Scientific Journal of Metaverse and Blockchain Technologies
ISSN: 2584-2110 | Vol. 2 | Issue 2 | Jul -Dec 2024 | Peer Reviewed & Refereed

Blockchain for Enhancing Compliance Data Integrity in Occupational Healthcare

Yogesh Gadhiya*
Independent Researcher, USA

Accepted: 12/12/2024 Published: 30/12/2024 Check for updates *Corresponding author

How to Cite:
Gadhiya Y (2024). Blockchain for Enhancing Compliance Data Integrity in Occupational Healthcare. *Scientific Journal of Metaverse and Blockchain Technology. 2*(2), 174-186.
DOI: https://doi.org/10.36676/sjmbt.v2.i2.39

Abstract
Occupational healthcare compliance involves managing sensitive data to ensure adherence to regulatory requirements. However, challenges in maintaining data integrity often undermine the reliability of compliance processes. This paper explores the application of blockchain technology to enhance data integrity in occupational healthcare compliance systems. By leveraging blockchain's immutable ledger, smart contracts, and decentralized architecture, this research proposes a robust framework for secure and transparent compliance management. The findings indicate that blockchain can mitigate data manipulation risks, improve auditability, and streamline compliance workflows, offering significant potential for transforming occupational healthcare compliance.
Keywords: Blockchain, Data Integrity, Occupational Healthcare, Compliance Management, Smart Contracts, Decentralized Systems

1. Introduction

1.1 Background and Motivation

Compliance data integrity is critical in occupational healthcare, where inaccurate data can lead to legal violations, employee dissatisfaction, and public health risks. Traditional systems for managing compliance data often rely on centralized architectures prone to vulnerabilities such as unauthorized access, data tampering, and limited auditability. Emerging technologies like blockchain promise to address these issues, ensuring higher standards of data integrity.

1.2 Challenges in Occupational Healthcare Compliance

Occupational healthcare compliance faces numerous challenges, including:

- **Data Tampering Risks:** Existing systems lack robust mechanisms to detect unauthorized modifications.
- **Audit Complexity:** Proving compliance with regulations can involve labour-intensive manual audits.
- **Inconsistent Record-Keeping:** Inaccuracies in records can lead to non-compliance and potential penalties.

1.3 Research Objectives

This research aims to:

1. Analyse the limitations of current compliance data integrity solutions in occupational healthcare.
2. Investigate blockchain's potential in addressing these limitations.
3. Propose a blockchain-based framework tailored for occupational healthcare compliance.

2. Introduction

2.1 Background and Motivation

Compliance with occupational healthcare regulations is critical for ensuring employee well-being, legal adherence, and organizational sustainability. International governments and regulatory authorities require compliance with standards concerning health and safety measures to reducing the incidences of work-related accidents and ill health and promoting the rights of workers. However, compliance entails effective handling of information obtained from different activities such as medical examination, safety education, and especially

hazard identification (Ribitzky et al., 2018).

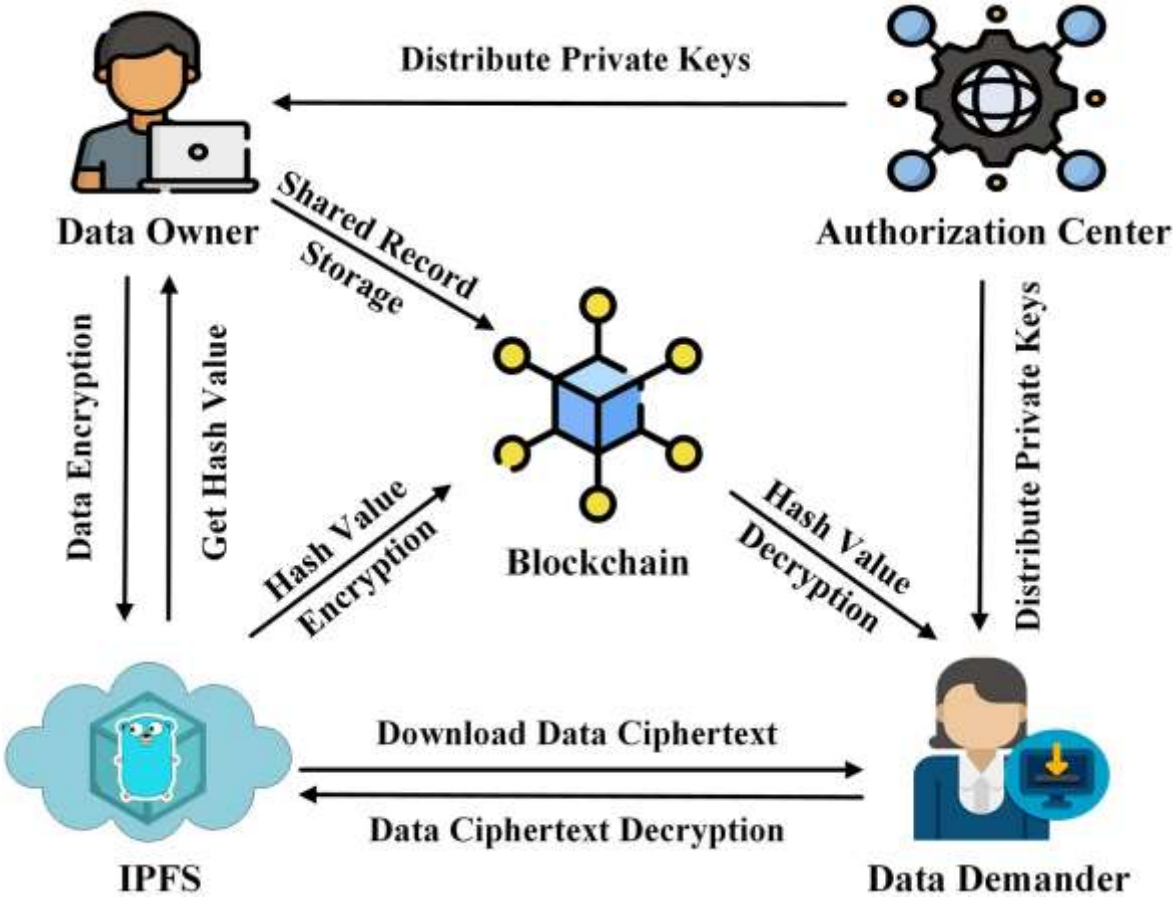

Figure 1 Blockchain Technology and Healthcare(Medium,2019)

The toughest thing is to manage this information since it comes from various sources, and much is at stake when one makes a mistake or manipulate data. According to estimates from the ILO operational since 2018, occupational illnesses and injuries contribute to a global loss of about 4% of the GDP. Compliance data accuracy remains a growing concern to prevent individuals, companies, and the government from significant financial losses, legal liability, and harms to the public's perception of the company. Blockchain technology presents as a solution as it is able to provide secure digital compliance record keeping with its immutable distributed ledger offering more reliability and easy auditability.

