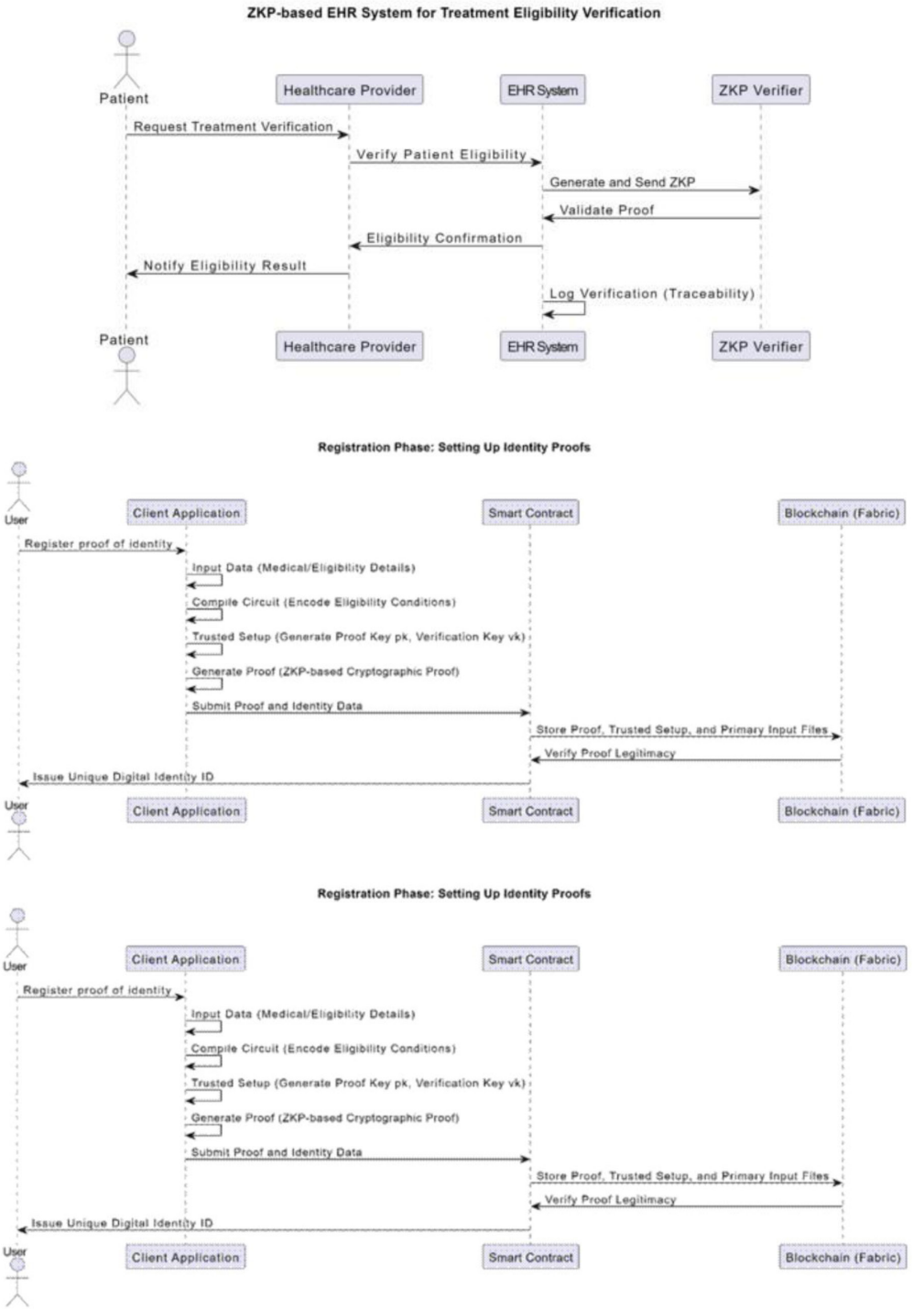
1. User: The individual registering their identity and eligibility.
2. Client Application: The interface used by the user to generate and submit cryptographic proofs.
3. Smart Contract: A blockchain-based contract that validates the proof and interacts with the ledger.
4. Blockchain: The distributed ledger that stores verified proofs securely.

Process Flow

The following are the process flow:

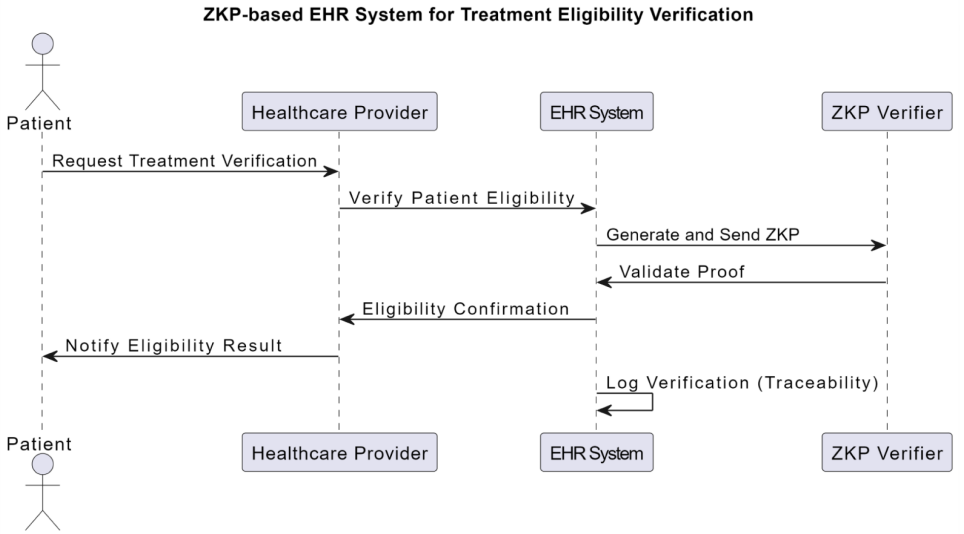
1. User Registration: The user initiates the registration by submitting identity and eligibility details via the client application.
2. Proof Generation: The client application processes the input data and executes cryptographic operations.
3. Compile Circuit: Encodes eligibility rules into a proof system.
4. Trusted Setup: Generates cryptographic keys.
5. Generate Proof: Creates a ZKP to validate eligibility without revealing sensitive details.
6. Proof Submission and Validation: The client application submits the proof and identity data to the smart contract. The smart contract then stores the proof data on blockchain.
7. Verification and Identity Issuance: The blockchain automatically verifies the proof's legitimacy. If valid, the smart contract issues a unique digital identity to the user, confirming their eligibility status.

Figure 4. ZKP-based identity & eligibility verification in healthcare blockchain



1. Patient Requests Treatment Verification: The patient submits a proof request to the EHR system, asking whether they qualify for a treatment.
2. EHR System Generates a ZKP: Instead of exposing the entire medical history, the system computes proof that verifies eligibility based on predefined medical criteria.
3. ZKP Verifier Validates the Proof: The proof is sent to the verifier, which checks its validity without learning any details about the underlying medical conditions.
4. Verifier Sends Confirmation to Healthcare Provider: If the proof is valid, the provider receives confirmation that the patient qualifies for the treatment.
5. Treatment Authorization and Traceability: The system logs the verification in an auditable record for compliance and regulatory purposes, ensuring GDPR compliance.

Figure 5. ZKP-based verification phase: Checking eligibility for treatment



Tokenized Access Control for Patient-Centric Data Management

Tokenized access control is a blockchain-based mechanism that empowers patients to manage access to their health data securely. By leveraging cryptographic tokens or smart contracts, patients can grant or revoke access to their medical records in real time, ensuring greater control and transparency. This approach addresses the limitations of traditional EHR systems, where patients often have little control over who accesses their data.

Smart Contracts

In blockchain-enabled EHR systems, smart contracts can automate access control by defining specific conditions under which data can be accessed. For example, a smart contract could grant a healthcare provider temporary access to a patient's records for a scheduled appointment and automatically revoke access once the appointment is completed (Azaria et al., 2016). This not only enhances security, but also ensures compliance with privacy regulations such as the GDPR's "right to be forgotten."

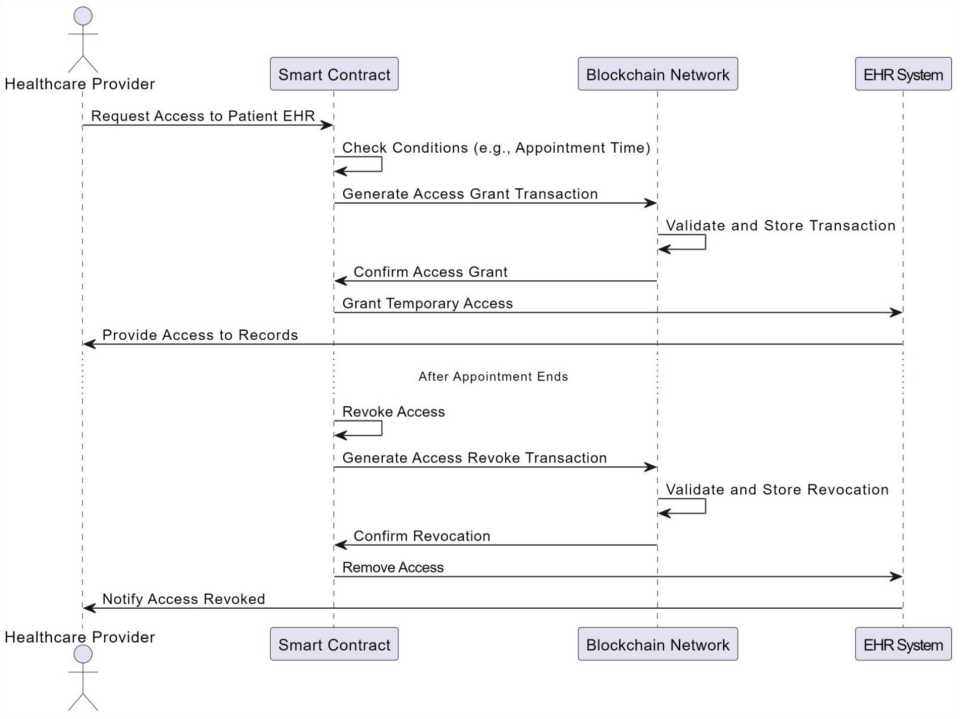
Figure 6 shows the sequence diagram description for blockchain-enabled EHR access control.

This sequence diagram illustrates how smart contracts automate access control in a blockchain-enabled EHR system. The diagram captures the process of granting and revoking access

to patient records based on predefined conditions, such as a scheduled appointment, as demonstrated in the following:

1. Healthcare Provider Requests Access: The healthcare provider submits a request to access a patient's EHR for a scheduled appointment.
2. Smart Contract Verifies Access Conditions: The smart contract checks whether the request meets predefined conditions, such as an upcoming appointment.
3. Blockchain Records Access Grant: If the conditions are met, the smart contract generates an access grant transaction and submits it to the blockchain network for validation and storage.
4. EHR System Grants Temporary Access: Once confirmed, the smart contract updates the EHR system, allowing the healthcare provider to retrieve the necessary medical records.
5. Automatic Access Revocation: After the appointment concludes, the smart contract triggers access revocation, generating a new blockchain transaction to remove access.
6. Blockchain Logs the Revocation: The revocation is validated and stored on the blockchain, ensuring transparency and compliance with privacy regulations such as the GDPR.

Figure 6. Sequence diagram description for blockchain-enabled EHR access control



Tokenization

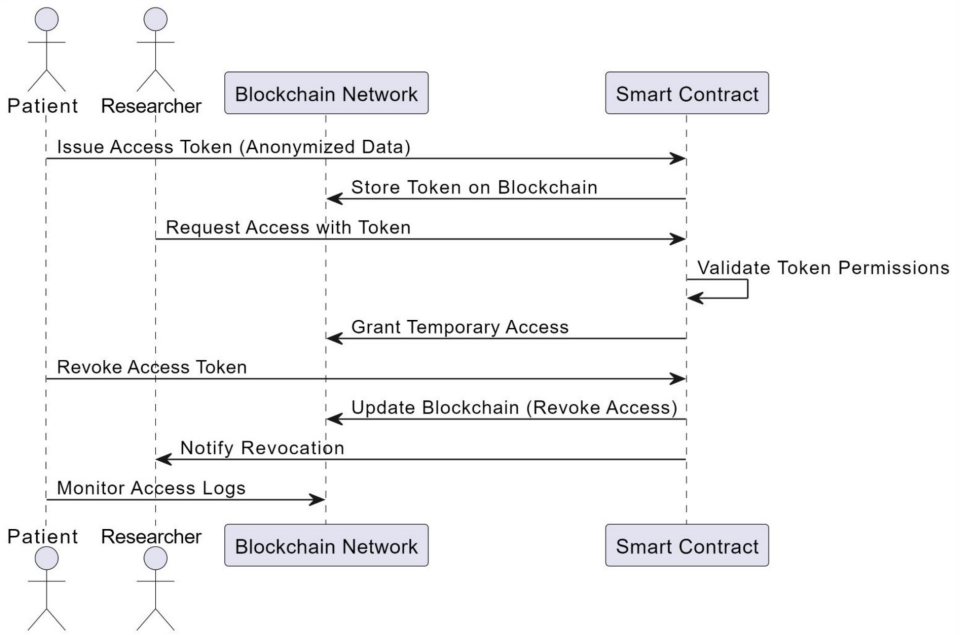
Tokenization uses digital tokens to represent access rights to healthcare data, allowing patients to manage whoever can view their information and under what conditions. For instance, a patient could create a token to grant a researcher access to anonymized health data while still having the ability to revoke that token at any time.

