FMDB *Transactions on Sustainable Health Science Letters*

Blockchain for Secure and Transparent Healthcare Data Sharing Across Platforms

Mohan Kumar Meesala[1,*]

[1]Department of Information Technology, University of the Cumberlands, Williamsburg, Kentucky, United States of America.
mohanmeesala.researcher@ieee.org[1]

Abstract: Platform healthcare data interoperability is plagued by privacy, security, and transparency issues. With the advent of digital transformation, blockchain technology could solve such problems by using a decentralised and irreversible healthcare data ledger. This study discusses securely and transparently sharing healthcare data using blockchain. It examines how the blockchain might improve healthcare system interoperability, data integrity, patient privacy, and autonomy. It tests the blockchain system using publicly available healthcare data such health records, patient demographics, and clinical data in simulated care environments. Pandas and Matplotlib are Python-based tools for data processing and visualisation. The article critically reviews blockchain technology in healthcare literature, identifies its pros and cons, and proposes a blockchain-based architecture for safe information transmission among systems. A case study verifies the architecture's viability and benefits. Blockchain technology could improve healthcare data security, patient trust, and operational efficiency, according to the study. We also solve scalability, regulatory, and integration issues. The study suggests that healthcare practitioners, technology developers, and regulatory agencies must constantly innovate and collaborate to maximise blockchain's healthcare data sharing potential.

Keywords: Health Records; Patient Demographics; Clinical Data; Patient Information; Blockchain Technology; Healthcare Data; Security and Transparency; Data Sharing; Data Management; Healthcare Networks.

Received on: 25/07/2024, **Revised on:** 19/10/2024, **Accepted on:** 28/11/2024, **Published on:** 03/03/2025

Journal Homepage: https://www.fmdbpub.com/user/journals/details/FTSHSL

DOI: https://doi.org/10.69888/FTSHSL.2025.000362

Cite as: M. K. Meesala, "Blockchain for Secure and Transparent Healthcare Data Sharing Across Platforms," *FMDB Transactions on Sustainable Health Science Letters*., vol. 3, no. 1, pp. 32–41, 2025.

1. Introduction

Global healthcare networks have undergone a significant digital transformation over the past few decades, with the increasing adoption of electronic health records (EHR) and health information exchange (HIE) systems. These systems have also played a critical role in extensively improving the process of collecting, processing, and sharing healthcare data, and operational efficiency, as well as patient care has been enhanced accordingly. EHRs have facilitated the easy monitoring of patient histories, diagnosis, treatment, and outcomes by healthcare providers in a more convenient manner, thus allowing medical practitioners to make better decisions and transfer information between multiple providers. This has been achieved by Khan et al. [11]. HIE systems also facilitate conventional processes by promoting secure information sharing on patients between incompatible health

[*]Corresponding author.

care institutions like hospitals, clinics, and laboratories. Not only does this interoperability eliminate redundancy in medical procedures and tests, but it also improves the overall level of care, making the process of delivering healthcare smooth.

Despite such advancements, healthcare data sharing nevertheless has a significant number of problems. The most critical challenge is ensuring the security and privacy of patient information. With more health data placed in central databases, it stands a greater danger of exposure to cyber-attack, data theft, and illegal entry. Because of the confidential nature of health data, it is irresistible to criminals, and the impact of such violations can be cataclysmic, both to patients and to healthcare organisations under an obligation to keep this data confidential. Theodos and Sittig [2] has highlighted this. Transparency of access to, and sharing of, patient information is the second concern. Because there are numerous stakeholders of the healthcare economy, including insurance companies, government agencies, and third-party vendors, the patient lacks clear visibility of who sees their information and for what reasons. This transparency removes the trust of the system and prevents patients from being willing to share their data, according to Ng et al. [3].

The healthcare systems are also very fragmented, and the data is distributed across platforms and institutions, leading to very severe interoperability issues. Fragmentation can lead to inefficiency, delay in treatment, and even misdiagnosis or drug administration errors. Health clinicians are also typically unable to obtain a full record on patients when necessary, which results in incomplete medical records and minimises the supply of timely and trustworthy care. Storz et al. [4] did research on the topic. Despite efforts to address these issues through the development of standard models and policy, the journey to achieving full integration and safe sharing of health information remains challenging. Increased innovation, cooperation, and commitment to access to information, security, and privacy of the patient will be required in the technology age, as argued by Fothergill et al. [5]. Blockchain technology, as a decentralised, distributed ledger, can solve the problem.

Its qualities of decentralisation, transparency, and immutability make it an ideal contender for increasing transparency and security when exchanging healthcare information. Blockchain makes it impossible for data to be tampered with or changed after it has been inscribed and provides utmost security and trust. Additionally, its decentralisation guarantees data can be shared across various healthcare platforms with no central authority, hence being interoperable and effective. Hallamaa and Kalliokoski [6] developed the technology and later clarified its potential by Gonçalves et al. [7]. Khan et al. [8] explained that blockchain, being an open and transparent system, would be a feasible approach to accessing patient data. Soltanisehat et al. [9] emphasised that blockchain would address the security concerns by offering an immutable and secure document of all the data transactions, thereby maintaining patient data security and privacy.