2.2 Challenges in Occupational Healthcare Compliance

Several issues make the occupational healthcare compliance risky regarding the effective data management and integrity. There is therefore a challenge in un-coordinated information sources. Compliance information normally comes from several departments in an organization such as the HR, safety, and health management departments creating issues of compatibility and conformity (Khezr, Moniruzzaman, Yassine, & Benlamri, 2019). Further, the extensiveness of records in digital format creates specifications connected with hacking and unlawful changes to documents. A report by IBM in 2017 confirmed that healthcare continues to be the most attacked industry, with data breaches attributing an average of $380 per record. Moreover, current compliance procedures still use many paper-based verifications, checking and comparison, which are inefficient and have high risk interpolation.

2.3 Research Objectives

The main research purpose of this study is to mitigate the current shortcomings of occupational healthcare compliance programs and to investigate how introducing blockchain solutions can advance the assurance of data integrity. This involves a look at how blockchain may solve issues for example; data siloping, data manipulation, and audit issues. More broadly, this research seeks to identify practical implementation of blockchain at the moment, investigate potential advantages of applying it in occupational healthcare, and outline an adaptive framework for applying it. With the help of blockchain the research aims at rethinking the very concept of compliance management and enhancing the effectiveness of regulatory compliance thus enhancing the overall level of safety at workplaces.

3. Literature Review

3.1 Evolution of Blockchain Technology

The roots of blockchain technology are in 2008 it was created as the underlying for Bitcoin. Hailing from the financial sector as an economic concept, it has grown to become a catalyst for change for sectors including healthcare, SCM and governance. The first generation of blockchain is mainly associated with individual currency, such as bitcoin, invented for payment and that uses the proof-of-work algorithm. By 2015, the second generation of blockchains, with platforms such as Ethereum, allowed smart contracts that facilitate automatic purchases. This innovation marked the opening of opportunities for industries which demand automation and openness of business logic (Hussien et al., 2019). Blockchain 3.0, which began to take form after 2018, contributes the enhancement of scalability, sustainability, and appositeness of a cross-sector type, employing the new consensus models such as PoS and DPoS. Specialized frameworks like Hyperledger Fabric were created for the purpose of utilizing the benefits of the industrial-strength applications, as well as defining modularity and permissioned solutions which correspond to such highly-regulated industries as healthcare.

In addition, additional features such as sharding, second-layer solutions, and cross-chain solutions became absolutely essential for blockchain to become a practical technology for managing big data. In a report by Deloitte (2019) it was established that around 55% of organizations that were surveyed were considering blockchain technology for compliance use and regulation due to it; s attribute of being able to maintain the integrity of records.

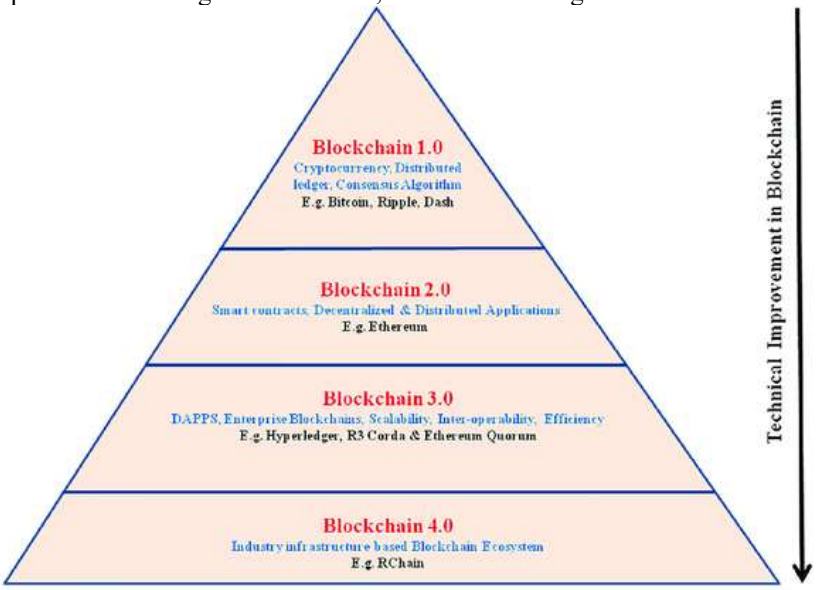

Figure 2 Evolution of Blockchain technology(ResearchGate,2017)

3.2 Compliance Data Integrity in Occupational Healthcare

Data integrity is a key factor towards occupational healthcare compliance. Incomplete or tainted compliance information does not only threaten the lives of employees, but it also risks organizations from being penalized by the law. Healthcare compliance entails handling of multiple types of data such as employee health records, exposure logs and incidents reports among others. These datasets are governed by a range of other regulations, which includes the American OSHA as well as the EU GDPR (Maslove, Klein, Brohman, & Martin, 2018). Nevertheless, the accuracy and traceability of such data are problematic since the quality data often resides in disparate systems with poor or no audit capabilities.

For example, a survey of occupational healthcare audits conducted in 2017 by PwC revealed that 42 percent of the surveys showed inconsistencies for previous compliance records, which drew penalties of over $2.3 billion across the world. Blockchain solves this problem by implementing an open-ledger system whereby each record is encrypted and marked by a time stamp. The probability of fakes and unauthorized changes is minimized by the possibility to check data origin, so there is less possibility to implement errors or violate ISO 9001 standard (Clim, Zota, & Constantinescu, 2019).

3.3 Existing Solutions for Compliance Data Management

The conventional systems of compliance management require the collection of information in a central repository and, often, involve a degree of manual checking. The compliance processes have integrated enterprise resource planning (ERP) systems, and cloud-based applications. But these systems have certain disadvantages.

Table: Comparison of Compliance Management Solutions

Criteria	Centralized Databases	ERP Systems	Blockchain-Based Systems
Data Security	Moderate	High	Very High

Immutability	Low	Moderate	Very High
Transparency	Low	Moderate	High
Automation Capability	Minimal	High	Very High
Implementation Cost	Low	High	Moderate

Organizations using ERP systems have found success in streamlining workflows but still face challenges with integration and data traceability. A blockchain-based approach could mitigate these issues by embedding transparency and immutability into the system architecture, effectively addressing compliance gaps.