This system has been successfully implemented in Estonia's blockchain-based healthcare platform, where patients can track who is accessing their data and revoke permissions instantly. This model enhances patient control and transparency, ensuring that only authorized individuals can access sensitive medical information and providing real-time oversight. Such systems are revolutionizing data privacy and security, giving patients more power over their own health records (Guardtime, 2021). Figure 6 illustrates how tokenization works to secure access and grant permissions in healthcare systems, as shown in the following:

1. Patient Issues Access Token: The patient generates a cryptographic token and grants the researcher permission to access anonymized data.
2. Blockchain Stores Token: The token is securely stored on the blockchain via a smart contract.
3. Researcher Requests Data: The researcher submits the token to the smart contract for validation.
4. Smart Contract Validates Token: If valid, the smart contract grants access.
5. Patient Revokes Access: At any time, the patient can revoke the token.
6. Blockchain Updates and Notifies Researcher: The revocation is recorded, and the researcher loses access.
7. Patient Monitors Access Logs: The patient can track data access history in real time.

While tokenized access control offers significant advantages, it also faces challenges such as scalability and interoperability with legacy systems. Additionally, the reliance on cryptographic keys introduces the risk of key loss or theft, which could compromise patient data. Furthermore, the usability of tokenized access control systems for patients with limited technical expertise remains a concern, necessitating the development of user-friendly interfaces and educational resources.

Figure 7. Cryptographic token-based access control in healthcare



Addressing Poor Interoperability Among Healthcare Providers With Blockchain

One of the most persistent challenges in the healthcare sector is the lack of interoperability among healthcare providers. Fragmented data systems, incompatible standards, and isolated information often hinder the seamless exchange of patient data across different healthcare organizations. This lack of interoperability not only compromises the quality of care, but also increases the risk of medical errors, delays in treatment, and inefficiencies in healthcare delivery. Blockchain technology, with its decentralized architecture, cryptographic security, and immutable ledger, offers a transformative solution to enhance interoperability in healthcare. This section explores how blockchain-based solutions, such as decentralized data sharing, standardized protocols, and smart contracts, can address the issue of poor interoperability among healthcare providers. Each solution is critically analyzed in terms of its technical mechanisms, real-world implementations, advantages, limitations, and feasibility for large-scale healthcare adoption.

Decentralized Data Sharing for Seamless Information Exchange

Blockchain technology enables decentralized data sharing, allowing healthcare providers to securely exchange patient information without relying on a central authority. By storing data on a distributed ledger, blockchain ensures that all authorized parties have access to the same information in real time, reducing the need for redundant data entry and minimizing the risk of data inconsistencies.

Distributed Ledger Technology

In a blockchain-enabled healthcare system, patient data is stored across a network of nodes, each maintaining a copy of the ledger. This decentralized approach eliminates the need for a central data repository, which is often a bottleneck in traditional systems. Healthcare providers can access and update patient records in real time, ensuring that all parties have access to the most current information.

The blockchain interoperability pilot project leverages blockchain technology to explore the potential of decentralized data sharing across industries, including healthcare. This project focuses on creating a more connected and transparent system by ensuring that multiple stakeholders, such as healthcare providers, patients, and pharmaceutical companies, can access and share accurate, up-to-date information.

In healthcare, blockchain's ability to securely manage and share data is particularly valuable. Just like the MediLedger project in pharmaceutical supply chain management, which enables real-time tracking of pharmaceutical products, the blockchain interoperability pilot project aims to extend this model to patient data. This approach could allow healthcare providers to seamlessly access and update medical records while ensuring transparency, security, and trust. By using blockchain to streamline data sharing, the project can enhance interoperability across the healthcare ecosystem, improving efficiency and patient outcomes.

Despite its potential, decentralized data sharing faces challenges such as scalability and data privacy. The computational and storage requirements of blockchain networks can be prohibitive for large-scale healthcare applications. Additionally, ensuring compliance with privacy regulations such as the GDPR and HIPAA requires careful design and implementation of blockchain systems, particularly in areas such as data anonymization and access control.

Standardized Protocols for Enhanced Interoperability

Standardized protocols are essential for ensuring seamless communication between different healthcare systems. Blockchain technology can facilitate the development and adoption of standardized protocols for data exchange, enabling healthcare providers to share information more effectively.

HL7 Fast Healthcare Interoperability Resources

The HL7 Fast Healthcare Interoperability Resources (FHIR) standard is a widely adopted framework in healthcare that defines how to exchange health data electronically. By combining blockchain with FHIR, healthcare organizations can significantly improve how patient data is shared between different systems, breaking down traditionally siloed or isolated data structures that hinder interoperability.

Blockchain helps ensure that patient information is exchanged in a consistent and standardized way, reducing errors and making it easier for healthcare providers to communicate. For example, by using blockchain to store FHIR resources, healthcare organizations can verify that the data is accurate and up-to-date. This way, all parties involved—whether doctors, hospitals, or insurance companies—can access the same reliable information, improving the quality of care and reducing the chances of data inconsistencies or confusion.

By pairing blockchain's security and immutability with FHIR's data format standards, this integration provides a more efficient and trustworthy system for managing and sharing healthcare information.

Proof of Interoperability

In healthcare, different systems often struggle to communicate with each other, which can lead to inefficiencies and errors in patient care. To address this, Peterson et al. proposed a blockchain-based solution that ensures seamless data exchange across various healthcare platforms. This system integrates with FHIR, a standard for sharing healthcare information.

The unique feature of their approach is the proof of interoperability mechanism. In simple terms, it is a process that ensures all clinical messages or data submitted to the blockchain follow the necessary standards for healthcare information. Just like a quality control system, this mechanism requires miners (participants who validate the blockchain) to check if the submitted data meets the required rules—both in terms of structure and meaning.

To make this work, Peterson et al. used a special type of blockchain called a Merkle-tree-based blockchain, which is a way of organizing data efficiently. By making sure all data complies with FHIR standards, this system promotes smooth and secure data sharing between different healthcare providers, improving communication and reducing errors while maintaining the security and trust benefits of blockchain.

However, the adoption of standardized protocols in blockchain-based healthcare systems requires significant investment in infrastructure and workforce training. Additionally, the integration of blockchain with existing healthcare systems poses interoperability challenges and middleware solutions.

Blockchain technology offers solutions to many challenges in healthcare, including data security, patient autonomy, and interoperability. However, its true impact is best illustrated through real-world implementations. The following section explores how blockchain is being applied in healthcare systems worldwide, highlighting its role in improving medical records management, pharmaceutical supply chains, and clinical research integrity.

Applications of Blockchain in Healthcare

Blockchain technology presents several solutions to the critical challenges faced by traditional healthcare systems, particularly in the areas of data security, patient control, and traceability. Its unique features of decentralization, immutability, transparency, and patient-centric control address the vulnerabilities present in centralized healthcare databases.

The implementation of blockchain technology in the healthcare sector holds the potential for a significant transformation in the manner by which healthcare data are managed. This is due to the innovative solutions that blockchain technology offers in terms of enhancing security, transparency,

and efficiency. This section examines the impact of blockchain technology on security and innovation in the context of previously discussed healthcare applications.

Blockchain in Estonia's Healthcare System

Estonia, recognized as a global leader in digital governance, has effectively integrated blockchain technology into its healthcare system, setting an example of how innovative solutions can enhance efficiency, transparency, and patient empowerment. This case study examines the implementation of blockchain in Estonia's healthcare infrastructure, focusing on its mechanisms, impacts, and challenges.

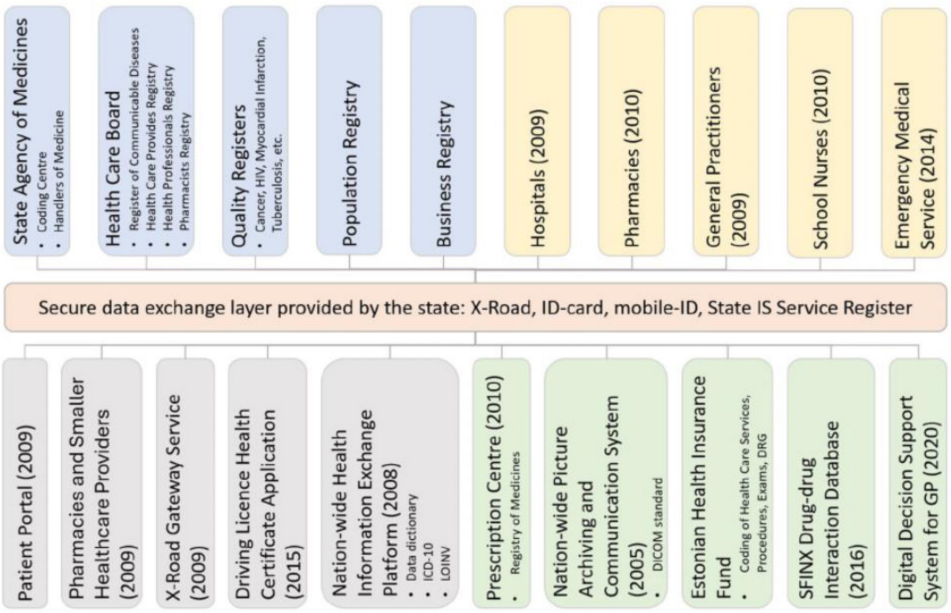
The cornerstone of Estonia's blockchain-enabled healthcare system is the keyless signature infrastructure (KSI) developed by Guardtime. Guardtime's KSI has been extensively documented as a pioneering solution in blockchain-based data integrity, providing tamper-evident verification mechanisms that enhance the reliability of critical digital systems (Guardtime, 2021). The KSI blockchain ensures the integrity of healthcare records by employing digital signatures, which provide tamper-proof verification of data authenticity. This system operates as a private, permissioned blockchain, meaning access is restricted to authorized entities. Data is processed through a hierarchical structure known as a hash tree, or Merkle tree, which enables efficient aggregation and verification of records. Each second, hashes of submitted data are aggregated into a global tree, and the root hash is stored on the KSI blockchain. This process ensures that any alterations to stored data would be immediately detectable (Guardtime, 2021).

The EHIS integrates various national registers, such as the population registry, quality registers, and health care board, which serve as centralized repositories for essential healthcare data. Key health service providers, including hospitals, pharmacies, general practitioners, school nurses, and emergency medical services, are connected to the system, enabling seamless data sharing to improve healthcare delivery. These services, deployed between 2009 and 2014, ensure a robust foundation for health information exchange. (Metsallik et al., 2018)

The architecture also incorporates central EHIS services, including the prescription center, the nationwide picture archiving and communication system, the Estonian health insurance fund, and the drug-drug interaction database. These services facilitate prescription management, medical imaging, insurance data handling, and clinical decision support. Additionally, external services, such as the patient portal and the nationwide health information exchange platform, utilize EHIS to provide patients and healthcare professionals with accessible and reliable digital tools.

The KSI blockchain supports the broader e-health initiative managed by Estonia's e-health foundation. This initiative encompasses various services, including secure digital medical records, e-prescriptions, and real-time access monitoring by patients. Through the X-road platform, a secure data exchange layer, healthcare providers can seamlessly access and share patient information, reducing administrative redundancies (E-Estonia, 2022). The integration of these technologies has allowed Estonia to digitize nearly all healthcare records, streamline operations, and enhance accessibility for both patients and medical professionals. One of the most notable outcomes of this integration is the significant improvement in efficiency. The streamlined processes have eliminated redundancies, saving an estimated 820 work-years annually, equivalent to approximately €5.6 billion in economic benefits (Bittroff & Sandner, 2020). Transparency has also been markedly improved, as patients are empowered to monitor access to their medical records in real time. This capability fosters accountability among healthcare providers and strengthens public trust in the system. Additionally, Estonia's e-prescription service, which issues 99.9% of prescriptions digitally, demonstrates how blockchain technology has reduced paperwork and minimized unnecessary visits to healthcare facilities (Kõnd & Lilleväli, 2019). The health portal, as seen in Figure 8 of the EHIS offers a user-friendly interface, enabling patients to access their health and medical data, submit declarations of intent, and view medical invoices. It also provides tools to restrict access to specific data sections and monitor activity logs, thereby ensuring transparency and accountability within the healthcare system.

Figure 8. The Estonian national health information system architecture



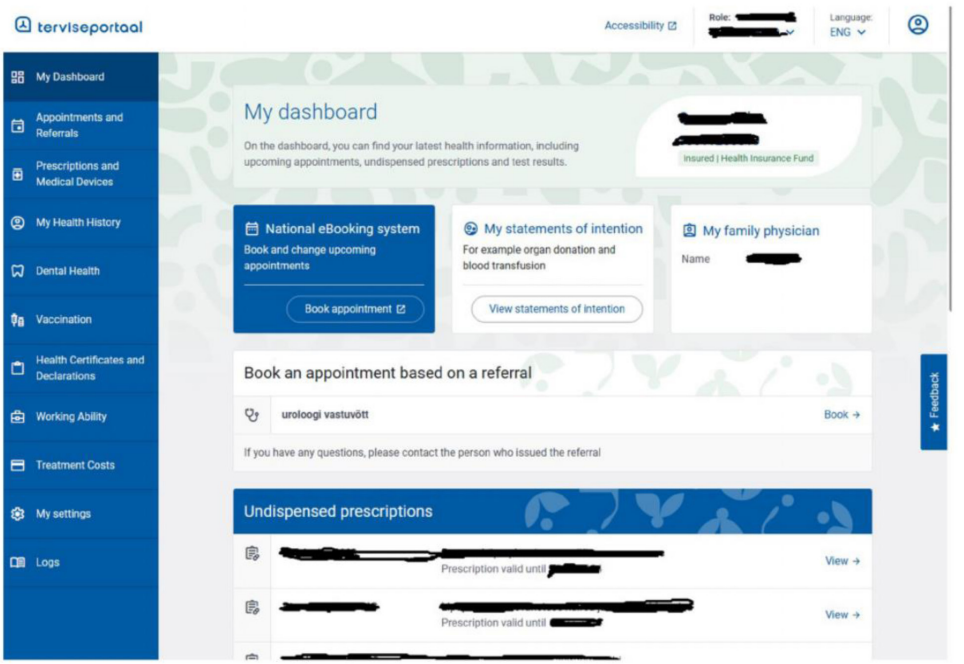
Despite its successes, the adoption of blockchain technology in Estonia's healthcare system faced challenges, particularly in achieving interoperability with legacy systems. This issue was addressed through the deployment of the X-road platform, which standardizes data exchange protocols and facilitates communication between various stakeholders. Estonia's healthcare system adheres to the GDPR, ensuring robust protection of patient data while enabling efficient health data management. A critical component of GDPR compliance is Article 17, which allows patients to request the deletion of personal data when it is no longer necessary for processing. Estonia addresses this through advanced pseudonymization and anonymization techniques within its blockchain framework.While Estonia has overcome challenges related to interoperability and the GDPR compliance, blockchain-based healthcare solutions, in general, often face limitations such as scalability, performance, and high costs. According to Mischa van Reede's analysis, these barriers are common in many blockchain projects, but Estonia's KSI blockchain demonstrates how these challenges can be mitigated. The KSI blockchain is highly scalable, capable of handling 10^12 signatures per second, far exceeding the capabilities of traditional blockchains (van Reede, 2020). Furthermore, KSI's performance is optimized, with response times 50% shorter and a 20% reduction in data storage costs compared to conventional blockchain solutions (van Reede, 2020). These improvements effectively address scalability and cost concerns, making the Estonian model a viable example for broader adoption in healthcare.