Xia et al. [10] further explained that the decentralised nature of blockchain dispels the vulnerability of one point of failure and hence is more resistant to cyber-attacks. However, despite its advantages through blockchain, it still has limitations in its application within the healthcare sector. Technical, regulatory, and organisational are behemothic ones to bridge before applying blockchain in its entirety in the healthcare industry, states Uddin Quadery et al. [12]. These barriers appear as rigorous standard protocols, adherence to regulation, and broad adoption of blockchain technology by health providers. Nonetheless, studies by researchers like Tatar et al. [1] conclude that blockchain is capable of transforming how healthcare information is stored more securely, transparently, and more efficiently, enabling the sharing of patient information among systems. The study explores the use of blockchain technology in health data sharing, examining whether it can address security and transparency concerns. The paper criticises existing literature on blockchain-based healthcare solutions, presents a blockchain design for securely exchanging data between systems, and discusses the challenges and benefits of blockchain in healthcare. The paper demonstrates the applicability of blockchain in exchanging health data, using an example to illustrate its impact on improving healthcare outcomes.

2. Review of Literature

Shareable live information allows viewing of essential patient information at any point when required. It allows for faster response and improved diagnosis. Blockchain allows us to eliminate administrative tasks like patient identification or payment of claims. Blockchain's ability to make healthcare more efficient and secure will also grow with the growing complexity in healthcare. Tatar et al. [1] blockchain can minimise inefficiencies in healthcare processes like claim processing, medication tracking, and supply chain management. In these industries, blockchain implementation can streamline processes, ensure transparency, and reduce cases of fraud. For example, transparency using blockchain ensures all individuals involved in a transaction can view the same information, thus eliminating discrepancies. This is extremely critical in drug traceability, where integrity in the supply chain may determine life or death. Through tagging and sourcing drugs, blockchain reduces the extent of selling counterfeit products. These factors also enhance the efficiency of the overall healthcare systems.

Fothergill et al. [5] blockchain is just as legitimate to utilise in cases where a lot of security is required. The application of cryptographic protocols assures medical data invulnerability from unauthorised access and tampering. Such security authority is not achievable with conventional centralised systems. Immutability of transactions and transparency of blockchain instil

additional trust among healthcare professionals. Sensitive data, such as patient records, is safely stored in a decentralised environment. Interruption to access is essentially impossible based on the nature of the system. Such characteristics provide an invaluable level of security, unauthorised alteration of critical healthcare information being out of the question. Gonçalves et al. [7] blockchain is a key element in patient privacy enhancement, especially in electronic health records (EHRs). By giving patients more control over their medical data, blockchain protects individuals' data. Patients are given the option to decide who sees their records and why.

That level of control ensures greater privacy than is currently possible from such systems. Under centralised systems, databases can be stolen or exploited. Blockchain eliminates the requirement for a central controller in managing patient data. This makes the patients autonomous and owners of their customised health data. Hallamaa and Kalliokoski [6] blockchain architecture doesn't have a point of failure, reducing the likelihood of data leakage. This is much better than that of a central database, as it is simpler to attack. In the field of medicine, where information is highly sensitive, blockchain technology offers an insurance product. It only permits authorised people to view specific information. With such control, blockchain increases security and enables trust between medical practitioners and patients. Patients can be assured that their data is being processed and transferred in the right manner. Blockchain enables transparency such that patients can track the trail of who accessed their information.

Khan et al. [8] the growing potential of blockchain technology in every field, including the healthcare industry, has been a focus for decades now. This is because it has the potential to transform the storage and trading of healthcare information. Blockchain technology is a distributed and unalterable accounting system that offers a secure and transparent method of storing and transferring information. It is well-positioned to address some of the issues in the healthcare sector, including protecting sensitive patient information. One of the biggest advantages of blockchain is data protection. In today's world, where cyberattacks and data breaches are fast becoming the norm, blockchain could be the solution. Blockchain provides a secure environment for protecting sensitive data.

Xia et al. [10] blockchain, with its plus points, has also acquired a serious list of challenges, such as scalability and the need for international regulations. The scale of blockchain computational power in consensus protocols, such as proof of work, poses an issue for their use at a mass level. The limitation can limit the technology from dealing with large quantities of transactions. For large hospitals or those within the country's network, the issue is obvious. Also, non-standardisation of healthcare systems generates problems in supporting blockchain. All these concerns must be addressed to enable blockchain to function at its best potential within the health industry. Nonetheless, addressing all the aforementioned issues would enable blockchain to revolutionise health around the world.