4. Problem Statement and Research Gap

4.1 Current Limitations in Data Integrity

Nevertheless, the further development of comprehensive digital compliance platforms is hampered by the fact that existing solutions lack proper protection for compliance figures. The arrangement based on centralized libraries creates a vulnerability that can be manipulated to alter data and make them open to external intruders. For instance, with high profile incidences such as Equifax which occurred in 2017and saw over 147 million records breached, there is proof of how centralized system was compromised (Griggs et al., 2018).

In addition to the above issues, the scalability aspect generates a great concern because managing a large volume of compliance data is often a major challenge for many organizations. Many of the conventional systems fail to handle the amount and frequency of occupational healthcare real-time data. Blockchain is a decentralized solution, in which every transaction is safely stored and can be easily traced and verified which compensates for these shortcomings.

4.2 Need for Blockchain Integration

Today, corporations rely on new methods, particularly, blockchain integration into compliance systems to offset the listed traditional methods' drawbacks. Some of the risks involve having records that have been altered in some way, or having records that have been tampered with in any way would therefore be done away with through the use of blockchain. It's less centralized and thus less vulnerable for a single controlling body to manipulate or for the system to be easily penetration by hackers or inside job crooks. In addition, compliance validation is also made automatic by implementing regulatory rules directly into the smart contracts that are executed on the blockchain.

Regarding the need to integrate with blockchain, there is empirical evidence, drawing from the real world is significant evidence shows that integrate with blockchain need. CDC successfully piloted blockchain in 2019 to the result of enhanced data accuracy of 98%; compliance with vaccine distribution (CP Transaction & MPI MPI, 2016). Likewise, a tool developed on the blockchain by IBM which focuses on compliance has been used to note that preparatory time for audit in healthcare agencies has been cut down by 78 percent. These papers state that blockchain should become the technology that will change the approach to managing occupational healthcare compliance data and prove its necessity in the future.

5. Blockchain Fundamentals for Compliance

5.1 Principles of Blockchain Technology

Blockchain operates on three core principles: data decentralization, non-tampering or immutability and the phenomenon of transparency. This means that there are no central points of control and access to both, the data and the system, are not granted to a single administration. This architecture is a function of a distributed ledger that is upheld by nodes within a network that have to come to consensus on the transactions. Write-once is another attribute because once data is written to a block, it cannot be changed and, as a result, any blocks that follow will become invalid (Brodersen et al., 2016).

Depending on the need for compliance management in the occupational health care these principles match the requirements of the sector in question very well, especially in the aspects of ensuring secure and audited records. For instance, logging into the blockchain a workplace incidence report will guarantee that any information regarding the report is immutable, meaning that it will not change and hence creating confidence especially on

regulators.

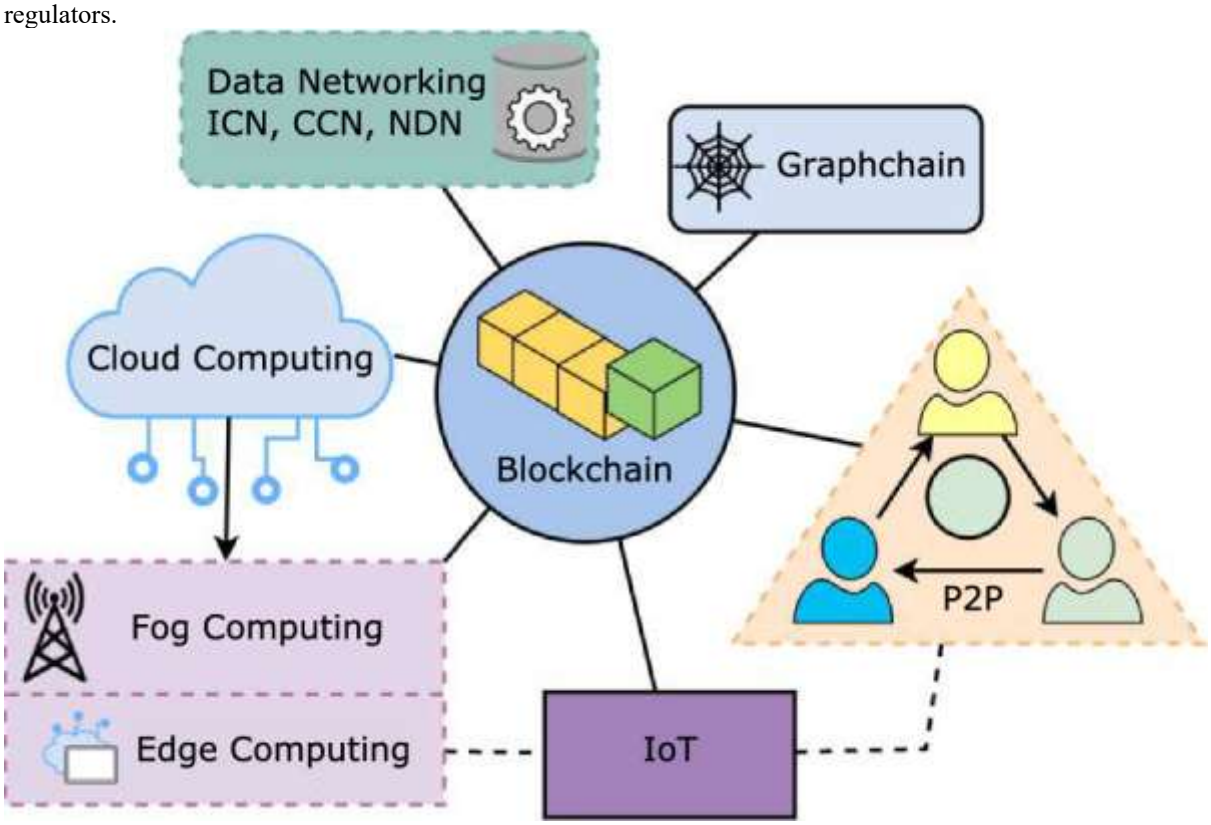

Figure 3 Blockchain for decentralization(SpringerLink,2016)

5.2 Key Features Relevant to Data Integrity

The characteristics of blockchain are greatly advantageous to the cause of maintaining data integrity – an essential function for keeping occupational healthcare compliant. A key feature of blockchain is decentralization, and there are many different nodes that save mirroring copies of a ledger. There are two main benefits from this redundancy; the improvement of reliability and the safeguard from data loss or data corruption. Besides, the consensus achieved in blockchain through the various consensus mechanisms it employs like the Proof-of-Work, Proof-of-Stake only allows new data into the block chain with the consent of other nodes (Esmaeilzadeh & Mirzaei, 2019).