Looking ahead, Estonia's blockchain-enabled healthcare system continues to evolve, with initiatives focusing on cross-border interoperability and personalized medicine. The e-prescription system has already enabled patients to access medications in 12 European Union countries, including Finland, Croatia, and Spain. Furthermore, 20% of Estonia's population has contributed genetic data to the Estonian genome center, supporting research and the development of personalized treatment plans. Current applications include genetic-based drug recommendations and early detection of diseases such as breast cancer (Estonian Genome Center, 2023).

Despite the success of Estonia's model, challenges such as interoperability with legacy systems, scalability, and cybersecurity remain barriers to widespread blockchain adoption globally. However, Estonia's ability to navigate these hurdles—such as through the X-road platform for data exchange—

demonstrates how these challenges can be mitigated. As more countries look to modernize their healthcare infrastructures, Estonia's blockchain-driven system offers valuable insights into the transformative potential of decentralized technologies.

Figure 9. A screenshot from the health portal of the Estonian national health information system



MediLedger Pilot Project

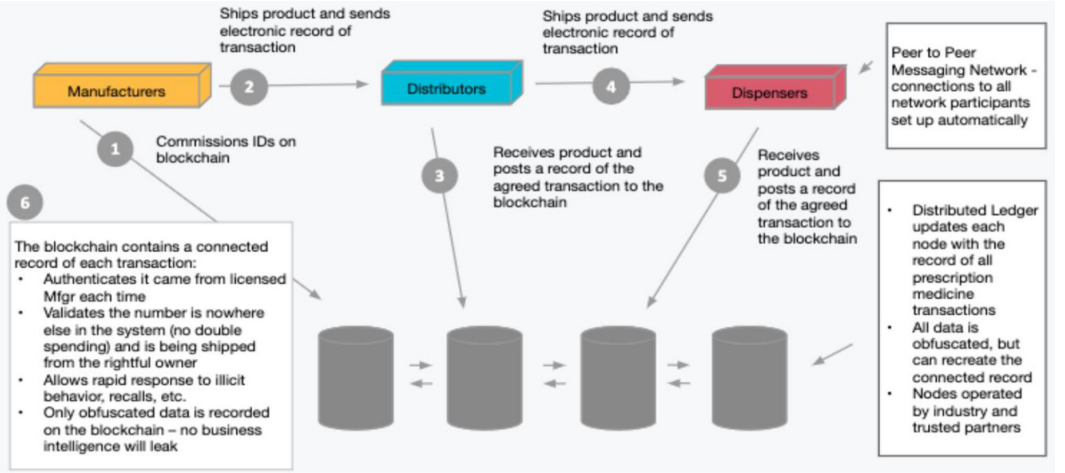
The MediLedger Drug Supply Chain Security Act (DSCSA) Pilot Project, a collaboration among key pharmaceutical industry players including AmerisourceBergen, Amgen, Cardinal Health, Genentech, and Pfizer, further explored blockchain's feasibility in meeting the requirements of the DSCSA, a U.S. federal law designed to enhance the security of the pharmaceutical supply chain. This project aimed to establish an electronic, interoperable system—one that enables seamless data exchange across different organizations and platforms—for tracking prescription medicines at the saleable unit and case packaging levels. By enhancing data sharing and system compatibility, the initiative addresses challenges related to fragmented supply chain data and ensures secure, verifiable transactions among participants (MediLedger DSCSA Pilot, 2023).

By leveraging blockchain, the pilot achieved high transaction throughput—over 2,000 transactions per second—sufficient to meet the American pharmaceutical market's peak demand of 4.5 billion prescription units annually. Each transaction was processed in under one second, enabling near real-time tracking and validation across the supply chain. Blockchain also provided robust data privacy through ZKPs, a cryptographic technique that allows verification of transaction validity without revealing sensitive data. Moreover, MediLedger introduced mechanisms for identifying counterfeit or suspect products, such as duplicate serial numbers or incorrect provenance, thereby reducing counterfeit risks and enabling faster recalls (MediLedger DSCSA Pilot, 2023).

The diagram, as seen in Figure 10, illustrates the MediLedger system, which uses blockchain technology to enhance the pharmaceutical supply chain's transparency and security. Manufacturers commission unique identities for products, which are authenticated and recorded on the blockchain.

Distributors and dispensers post transaction records to the blockchain as products are shipped and received. This system validates transaction integrity, prevents double spending, and ensures ownership. MediLedger supports rapid responses to recalls and illicit activities, with all data obfuscated to protect business intelligence. A peer-to-peer messaging network connects participants with nodes managed by trusted industry partners. Regarding supply chain transparency, blockchain technology enables authorized parties to monitor the progress of medicines in real-time, from production to delivery. This level of transparency facilitates the quick identification of issues such as delayed deliveries or temperature variations during transportation. Furthermore, regulatory authorities can readily access blockchain data for audits and compliance checks, ensuring that all distributed medicines meet quality and safety standards.

Figure 10. MediLedger blockchain system in pharmaceutical supply chain



The MediLedger project demonstrated operational cost reductions, estimating data storage costs at $4,000 annually for up to 100 terabytes. The total annual operating cost for the entire pharmaceutical industry was projected to be between $5 million and $10 million, a cost-effective solution for the system's scale. Beyond cost savings, blockchain's enhanced security capabilities facilitated real-time identification of counterfeit or stolen products, enabling faster recalls and more efficient investigations. Furthermore, MediLedger highlighted the importance of industry-led governance to standardize blockchain implementation and ensure interoperability across the pharmaceutical sector (MediLedger DSCSA Pilot, 2023).

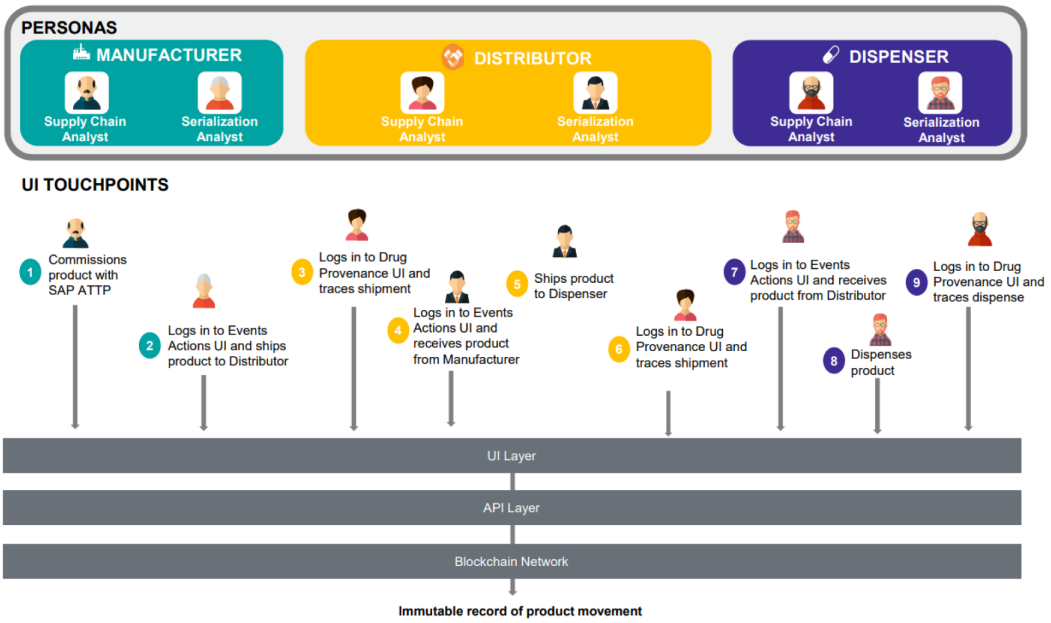
Despite its advantages, implementing blockchain in the pharmaceutical supply chain comes with notable challenges. Integrating blockchain systems with legacy supply chain management software requires significant investment in infrastructure, workforce training, and technical expertise. For example, early implementations of MediLedger faced interoperability issues with older enterprise systems, highlighting the need for standardized protocols (MediLedger DSCSA Pilot, 2023). Furthermore, the lack of global standards for blockchain technology creates fragmentation across international supply chains, complicating compliance with diverse regulatory frameworks like the drug supply chain security act and the European falsified medicines directive (European Medicines Agency, 2023). Smaller pharmaceutical companies and distributors, particularly in low-resource regions, often encounter barriers to adoption due to limited technical resources and financial constraints (Hammi et al., 2023).

Blockchain Interoperability Pilot Project

IBM, KPMG, Merck, and the Walmart pilot project demonstrated substantial improvements in the efficiency, security, and cost-effectiveness of the pharmaceutical supply chain through the integration of blockchain technology. This initiative aimed to address the regulatory requirements outlined in the drug supply chain security act while exploring the broader potential of blockchain to transform industry operations (FDA DSCSA Blockchain Interoperability Pilot, 2020).

Figure 11 illustrates how each organization's user personas can record product movement actions that are recorded in an immutable ledger on the blockchain. This visual representation highlights the transparency and traceability that blockchain brings to the pharmaceutical supply chain, which can be similarly applied to clinical trials to ensure the integrity and traceability of data throughout the study process.

Figure 11. Blockchain-enabled traceability in pharmaceutical supply chains and clinical trials



One of the pilot's most notable outcomes was the significant improvement in operational efficiency. Traditional processes for notifying supply chain partners of drug recalls often took up to three days, which posed substantial risks to patient safety and increased operational burdens. By leveraging blockchain technology, the pilot demonstrated that this notification process could be expedited to as little as 10 seconds. This drastic reduction in response time minimizes delays in isolating affected products, ensuring that impacted stakeholders can take immediate corrective actions. Additionally, the use of blockchain facilitated real-time traceability of pharmaceutical products across the supply chain. The system's ability to provide an immutable and transparent record of drug provenance eliminated reliance on manual processes and reduced errors associated with fragmented systems (FDA DSCSA Blockchain Interoperability Pilot, 2020).

The pilot also highlighted significant advancements in supply chain security. By utilizing a permissioned blockchain, the project ensured that data privacy was maintained and access to sensitive information was restricted to authorized participants. Furthermore, the integration of

serialization into the blockchain platform provided an additional layer of security. This feature ensured that drugs could not be dispensed more than once, effectively preventing the distribution of counterfeit or illegitimate medications. The immutable nature of blockchain records also enhanced trust among supply chain participants by providing verifiable evidence of a drug's journey from manufacturing to dispensation (FDA DSCSA Blockchain Interoperability Pilot, 2020).

Cost reduction was another critical outcome of the pilot project. The automation of recall processes significantly reduced the financial and operational costs associated with manual intervention and unnecessary quarantining of unaffected products. Additionally, the system's ability to streamline communication and eliminate inefficiencies across the supply chain contributed to further cost savings. While exact financial metrics were not disclosed, the reductions in pharmaceutical waste and operational overheads underscore the economic benefits of blockchain implementation (FDA DSCSA Blockchain Interoperability Pilot, 2020).

However, the IBM pilot project also highlighted significant challenges that resonate with the adoption of blockchain in clinical trials. One of the primary obstacles was achieving interoperability between disparate systems. In both pharmaceutical supply chains and clinical research, stakeholders often rely on a wide array of platforms that lack seamless integration. The project emphasized the need for developing standardized processes and robust frameworks to address this fragmentation (FDA DSCSA Blockchain Interoperability Pilot, 2020).

Another critical challenge lies in establishing governance models that ensure equity and inclusivity. The decentralized nature of blockchain, while a key advantage, requires collaborative decision-making to prevent dominance by a single entity. This challenge is equally relevant in clinical trials, where managing collaborative research across institutions demands transparent and fair governance structures.

Scalability and performance were also highlighted as pressing concerns in the pilot project. Managing large data volumes and ensuring timely response times are critical in pharmaceutical supply chains and clinical research. These challenges underscore the need for blockchain systems that can handle complex workflows, such as tracking serialized drugs or maintaining trial data integrity, without compromising speed or efficiency (FDA DSCSA Blockchain Interoperability Pilot, 2020).

Maintaining data privacy and provenance emerged as a further challenge, as blockchain's transparency must be balanced with strict confidentiality requirements. The project demonstrated how a permissioned blockchain could address this issue by granting access only to authorized stakeholders. Similarly, in clinical trials, ensuring the secure storage of sensitive patient data while maintaining traceability is essential to upholding both ethical and regulatory standards.

The exclusion of complex scenarios from the pilot project, such as reverse distribution or product returns, highlights the iterative nature of blockchain adoption. Likewise, clinical trials must continue to evolve blockchain applications to address intricate issues such as multi-phase studies and protocol deviations. These limitations, while significant, serve as opportunities for further refinement and innovation.