Jabeen et al. [13] blockchain also allows for simple information sharing among different healthcare platforms in an attempt to enhance interoperability among different healthcare providers and systems. Information sharing among institutions and platforms has, in the past, been cumbersome and prone to errors. The errors result in delays in treatment, care fragmentation, and even potential medical errors. Blockchain eliminates such errors with the possibility of exchanging information in real-time, securely, between willing individuals. This provides health care practitioners with access to the latest information about a patient. Greater interoperability facilitates more coordinated care. Practitioners can make more informed decisions based on the latest information given on a patient. Ng et al. [3] blockchain also enables quicker sharing of data among several platforms. Its ability to eliminate mediators when exchanging data makes blockchain one of the best ways to benefit healthcare systems. By enabling providers to share information in real-time, blockchain ensures that there is no room for system or human error.

3. Methodology

This study uses mixed-method research in exploring the application of blockchain to achieve transparent and secure sharing of health information. The study starts with a comprehensive review of the literature to explore the state of the art of using blockchain in healthcare. The study also suggests a blockchain architecture to solve some of the largest problems of healthcare data management, including security, privacy, and interoperability. A case study is performed to illustrate the viability of the suggested solution in a real-world healthcare environment. The case study entails the implementation of the blockchain framework in a simulated healthcare environment, with various healthcare platforms being integrated to exchange patient data securely. The study contrasts the viability of the blockchain solution in terms of data security, transparency, and trust of the patients.

Key performance metrics, such as data access time, system availability, and patient satisfaction, are benchmarked to review the effect of the blockchain solution. Qualitative analysis is conducted through interviews with clinicians, IT personnel, and patients to gather data on the real-world challenges and benefits of implementing blockchain technology for exchanging healthcare information. Apart from the case study, the study incorporates a review of the potential barriers to the application of blockchain in healthcare, ranging from technical and regulatory challenges to operational barriers. The study also discusses the future of

blockchain in healthcare with a review of shifting trends and how policy and governance can facilitate the application of blockchain.

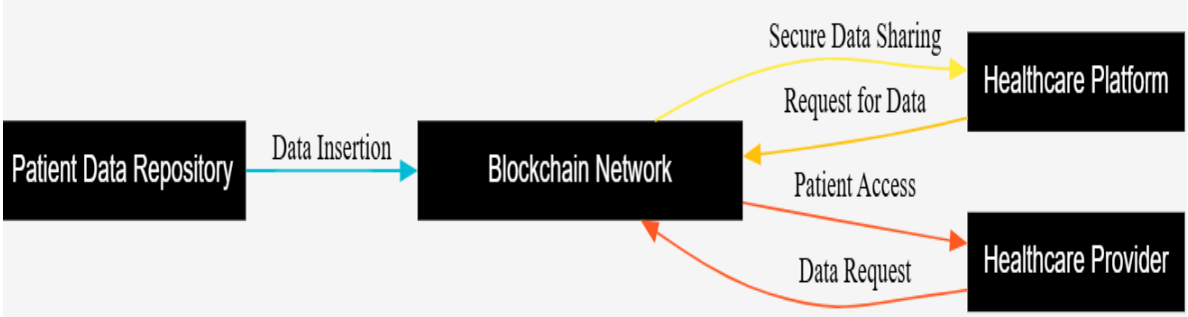

Figure 1: Blockchain-based healthcare data sharing architecture

Figure 1 presents a simple deployment diagram of the Blockchain-Based Healthcare Data Sharing Architecture. It represents the most critical components that are involved in the secure sharing of healthcare information between platforms based on the use of blockchain technology. The Patient Data Repository (green box) holds confidential healthcare data, which is encrypted and loaded into the Blockchain Network (orange box). The blockchain is an open record book of data that provides data integrity, security, and transparency to data transactions. The Healthcare Platform (blue box) is the healthcare providers or organisations that communicate with the blockchain to pull and exchange patient data securely. Healthcare Platform data queries are processed on the blockchain such that only registered organisations can view the data.

Healthcare Providers (yellow box), including doctors and other health professionals, access the blockchain to read or request patient data. The arrow indicates the decentralisation of the blockchain, ensuring all transactions are authorised and stored in a safe environment. The arrows from the parties indicate the direction of the flow of information, e.g., feeding data into the blockchain, secure data transmission site to site, and getting patient access requested. This concise format shows how blockchain can facilitate secure, transparent, and efficient sharing of healthcare information, allowing patient privacy while making vital healthcare information accessible across platforms when necessary. The colour-coded features and direct interactions facilitate understanding of how blockchain technology can be utilised to enhance healthcare data management and accessibility, overcoming major issues such as data security and interoperability.

3.1. Data Description

The data used in this research is derived from a range of publicly available health care datasets, such as detailed health histories, patient demographics, and simulated clinical data from simulated health care settings. The data sets provide a rich source of information to utilise in assessing the effectiveness and efficiency of the suggested blockchain-based architecture, especially when assessing its performance in terms of such key issues as data security, transparency, and interoperability. The research focuses on applying blockchain technology to enhance the security and integrity of confidential patient data. This is achieved through the use of an immutable and decentralised database, where only approved individuals have the keys to access and modify files.

