# Blockchain-Enhanced Security and Efficiency for Thailand's Health Information System

Thattapon Surasak
Department of Computer and Information Science, Faculty of Applied Science
King Mongkut's University of Technology North Bangkok, Bangkok, Thailand

***Abstract*—This study seeks to enhance the security, efficiency, and usability of Thailand's health information system through the integration of blockchain technology and a user-friendly web application. Blockchain's inherent strengths in secure data storage and sharing make it particularly well-suited for addressing the critical challenges of healthcare data management. Currently, Thai citizens face significant barriers when seeking medical treatment across multiple hospitals, as they must manually request and transfer both their Electronic Medical Records (EMRs) and paper-based medical records. This fragmented system creates delays and inefficiencies, as each hospital operates its own isolated data silo. To overcome these challenges, this study proposes a solution utilising a private blockchain to securely store and manage patient medical histories and prescriptions. This approach ensures data integrity while implementing robust authorisation mechanisms to restrict access to sensitive information exclusively to verified individuals. The system's security is further strengthened by blockchain's encryption features and the use of smart contracts. A well-designed web application serves as the interface between the secure blockchain database and end-users, offering a seamless experience for both healthcare providers and patients. In addition, User Experience (UX) testing was conducted with healthcare providers to assess the system's usability and functionality. The results highlight the system's user-friendly interface, confirming its potential for widespread adoption. By fostering efficient, secure, and patient-centric health information exchange, this study has the potential to significantly enhance healthcare delivery and outcomes in Thailand.**

***Keywords*—*Blockchain technology; healthcare information system; Electronic Medical Records (EMRs); user experience (UX) testing; web application; data security***

## I. Introduction

The digital transformation of healthcare systems has brought significant advancements in patient care, enabling more efficient diagnosis, treatment, and management of health conditions. However, this shift towards digital systems has also highlighted several critical challenges, particularly in the areas of managing and securing sensitive medical data [1]. While the adoption of electronic health records (EHRs) and other digital tools has improved the accessibility of patient information and streamlined healthcare processes, it has also introduced new complexities in ensuring data privacy, interoperability, and compliance with regulatory standards. The rapid expansion of healthcare data, coupled with increasing cyber threats, has made it essential to implement robust solutions for safeguarding patient information and ensuring the seamless exchange of medical data across different healthcare providers and institutions [2].

Thailand's healthcare system faces unique challenges stemming from infrastructural, administrative, and technological limitations, which are compounded by the fragmented handling of both digital and paper-based medical records [3], [4]. Patients frequently encounter inefficiencies when seeking care across multiple hospitals, as they must manually request and transfer their medical records, leading to delays in treatment and posing risks of incomplete information for healthcare providers [5], [6]. Moreover, limited interoperability between data systems and fragmented administrative structures exacerbate these issues, creating bottlenecks in the seamless exchange of critical patient information [7].

Concerns regarding infection control and the management of patient movement within healthcare facilities further highlight the urgent need for secure, real-time access to medical data. Blockchain technology, with its decentralised architecture and capacity for creating immutable records, offers a robust solution to these challenges. By integrating blockchain into Thailand's healthcare system, hospitals can streamline the sharing and retrieval of medical information, reduce administrative inefficiencies, and improve overall care quality. Furthermore, adopting blockchain technology aligns with ongoing efforts to modernise healthcare infrastructure and address gaps in service delivery, paving the way for a more patient-centred and efficient system [8].

Blockchain technology has emerged as a promising solution to these challenges, providing a decentralised and secure framework for data storage and exchange. A blockchain is a shared, distributed ledger that stores data across multiple nodes, ensuring that once information is recorded, it is extremely difficult to alter. This is achieved through cryptographic techniques and consensus mechanisms that validate data consistency across the network. While blockchain is often associated with cryptocurrencies such as Bitcoin, its applications in healthcare are particularly valuable due to its immutability, transparency, and robust data security features [9].

Among the many technological advancements, blockchain stands out for its unique ability to protect data from tampering and unauthorised access. Data is stored across a distributed network, allowing every member to access and verify information simultaneously, ensuring transparency. In the context of healthcare, blockchain can securely store patient records, safeguarding them against unauthorised modifications or breaches. Additionally, only authorised stakeholders, such as doctors and healthcare providers, can access these medical histories, enabling the provision of more continuous and improved care. This study aims to demonstrate how blockchain technology can transform Thailand's health information system, resulting in better healthcare outcomes and an enhanced quality of life for its citizens.

This proposed system utilises blockchain technology, specifically Hyperledger Fabric, to enable fast, secure, and seamless sharing of patient records. By integrating blockchain with a user-friendly web platform, the system enhances the efficiency of health data exchange in Thailand. Blockchain's encryption and smart contracts ensure that only authorised individuals can access patient information, thereby safeguarding data integrity. The system also significantly reduces the time required for transferring medical records between providers, facilitating faster and more accurate diagnoses and treatments. Furthermore, it empowers patients by granting them greater control over their medical data, representing a critical step towards a more patient-centric healthcare system.

The remainder of this paper is structured as follows: Section II provides a comprehensive review of previous studies in the field, examining the historical context of health information systems alongside recent advancements in blockchain technology for healthcare. Section III presents a detailed description of the design of the proposed system, highlighting the foundational principles of the blockchain-based solution. Section IV discusses the results, including the development of a user-friendly web application that interfaces with the blockchain. Finally, Section V synthesises the key findings, reflects on the contributions of this work to the field, considers its broader implications, and outlines promising directions for future research.

## II. Related Work

Blockchain technology is increasingly being studied for its potential to address critical challenges in healthcare, particularly in securing sensitive patient data, ensuring interoperability, and enhancing the transparency of medical record transactions. Amid the ongoing challenges posed by fragmented record-keeping systems, blockchain offers a decentralised solution that balances privacy with real-time accessibility to medical data [10].