The IBM, KPMG, Merck, and Walmart pilot project successfully demonstrated the potential of blockchain technology to meet DSCSA compliance requirements while delivering measurable improvements in efficiency, security, and cost-effectiveness. These findings suggest that blockchain could play a transformative role in addressing key challenges in the pharmaceutical industry and enhancing patient safety. At the same time, the project underscored critical challenges, such as achieving interoperability, establishing equitable governance frameworks, ensuring scalability, and maintaining data privacy. Overcoming these barriers is essential for leveraging blockchain's full potential in transforming the pharmaceutical supply chain and clinical trials. Blockchain technology is revolutionizing the healthcare sector by addressing critical issues such as data security, patient control, and operational inefficiencies. Through innovative applications like medical records management, medicine traceability, and research data integrity, blockchain has demonstrated its potential to transform traditional systems into secure, transparent, and efficient ecosystems.

Table 2 summarizes the blockchain applications previously discussed, illustrating their benefits and real-world implementations and the challenges they address. This consolidated view helps highlight blockchain's versatility in addressing key healthcare challenges.

Table 2. Summary of blockchain applications in healthcare

Application	Area	Case Study Examples	Key Benefits	Challenges Addressed
Medical Records	Data security, access control, audit trail	Estonia	Interoperability, data integrity	Interoperability, data integrity
Pharmaceutical	Traceability	MediLedger	Counterfeit prevention, real-time tracking	Supply chain transparency
Clinical Trials	Data transparency, collaboration	IBM DSCSA Pilot	Data transparency, collaboration	Data manipulation, inefficiencies

The summarized case studies reveal blockchain's ability to tackle diverse issues in healthcare, from securing medical records to enhancing supply chain transparency and improving clinical trial processes. As the next section demonstrates, these applications provide a foundation for addressing broader security challenges.

This comparative overview highlights the versatility of blockchain technology in addressing critical healthcare challenges. Estonia's national healthcare system demonstrates the integration of blockchain for secure medical record management, ensuring data access control and audit trails. MediLedger addresses pharmaceutical supply chain inefficiencies by enabling real-time tracking and counterfeit prevention. Similarly, the IBM DSCSA Pilot showcases blockchain's role in enhancing clinical trial data transparency, fostering collaboration and improving stakeholder trust.

While the benefits of blockchain are significant, challenges persist, including interoperability with existing systems, regulatory compliance, and scalability. Addressing these barriers is crucial to unlocking the full potential of blockchain and building a secure, efficient, and transparent healthcare ecosystem.

Case studies such as Estonia's healthcare system and the MediLedger initiative underscore blockchain's ability to mitigate challenges like data integrity, counterfeiting, and inefficiencies. At the same time, they highlight the need to overcome hurdles such as scalability and compliance for broader adoption.

As blockchain continues to evolve and reshape the healthcare landscape, it introduces new opportunities and challenges. In the following section, we explore its role in enhancing security, mitigating risks, and addressing emerging concerns surrounding data protection and system integrity

CHALLENGES OF BLOCKCHAIN IN HEALTHCARE: SECURITY, COMPLIANCE, AND ETHICS

Security Implications of Blockchain in Healthcare

Blockchain technology is considered as a robust and secure data storage solution. However, it is still vulnerable to threats, as attackers are becoming increasingly ingenious at penetrating blockchain networks to obtain funds or interfere with normal operations. This section offers a summary of the most prevalent attacks on blockchain systems (Guru et al., 2023; Kaushik & El Madhoun, 2023).

The 51% Attack

This type of attack typically occurs in public blockchains that employ the PoW consensus mechanism when an individual or group of attackers secures control of more than 51% of the network's hash power. With this dominant position, they can manipulate the validation process for new blocks, reverse transactions by creating longer branches of the blockchain, or execute double-spending by validating a transaction on the main chain while simultaneously canceling it on a separate chain that they continue to develop secretly (Ye et al., 2018). Below are documented cases involving Ethereum Classic and Bitcoin; these illustrate the practical risks and resilience of PoW systems.

Ethereum Classic, a PoW blockchain diverged from Ethereum, suffered 51% attacks in January 2019 and August 2020 and three repeated attacks in a month, resulting in the theft of more than $6.7 million (Badertscher et al., 2021; Berg, 2020).

In the context of healthcare, a 51% attack could lead to the unauthorized alteration of medical records, fraud, or financial manipulation. For example, an attacker could modify EHRs to introduce fraudulent data, potentially leading to incorrect diagnoses or treatments. Additionally, if blockchain is used for insurance claims processing, an attacker could falsify transactions, causing financial fraud and disrupting patient care (Agbo et al., 2019; Vazirani et al., 2020). The decentralized trust that blockchain offers would be severely undermined if a malicious actor successfully executed such an attack.

Sybil Attack

This attack occurs when a malicious actor creates many fake identities in a decentralized network to gain control and disrupt operations (Hammi et al., 2022). By utilizing these fake identities, the attacker can exert disproportionate influence over the network, potentially disrupting consensus or reputation systems. This could involve manipulating votes for protocol changes or engaging in actions that undermine trust and security, such as fraudulently confirming invalid transactions or blocks (Hafid et al., 2022). In healthcare, a Sybil attack poses a serious threat to data integrity, security, and privacy by exploiting the trust model of blockchain networks. A malicious actor could manipulate clinical trial data by controlling multiple fraudulent identities, altering research outcomes, and potentially influencing drug approval processes in harmful ways. In patient data-sharing networks, such an attack could enable unauthorized entities to gain access to sensitive medical records, leading to severe privacy violations and non-compliance with regulations such as the HIPAA and GDPR. By overwhelming the network with fake nodes, an attacker could also disrupt legitimate transactions, delaying critical medical updates or obstructing access to essential healthcare services. While many healthcare blockchains rely on permissioned or hybrid models to mitigate Sybil risks, the threat remains significant in public blockchain implementations, where identity verification mechanisms may be weaker. To counteract these threats, researchers have proposed various solutions. For instance, Raghav and Bhola (2023) suggest using a universal unique identifier code to prevent Sybil attacks in blockchain-based healthcare systems. Additionally, Iqbal and Matulevičius (2021) explore security risk management frameworks to address Sybil and double-spending risks in blockchain systems.

Routing Attack

A routing attack disrupts the communication between computers, or nodes, in a blockchain network by interfering with the flow of data. The attacker may use techniques such as border gateway protocol hijacking, which involves manipulating internet routing paths to redirect data, or a man-in-the-middle attack, where the attacker secretly intercepts and potentially alters communications between two parties without their knowledge. These attacks can cause delays in the sharing of new blocks, isolate specific nodes from the network, or expose sensitive information (Chaganti et al., 2022).

In this context, a blockchain network refers to a group of interconnected computers that collectively maintain the blockchain. Border gateway protocol hijacking manipulates how internet traffic is routed, tricking data into passing through the attacker's path. A

man-in-the-middle attack allows an attacker to intercept and alter communication without detection. Block propagation refers to the process of distributing new data, or blocks, to all nodes in the network.

In the healthcare sector, routing attacks present a significant threat by compromising the integrity and reliability of blockchain-based systems. Medical transactions, such as prescription issuance, test results, and insurance approvals, may be intercepted before reaching their intended recipients, resulting in delays that could hinder critical healthcare services. Attackers could alter or discard blockchain updates, leading to inconsistencies in patient records that undermine the accuracy and trustworthiness of medical information. When blockchain is employed for medical device monitoring, a routing attack could disrupt real-time updates on patient conditions, potentially causing life-threatening delays in care. Given that healthcare networks integrate multiple interconnected systems, routing attacks may also serve as entry points for more extensive security breaches. By exploiting vulnerabilities in hospital networks or cloud-based health services, attackers could manipulate blockchain communications to gain unauthorized access to sensitive medical data, posing a severe risk to patient privacy and system security.

Double Spending Attack

In this attack, an adversary spends the same unit of digital currency multiple times. The attacker successfully sends a transaction to one recipient and then quickly initiates another transaction using the same funds directed to another destination under their control. If the attacker can manipulate the network so that the second transaction is confirmed before the first, they can effectively spend the same amount twice. This attack is particularly feasible on blockchains without robust double-spending prevention mechanisms, such as multi-node transaction confirmation (Begum et al., 2020).

In healthcare, a double spending attack poses a significant threat by exploiting vulnerabilities in blockchain consensus mechanisms and transaction validation processes. By submitting the same insurance claim multiple times, attackers could commit financial fraud, leading to unnecessary payouts and resource misallocation. Duplicate prescription transactions could enable patients to obtain excess medication illegally, increasing the risk of drug abuse and black-market distribution. Manipulating supply chain records may result in falsified transactions within pharmaceutical logistics, potentially allowing counterfeit drugs to enter the system and compromise patient safety.

Smart Contract Vulnerabilities

These arise from coding or logical errors in smart contracts deployed on the blockchain, including poorly designed functions, data manipulation errors, or unforeseen security flaws. Attackers can exploit these vulnerabilities to misappropriate funds, manipulate contract behavior, or disrupt automated processes. This includes attacks such as reentrancy (where one contract maliciously and repetitively calls another), numerical overflows or underflows, or exploiting function visibility issues (Khan & Namin, 2020).

In the healthcare sector, vulnerabilities in smart contracts can lead to severe security and privacy risks, undermining the integrity of blockchain-based medical systems. Poorly implemented access control mechanisms may allow unauthorized parties to gain access to sensitive patient records, violating privacy regulations and exposing individuals to potential misuse of their medical information. Automated billing systems reliant on smart contracts could be exploited to generate fraudulent claims or overcharge patients and insurers, resulting in financial losses and inefficiencies. Manipulation of clinical trial data through smart contract vulnerabilities may lead to altered research outcomes before they are permanently recorded, compromising the reliability of medical studies and regulatory decisions.

A well-documented example of smart contract vulnerabilities is the decentralized autonomous organization hack in 2016 on the Ethereum blockchain, where a reentrancy attack led to significant financial losses. The decentralized autonomous organization raised approximately $150 million in Ether before being exploited, resulting in the theft of about 3.6 million Ether, valued at around $50

million at the time. The attack took advantage of flaws in the smart contract's code, specifically a reentrancy vulnerability that allowed the attacker to repeatedly withdraw funds without updating the contract's balance (Mehar, 2019). Similar weaknesses in healthcare blockchain systems could jeopardize patient privacy, financial security, and compliance with industry regulations. The implications of such vulnerabilities highlight the need for robust security measures in blockchain applications, especially those handling sensitive data like healthcare information.

Mitigation Strategies

In this section, we discuss the various prevention strategies that healthcare applications using blockchain can adopt to mitigate the prevalent attacks on blockchain technology.

Preventing 51% and Sybil Attacks

Utilizing permissioned blockchains can effectively prevent 51% and Sybil attacks. The prevention strategies vary depending on the application type (Asiri & Miri, 2018).

In medical records management, blockchain nodes are exclusively operated by accredited medical entities, such as recognized hospitals and healthcare organizations. These nodes are selected based on stringent criteria related to data security compliance and computing capabilities. Implementing specific consensus mechanisms, like PoA, enhances security by restricting new block creation to trusted entities. In medicine traceability, incorporating nodes managed by pharmaceutical regulatory authorities ensures rigorous oversight. Appropriate consensus mechanisms may include variants of PoS, where the ability to validate transactions correlates with the reputation or commitment of the regulatory nodes.

In research and clinical trials, nodes run by recognized research institutions help guarantee data integrity and can employ hybrid consensus systems. These systems may combine validation by authorized entities with algorithmic methods to detect and thwart attempted takeovers.

Preventing Routing Attacks

Securing communication channels is essential to avoiding routing attacks. The prevention strategies vary by application type (Iqbal & Matulevicius, 2021).

In medical records management, virtual private networks specifically designed for secure medical data transfer can be implemented. These virtual private networks utilize advanced encryption protocols, such as Transport Layer Security (TLS) and its predecessor, Secure Sockets Layer (SSL), which establish encrypted connections to ensure the confidentiality and integrity of data during exchanges between hospitals and practitioners. TLS, the more secure and updated version of SSL, is widely used to protect sensitive healthcare information from interception and tampering. Additionally, network segmentation techniques can be employed to isolate sensitive data and protect it from unauthorized access.

In the traceability of medicines, secure channels must be established between distributors and pharmacies, using end-to-end encryption technologies to ensure that the data related to medicine movement remains secure and unaltered. Moreover, employing asymmetric cryptography guarantees that only authorized parties can access and verify the authenticity of traceability information. In research and clinical trials, safeguarding the data exchanged among various involved parties requires particular attention. Employing encryption protocols tailored to this field ensures the security of sensitive information.

Preventing Double Spending Attacks

To mitigate double-spending attacks in healthcare applications, specific technical strategies should be implemented for each application type (Akkaoui et al., 2020).

In medical records management, implementing the PoA consensus protocol is vital, as only authorized nodes from recognized healthcare entities can validate

transactions. This approach enhances record integrity by preventing duplicate entries. Additionally, a layered verification system is utilized, requiring multiple authorized nodes to validate each transaction, adding an extra layer of security.

In medicine traceability, multi-node validation mechanisms involve participation from various stakeholders in the pharmaceutical supply chain, including manufacturers, distributors, and pharmacies. Each transaction (i.e., the transfer of a medication batch) must be validated by several entities to ensure that no single unit of medication is recorded more than once. This decentralized yet coordinated method effectively prevents attempts to double-count within the system.

In research and clinical trials, ensuring data integrity involves employing appropriate consensus protocols, such as modified versions of PoS or proof of elapsed time. In these protocols, data validation depends on the reliability and reputation of the research institutions involved in the blockchain, ensuring that clinical trial data is not falsified or inaccurately recorded.

Preventing Smart Contract Vulnerabilities

Regular security audits and penetration testing for smart contracts can help prevent vulnerabilities (Kongmanee et al., 2019; Sayeed et al., 2020).

In medical records management, conducting regular security audits, especially for compliance with healthcare data protection standards like the HIPAA, includes thorough penetration tests to identify potential security weaknesses. Continuous monitoring of smart contracts can also ensure that modifications or updates comply with patient data confidentiality requirements.

In medical traceability, smart contracts should incorporate built-in defenses against data manipulation and errors. They must feature cross-validation of transactions at each step in the supply chain and automated clauses to flag inconsistencies. Regular audits should be conducted to ensure compliance with pharmaceutical regulations and to prevent unauthorized data alterations.