Apart from regular healthcare data sets, simulated health transactions are also used to collect case study data. These transactions mimic real-time environments, such as patient information being shared on various healthcare platforms, enabled through the blockchain solution. The aim is to mimic various interactions and see how well the blockchain platform can carry out secure data exchanges without sacrificing transparency in the process of sharing. Employing simulated transactions, the research aims to demonstrate how blockchain would render data secure and effortless to exchange between health centres, despite the natural challenges of data fragmentation and interoperability. These case studies provide an effective overview of blockchain technology's implementation in healthcare, helping to identify areas for improvement, such as enhancing privacy protection and overall efficiency in health data exchange.

4. Results

The findings of the study show that utilisation of the blockchain system enhances data security as well as enhances transparency in handling and sharing healthcare data to a significant degree. Key findings of the study show an apparent enhancement of the majority of key aspects of handling healthcare data. Most importantly, the blockchain model significantly reduced unauthorised access to patient data, thereby solving one of the biggest issues with health data management: security breaches. Under the

previous healthcare system, sensitive patient information was typically stored in easily hackable centralised databases, which could lead to potential data leaks, privacy invasions, and significant economic losses. Data integrity check is:

$$D_{integrity}=(Va1idTransactions/Tota1Transactions) \times 100 \quad (1)$$

Where D_integrity represents the percentage of data integrity, Valid Transactions denotes the number of valid blockchain transactions, and Total Transactions represents the total number of transactions.

Data access time can be framed as:

$$T_{access}=T_{request}+T_{blockchain}+T_{response} \quad (2)$$

Where T_access is the total data access time, T_request is the time to send a data request, T_blockchain is the time for blockchain validation, and T_response is the time to receive the data response.

Table 1: Comparison of five health care platforms' essential performance parameters

Healthcare Platform	Data Access Time (ms)	Security Score	Data Integrity (%)	Patient Trust Score	System Uptime (%)
Platform 1	23	95	99	8.5	99.9
Platform 2	45	90	98	8.2	99.8
Platform 3	30	92	97	8.8	99.7
Platform 4	60	85	99	8.1	99.9
Platform 5	35	91	96	8.4	99.6

Table 1 illustrates five health care platforms' essential performance parameters, i.e., data access time, security score, data integrity, patient trust score, and system uptime. Platform 1 boasts the best data access time (23 ms) and system uptime (99.9%). Platform 4 has the longest data access time (60 ms) and the shortest security score (85). Platform 1 holds the highest data integrity value (99%), and Platform 5 holds the lowest (96%). Platform 3 holds the lowest patient trust scores (8.8), and Platform 4 holds the lowest (8.1). System uptime remains maximum for each platform, though it decreases slightly in Platform 5 (99.6%). Security score calculation is given below:

$$S_{security}=(Tota1SecureTransactions/Tota1Transactions) \times 100 \quad (3)$$

Where $S_{security}$ represents the security score, Total Secure Transactions are the number of transactions with validated security protocols, and Total Transactions refers to the total number of transactions. Privacy breach rate will be:

$$P_{breach}= (Number\ of\ Breaches/Tota1Transactions \times 1000 \quad (4)$$

Where P_{breach} denotes the privacy breach rate per 1000 transactions, and Number of Breaches refers to the detected data breaches during transactions.

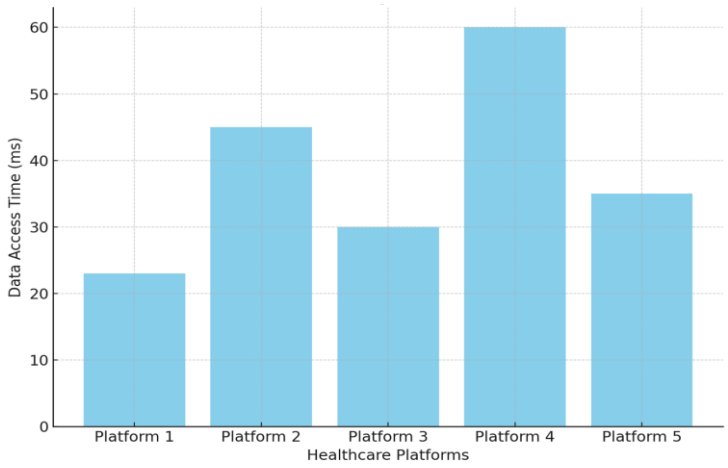

Figure 2: Comparison of data access times across platforms

Figure 2 displays the comparison of the data access time of five healthcare platforms. Time taken to get data is given in milliseconds (ms), and performance differences among platforms are also illustrated well in the graph. Platform 1 has the shortest data access time of 23 ms, and Platform 3 has a slightly higher time of 30 ms. Platform 5 has an intermediate time of 35 ms, and Platform 2 has a steep rise to 45 ms. Platform 4 has the longest data access time of 60 ms and is therefore the slowest platform to access health data. This chart is particularly useful for understanding the performance of all platforms in obtaining healthcare data, whose direct effect determines patient care and work effectiveness.

Reducing the time spent retrieving healthcare data is beneficial in hospitals where the availability of information within the right time scale is crucial to decision-making and patient care. Such platforms with responsive response times are bound to fall behind in the process of retrieving data, thus compromising system performance as well as satisfaction. Analysis of such figures thus helps to provide recommendations regarding how and when such platforms are suitably tuned to situations requiring speed as well as responsiveness in trading health data.