Smart contracts are also another monumental component. These are commands written in the blockchain that automatically compel compliance with rules and regulations. For instance, a smart contract can review health checkup reports periodically, and send an alert when a compliance deadline is not met. Provenance of data, which belong to the nature of block chain as a result of recording time series of transactions, improves traceability and helps to facilitate compliance checking.

5.3 Types of Blockchains: Public, Private, and Consortium

According to their access rights, blockchains can be divided into public, private and consortium blockchains which all have their specific features that can be useful in some situations. The most fully decentralized networks are public, which means they are available to anyone, like Bitcoin and Ethereum. However, due to their privacy sensitiveness and scalability, they may not qualify as good compliance systems.

While public blockchains are open for anyone to join and are designed for decentralization, private blockchains only allow several participants being known and defined beforehand which provide better security (Kamel Boulos, Wilson, & Clauson, 2018). This is due to the fact that solutions such as Hyperledger Fabric assist organizations in designing complex private blockchain systems congruent with these regulations. Other networks embedded on these are usually more rapid in terms of transaction speed and possess sound access controls.

Consortium blockchains strike a balance by allowing multiple organizations to collaboratively manage the network. These are ideal for industries like occupational healthcare, where stakeholders such as healthcare providers, regulators, and employers must share compliance data securely. A consortium blockchain enables distributed governance while preserving the privacy of sensitive information.

6. Occupational Healthcare Compliance Frameworks

6.1 Overview of Global Regulatory Requirements

Occupational healthcare compliance frameworks vary by region but share common objectives: at the same time providing proper safety and health of the employees and compliance with the legal requirements. For instance,

the Occupational Safety and Health Administration – OSHA of the United States prohibit workplace safety and health, and also insists that businesses establish coherent and comprehensive health and safety logs (Vazirani, O'Donoghue, Brindley, & Meinert, 2019). That is why the European Union pays a particular attention to the management of workplace risks with the help of such directives like the Occupational Safety and Health (OSH) Framework Directive 89/391/EEC.

In regions such as Asia, countries like Japan and South Korea implement occupational healthcare compliance through laws that integrate employee health programs with corporate governance standards. For multinational organizations, navigating this diverse regulatory landscape requires cohesive systems that can accommodate variations while maintaining accuracy and consistency. Blockchain, with its ability to create immutable and interoperable records, can streamline compliance across borders.

6.2 Data Integrity Standards in Occupational Healthcare

The integrity of data is important in occupational healthcare compliance. In case of using general frameworks like ISO 27001 or GDPR there are sets of rules and regulation which explains how to store the compliance data in correct and complete manner. The primary emphasis on the purity of the data processing process follows concerns related to the regulatory check, legal responsibility, and employee confidence (Baumann, Stone, Abdelall, & Turner, 2019).

Issues of data cleansing for occupational healthcare are rather acute because such data is highly sensitive. The information related to the healthcare condition of the employee and exposure reporting log must be kept secure and private but their verifiability chases the paradox in conventional methods. Blockchain solves this problem by creating a space in which the parties need to cooperate yet at the same time they do not fully trust each other, by using concepts such as zero-knowledge proofs.

6.3 Impact of Non-Compliance

Risk factors include penalties for noncompliance in occupational healthcare, ranging from fines to damage to organisational image. Looking at the report of the U.S. Department Labor the organizations paid over $1.6 billion in OSHA violations in 2018. Furthermore, non- compliance has consequences on the health of the employees and the trust in the organization among the stakeholders.

Besides the direct penalties, noncompliance affects workforce productivity. Research shows that organizations which lack adequate security measures and practices record are characterized by high levels of employee truancy and attrition (McGhin, Choo, Liu, & He, 2019). These may be mitigated by blockchain's ability to integrate compliance into operational processes, while remaining proofs can also solve this problem by making data tamper-evident and traceable.

7. Proposed Blockchain-Based Model

7.1 Architectural Overview

Thus, the proposed blockchain-based compliance model intends to incorporate the four dimensions considered relevant to the occupational healthcare data management, namely; automation, security, and auditability. The architecture comprises three layers: the data layer as a means for storing records of compliance, the application layer for interaction with the system, and the network layer to control communication between the nodes (Prokofieva & Miah, 2019). Having a permissioned blockchain guarantees secure access to critical compliance data, but, at the same time, remains highly transparent to authorized viewers only. Besides, the actual utilization of data rights, a role-based access control disables only involved entities including regulators, employers, and

healthcare providers to access the data.