In research and clinical trials, smart contracts should integrate advanced security clauses to protect sensitive data. These clauses may include mechanisms for encrypting data both at rest and in transit, along with automated verification protocols to ensure the integrity of collected data. Frequent audits must be performed to ensure that these contracts adhere to the strict ethical and regulatory standards governing clinical research.

Regulatory Compliance Challenges

The integration of blockchain technology into healthcare systems offers promising advancements in data management, security, and interoperability. However, it also presents significant regulatory compliance challenges, particularly concerning frameworks such as the HIPAA in the United States and the GDPR in the European Union. This section examines these challenges and their implications for healthcare organizations.

HIPAA Compliance Challenges

The Health Insurance Portability and Accountability Act (HIPAA) is a critical regulation in the United States that mandates the protection of protected health information (PHI). However, blockchain's immutability poses significant challenges in relation to HIPAA's requirements, particularly the right to amend health records. According to HIPAA's Privacy Rule, patients have the right to request modifications or corrections to their health records if they contain errors or if new medical information arises (HHS, 2013). However, once data is written to a blockchain, it becomes permanent and cannot be modified, which directly conflicts with HIPAA's stipulation that records must be amendable (Benchoufi & Ravaud, 2017). This feature of blockchain becomes problematic, especially in situations where a patient requests changes or updates to their health records, such as when errors are discovered or additional treatments are needed. Researchers have suggested hybrid blockchain solutions—where off-chain storage mechanisms enable compliance with HIPAA while maintaining the security and integrity benefits of blockchain (Kuo et al., 2017).

The central issue concerning HIPAA compliance with blockchain lies in the immutability of blockchain data. The HIPAA guarantees patients the right to amend their health records to correct errors or add new information. Once data is written onto the blockchain, it becomes permanent and cannot be modified, creating a direct conflict with the HIPAA requirement for data amendment (Pollak, 2006). This challenge is explored in Charles et al. (2019), who explain that blockchain's permanent record makes it difficult to meet the HIPAA's provision that health information should be editable. To address this, Hasselgren et al. (2020) suggest incorporating hybrid blockchain models, where sensitive data is kept off-chain, while the blockchain records transaction metadata and hashes. This would preserve the integrity and auditability features of blockchain without conflicting with the requirement to modify health records. This off-chain solution allows healthcare providers to amend or delete sensitive health data, which aligns with the HIPAA's data amendment requirements while still benefiting from blockchain's secure framework.

Another significant challenge is related to data access control. The HIPAA mandates that PHI be accessed only by authorized individuals who require it for treatment, payment, or healthcare operations. The decentralized nature of blockchain makes it inherently difficult to ensure that only authorized parties have access to sensitive health data. In public or permissionless blockchains, this issue is even more pronounced, as the transparency feature of blockchain enables any participant in the network to potentially view all data unless strict access control mechanisms are integrated (Reinhardt, 2019). As Hasselgren et al. (2020) note, implementing robust access controls in blockchain applications can mitigate this issue by using advanced encryption techniques, multi-signature protocols, and public key infrastructures to secure data transmission and ensure that only authorized individuals or entities can access PHI.

GDPR Compliance Challenges

Similar to the HIPAA, the GDPR sets forth strict regulations regarding the processing and storage of personal data, with a particular emphasis on data subject rights and data privacy. However, blockchain's immutable and decentralized design presents challenges in complying with several key provisions of the GDPR, particularly with the right to be forgotten and accountability.

The right to be forgotten allows individuals to request the deletion of their personal data under certain conditions. Blockchain's immutability creates a direct conflict with this right, as once data is recorded on a blockchain, it cannot be erased. This presents a significant challenge for healthcare applications that rely on blockchain to store personal health data. As Hasselgren et al. (2020) explain, healthcare organizations may need to maintain the ability to erase patient data or grant patients the ability to control the removal of their data when necessary. Blockchain's transparent and unalterable ledger makes this particularly difficult, especially if patient consent or preferences change or if the data is incorrect. The solution, according to Charles et al. (2019), lies in using hybrid blockchain systems, where sensitive data is kept off-chain, but the integrity of the transaction and metadata is maintained on-chain. This approach would allow the deletion of sensitive information stored off-chain, thereby providing a way to comply with the right to erasure while retaining the benefits of blockchain's auditability.

In addition to the right to be forgotten, the GDPR mandates clear accountability regarding the processing of personal data. The decentralized nature of blockchain introduces ambiguity about who is responsible for ensuring compliance, as it lacks central authority. According to Charles et al. (2019), in public blockchain systems, where multiple independent participants are involved in processing data, it is often unclear who assumes the role of the data controller or data processor. This creates challenges in assigning accountability, as blockchain's distributed ledger does not inherently designate responsibility for ensuring that the principles of the GDPR—such as data minimization and purpose limitation—are respected. To address these challenges, blockchain developers could consider using permissioned blockchain networks, where participants are pre-approved and can be held accountable for processing data (Hasselgren et al., 2020).

Furthermore, smart contracts could be deployed to automate the tracking of data usage and ensure that each transaction complies with the GDPR's transparency and consent requirements.

Finally, the GDPR requires that personal data be anonymized or pseudonymized to protect individuals' privacy. While blockchain can pseudonymize data, its transparency presents challenges in ensuring that data is fully anonymized, as individuals may be re-identified through cross-referencing blockchain data with external sources. As Charles et al. (2019) suggest, blockchain applications in healthcare could use ZKPs and advanced cryptographic techniques to ensure that sensitive personal health data is not exposed while maintaining the integrity of the system. These techniques would allow verification without revealing sensitive information, aligning with the GDPR's goal to protect privacy while ensuring the system's integrity.

Proposed Solutions and Design Considerations

To overcome these regulatory challenges, several design strategies can be employed. First, hybrid blockchain models offer a promising solution by combining blockchain's integrity and auditability with off-chain data storage. This ensures that the GDPR's right to be forgotten and the HIPAA's right to amend are respected while preserving the benefits of blockchain's immutability for critical metadata.

Second, the use of smart contracts can automate data access and consent management, ensuring that patients have control over who accesses their health data and for what purposes. Smart contracts can also help track and enforce compliance with both the HIPAA and the GDPR, particularly by automating the collection and revocation of consent (Charles et al., 2019).

Lastly, adopting permissioned blockchains and cryptographic privacy techniques like homomorphic encryption and ZKPs can mitigate concerns about data access and ensure that sensitive data is only visible to authorized entities, thus satisfying regulatory requirements for privacy and accountability (Hasselgren et al., 2020).

Blockchain technology offers transformative healthcare potential, particularly in data security, interoperability, and privacy. However, its adoption in healthcare must navigate complex regulatory landscapes such as the HIPAA and GDPR. The immutability, decentralization, and transparency of blockchain introduce conflicts with several key provisions of these privacy laws, particularly around data modification, deletion, and access control. By employing hybrid blockchain models, smart contracts, and advanced cryptographic techniques, healthcare applications can be designed to comply with regulatory standards while preserving the security, transparency, and integrity that blockchain offers.

Ethical Considerations

The ethical implications of blockchain technology are crucial to its successful adoption, especially in the healthcare sector. While ethical challenges in information systems and emerging technologies have been widely studied, research specifically addressing blockchain ethics remains limited. As blockchain technology permeates diverse sectors, it becomes imperative to evaluate its potential ethical and moral challenges to ensure responsible implementation (Tang et al., 2018).

In blockchain, ethical frameworks have been applied differently. Tang et al. (2018) suggest that ethical issues in complex technologies like blockchain cannot be simplistic. They present an ethics framework for blockchain, categorizing issues into three levels: micro (technological domain), meso (application-specific issues), and macro (impact on institutions and society). While these issues share commonalities, their implications vary depending on the application. Dierksmeier and Seele (2020) use classical ethical frameworks to classify blockchain's morally favorable, unfavorable, and ambivalent aspects, particularly in trust, job platforms, and privacy. These studies emphasize the need for regulatory mechanisms to ensure blockchain transparency, participation, and openness.

Across different blockchain applications, ethical considerations can be grouped into common parameters:

1. Accountability is a cornerstone of ethics, requiring individuals and organizations to take responsibility for their actions and be liable for any harm caused. This becomes particularly important in blockchain applications, where the responsibility for actions must be traced to either human or software agents (Thekkilakattil & Dodig-Crnkovic, 2015).
2. Fairness in blockchain means ensuring non-discrimination and inclusion. However, blockchain technologies, like cryptocurrencies, can exacerbate existing social biases and inequalities (Lapointe & Fishbane, 2018). Achieving fairness requires understanding the social context in which the technology operates and its potential unintended consequences (Selbst et al., 2019).
3. Privacy in blockchain concerns how personal data is collected, processed, and used (Birnhack, 2011; Lazaro & Le Métayer, 2015). While blockchains ensure transparency, they can also raise privacy concerns, especially in public blockchains where access to data is unrestricted. Privacy challenges must be addressed both at the technological and application levels (Tang et al., 2018).
4. Accuracy blockchain ensures accuracy by validating data, but challenges like "zero-state" issues remain, especially with historical data that precedes the blockchain (Lapointe & Fishbane, 2018). For example, falsified records before the blockchain's inception could affect the accuracy of the entire system, such as in land title registries.
5. For data access, in terms of information technologies, access defines how a person can interact with and use any system. Access addresses what and how much information can be accessed, when access will be permitted, who will grant permissions, and what mechanisms will be used to safeguard access. It is also essential to identify and establish that data is used only for the purpose for which it was collected and should be used only by authorized persons after obtaining explicit consent. Any other use of the data may be conditional or prohibited. Even with explicit consent, the need to guarantee it is used appropriately is essential. Transparency in blockchains means that all nodes have access to all data in the chain. Such high visibility of all transactions can be intrusive for the individual's privacy, more so in the case of public blockchains that are accessible to anyone. In terms of blockchain, according to Lapointe and Fishbane (2018), ethical issues pertaining to access imply clear definitions about the scope of access and who can access it while having mechanisms to prevent exploitation.
6. Data ownership blockchain's decentralized nature empowers users to control their data, but issues like data ownership and control remain unresolved. Ethical dilemmas arise over who owns the data and how it is processed, especially when individuals have limited access or understanding of blockchain systems. Further, issues pertaining to data subjects having the right to access their personal data, verify its accuracy, and request correction are also required. Despite the decentralized nature of the operation, the ethical dilemmas around digital literacy, and the effective ability to access the system, also become important in the context of blockchains.
7. Governance in blockchain refers to decision-making processes and authority structures, whether centralized or decentralized. Thus, it has a direct impact on organizational operations. In the context of blockchains, governance is based on the models of authority structure and the extent to which decision-making processes are automated. While these are more specific to defining the governance structure, a more important ethical dilemma of blockchain implementation appears at the algorithmic level. Algorithmic governance implemented via smart contracts, while desirable for preventing criminal activities, may also lead to discrimination. Individuals whose public key has been erroneously associated with a criminal identity—based on limited and potentially flawed data, as discussed by Lazaro and Le Métayer (2015)—could face unjust restrictions. As organizations see the immense potential of blockchains, pertinent questions are raised with respect to the algorithm.

FUTURE DIRECTIONS

The integration of the IoMT, AI, and blockchain technology is set to revolutionize healthcare delivery, enhancing patient outcomes, improving operational efficiencies, and ensuring data security. This comprehensive analysis explores the future directions of these technologies, focusing on their synergistic potential and real-world applications and the challenges that must be addressed to fully realize their benefits.

Blockchain's Role in Securing IoMT Data

The integration of blockchain technology into IoMT systems addresses critical data privacy and security concerns. Blockchain's decentralized architecture ensures that patient data is stored securely and is immutable, thereby enhancing data integrity and traceability (Benaich, 2023; Ghadi, 2024). This is particularly important in healthcare, where sensitive patient information is frequently exchanged among various stakeholders. By utilizing blockchain, healthcare providers can ensure that data sharing is conducted securely, with a transparent audit trail that tracks who accessed the data and when (Al-Aswad et al., 2021; Handayani, 2023).

Blockchain technology can also enhance patient consent management, allowing patients to control who has access to their health information. This capability is crucial in fostering trust between patients and healthcare providers, as patients are more likely to share sensitive information when they know it is protected (Mallick et al., 2023; Rattanawiboomsom, 2023). Furthermore, blockchain can facilitate interoperability among different healthcare systems, enabling seamless data exchange while maintaining stringent security protocols (Srivastava et al., 2022; Zhao et al., 2018).

The integration of blockchain technology into IoMT enhances data integrity, security, and accessibility. A blockchain-based IoMT ecosystem enables a patient-centric model, where health data is owned and controlled by the patient rather than centralized entities (Griggs et al., 2018). This model ensures that data generated by IoMT devices are filtered through intelligent systems that determine their relevance and securely store them on the blockchain when necessary.

Blockchain for Secure IoMT Networks

Blockchain has been proposed as a solution to IoMT security challenges by integrating decentralized, tamper-resistant data storage with real-time access controls. For example, Griggs et al. (2018) introduced a wireless body area network integrated with blockchain technology to enable secure, real-time patient monitoring. This system evaluates patient health data based on personalized threshold values, ensuring that only relevant information is stored while reducing unnecessary data transmission.

Similarly, Zhang et al. (2017) proposed a blockchain-enabled pervasive social network model to enhance secure data sharing among multiple healthcare nodes. Their solution includes two distinct protocols: an IEEE-based secure link protocol optimized for low-computation mobile devices and a blockchain-based data-sharing mechanism that ensures tamper-proof data exchange.

Other researchers have explored hybrid solutions, combining centralized and decentralized architectures for scalable blockchain-based IoMT systems (Fan et al., 2018). By dividing networks into edge and core layers, these models improve efficiency, scalability, and adaptability to dynamic healthcare environments.

However, the implementation of blockchain in IoMT systems is not without challenges. Issues such as scalability, regulatory compliance, and the need for standardization must be addressed to ensure the successful integration of blockchain technology in healthcare (Han et al., 2022). Solutions such as off-chain storage for large datasets and the development of regulatory frameworks that accommodate blockchain's unique characteristics are essential for overcoming these barriers (Haddad et al., 2022; Zheng et al., 2017).