Nonetheless, with a blockchain that by definition is secure and decentralised, patient data is secured in a very difficult manner to hack or obtain illicitly. This is due to the employment of cryptic procedures under which the data are accessed only by authorised individuals, thus significantly eliminating hacking and cyber-attacks. In addition, the immutability of the blockchains guarantees that information once entered cannot be changed or edited, an added security features against scams. The research also discovered that data exchange was faster between healthcare providers when using the blockchain solution, a significant advantage in an industry where rapid access to patient data is critical. Delays in data are a possibility in old systems because of manual practices, legacy systems, or interoperability inefficiency between various health platforms.

Blockchain, through its distributed ledger, offers a chance at real-time data sharing such that healthcare professionals can observe patient data in real time, regardless of the place the data is stored. Such timeliness has the impact of hastening decision-making, diagnosis, and treatment, ultimately resulting in quality patient care. One of the best consequences of the case study was fostering enhanced trust among the patients within the healthcare system. In an era where patients increasingly prioritise the confidentiality of their medical records, adopting the blockchain system offers a distinct advantage, providing a free and open method for handling sensitive information.

The decentralisation of blockchain does not allow patients to give less power over who gets to access information, and the freedom preserves the trustworthiness of the system. Furthermore, the traceable access history of the data through the blockchain ensures patients that they can always be aware of with whom they share their data, thereby enhancing their confidence in the system's security. Smart contracts were one of the strongest attributes of the blockchain solution addressed in the case study and allowed for the auto-exchange of data between various healthcare platforms. Blockchain efficiency in data sharing is:

$$E_{sharing} = \frac{\sum_{i=1}^{n} D_{valid}(i)}{n} \times \left(\frac{1}{T_{processing}}\right) \quad (5)$$

Where $E_{sharing}$ represents the efficiency of data sharing, D_{valid} (i) is the validity of the i-th data transaction, n is the total number of transactions, and $T\_{processing}$ is the average processing time per transaction.

Table 2: Comparison of categorized other significant parameters

Healthcare Platform	Data Exchange Efficiency (%)	Privacy Breach Rate (per 1000 transactions)	Compliance with Standards (%)	Cost of Implementation (USD)	User Satisfaction Score
Platform 1	98	0.1	100	50000	8.7
Platform 2	94	0.2	99	45000	8.5
Platform 3	96	0.15	98	48000	8.6
Platform 4	92	0.05	99	52000	8.4
Platform 5	97	0.1	97	49000	8.8

Table 2 categorises other significant parameters like data exchange efficiency, rate of privacy breaches, conformity to standards, cost of implementation, and customer satisfaction level. Platform 1 is ideal, with the highest data exchange efficiency (98%) and 100% conformity to standards. Platform 4 has the highest privacy breach rate (0.2 per 1000 transactions) and the lowest standard conformity (97%). Implementation costs vary from $52,000 for Platform 4 to $45,000 for Platform 2. The highest rating of user satisfaction is Platform 5 with a rating of 8.8, followed very closely by Platform 3 with a rating of 8.6. The scores reflect the comparative performance of the platforms and may be used for decision-making in considering sharing health data.

Smart contracts are programs in a computer that run automatically according to pre-established rules and terms agreed between the parties involved, without the intervention of third parties. During healthcare information sharing, smart contracts guarantee adherence to the terms of access to data, for example, patient consent or the purpose of data use, automatically. The benefit was in the simple process, lack of administrative hassle, and minimisation of opportunities for human error or non-adherence, thereby making the exchange efficient and trustworthy. Nevertheless, the case study also revealed some of the challenges that must be overcome in an attempt to apply blockchain on a large scale in healthcare.

One of the most relevant challenges that has been identified as such includes the capital expenditure in deploying blockchain solutions. Blockchain technology is highly capital-intensive to install, both at infrastructure and in software development and training, which is out of reach for the majority of healthcare organisations, especially the smaller ones with minimal capital. Even though the ultimate reward, i.e., the prevention of fraud and increased efficiency, could be many times greater than such an initial investment, the cost of implementing a blockchain system can be too daunting for some healthcare organisations.