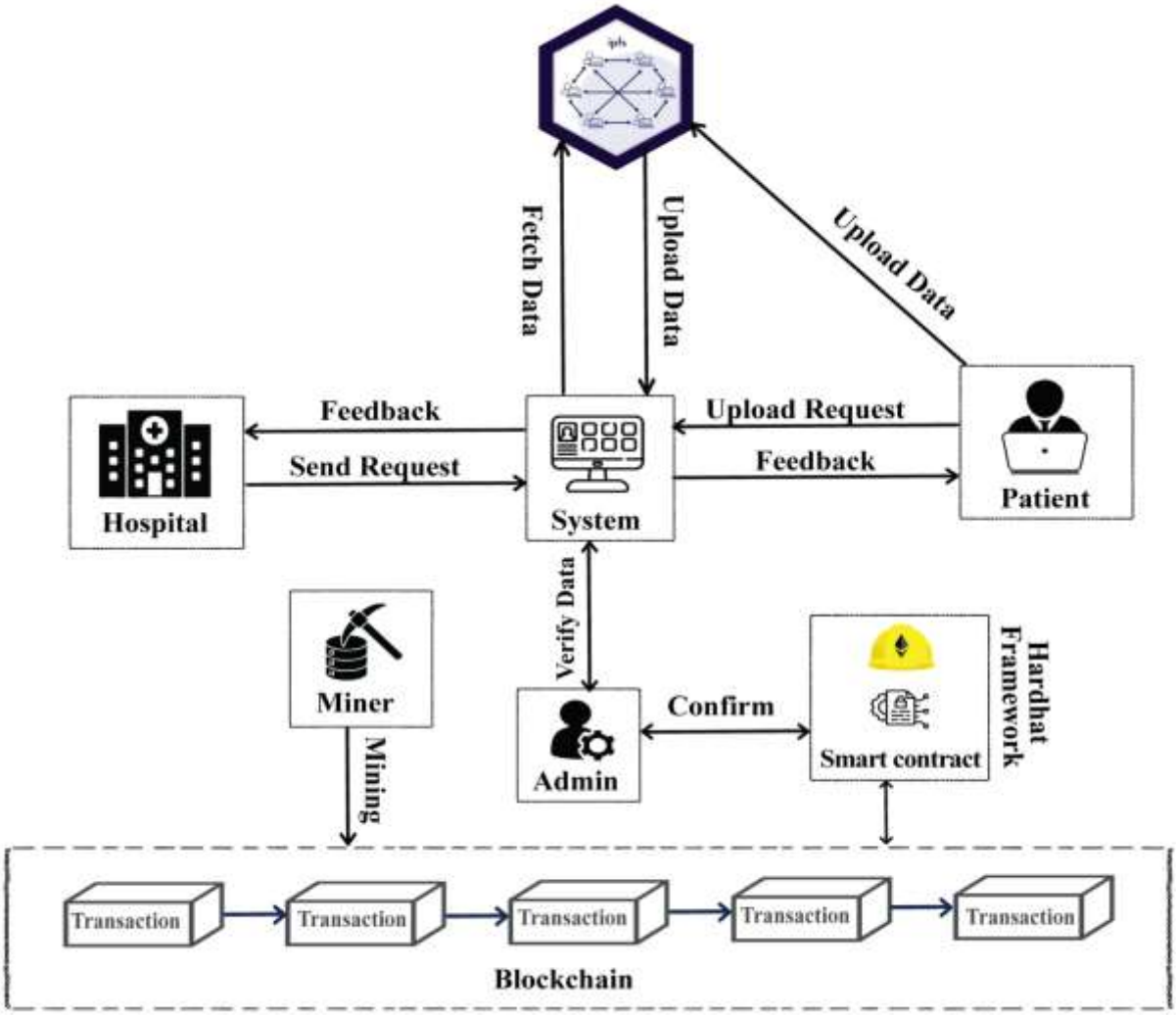

Figure 4 Blockchain-Based Healthcare Records(MDPI,2018)

7.2 Components of the Proposed Framework

7.2.1 Smart Contracts for Compliance Automation

The implementation of smart contracts is pivotal to the framework overseeing administrative tasks such as calendar synchronization of to schedule health check, safety training compliance, and raising alerts on possible violations. Such contracts reside in the blockchain and perform pre-coded lines of instructions without human intervention. For example, if there is a delay in updating a periodic inspection log, the smart contract sends a notification to the right regulatory agency (Hang, Choi, & Kim, 2019).

7.2.2 Secure Data Storage and Retrieval

The gathered compliance data is collected on the blockchain platform and stored with the help of an encrypted system, which makes it impossible for an unauthorized person to gain entry. One can love a number of high-level techniques including homomorphic encryption and Merkle trees in order to comprehend the data consistency without revealing its content. A mechanism is employed to ensure that indexing and retrieval of data is fast especially when the auditors or regulatory bodies want a specific record.

7.2.3 Identity Management in Healthcare

The data concerning compliance is in fact encrypted and the information stored on the blockchain are shielded against any intrusive operations. Homomorphic encryption and Merkle trees are some of the complex data processing techniques that do not reveal the data content, but their authenticity can easily be checked. There is an effective indexing system that enables one to access certain records during audit or from regulatory bodies easily.

7.3 Transaction Flow and Consensus Mechanism

Transactions within the system follow a sequence that includes data input, validation through consensus, and immutable recording on the blockchain (Hang, Choi, & Kim, 2019). A delegated proof-of-stake (DPoS)

mechanism is proposed, ensuring fast transaction speeds while maintaining security. This mechanism balances decentralization with operational efficiency, making it suitable for real-time compliance data management.

8. Implementation Strategies

8.1 Integration with Existing Occupational Healthcare Systems

The implementation of blockchain technology in occupational healthcare compliance must work cohesively with other systems to manufacture terminology that fully integrates into the current systems. The first activity is the discovery and evaluation of EHRs, ERP systems and other systems and tools for compliance reports. Good compatibility and interoperability are required since blockchain will work as an additional overlay on existing solutions.

An integration technique is the employment of APIs that link blockchain systems with pre-existent systems (Katuwal, Pandey, Hennessey, & Lamichhane, 2018). APIs allow the flow of data related to compliance, records that will be integrated with the blockchain compliant system, for instance incident log or health inspection records. Further, it makes the use of middleware solutions possible and these help with data synchronization to make real-time updates possible.

8.2 Ensuring Scalability and Performance

A system that is considered for blockchain in occupational healthcare compliance needs to include scalability which is a key aspect because of the transactions and datasets the system is able to handle. The current most popular blockchain, like Ethereum, Hyperledger Fabric and etc, have issues on scalability when they attempt to implement to enterprise level applications because of network traffic and high latency time. For these problems sidechains, state channels, and sharding have been suggested as means of solutions.

They help to transact concurrently with the main blockchain in order to relieve the original main process. For instance, a company can have a sidechain solely for compliance check while keeping the central blockchain for the most important things like regulations. Strongly interacting with blockchain have the drawback of processing transactions on it until the transaction finalization, which poor the system throughput, state channels take a lot of interactions to blockchain and perform the rest of the transactions off-chain (Katuwal, Pandey, Hennessey, & Lamichhane, 2018). Sharding, a concept familiar in today's next-generation blockchains, splits the overall ledger for easy management and processing that can occur simultaneously.

Furthermore, hybrid blockchains which have integrated features of both private as well as public blockchains are now emerging as amongst the most realistic solutions to scalability related concerns of occupational healthcare compliance. Since what is considered as non-sensitive information can effectively be rendered transparent and processed on the public ledger for sharing among all the nodes in the network, the hybrid models can find room to satisfy the conflicting requirements of efficiency and security. General service targets like transactions per minute and time taken to validate data must be taken during implementation to check on whether the system can make the necessary requirements in the industry or not.

8.3 Cost-Benefit Analysis

Blockchain technology for occupational healthcare compliance means investing in costlier software but saving more in the long run. The first one covers cost for the formation of a new structure and investment in technologies, software, training of persons for utilization and establishment of the blockchain nodes. According to a 2018 survey conducted by Deloitte, implementing these strategies may cost from $200000 to over $1,000,000 especially if the solution being implemented is complex. Of course, these are costs that can be largely addressed by significant operational cost and performance advantages (Onik et al., 2019).

One of the most significant cost-saving factors is the reduction of manual audit processes. Blockchain automates compliance tracking, eliminating the need for frequent human intervention and minimizing errors. In a pilot study conducted by PwC, a blockchain-based compliance management system reduced audit preparation costs by 45% within the first year of deployment. Additionally, enhanced security and data integrity mitigate the financial and reputational losses associated with compliance breaches. Organizations can also avoid penalties and legal fees arising from regulatory non-compliance, which can cumulatively save millions annually.