Blockchain-AI Integration in Healthcare

The convergence of AI and blockchain presents a transformative opportunity for healthcare systems. By securing AI-driven healthcare models with blockchain technology, organizations can enhance data security while automating data processing and decision-making in patient care (Khatoon, 2020; Sicari et al., 2022). For instance, AI algorithms can analyze patient data stored on a blockchain to identify trends and make predictions, while the blockchain ensures that this data remains secure and tamper-proof. The potential benefits of this integration are substantial. AI can improve the accuracy of diagnoses and treatment recommendations, while blockchain can provide a secure framework for sharing this information among healthcare providers (Ali, 2023). However, the integration of these technologies also raises technical and ethical challenges, including issues related to data access management, scalability, and regulatory compliance. Addressing these challenges will require collaboration among stakeholders, including healthcare providers, technology developers, and regulatory bodies, to establish best practices and standards for the use of AI and blockchain in healthcare.

Ethical, Legal, and Regulatory Considerations

The implementation of AI, IoMT, and blockchain in healthcare raises significant ethical, legal, and regulatory challenges. Issues such as patient privacy, data sovereignty, and compliance with existing regulations—including the GDPR in the European Union and the HIPAA in the United States—must be carefully navigated (Linn & Koo, 2016). These regulations aim to ensure that patient data is handled securely and transparently while maintaining patient autonomy over their health records (Kshetri, 2018).

One of the primary concerns regarding blockchain-based healthcare systems is the immutability of data. While blockchain ensures tamper-proof record-keeping, it also raises challenges in data modification and patient rights, particularly regarding the right to be forgotten, as stipulated in the GDPR (Shahnaz et al., 2019). The integration of privacy-preserving mechanisms, such as ZKPs and off-chain storage, can help address these legal concerns while maintaining the benefits of decentralization (Zheng et al., 2017).

To address these regulatory and ethical issues, healthcare stakeholders must develop robust data governance frameworks that prioritize patient rights, consent management, and security standards. These frameworks should integrate smart contract-based access control systems that allow patients to define granular permissions for their medical records (Azaria et al., 2016).

Additionally, ongoing stakeholder collaboration is necessary to establish industry-wide guidelines for responsible AI, IoMT, and blockchain deployment. Policymakers, healthcare providers, and technology developers must engage in interdisciplinary discussions to balance innovation with ethical responsibility while maintaining regulatory compliance (Bataineh et al., 2022).

CONCLUSION

Blockchain technology has the potential to revolutionize the healthcare sector by addressing longstanding challenges related to data security, interoperability, transparency, and patient control over personal health information. The increasing digitization of medical records, expansion of telemedicine, and integration of emerging technologies such as the IoMT and AI highlight the urgent need for robust and decentralized solutions that ensure data integrity and security. Traditional centralized healthcare systems have proven insufficient in mitigating risks such as cyberattacks, data breaches, and fraudulent activities. Blockchain, with its immutable ledger, cryptographic security, and decentralized architecture, offers a transformative approach to enhancing data management, fostering patient empowerment, and improving healthcare outcomes.

One of the primary advantages of blockchain in healthcare is its ability to enhance data security. By leveraging cryptographic hash functions, digital signatures, and consensus mechanisms, blockchain ensures the integrity and confidentiality of sensitive patient records. Traditional EHR systems have been plagued by vulnerabilities, including unauthorized access, lack of patient control, and interoperability challenges. Blockchain addresses these issues by enabling patient-centric data access, ensuring that only authorized individuals can view and modify health information. Tokenized access control mechanisms and smart contracts provide additional layers of security, allowing patients to manage permissions dynamically and revoke access when necessary. Estonia's blockchain-enabled healthcare system exemplifies how such implementations can enhance security and efficiency while complying with stringent data protection regulations such as the GDPR.

Moreover, blockchain's role in ensuring pharmaceutical traceability and combating counterfeit drugs has been widely recognized. The MediLedger project and IBM's DSCSA pilot have demonstrated how blockchain enhances supply chain transparency by enabling real-time tracking of pharmaceuticals from manufacturers to end-users. Counterfeit medicines pose significant threats to public health, particularly in regions with fragmented supply chains and weak regulatory oversight. Blockchain's immutable ledger and smart contract capabilities help authenticate drug sources, track temperature-sensitive shipments, and facilitate rapid recalls in cases of contamination or fraud. By integrating blockchain with internet of things sensors, healthcare stakeholders can further enhance supply chain security and ensure compliance with regulatory standards.

Beyond securing patient data and improving pharmaceutical traceability, blockchain is transforming clinical research and medical trials. Traditional research methodologies suffer from inefficiencies related to data manipulation, lack of transparency, and difficulties in obtaining informed consent. Blockchain-based solutions such as ZKPs and secure multi-party computation provide privacy-preserving mechanisms for secure data sharing, ensuring that clinical trial data remains tamper-proof and verifiable. By maintaining an immutable audit trail of research activities, blockchain fosters trust among researchers, regulators, and participants while accelerating the drug development process.

Despite its vast potential, blockchain adoption in healthcare faces significant challenges. Scalability remains a primary concern, as blockchain networks must handle vast amounts of medical data without compromising performance. Energy-intensive consensus mechanisms such as PoW present sustainability challenges, necessitating the exploration of more efficient alternatives like PoS or PBFT. Additionally, regulatory compliance and interoperability with existing healthcare infrastructures require concerted efforts from industry stakeholders, policymakers, and technology developers. Integrating blockchain with healthcare's legacy systems demands standardized frameworks, cross-industry collaboration, and substantial investments in infrastructure and training.

Moving forward, the successful deployment of blockchain in healthcare will depend on addressing these challenges through interdisciplinary collaboration and technological innovation. Governments, research institutions, and private enterprises must work together to develop scalable, secure, and regulation-compliant blockchain ecosystems. Pilot projects, such as Estonia's healthcare blockchain initiative and the MediLedger project, provide valuable insights into best practices for implementation and governance. Furthermore, integrating blockchain with AI and IoMT will unlock new opportunities for personalized medicine, predictive analytics, and automated healthcare processes, enhancing patient outcomes and system efficiency.

In conclusion, blockchain technology represents a paradigm shift in healthcare data management, offering unprecedented levels of security, transparency, and efficiency. By mitigating cybersecurity threats, improving patient control, and ensuring the integrity of medical records and pharmaceutical supply chains, blockchains have the potential to reshape the future of healthcare. While challenges remain, ongoing research and real-world implementations provide a solid foundation for further advancements. As the industry moves toward digital transformation, embracing blockchain technology will be crucial in building a more resilient, patient-centric, and secure healthcare ecosystem.

COMPETING INTERESTS STATEMENT

The authors of this publication declare there are no competing interests.

FUNDING STATEMENT

This research received no specific grant from any funding agency in the public, commercial, or not-for-profit sectors. Funding for this research was covered by the authors of the article.

CORRESPONDING AUTHOR

Correspondence should be addressed to Aizhan Kenzhegarina; aizhankenzhegarina@gmail.com

PROCESSING DATES

03, 2025

This manuscript was initially received for consideration for the journal on 11/15/2024, revisions were received for the manuscript following the double-anonymized peer review on 01/31/2025, the manuscript was formally accepted on 02/21/2025, and the manuscript was finalized for publication on 03/13/2025

REFERENCES

Adeghe, N. E. P., Okolo, N. C. A., & Ojeyinka, N. O. T. (2024). Evaluating the impact of blockchain technology in healthcare data management: A review of security, privacy, and patient outcomes. *Open Access Research Journal of Science and Technology, 10*(2), 013–020. DOI: 10.53022/oarjst.2024.10.2.0044

Agbo, C., Mahmoud, Q., & Eklund, J. (2019). Blockchain technology in healthcare: A systematic review. *Health Care*, *7*(2), 56. DOI: 10.3390/healthcare7020056 PMID: 30987333

Akkaoui, R., Hei, X., & Cheng, W. (2020). Edgemedichain: A hybrid edge blockchain-based framework for health data exchange. *IEEE Access: Practical Innovations, Open Solutions*, *8*, 113467–113486. DOI: 10.1109/ACCESS.2020.3005926

Al-Aswad, H., El-Medany, W. M., Balakrishna, C., Ababneh, N., & Curran, K. (2021). BZKP: Blockchain-based zero-knowledge proof model for enhancing healthcare security in Bahrain IoT smart cities and COVID-19 risk mitigation. *Arab Journal of Basic and Applied Sciences*, *28*(1), 154–171. DOI: 10.1080/25765299.2020.1870812

Ali, A., Ali, H., Saeed, A., Ahmed Khan, A., Tin, T. T., Assam, M., Ghadi, Y. Y., & Mohamed, H. G. (2023). Blockchain-Powered Healthcare Systems: Enhancing Scalability and Security with Hybrid Deep Learning. *Sensors (Basel)*, *23*(18), 7740. DOI: 10.3390/s23187740 PMID: 37765797

Alnssayan, A. A., Hassan, M. M., & Alsuhibany, S. A. (2021). VacChain: A blockchain-based EMR system to manage child vaccination records. *Computer Systems Science and Engineering*, *40*(3), 927–945. DOI: 10.32604/csse.2022.016734

American Medical Association. (2022, Jul 20). Patient survey shows unresolved tension over health data privacy. https://www.ama-assn.org/press-center/press-releases/patient-survey-shows-unresolved-tension-over-health-data-privacy

Anshari, M. (2019). Redefining electronic health records (EHR) and electronic medical records (EMR) to promote patient empowerment. *International Journal on Informatics for Development*, *8*(1), 35–39. DOI: 10.14421/ijid.2019.08106

Anwar, M. R., Apriani, D., & Adianita, I. R. (2021). Hash Algorithm In Verification Of Certificate Data Integrity And Security. *Aptisi Transactions on Technopreneurship*, *3*(2), 67–74. DOI: 10.34306/att.v3i2.212

Asiri, S., & Miri, A. (2018). *A Sybil resistant IoT trust model using blockchains. In 2018 IEEE international conference on internet of things*., DOI: 10.1109/iThings.2018.00183

Azaria, A., Ekblaw, A., Vieira, T. A., & Lippman, A. (2016). Medrec: Using blockchain for medical data access and permission management. *2016 2nd International Conference on Open and Big Data (OBD)*. DOI: 10.1109/OBD.2016.11

Badertscher, C., Lu, Y., & Zikas, V. (2021). A rational protocol treatment of 51% attacks. In Malkin, T., & Peikert, C. (Eds.), *Advances in cryptology – CRYPTO 2021* (*Vol. 12827*). Springer., DOI: 10.1007/978-3-030-84252-9_1

Banerji, A., Riedl, M. A., Bernstein, J. A., Cicardi, M., Longhurst, H., Zuraw, B. L., & Maurer, M. (2018). Effect of lanadelumab compared with placebo on prevention of hereditary angioedema attacks. *Journal of the American Medical Association*, *320*(20), 2108. Advance online publication. DOI: 10.1001/jama.2018.16773 PMID: 30480729

Bard, D. A., Kearney, J. J., & Perez-Delgado, C. A. (2021). Quantum advantage on proof of work. *arXiv.* DOI: 10.48550/arxiv.2105.01821

Bataineh, M., Mardini, W., Khamayseh, Y., & Yasin, M. (2022). Novel and secure blockchain framework for health applications in IoT. *IEEE Access: Practical Innovations, Open Solutions*, *10*, 1–1. DOI: 10.1109/ACCESS.2022.3147795

Begum, A., Tareq, A., Sultana, M., Sohel, M., Rahman, T., & Sarwar, A. (2020). Blockchain attacks analysis and a model to solve double spending attack. *International Journal of Machine Learning and Computing*, *10*(2), 352–357. DOI: 10.18178/ijmlc.2020.10.2.898

Benaich, R., el Mendili, S., & Gahi, Y. (2023). Advancing healthcare security: A cutting-edge zero-trust blockchain solution for protecting electronic health records. *HighTech and Innovation Journal*, *4*(3), 630–652. Advance online publication. DOI: 10.28991/HIJ-2023-04-03-012

Benchoufi, M., & Ravaud, P. (2017). Blockchain technology for improving clinical research quality. *Trials*, *18*(1), 335. DOI: 10.1186/s13063-017-2035-z PMID: 28724395

Berg, C., Davidson, S., & Potts, J. (2020). Proof of work as a three-sided market. *Frontiers in Blockchain*, *3*, 2. DOI: 10.3389/fbloc.2020.00002

Bhuvana, R., & Aithal, P. (2020). Blockchain based service: A case study on IBM blockchain services and hyperledger fabric. *International Journal of Case Studies in Business and Education*, 94–102. DOI: 10.47992/IJCSBE.2581.6942.0064

Birnhack, M. D. (2011). A quest for a theory of privacy: Context and control. *Jurimetrics*, *51*(4), 447–479. https://www.jstor.org/stable/41307137

Bittroff, V., & Sandner, P. (2020). *Opportunities Through Blockchain Technology for the German Healthcare Market*. Hamburg University.

Blais, D. (2022). Strategies for preventing and mitigating counterfeit medication from entering the US supply chain.