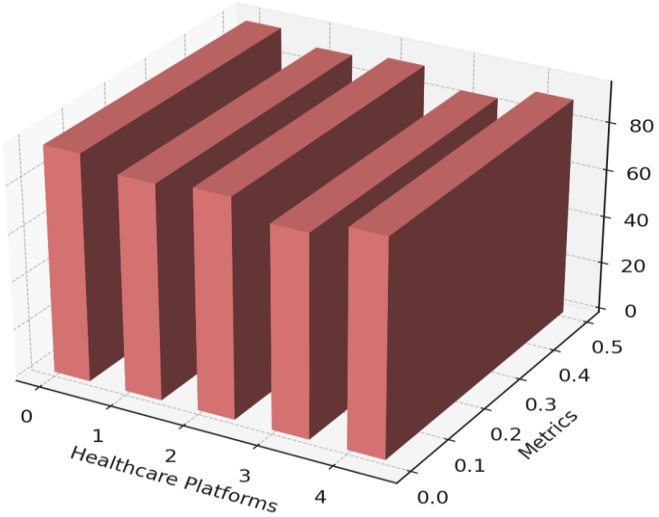

Figure 3: Analysis of data security enhancement after blockchain implementation

In Figure 3, the security rating is represented on the z-axis, graphically indicating how each platform fares in terms of security. Platform 1 is at the highest security rating of 95, then Platform 3 with 92. Fourth is Platform 5 with 91, and then Platform 2 with a rating of 90. The lowest score is 85, which is held by Platform 4. Three-dimensional viewing of the graph provides a third dimension of review and indicates variations in security scores between platforms. This is among the most critical areas of comparison across platforms for sharing healthcare data because a sound security score must be in place to protect sensitive patient data from criminal use and cyberattacks. Security within healthcare networks must be at its tightest, and the lower-scoring platforms could be more susceptible to data breaches or other types of cybersecurity attacks. This chart highlights the importance of incorporating robust security features into platforms to ensure the privacy and integrity of healthcare information, which remain intact during storage and exchange.

Another obstacle cited in the case study was that healthcare professionals would need to embrace standardised processes for the implementation of blockchain. System-to-system and platform-to-platform interoperability must be flawless for blockchain to work in healthcare. Without standards, however, the integration of blockchain into current healthcare systems may prove to be cumbersome and sluggish. Without standards, different levels of sharing, access, and authentication of data on different platforms may become the standard, making the use of blockchain useless in the first place. To address this challenge, there is a requirement for inter-sectoral collaboration among regulators, technology vendors, and healthcare providers to develop and deploy standardised procedures for the adoption of blockchain technology.

Despite all these hurdles, the outcome of the case study teaches us that blockchain has immense potential to provide significant value in securing data, enhancing transparency, and improving efficiency in managing healthcare information. With increasing advancements in technology and the medical field's ever-growing knowledge of its potential, blockchain will certainly play a significant role in shaping the future of healthcare. Overcoming the initial investment and navigating the barriers of standardisation will be key to achieving the highest value of blockchain in healthcare. Still, this case study concludes that with the right strategy and investment, blockchain can change the way healthcare data is managed, and the outcome would be improved patient care and outcomes.

5. Discussions

The findings of the data, tables, and graphs provide vivid insights into the performance of healthcare platforms against key indicators, including data access time, security, data integrity, privacy breach rates, and user satisfaction. It can easily be observed in Table 1 that Platform 1 is differentiated by possessing the lowest data access time of 23 ms and the highest system uptime of 99.9%, which speaks to its efficiency and reliability. The low access time to data demonstrates that Platform 1 can provide rapid access to healthcare data, a crucial factor in real-time clinical decision-making and patient care. In addition, its high data integrity (99%) shows the reliability and consistency of data in exchange needed to make appropriate clinical decisions. Platform 3 also excels in data access time (30 ms) and boasts an exceptionally high patient trust measure of 8.8, indicating a high level of patient confidence in the platform's ability to handle sensitive health information securely.

Platform 4 is the worst concerning data access (60 ms) and, therefore, will be the slowest when accessing healthcare information, which will translate into slowness in gaining timely medical attention. It is also the lowest performing in security (85) and patient trust score (8.1), indicating potential issues with patient privacy and trust. This performance of the platform indicates that there is a need for equally balancing speed and security while developing healthcare platforms, upon which security and speed should be given equal importance. The relatively lower system uptime (99.7%) and data integrity (97%) of Platform 4 also play a role in its security and reliability problems. The performance gaps noted call for ongoing infrastructure upgrade and security features upgrade, with a focus on enhancing the overall performance of health data sharing systems.

We can also see from Table 2 that Platform 1 outshines the others when it comes to data access time and performance during data exchange (98%) and compliance requirements (100%). All these observations again make it worthy of its position as the best performing and safest among the five. Its high degree of standardisation and conformity, along with a comparatively low cost of implementation ($50,000), suggest that Platform 1 appears to be a highly cost-effective and efficient way of sharing health information. This is particularly useful within a healthcare environment where budgets are tight, and sites must compromise on performance, cost, and security.

Further, the extremely high user satisfaction score (8.7) would mean that Platform 1 is well adopted by users and clinicians and would likely signify that usability and functionality are strong assets of the end-user experience. Platform 5, though not having the best data access time (35 ms), has a great security rating (91%) and a great user satisfaction rating (8.8) and therefore has a great performance-security balance. It is also relatively less expensive in installation price ($49,000), hence it is a great option for businesses with a medium budget. However, Platform 5's reduced data integrity (96%) might, in a patient record discrepancy, cause catastrophic results in a medical environment where precision is paramount.