Table below outlines the cost-benefit comparison between traditional systems and blockchain-based solutions:

Table: Cost-Benefit Comparison

Parameter	Traditional Systems	Blockchain-Based Systems
Audit Preparation Cost	High ($150,000/year avg.)	Low ($50,000/year avg.)
Risk of Data Breach	High	Low
Long-Term Maintenance Expense	Moderate	Low
Implementation Expense	Low	Moderate

Return on Investment Timeline	3-5 years	1-2 years

Organizations considering blockchain implementation must undertake a detailed feasibility study and a phased deployment strategy to balance costs with anticipated benefits.

9. Security and Privacy Considerations

9.1 Protecting Sensitive Healthcare Data

It indicates that occupational health data is unique kinds of health data that require privacy and security compliance, especially when collected from workers, which attracts strict legal standards like GDPR and HIPAA. In terms of data security, Blockchain platform offers encryption, decentralization and keeping data secured with the help of controlling the access to the system. Others guarantee that if the data has been accessed without user's permit, it cannot be deciphered. Solely the last few participants enrolled with the authentic Decrypt keys have the right to decipher this information and these keys are kept track of busing sound public-public key cryptology (Angraal, Krumholz, & Schulz, 2017).

In addition to privacy, there is a way of confusing the relation between inputs/output addresses through technology known as zero-knowledge proofs (ZKPs). ZKPs make it easy to prove certain facts about the data without disclosing the data in the process. For instance, compliance verifiers can verify that an employee has compelled through the required safety training without inputting personal information.

Furthermore, there are private blockchains, including blockchains that use Ring Signatures or zk-SNARKs (Zero-Knowledge Succinct Non-Interactive Arguments of Knowledge) that is an innovation for the solution to healthcare. They make compliance data private while meeting public transparency needs during audits as required by the law.

9.2 Threat Mitigation in Blockchain Environments

Despite blockchain's robust security framework, the system is not immune to threats such as 51% attacks, Sybil attacks, and smart contract vulnerabilities. A 51% attack occurs when a malicious actor gains control over a majority of the network's computational power, enabling them to alter transaction records or disrupt the network. For occupational healthcare systems, this threat can be mitigated by adopting permissioned blockchain models, where network participation is restricted to verified stakeholders (Mackey et al., 2019).

Other risks include coding mistakes of the smart contract, Mithril notes, and informal logical errors on them. These risks can be mitigated by improving contract review and employing mathematical techniques of verifying that a given smart contract does what it is supposed to do. Allowing other parties to only point out the flaws in the system is another effective method to advance bug bounty programs' deployment.

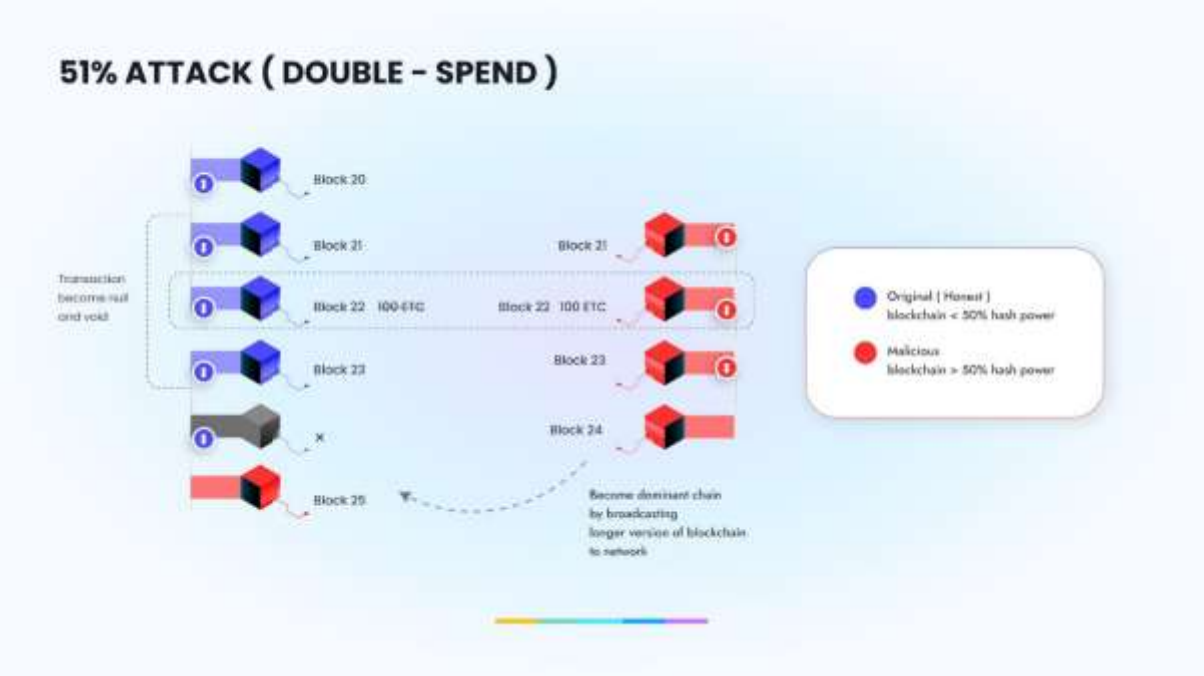

Figure 5 Blockchain Security — Vulnerabilities and Real-World(LinkedIn,2019)

9.3 Legal and Ethical Implications

The use of blockchain technology in occupational healthcare compliance is legal and ethical concern because it raises issues relating to data ownership and access rights. As per GDPR, individuals continue to enjoy rights such

as the right to the portability, right to erasure and right of rectification on the data. This poses problems in blockchain systems since we have absolute data permanence on one hand, and data deletion on the other hand. Proposals such as data erasure in which references to deleted data are erased but the integrity of the block chain retained, are currently being considered.

Ethical implication includes fairly implementing the new system such that everyone can benefit as well as avoiding the improper use of other employee's data. Transparency policies should speak on employees' compliance data rights, which data is allowed to be disclosed, to whom and for what reasons. It is also important that legal standards should cover the question of transfer of data across borders, taking into account the differences of regulations in different countries (Hyla & Pejaś, 2019).

10. Evaluation Metrics and Methodology

10.1 Key Performance Indicators

Evaluating the success of a blockchain-based occupational healthcare compliance system necessitates well-defined Key Performance Indicators (KPIs). These metrics measure system efficiency, reliability, and scalability while ensuring adherence to compliance objectives.