Chaganti, R., Boppana, R. V., Ravi, V., Munir, K., Almutairi, M., Rustam, F., Lee, E., & Ashraf, I. (2022). *A comprehensive review of denial-of-service attacks in blockchain ecosystem and open challenges*. IEEE., DOI: 10.1109/ACCESS.2022.3205019

Charles, W., Marler, N., Long, L., & Manion, S. (2019). Blockchain compliance by design: Regulatory considerations for blockchain in clinical research. *Frontiers in Blockchain*, *2*, 18. Advance online publication. DOI: 10.3389/fbloc.2019.00018

Chen, J., Farid, F., & Polash, M. (2023). Federated learning: An alternative approach to improving medical data privacy and security. In *Current and future trends in health and medical informatics* (pp. 277–297). Springer., DOI: 10.1007/978-3-031-42112-9_13

Coombes, R. (2012). GlaxoSmithKline grants researchers access to clinical trial data. *BMJ (Clinical Research Ed.)*, *345*(oct12 5), e6909–e6909. DOI: 10.1136/bmj.e6909 PMID: 23065357

Custers, B., Dechesne, F., & Sears, A. M. (2017). A comparison of data protection legislation and policies across the EU. *Computer Law & Security Review*. Advance online publication. DOI: 10.1016/j.clsr.2017.09.001

Dagher, G. G., Mohler, P., Milojkovic, M., & Marella, J. (2018). Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustainable Cities and Society*, *39*, 283–297. DOI: 10.1016/j.scs.2018.02.014

De Angelis, F., De Blasio, C., & Sorniotti, A. (2019). PBFT vs proof of authority: Applying the CAP theorem to permissioned blockchain. In *Proceedings of the IEEE TrustCom* (pp. 556–563). DOI: 10.1109/TrustCom/BigDataSE.2019.00083

Drosatos, G., & Kaldoudi, E. (2019). Blockchain applications in the biomedical domain: A scoping review. *Computational and Structural Biotechnology Journal*, *17*, 229–240. DOI: 10.1016/j.csbj.2019.01.010 PMID: 30847041

Du, Y., Wang, Z., Li, J., Shi, L., Jayakody, D. N. K., Chen, Q., Chen, W., & Han, Z. (2022). Blockchain-aided edge computing market: Smart contract and consensus mechanisms. *IEEE Transactions on Mobile Computing*, *22*(6), 3193–3208. DOI: 10.1109/TMC.2021.3140080

E-Estonia. (2022). Estonian e-Health Records. E-Estonia. https://e-estonia.com/solutions/e-health/e-health-records/

Estonian Genome Centre. (2023). *Estonian Biobank*. University of Tartu. https://genomics.ut.ee/en/content/estonian-biobank

European Commission. (2022). Assessment of the EU Member States' rules on health data in the light of GDPR. https://health.ec.europa.eu/system/files/2021-02/ms_rules_health-data_en_0.pdf

Fan, T., He, Q., Nie, E., & Chen, S. (2018). A study of pricing and trading model of blockchain & big data-based Energy-Internet electricity. *IOP Conference Series. Earth and Environmental Science*, *108*, 052083. DOI: 10.1088/1755-1315/108/5/052083

FDA DSCSA Blockchain Interoperability Pilot. (2020). https://www.fda.gov/media/169883/download?attachment

Feng, Y., Yan, W., Zuo, M., & Zhang, Q. (2022). Consortium blockchains based traceability system for chicken product supply chain. *MATEC Web of Conferences, 355*, 02037. DOI: 10.1051/matecconf/202235502037

Ghadi, Y. Y., Mazhar, T., Shahzad, T., Amir khan, M., Abd-Alrazaq, A., Ahmed, A., & Hamam, H. (2024). The role of blockchain to secure Internet of Medical Things. *Scientific Reports*, *14*(1), 18422. DOI: 10.1038/s41598-024-68529-x PMID: 39117650

Griggs, K. N., Ossipova, O., Kohlios, C. P., Baccarini, A. N., Howson, E. A., & Hayajneh, T. (2018). Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *Journal of Medical Systems*, *42*(7), 130. DOI: 10.1007/s10916-018-0982-x PMID: 29876661

Guardtime. (2021). Technology. Guardtime. https://guardtime.com/technology

Guru, A., Mohanta, B. K., Mohapatra, H., Al-Turjman, F., Altrjman, C., & Yadav, A. (2023). A survey on consensus protocols and attacks on blockchain technology. *Applied Sciences (Basel, Switzerland)*, *13*(4), 2604. DOI: 10.3390/app13042604

Hafid, A., Hafid, A. S., & Samih, M. (2022). A tractable probabilistic approach to analyze Sybil attacks in sharding-based blockchain protocols. *IEEE Transactions on Emerging Topics in Computing*, *11*(1), 126–136. DOI: 10.1109/TETC.2022.3179638

Hammi, B., Idir, Y. M., Zeadally, S., Khatoun, R., & Nebhen, J. (2022). Is it really easy to detect Sybil attacks in C-its environments: A position paper. *IEEE Transactions on Intelligent Transportation Systems*, *23*(10), 18273–18287. Advance online publication. DOI: 10.1109/TITS.2022.3165513

Hammi, B., Zeadally, S., & Nebhen, J. (2023). Security threats, countermeasures, and challenges of digital supply chains. *ACM Computing Surveys*, *55*(14s), 1–40. Advance online publication. DOI: 10.1145/3588999

Han, Y., Zhang, Y., & Vermund, S. (2022). Blockchain technology for electronic health records. *International Journal of Environmental Research and Public Health*, *19*(23), 15577. DOI: 10.3390/ijerph192315577 PMID: 36497654

Handayani, D. I., Vanany, I., & Ciptomulyono, U. (2023). Blockchain application in food supply chains: Bibliometric analysis and future research. *International Journal on Food System Dynamics*, *14*(2). Advance online publication. DOI: 10.22004/ag.econ.346701

Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A. (2019). Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, *134*, 104040. DOI: 10.1016/j.ijmedinf.2019.104040 PMID: 31865055

Iqbal, M., & Matulevičius, R. Iqbal, M., & Matulevičius, R. (2021). Exploring Sybil and double-spending risks in blockchain systems. IEEE Access, PP, 1–1. DOI: 10.1109/ACCESS.2021.3081998

Jamil, F., Kahng, H. K., Kim, S., & Kim, D. (2021). Towards secure fitness framework based on IoT-enabled blockchain network integrated with machine learning algorithms. *Sensors (Basel)*, *21*(5), 1640. DOI: 10.3390/s21051640 PMID: 33652773

Journal, H. I. P. A. A. (2022). 2022 healthcare data breach report. https://www.hipaajournal.com/2022-healthcare-data-breach-report/

Journal, H. I. P. A. A. (2022,). Study explores how medical apps are sending health data to Facebook and others. https://www.hipaajournal.com/study-explores-how-medical-apps-are-sending-health-data-to-facebook-and-others/

Journal, H. I. P. A. A. (2024). Cost of a data breach HIPAA Journal. https://www.hipaajournal.com/cost-healthcare-data-breach-2024

Kahn, J. (2022, Aug 15). *Digital medical companies funnel patient data to Facebook for advertising*. Forbes. https://www.forbes.com/sites/alexandralevine/2022/08/15/digital-medical-companies-funnel-patient-data-to-facebook-for-advertising/?utm_source=chatgpt.com

Kamangar, Z. U., Memon, R. A., Memon, G. M., & Kamangar, U. A. (2023). Integration of internet of things and blockchain technology in healthcare domain: A systematic literature review. *International Journal of Communication Systems*, *36*(16), e5582. Advance online publication. DOI: 10.1002/dac.5582

Kaur, J., & Singh, G. (). A blockchain-based machine learning intrusion detection system for internet of things. In Daimi, K., Dionysiou, I., & El Madhoun, N. (Eds.), *Principles and practice of blockchains*. Springer., DOI: 10.1007/978-3-031-10507-4_6

Kaushik, S., & El Madhoun, N. (2023). Analysis of blockchain security: Classic attacks, cybercrime, and penetration testing. *Proceedings of the IEEE MobiSecServ*, *58080*, 10329210. DOI: 10.1109/MobiSecServ58080.2023.10329210

Khan, Z. A., & Namin, A. S. (2020). *Ethereum smart contracts: Vulnerabilities and their classifications. In 2020 IEEE international conference on big data*., DOI: 10.1109/BigData50022.2020.9377755

Khatoon, A. (2020). A blockchain-based smart contract system for healthcare management. *Electronics (Basel)*, *9*(1), 94. DOI: 10.3390/electronics9010094

Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences (Basel, Switzerland)*, *9*(9), 1736. DOI: 10.3390/app9091736

Kiktenko, E. O., Pozhar, N. O., Anufriev, M. N., Trushechkin, A. S., Yunusov, R. R., Kurochkin, Y. V., Lvovsky, A. I., & Fedorov, A. K. (2018). Quantum-secured blockchain. *Quantum Science and Technology*, *3*(3), 035004. DOI: 10.1088/2058-9565/aabc6b

Kõnd, K., & Lilleväli, A. (2019). E-prescription success in Estonia: The journey from paper to pharmacogenomics. *Eurohealth (London)*, *25*(2), 18–20.

Kongmanee, J., Kijsanayothin, P., & Hewett, R. (2019). Securing smart contracts in blockchain. In *2019 34th IEEE/ACM international conference on automated software engineering workshop* (pp. 69–76). DOI: 10.1109/ASEW.2019.00032

Kshetri, N. (2018). Blockchain and electronic healthcare records [Cybertrust]. *Computer*, *51*(12), 59–63. DOI: 10.1109/MC.2018.2880021

Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association : JAMIA*, *24*(6), 1211–1220. DOI: 10.1093/jamia/ocx068 PMID: 29016974

Lacity, M. C., Sabherwal, R., & Sørensen, C. (2019). Delivering business value through enterprise blockchain applications. *MIS Quarterly Executive*, *18*(4), 3.

Lapointe, C., & Fishbane, L. (2018). The blockchain ethical design framework. *Innovations: Technology, Governance, Globalization*, *12*(3–4), 50–71. DOI: 10.1162/inov_a_00275

Lasla, N., Al-Sahan, L., Abdallah, M., & Younis, M. (2022). Green-PoW: An energy-efficient blockchain proof-of-work consensus algorithm. *Computer Networks*, *214*, 109118. DOI: 10.1016/j.comnet.2022.109118

Lazaro, C., & Metayer, D. L. (2015). Control over personal data: True remedy or fairy tale. *Script-ed*, *12*(3). Advance online publication. DOI: 10.2966/scrip.120115.3

Li, C., & Palanisamy, B. (2020). Comparison of decentralization in DPOS and POW blockchains. In *Lecture notes in computer science* (pp. 18–32). DOI: 10.1007/978-3-030-59638-5_2

Li, C., Xu, R., & Duan, L. (2023). Characterizing coin-based voting governance in DPOS blockchains. *Proceedings of the International AAAI Conference on Web and Social Media, 17*, 1148–1152. DOI: 10.1609/icwsm.v17i1.22225

Linn, L. A., & Koo, M. B. (2016). Blockchain for health data and its potential use in health IT and health care related research. In ONC/NIST Use of Blockchain for Healthcare and Research Workshop (pp. 1-10). ONC/NIST.

Liu, S., Zhang, R., Liu, C., Xu, C., & Wang, J. (2023). An improved PBFT consensus algorithm based on grouping and credit grading. *Scientific Reports*, *13*(1), 13030. DOI: 10.1038/s41598-023-28856-x PMID: 37563158

Liu, Y., Wang, K., Liu, Y., Liu, X., Wang, W., & Zhang, X. (2019). A blockchain-based medical data sharing and protection scheme. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 118943–118953. DOI: 10.1109/ACCESS.2019.2937685

Lubin, J. S., & Shah, A. (2022). An incomplete medical record: Transfer of care from emergency medical services to the emergency department. *Cureus*, *14*(2), e22446. DOI: 10.7759/cureus.22446 PMID: 35345754

Mackey, T. K., Kuo, T., Gummadi, B., Clauson, K. A., Church, G. M., Grishin, D., Obbad, K., Barkovich, R., & Palombini, M. (2019). 'Fit-for-purpose?'—Challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Medicine*, *17*(1), 68. Advance online publication. DOI: 10.1186/s12916-019-1296-7 PMID: 30914045

Madhoun, N. E., Hatin, J., & Bertin, E. (2020). A decision tree for building IT applications. *Annales des Télécommunications*, *75*(1), 41–52. DOI: 10.1007/s12243-020-00814-y

Mallick, P. K., Salling, K. B., Pigosso, D. C., & McAloone, T. C. (2023). Closing the loop: Establishing reverse logistics for a circular economy, a systematic review. *Journal of Environmental Management*, *328*, 117017. DOI: 10.1016/j.jenvman.2022.117017 PMID: 36521223

Marbouh, D., Abbasi, T., Maasmi, F., Omar, I. A., Debe, M. S., Salah, K., Jayaraman, R., & Ellahham, S. (2020). Blockchain for COVID-19: Review, Opportunities, and a Trusted Tracking System. *Arabian Journal for Science and Engineering*, *45*(12), 9895–9911. DOI: 10.1007/s13369-020-04950-4 PMID: 33072472

Martínez, J. M. G., Carracedo, P., Comas, D. G., & Siemens, C. H. (2022). An analysis of the blockchain and COVID-19 research landscape using a bibliometric study. *Sustainable Technology and Entrepreneurship*, *1*(1), 100006. DOI: 10.1016/j.stae.2022.100006

Mattke, J., Maier, C., Hund, A., & Weitzel, T. (2019). How an enterprise blockchain application in the U.S. pharmaceuticals supply chain is saving lives. *MIS Quarterly Executive*, *18*(4), 245–261. Advance online publication. DOI: 10.17705/2msqe.00019

Mayer, A. H., Da Costa, C. A., & Da Rosa Righi, R. (2019). Electronic health records in a blockchain: A systematic review. *Health Informatics Journal*, *26*(2), 1273–1288. DOI: 10.1177/1460458219866350 PMID: 31566472

MediLedger DSCSA Pilot. (2023). https://www.fda.gov/media/168283/download?attachment

Mehar, I., Shier, C., Giambattista, A., Gong, E., Fletcher, G., Sanayhie, R., Kim, H., & Laskowski, M. (2019). Understanding a revolutionary and flawed grand experiment in blockchain: The DAO attack. *Journal of Cases on Information Technology*, *21*(1), 19–32. DOI: 10.4018/JCIT.2019010102

Metsallik, J., Ross, P., Draheim, D., & Piho, G. (2018, Jun). Ten years of the e-health system in Estonia. *CEUR Workshop Proceedings*, *2336*, 6–15.

Mohanan, N., & D, S. (2023). Comparative study of blockchain consensus algorithms in cryptocurrency. *International Journal of Scientific Research in Engineering and Management*, *7*(9), 1–11. DOI: 10.55041/IJSREM25787

Moosavi, N., & Taherdoost, H. (2023). Blockchain technology application in security: A systematic review. *Blockchains*, *1*(2), 58–72. DOI: 10.3390/blockchains1020005

Morris, V., Adivi, R., Asara, R., Cousens, M., Gupta, N., Lincoln, N., Mosakowski, B., & Sun, H. W. (2018). *Developing a blockchain business network with hyperledger composer using the IBM blockchain platform starter plan*. IBM Redbooks.