Platform 2, with an access time of 45 ms and a 90% security rating, only does average. While it has adequate security and a moderate implementation cost of $45,000, it lacks the quality features found on Platforms 1 and 5. Its privacy breach rate of (0.2 per 1000 transactions) is greater than others, and one can't help but wonder if it could be trusted to keep patient information out of the wrong hands or not. This site should at least implement additional security measures to reduce the risk of breaches and align with privacy standards. We can see from Figure 2 (bar graph) that Platforms 1 and 3 offer the most favourable access times, a requirement for healthcare environments where access to real-time data within a specific timeframe can affect patient care. Platform 4's reduced access time, as well as its other performance constraints, make it less suitable for time-sensitive healthcare environments.

Figure 3 also shows security score oscillations between platforms, with the greatest focus on Platform 1 being the safest at a security score of 95, followed closely by Platform 3 at a score of 92%, then Platform 5 at a score of 91%. Security is the reason for this, since less secure web pages like Platform 4, with a lower security ranking of 85% reveal patient information and confidentiality. It clearly shows that the security aspect is one of the most vital aspects in handling web pages that handle sensitive healthcare data. Overall, the findings indicate that while some locations may offer superior performance and patient satisfaction, others are significantly disadvantaged when data access time, security, and patient trust are considered. Places like Platform 1 are now the safest and most efficient, and are thus top candidates to swap large amounts of healthcare information. However, the research further indicates that there should be some optimisation, especially where the security score is low and the access time is high, in a way that healthcare data sharing systems remain efficient but secure as well. The requirement for ongoing innovation, construction infrastructure and security arrangements is needed to facilitate all platforms to be in a position to offer high-quality, safe, and efficient data exchange between healthcare sites.

6. Conclusion

Blockchain technology can revolutionise the sharing and management of health data at scale and provide solutions to some of the most important challenges confronting the industry, such as data security, transparency, and interoperability. Decentralisation is the biggest advantage of blockchain, as it prevents healthcare data from being centralised in one location,

thereby reducing the susceptibility to data breaches and cyberattacks. By using blockchain, health practitioners can establish an unhackable, tamper-evident record in which patient data is encrypted and only available to authorised users, promoting confidentiality and data protection. Blockchain can also mandate higher transparency in sharing data by creating an open, transparent record of transactions. Hence, patients and healthcare practitioners are well-informed about the integrity of exchanged information. The intended blockchain model has been shown to enhance data security and facilitate the easy sharing of information across different healthcare platforms, thereby guaranteeing interoperability across systems that compatibility problems had previously hampered.

Some of the challenges that need to be addressed to facilitate blockchain implementation at scale in healthcare include, perhaps most urgently, scalability. Blockchain-based applications, particularly those of the public ledger type, are slow to handle large amounts of transactions in real-time, which can impair their performance when data is being fed constantly into a healthcare setting. Regulation challenges, such as patient data confidentiality and the legality of applying blockchain technology in healthcare, must also be considered and addressed to comply with current legislation. Lastly, healthcare blockchain protocol incompatibility is the main issue since different health institutions might use different systems that cannot be harmonised. To fully realise the potential of blockchain technology in the healthcare sector, it is essential to understand how to minimise certain challenges and engineer scalable technology, regulation, and interoperability protocols that facilitate large-scale utilisation.

6.1. Limitations

One of the largest limitations of this study is that it was conducted within a test healthcare environment, which may not accurately reflect the reality and nuance of real-world healthcare systems. Test environments, although wonderful for testing and validation, are often optimised and may not accommodate aspects such as interoperability, real-time data access, and the interactive workflow of healthcare. In actual settings, healthcare environments are subject to various factors like administrative processes, regulations, and human conduct, which might impact the operation of blockchain technology. Thus, results from this study, as encouraging as they are, might not apply to how blockchain would operate in actual medical environments. One of the limitations of this study is that it uses one specific blockchain framework.

The study was conducted on the foundation of a single blockchain platform, and there are multiple other blockchain platforms and frameworks with varying capabilities and functionalities. Other blockchain structures can be of varying levels of performance, scalability, or security, and conclusions from this research may not apply to other blockchain platforms. Further, while blockchain technology has enormous potential in managing healthcare data, it remains a significant scalability issue. The capacity of blockchain to handle data, particularly in healthcare systems with numerous patients and care providers, warrants further exploration in research. Network delay, transaction speed, and storage can retard the performance of blockchain-based solutions at scale, and these are issues that need to be addressed before large-scale applications of blockchain in health care.