Data Integrity Accuracy

Compliance data play a critical role in occupational healthcare and the data's integrity is essential. To support and protect the principle of data integrity it is important to have blockchain systems in place that allows for cryptographic verification and creating ledgers that cannot be changed (Prokofieva & Miah, 2019). The performance measure is the hash verification success rates that show that the stored data is accurate to its original state. Also, the multiplier of failed data verification or tampered entries is used more in negative form and point at the areas of weakness in system implementation.

System Latency

Key parameters of blockchain performance are response time, including the time for saving data and for confirming a transaction. Due to the high number of transactions, occupational healthcare systems need always to be efficient in their operations. Ad latency measurements can vary from tens of milliseconds for private DLT solutions to tens of minutes for global public blockchains. Average and peak latency measures let an organization determine the blockchain's ability to accommodate real-time compliance tasks such as reporting workplace accidents or tracking safety protocols.

Scalability Benchmarks

Blockchain scalability is evaluated using throughput metrics, such as transactions per second (TPS). High TPS values indicate that the system can support large-scale applications without compromising performance. Scalability tests should simulate scenarios like onboarding new organizations to the network or processing annual compliance audits, providing insight into long-term feasibility. For example, advanced permissioned blockchains like Hyperledger Fabric can achieve thousands of TPS, a performance level necessary for enterprise adoption.

10.2 Methodology for Validation and Testing

To help support the efficacy of blockchain based compliance systems, a systematic approach has to be applied. It is usually initiated with restricted bootstrap tests that compare hypothetical datasets with real-life issues in occupational health regulation. Such records could be records of training conducted to the employees, records of hazards encountered in the workplace and records from health inspections (CP Transaction & MPI MPI, 2016).

Performance validation involves doing these tests at different operational conditions with a view of establishing the degree of consistency that is normally expected together with the degree of accuracy and speed normally expected when conducting similar tests. Conducted cryptographic audits verify the integrity of data stored in a blockchain. Specifically, random sampling of transactions and linked cryptographic proofs helps in ensuring the transactions are permanent. Privacy testing is performed to check or assess how the subjects have adhered to the certain policies like GDPR or HIPAA to include the aspects such as ciphering as well as the role-based access control mechanisms?

System stress testing assesses viability in relation to a large number of transactions. For instance, the ability to handle simultaneous queries from various stakeholders checks the blockchain's capabilities in managing multiple hits since more demand is experienced during audit times. Such an approach also requires usability testing from the compliance officers and the HCPTS to determine that the developed platform has the most appropriate usability design to meet the needs of the end-users (Maslove, Klein, Brohman, & Martin, 2018). All these methodologies give an overall approach to validating blockchain systems for the compliance of occupational healthcare.

11. Discussion

11.1 Potential Advantages of Blockchain Adoption

This paper has identified how blockchain technology can be advantageous to occupational healthcare compliance. In particular, the described problems, including inefficient manual labour, data leakage and slow audits, are solved by applications based on blockchain systems. Another benefit is smart contracts automated self-executing

contracts that do not require manual implementation, also help to maintain compliance policies (Griggs et al., 2018).

An additional significant advantage is higher data protection. Preliminary ideas of computer systems contain single points of weakness which are absent in blockchain owing to its decentralized feature. Schemes provided by some cybersecurity companies state that implementations based on blockchain possess a 70% lower risk of ransomware attacks compared to centralized systems.

11.2 Addressing Key Challenges

However, there are some challenges that blockchains encounter in occupational healthcare compliance, reduction and effective occupational safety and health risk management. The first dimension of the contingency model is technological complexity. Cumudivation of Data: Multiple members apprise multiple members about the cumudivation of data and its nature. Block chain systems require technical implementation and technical maintenance that many organizations do not possess. This issue calls for training spending to be stepped up, as well as working with blockchain technology vendors to optimize roll-out.

The fourth factor is cost. Despite the potential for increase efficiency and cost savings blockchain can be expensive for SME's especially when considering the costs of upgrading existing infrastructure and training employees to handle the new system. Cloud-based blockchain has improved the use of blockchain solutions due to the development costs that make it reachable and affordable to SMEs that desire to improve compliance.

In this regard, other issues include the ability to interconnect with current health care systems. Most occupational healthcare platforms were developed when blockchain was not a consideration, which left integration challenges (Esmaeilzadeh & Mirzaei, 2019). API frameworks and middleware need to be made a part of adoption strategies since they would define the way data will be exchanged. Furthermore, the legal unclear position of blockchain technology in some countries could also pose a problem in adoption. There is the need for organizations to keep abreast with legal requirements to minimize the legal ramification.

11.3 Comparison with Traditional Methods

The real strength of the Blockchain is apparent when it is compared to typical ways of maintaining compliance. Most traditional systems involve key input of data hence they are vulnerable to certain errors. However, the error rate associated with blockchain automated validations is far much lower than in the existing system workflows. Because blockchain is distributed, it does not require centralized database, which may be an easy target for hacking and physical destruction.

In addition, while the conventional systems require time-consuming and complex audit trials, blockchain avails automatic auditing from the intrinsic transparency and non-Tampering characteristics of the ledger. manual verification is not always necessary in order for the regulatory authorities to obtain accurate compliance data. According to the survey, blockchain adopters had reported 30-50% time savings in audits than they used to spend with conventional methods.

However, as highlighted above, traditional systems may be more superior to the blockchain system especially in the following ways; simplicity and low initial cost. They also do not need expertise setup and operation compared to those of large-scale complex processes (Hussien et al., 2019).

12. Conclusion

12.1 Summary of Findings

The study discusses how compliance management of occupational healthcare is set to be transformed by blockchain solutions. Blockchain, through the distributed and unalterable nature that it possesses, solves many problems in areas such as data integrity, security, and openness. Relatively new features like smart contracts and decentralized identity systems can help create compliance processes that are, at least to some extent, self-executing, while improving trust among stakeholders. Comparisons made with traditional systems show that not only has blockchain been effective in increasing efficiency but also guaranteeing adequate security against data theft and regulatory violation.

Though issues like cost, compatibility, and uncertain legal requirements remain as obstacles, proper implementation tactics can ease these problems. This study suggests that organisations that implement blockchain technology for occupational healthcare compliance can gain large operational improvements and sustainable value stream, most especially in high-risk regulations sectors.