Nishad, D. K., & Tripathi, D. R. (2020). Internet of medical things: Applications and challenges. *Turkish Journal of Computer and Mathematics Education*, *11*(3), 2885–2889. DOI: 10.61841/turcomat.v11i3.14654

Nourani, A., Ayatollahi, H., & Dodaran, M. S. (2019). Clinical trial data management software: A review of the technical features. *Reviews on Recent Clinical Trials*, *14*(3), 160–172. DOI: 10.2174/1574887114666190207151500 PMID: 30734683

O'Brien, N., Ghafur, S., Arvind, S., & Durkin, M. (2022). Cyber-attacks are a permanent and substantial threat to health systems: Education must reflect that. *Digital Health*, *8*, 205520762211046. DOI: 10.1177/20552076221104665 PMID: 35746951

Peterson, K.J., Deeduvanu, R., Kanjamala, P., & Mayo, K.B. (2016). A Blockchain-Based Approach to Health Information Exchange Networks.

Pineda, M., Jabba, D., Nieto-Bernal, W., & Pérez, A. (2024). Sustainable consensus algorithms applied to blockchain: A systematic literature review. *Sustainability (Basel)*, *16*(23), 10552. DOI: 10.3390/su162310552

Priestman, W., Anstis, T., Sebire, I. G., Sridharan, S., & Sebire, N. J. (2019). Phishing in healthcare organisations: Threats, mitigation, and approaches. *BMJ Health & Care Informatics*, *26*(1), e100031. DOI: 10.1136/bmjhci-2019-100031 PMID: 31488498

Raghav, N., & Bhola, A. K. (2023). Detecting Sybil Attack in Blockchain and Preventing through Universal Unique Identifier in Health Care Sector for privacy preservation. *International Journal on Recent and Innovation Trends in Computing and Communication*, *11*(8), 276–284. DOI: 10.17762/ijritcc.v11i8.7955

Rattanawiboomsom, V., Korejo, M., Ali, J., & Thatsaringkharnsakun, U. (2023). Blockchain-enabled Internet of Things (IoT) applications in healthcare: A systematic review of current trends and future opportunities. International Journal of Online and Biomedical Engineering (iJOE, 19, 99–117. DOI: 10.3991/ijoe.v19i10.41399

Regulation (EU) 2016/679 of the European Parliament and of the Council. (2016). *General Data Protection Regulation*. Official Journal of the European Union. Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX%3A32016R0679

Reinhardt, J. (2019). *Gameful Second and Foreign Language Teaching and Learning*. Introduction. Palgrave-Macmillan., DOI: 10.1007/978-3-030-04729-0

Riso, B., Tupasela, A., Vears, D. F., Felzmann, H., Cockbain, J., Loi, M., Kongsholm, N. C. H., Zullo, S., & Rakic, V. (2017). Ethical sharing of health data in online platforms - which values should be considered? *Life Sciences, Society and Policy*, *13*(1), 12. DOI: 10.1186/s40504-017-0060-z PMID: 28825221

Rizzoni, F., Magalini, S., Casaroli, A., Mari, P., Dixon, M., & Coventry, L. (2022). Phishing simulation exercise in a large hospital: A case study. *Digital Health*, *8*, 205520762210817. DOI: 10.1177/20552076221081716 PMID: 35321019

Sahoo, M., Singhar, S. S., & Sahoo, S. S. (2020). A blockchain based model to eliminate drug counterfeiting. DOI: 10.1007/978-981-15-1884-3_20

Sayeed, S., Marco-Gisbert, H., & Caira, T. (2020). Smart contract: Attacks and protections. *IEEE Access : Practical Innovations, Open Solutions*, *8*, 24416–24427. DOI: 10.1109/ACCESS.2020.2970495

Security, I. B. M. (2024). Cost of a data breach report 2024. *IBM*. https://www.ibm.com/security/data-breach

Selbst, A. D., Boyd, D., Friedler, S. A., Venkatasubramanian, S., & Vertesi, J. (2019). Fairness and abstraction in sociotechnical systems. *Association for Computing Machinery*, 59–68. DOI: 10.1145/3287560.3287598

Shabani, M., & Marelli, L. (2019). Re-identifiability of genomic data and the GDPR: Assessing the re-identifiability of genomic data in light of the EU General Data Protection Regulation. *EMBO Reports*, *20*(6), e48316. DOI: 10.15252/embr.201948316 PMID: 31126909

Shahnaz, A., Qamar, U., & Khalid, A. (2019). Using blockchain for electronic health records. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 147782–147795. DOI: 10.1109/ACCESS.2019.2946373

Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2022). Insights into security and privacy towards fog computing evolution. *Computers & Security*, *120*, 102822. DOI: 10.1016/j.cose.2022.102822

Srivastava, S., Pant, M., Jauhar, S. K., & Nagar, A. K. (2022). Analyzing the Prospects of Blockchain in Healthcare Industry. *Computational and Mathematical Methods in Medicine*, *3727389*, 1–24. Advance online publication. DOI: 10.1155/2022/3727389 PMID: 36506597

Staunton, C., Slokenberga, S., & Mascalzoni, D. (2019). The impact of the General Data Protection Regulation on health research. *British Medical Bulletin*, *128*(1), 109–118. DOI: 10.1093/bmb/ldy038 PMID: 31583398

Tang, H., Shi, Y., & Dong, P. (2018). Public blockchain evaluation using entropy and TOPSIS. *Expert Systems with Applications*, *117*, 204–210. DOI: 10.1016/j.eswa.2018.09.048

Thekkilakattil, A., & Dodig-Crnkovic, G. (2015). Ethics aspects of embedded and cyber-physical systems. In *2015 IEEE 39th annual computer software and applications conference* (pp. 39–44). IEEE. DOI: 10.1109/COMPSAC.2015.41

Trautmann, L., Hübner, T., & Lasch, R. (2022). Blockchain concept to combat drug counterfeiting by increasing supply chain visibility. *International Journal of Logistics Research and Applications*, 1–27.

Treiblmaier, H., Rejeb, A., & Ahmed, W. A. (2022). Blockchain technologies in the digital supply chain. *The Digital Supply Chain*, 127–144. DOI: 10.1016/B978-0-323-91614-1.00008-3

Umrao, D., Mathur, A., Patel, C. S., Awasthi, A., & Tiwari, A. (2022). Blockchain technology in the health sector. *International Journal of Health Sciences*. Advance online publication. DOI: 10.53730/ijhs.v6nS1.8120

U.S. Department of Health & Human Services (HHS). (2013). Summary of the HIPAA Privacy Rule. Retrieved from https://www.hhs.gov/hipaa/for-professionals/privacy/laws-regulations/index.html

van Reede, M. (2020). Evaluating the practicality of using blockchain technology in different use cases in the healthcare sector (Master's thesis, Radboud University). Radboud Repository.

Vazirani, A., O'Donoghue, O., Brindley, D., & Meinert, E. (2020). Blockchain vehicles for efficient medical record management. *npj. Digital Medicine*, *3*(1), 1. DOI: 10.1038/s41746-019-0211-0 PMID: 31934645

Vukovic, J., Ivankovic, D., Habl, C., & Dimnjakovic, J. (2022). Enablers and barriers to the secondary use of health data in Europe: General data protection regulation perspective. *Archives of Public Health = Archives Belges de Santé Publique*, *80*(115), 115. Advance online publication. DOI: 10.1186/s13690-022-00866-7 PMID: 35397557

Wang, W., Hoang, D. T., Hu, P., Xiong, Z., Niyato, D., Wang, P., Wen, Y., & Kim, D. I. (2019). A survey on consensus mechanisms and mining strategy management in blockchain networks. *IEEE Access : Practical Innovations, Open Solutions*, *7*, 22328–22370. DOI: 10.1109/ACCESS.2019.2896108

White, T., Blok, E., & Calhoun, V. D. (2022). Data sharing and privacy issues in neuroimaging research: Opportunities, obstacles, challenges, and monsters under the bed. *Human Brain Mapping*, *43*(1), 278–291. Advance online publication. DOI: 10.1002/hbm.25120 PMID: 32621651

WHO. (2017). 1 in 10 medical products in developing countries is substandard or falsified. *WHO*. https://www.who.int/news/item/28-11-2017-1-in-10-medical-products-in-developing-countries-is-substandard-or-falsified

WHO. (2023). Medical product alert N°1/2023: Substandard (contaminated) liquid dosage medicines. WHO. https://www.who.int/teams/regulation-prequalification/incidents-and-SF/full-list-of-who-medical-product-alerts

Wong, D., Bhattacharya, S., & Butte, A. (2019). Prototype of running clinical trials in an untrustworthy environment using blockchain. *Nature Communications*, *10*(1), 917. Advance online publication. DOI: 10.1038/s41467-019-08874-y PMID: 30796226

World Health Assembly. (2010). Counterfeit medical products: Report by the secretariat. *WHO*. https://iris.who.int/handle/10665/23931

World Health Organization. (2010). *Counterfeit medicines: Fact sheet*. WHO. https://www.who.int/news-room/fact-sheets/detail/counterfeit-medicines

Xu, G., Yao, T., Zhang, K., Meng, X., Liu, X., Xiao, K., & Chen, X. (2023). An Optimized Byzantine Fault Tolerance Algorithm for Medical Data Security. *Electronics (Basel)*, *12*(24), 5045. DOI: 10.3390/electronics12245045

Yang, F., Zhou, W., Wu, Q., Long, R., Xiong, N. N., & Zhou, M. (2019). Delegated proof of stake with downgrade: A secure and efficient blockchain consensus algorithm with downgrade mechanism. *IEEE Access: Practical Innovations, Open Solutions*, *7*, 118541–118555. DOI: 10.1109/ACCESS.2019.2935149

Ye, C., Li, G., Cai, H., Gu, Y., & Fukuda, A. (2018). Analysis of security in blockchain: Case study in 51%-attack detecting. *2018 5th International Conference on Dependable Systems and Their Applications (DSA)*. DOI: 10.1109/DSA.2018.00015

Yeng, P. K., Fauzi, M. A., Yang, B., & Nimbe, P. (2022). Investigation into phishing risk behaviour among healthcare staff. *Information (Basel)*, *13*(8), 392. DOI: 10.3390/info13080392

Zhang, P., White, J., Schmidt, D. C., & Lenz, G. (2017). Applying blockchain technology for secure healthcare management systems. In *Proceedings of the 10th IEEE international conference on health informatics* (pp. 514–519). DOI: 10.1109/HealthInf.2017.7916501

Zhao, S., Wang, B., Li, Y., & Li, Y. (2018). Integrated energy transaction mechanisms based on blockchain technology. *Energies*, *11*(9), 2412. DOI: 10.3390/en11092412

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An overview of blockchain technology: Architecture, consensus, and future trends. In *Proceedings of the IEEE international congress on big data* (pp. 557–564). DOI: 10.1109/BigDataCongress.2017.85

Ziegler, Y., & Uli, V. (2021). Supply chain management and blockchain: Bridging the antecedents of the technology with the status quo of use case applications. *International Journal of Value Chain Management*. DOI: 10.1504/ijvcm.2021.118

Yelezhanova Shynar is a candidate of Physical and Mathematical Sciences, Acting Professor of the Department of «Software Engineering», NAO «Atyrau University named after H.Dosmukhamedov», Atyrau, Kazakhstan

Altynbek Seytenov is a PhD student (doctoral candidate) in the Department of Information Systems at L.N. Gumilyov Eurasian National University as well as a senior lecturer in the Department of Computer Engineering at Astana IT University. My research interests consider the development of medical information systems, telemedicine, blockchain technologies, and data analytics. In a recent publication, he presented the development of a medical information system to enhance the quality of healthcare services in Kazakhstan.

Aizhan Kenzhegarina is a graduate student pursuing a Master of Science degree in Computer Science and Engineering at Astana IT University, Kazakhstan. She holds a Bachelor of Science degree in Software Engineering, and her research interests include blockchain technology, its applications in healthcare, and its integration with machine learning.

Amir Kenzhetayev is a graduate student at Boston University, pursuing a Master's degree in Healthcare Informatics with a concentration in Data Analytics. His academic and professional background bridges the fields of medicine, data science, and cybersecurity, with a focus on leveraging data-driven solutions to enhance healthcare systems. Amir has worked as a Research Assistant in infectious diseases and healthcare analytics, applying machine learning techniques to improve patient outcomes and hospital operations. His research interests include healthcare data security, interoperability, and the application of AI in clinical decision-making.

Ayan Kemel: Master of Engineering, Lecturer, Department of Computer Engineering, Astana IT University, Astana, Kazakhstan.

Nurzhan Ualiyev: Senior lecturer at Zhetysu University, holding a Candidate of Physical and Mathematical Sciences degree. He has been honored with the Y. Altynsarin badge for his achievements.

Alua Myrzakerimova is a PhD, assistant professor, Department of Computer Engineering, Astana IT University, Astana, Kazakhstan. Author of more than 16 scientific paper, including 6 articles in the Scopus database

Gulzhan Mursakimova is a lecturer at Zhetysu University, specializing in Information Systems. She earned her degree in Information Systems in Business from Al-Farabi Kazakh National University in 2000, qualifying as a mathematician and specialist in business information systems. In 2002, she obtained a Master of Science in Informatics from Abai Kazakh National Pedagogical University.

Alibek Orynbek holds a Bachelor's degree in Computer Science, a Master's degree in Economic Science, and is a PhD candidate in Mathematics. He is currently the Deputy Director of the Department of Computer Engineering at Astana IT University. His research interests include artificial intelligence and financial technology, with a focus on machine learning applications, data-driven decision-making, and innovative financial solutions.

Aivar Sakhipov PhD, assistant professor, Department of Computer Engineering, Astana IT University, Astana, Kazakhstan. Author of more than 30 scientific paper, including 8 articles in the Scopus database and 10 copyright certificates.