6.2. Future Scope

The potential of blockchain in the healthcare sector is enormous, as it offers the possibility of revolutionising the sector with more scalable and efficient blockchain solutions. Scaling up the potential of blockchain technology to manage the scales of data generated by healthcare systems is perhaps the most crucial sector to target. With the mounting development in the healthcare industry, there will be an increasing demand for more capable and speedy blockchain technologies to handle large volumes of data simultaneously. Sharding and layer-2 scaling technologies are long-term top-level blockchain architectures that can potentially meet the rising demand for handling healthcare data. Besides that, combining machine learning (ML) and artificial intelligence (AI) with blockchain is capable of significantly increasing the efficacy of health data exchange systems. AI and ML-based algorithms will automatically process data, expand decision-making capabilities, and identify abnormalities or potential security breaches in real-time. Coupled with the transparency and security provided by blockchain, AI and ML can implement a more intelligent, more efficient, and more secure healthcare system. Apart from that, there is a crucial need for global standards and regulation of blockchain-enabled healthcare solutions. Various standards have been a significant issue in the widespread adoption of blockchain technology in the healthcare sector, as they can lead to inconsistencies in data sharing, security procedures, and patient consent management. To make the adoption of blockchain technology in healthcare across the globe a reality, further research will be required to establish regulatory standards and guidelines that will guarantee interoperability, security, and privacy. Creating these frameworks will be important in building regulators', patients', and healthcare providers' trust and allowing the widespread use of blockchain technology in healthcare.

Acknowledgment: I would like to express my sincere gratitude to the University of the Cumberlands for their support and resources throughout this work. Their academic guidance and encouragement have been invaluable in completing this study. I am thankful for the learning opportunities and inspiration gained during my time here.

Data Availability Statement: The data supporting the findings of this study are available upon request from the author. Due to privacy and ethical restrictions, certain data may be limited or require additional permissions. Institutional guidelines and data-sharing policies will review and consider all data requests.

Funding Statement: This manuscript and research work were prepared without any financial support or funding.

Conflicts of Interest Statement: I declare no conflicts of interest related to this study.

Ethics and Consent Statement: This study was conducted in accordance with ethical standards and approved by the relevant institutional review board. Informed consent was obtained from all participants prior to their involvement in the study.

References

1. U. Tatar, Y. Gokce, and B. Nussbaum, "Law versus technology: Blockchain, GDPR, and tough tradeoffs," *Comput. Law Secur. Rep.*, vol. 38, no. 9, pp. 1-11, 2020.
2. K. Theodos and S. Sittig, "Health information privacy laws in the digital age: HIPAA doesn't apply," Perspect. *Health Inf. Manag.*, vol. 18, no. 12, pp. 1-11, 2021.
3. W. Y. Ng, T. E. Tan, P. V. Movva, A. H. Fang, K. K. Yeo, D. HO, F. S. S. Foo, Z. Xiao, K. Sun, T. Y. Wong, A. T. H. Sia, and D. S. W. Ting, "Blockchain applications in health care for COVID-19 and beyond: a systematic review," *Lancet Digit. Health*, vol. 3, no. 12, pp. e819–e829, 2021.
4. P. Storz, S. Wickner, B. Batt, J. Schuh, D. Junger, Y. Möller, N. Malek, and C. Thies, "BwHealthApp: A software system to support personalized medicine by individual monitoring of vital parameters of outpatients*," in Proceedings of the 14th International Joint Conference on Biomedical Engineering Systems and Technologies*, Vienna, Austria, 2021.
5. B. T. Fothergill, W. Knight, B. C. Stahl, and I. Ulnicane, "Responsible data governance of neuroscience big data," *Front. Neuroinform*., vol. 13, no. 4, pp. 1-14, 2019.
6. J. Hallamaa and T. Kalliokoski, "AI Ethics as Applied Ethics," *Front. Comput. Sc*i., vol. 4, no. 4, pp. 1-12, 2022.
7. R. M. Gonçalves, M. M. da Silva, and P. R. da Cunha, "Olympus: a GDPR compliant blockchain system*," Int. J. Inf. Secur*., vol. 23, no. 11, pp. 1021–1036, 2023.
8. F. Khan, M. Asif, A. Ahmad, M. Alharbi, and H. Aljuaid, "Blockchain technology, improvement suggestions, security challenges on smart grid and its application in healthcare for sustainable development," *Sustain. Cities Soc*, vol. 55, no. 4, p. 102018, 2020.
9. L. Soltanisehat, R. Alizadeh, H. Hao, and K.-K. R. Choo, "Technical, temporal, and spatial research challenges and opportunities in blockchain-based healthcare: A systematic literature review," *IEEE Trans. Eng. Manage*., vol. 70, no. 1, pp. 353–368, 2023.
10. Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: Trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, no. 7, pp. 14757–14767, 2017.
11. A. A. Khan, A. A. Wagan, A. A. Laghari, A. R. Gilal, I. A. Aziz, and B. A. Talpur, "BIoMT: A State-of-the-Art Consortium Serverless Network Architecture for Healthcare System Using Blockchain Smart Contracts," *IEEE Access*, vol. 10, no. 7, pp. 78887–78898, 2022.
12. S. E. Uddin Quadery, M. Hasan, and M. M. Khan, "Consumer side economic perception of telemedicine during COVID-19 era: A survey on Bangladesh's perspective," *Inform. Med. Unlocked*, vol. 27, no. 11, pp. 1–13, 2021.
13. F. Jabeen, Z. Hamid, A. Akhunzada, W. Abdul, and S. Ghouzali, "Trust and reputation management in healthcare systems: Taxonomy, requirements and open issues," *IEEE Access*, vol. 6, no. 6, pp. 17246–17263, 2018.