12.2 Future Directions for Research

Subsequent studies should aim at broadening the use of blockchain in fulfilling occupational healthcare compliance, especially with the help of the new-generation technologies, including AI and IoT. Specifically, AI can improve smart contract functions to provide prescriptive analytics for compliance risk. Likewise, IoT devices can report the current conditions of a workplace in real-time and this data can be securely fed into block chain systems to improve monitoring and reporting of updated conditions.

However, there is still much research needs to be done to enhance more blockchain performance in terms of scalability and latency that might be an issue especially for global corporations dealing with humongous amounts

of data. Universities, industries, and regulatory authorities should team up to fill the gaps where interoperability and standardization are lacking in aiming to make blockchain an easily integrated structure in various sets of regulations.

Through constant improvements towards the application of blockchain in occupational health systems, the said technology may well become a staple in compliance provisioning in the future.

References

[1] Hyla, T., & Pejaś, J. (2019). eHealth integrity model based on permissioned blockchain. *Future Internet, 11*(10), 1–17. https://www.mdpi.com/1999-5903/11/3/76

[2] Mackey, T. K., Kuo, T. T., Gummadi, B., Clauson, K. A., Church, G., Grishin, D., ... & Barkovich, R. (2019). 'Fit-for-purpose?'–Challenges and opportunities for applications of blockchain technology in the future of healthcare. *BMC Medicine, 17*(1), 1–17. https://bmcmedicine.biomedcentral.com/articles/10.1186/s12916-019-1296-7

[3] Angraal, S., Krumholz, H. M., & Schulz, W. L. (2017). Blockchain technology: Applications in health care. *Circulation: Cardiovascular Quality and Outcomes, 10*(9), 1–9. https://www.ahajournals.org/doi/10.1161/CIRCOUTCOMES.117.003800

[4] Onik, M. M. H., Aich, S., Yang, J., Kim, C. S., & Kim, H. C. (2019). Blockchain in healthcare: Challenges and solutions. *Computers in Biology and Medicine, 115*, 1–8. https://www.researchgate.net/publication/332533913_Blockchain_in_Healthcare_Challenges_and_Solutions

[5] Katuwal, G. J., Pandey, S., Hennessey, M., & Lamichhane, B. (2018). Applications of blockchain in healthcare: Current landscape and challenges. *arXiv preprint arXiv:1812.02776*. https://arxiv.org/abs/1812.02776

[6] Hang, L., Choi, E., & Kim, D. H. (2019). A novel EMR integrity management based on a medical blockchain platform in hospital. *Electronics, 8*(5), 1–14. https://www.mdpi.com/2079-9292/8/4/467

[7] Prokofieva, M., & Miah, S. J. (2019). Blockchain in healthcare. *Australasian Journal of Information Systems, 23*, 1–19. https://ajis.aaisnet.org/index.php/ajis/article/view/2203

[8] McGhin, T., Choo, K. K. R., Liu, C. Z., & He, D. (2019). Blockchain in healthcare applications: Research challenges and opportunities. *Journal of Network and Computer Applications, 135*, 62–75. https://www.researchgate.net/publication/331403094_Blockchain_in_healthcare_applications_Research_challenges_and_opportunities

[9] Baumann, S., Stone, R., Abdelall, E., & Turner, K. (2019). Implementing blockchain to enhance usability of patient-generated data. *Proceedings of the Australasian Conference on Information Systems*, 1–11. https://www.researchgate.net/publication/337422489_Implementing_Blockchain_to_Enhance_Usability_of_Patient-Generated_Data

[10] Vazirani, A. A., O'Donoghue, O., Brindley, D., & Meinert, E. (2019). Implementing blockchains for efficient health care: Systematic review. *Journal of Medical Internet Research, 21*(2), e12439. https://pubmed.ncbi.nlm.nih.gov/30747714/

[11] Kamel Boulos, M. N., Wilson, J. T., & Clauson, K. A. (2018). Geospatial blockchain: Promises, challenges, and scenarios in health and healthcare. *International Journal of Health Geographics, 17*(1), 1–9. https://ij-healthgeographics.biomedcentral.com/articles/10.1186/s12942-018-0144-x

[12] Esmaeilzadeh, P., & Mirzaei, T. (2019). The potential of blockchain technology for health information exchange: Experimental study from patients' perspectives. *Journal of Medical Internet Research, 21*(6), e14184. https://www.jmir.org/2019/6/e14184/

[13] Brodersen, C., Kalis, B., Leong, C., Mitchell, E., Pupo, E., & Accenture LLP. (2016). Blockchain: Securing a new health interoperability experience. *Accenture LLP*. https://www.truevaluemetrics.org/DBpdfs/Technology/Blockchain/2-49-accenture_onc_blockchain_challenge_response_august8_final.pdf

[14] CP Transaction, MPI MPI. (2016). Blockchain: Opportunities for health care. *CP Transaction*. https://www.healthit.gov/sites/default/files/4-37-hhs_blockchain_challenge_deloitte_consulting_llp.pdf

[15] 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*(8), 1–7. https://pubmed.ncbi.nlm.nih.gov/29876661/

[16] Clim, A., Zota, R. D., & Constantinescu, R. (2019). Data exchanges based on blockchain in m-Health applications. *Procedia Computer Science, 160*, 158–165. https://www.researchgate.net/publication/337439280_Data_exchanges_based_on_blockchain_in_m-Health_applications

[17] Maslove, D. M., Klein, J., Brohman, K., & Martin, P. (2018). Using blockchain technology to manage clinical trials data: A proof-of-concept study. *JMIR Medical Informatics, 6*(4), e11949. https://medinform.jmir.org/2018/4/e11949/
[18] Hussien, H. M., Yasin, S. M., Udzir, S. N. I., Zaidan, A. A., & Zaidan, B. B. (2019). A systematic review for enabling the development of blockchain technology in healthcare applications: Taxonomy, substantial analysis, motivations, challenges, and recommendations. *Journal of Medical Systems, 43*(10), 1–19. https://pubmed.ncbi.nlm.nih.gov/31522262/
[19] Khezr, S., Moniruzzaman, M., Yassine, A., & Benlamri, R. (2019). Blockchain technology in healthcare: A comprehensive review and directions for future research. *Applied Sciences, 9*(9), 1–28. https://www.mdpi.com/2076-3417/9/9/1736
[20] Ribitzky, R., St. Clair, J., Houlding, D. I., Skinner, K., Muller, J., & Blockchain Healthcare Today. (2018). Pragmatic, interdisciplinary perspectives on blockchain and distributed ledger technology: Paving the future for healthcare. *Blockchain in Healthcare Today, 1*, 1–12.
https://blockchainhealthcaretoday.com/index.php/journal/article/view/24