Early applications of blockchain in healthcare included MedRec, a system designed for managing Electronic Medical Records (EMRs). Leveraging Ethereum and smart contracts, MedRec aimed to facilitate the secure sharing of patient data among healthcare providers. By addressing data silos while maintaining patient control over access, it demonstrated blockchain's significant advantage: immutable record-keeping, which ensures the integrity of medical records [11]. Blockchain technology presents a solution to the fragmented nature of healthcare systems. At present, patient records are siloed within individual institutions, limiting the delivery of comprehensive care. By establishing a unified ledger, blockchain enables authorised providers to access and update patient records in real time. This enhanced interoperability has the potential to improve care continuity, reduce redundant testing, and minimise medical errors [12]. Blockchain technology addresses critical healthcare challenges related to data provenance and record integrity. Through its consensus mechanisms, all modifications to medical records are verified and permanently recorded, creating an immutable and auditable history. This enhances transparency and fosters trust among patients, providers, and institutions. By tracking who accessed or modified records and when, blockchain provides a robust solution for safeguarding the integrity of sensitive medical information [13]. In addition to enhancing security and transparency, blockchain's use of smart contracts has been extensively studied as a tool to automate and enforce access control policies. In healthcare settings, these programmable contracts enable sophisticated access control by verifying the credentials of healthcare providers and granting access to patient records only under predefined conditions. For instance, a doctor can access a patient's history only if directly involved in their care and appropriately authorised. This dynamic model minimises the risk of unauthorised access while facilitating necessary data interactions. As a result, smart contracts improve both the security and efficiency of managing sensitive medical information [14], [15]. Permissioned blockchains, such as Hyperledger Fabric, have significantly enhanced blockchain's applicability in healthcare. Unlike public blockchains, these systems restrict network access to known and trusted participants, addressing the critical need for privacy in healthcare environments. Hyperledger Fabric's modular architecture supports secure transactions and smart contract integration while maintaining stringent control over access to medical records. This makes it particularly well-suited for healthcare settings, where confidentiality is paramount. Studies confirm its viability for applications requiring controlled viewing and updating of medical records [16]. However, storage limitations remain a challenge, especially when dealing with large volumes of medical data. While blockchain excels at storing transaction records and hashes of medical data, storing actual medical records on-chain is inefficient and costly in terms of both storage and computation. To overcome these limitations, hybrid systems combining blockchain with traditional relational databases, such as MariaDB, have been proposed. These systems store sensitive data on-chain while offloading larger, non-sensitive data to off-chain databases. This hybrid approach preserves the core benefits of blockchain, such as immutability and security, while addressing the performance challenges associated with large-scale data storage [17], [18].

In conclusion, blockchain technology has demonstrated significant potential in addressing key challenges in healthcare, particularly in the secure and efficient management of Electronic Medical Records (EMRs) [19]. The literature highlights blockchain's decentralised, immutable, and secure nature as a foundation for enhancing privacy, interoperability, and trust in healthcare data management [20]. Notable studies, such as MedRec, have explored the use of Ethereum and smart contracts for patient data sharing, while others have investigated the integration of blockchain with IoT systems for real-time data collection and the secure management of medical information [16]. However, despite its advantages, blockchain faces limitations, including scalability and storage constraints, which must be addressed for broader adoption. To mitigate these challenges, hybrid systems combining blockchain with traditional databases, such as MariaDB, have been proposed. These systems store sensitive data on-chain while offloading larger, non-sensitive data to off-chain databases, thereby maintaining performance without compromising security.

This proposed system builds on these foundations, leveraging Hyperledger Fabric, a permissioned blockchain specifically designed to provide robust security and privacy in a decentralised environment. Unlike Ethereum, which incurs transaction fees, Hyperledger Fabric is open-source and free from such costs, making it a more practical choice for healthcare applications [21], [22]. Its modular architecture enables the integration of smart contracts to control access to EMRs, ensuring that only authorised individuals can view or update sensitive medical information [23], [24]. The design of the Blockchain-Based Healthcare Information System (discussed in Section III) combines blockchain with a user-friendly web application, offering seamless access to EMRs while maintaining the highest levels of security. By employing smart contracts and a hybrid storage solution, this proposed system addresses the limitations identified in previous systems. This approach not only ensures the integrity of patient records but also enhances data sharing between healthcare providers, enabling faster diagnoses and more accurate treatments. Furthermore, this study advances the existing literature by demonstrating how blockchain, when integrated with modern web technologies and efficient storage solutions, can resolve critical challenges related to data security, privacy, and interoperability in healthcare. Future work will focus on scaling the system to accommodate larger networks and incorporating advanced privacy-preserving techniques to further enhance the security of healthcare data.

## III. Proposed System

The proposed Blockchain-Based Healthcare Information System (HIS) has been designed to address the inefficiencies and security vulnerabilities inherent in traditional centralised systems for managing Electronic Medical Records (EMRs). By leveraging Hyperledger Fabric, an open-source, permissioned blockchain, the system provides a secure and decentralised solution for managing patient records. Additionally, it enforces strict access control through the integration of smart contracts, ensuring that sensitive medical information remains accessible only to authorised individuals.

### A. System Architecture

The system consists of three primary components:

*1) Blockchain Database:* The blockchain network forms the core of the system and is built on Hyperledger Fabric. This platform was selected for its numerous advantages over alternatives such as Ethereum, including its open-source nature, absence of transaction fees, and robust security features. Hyperledger Fabric's permissioned network restricts access to verified participants, ensuring that sensitive medical data can only be accessed by authorised users. Its modular architecture supports a wide range of applications, making it particularly adaptable for healthcare implementations.

*2) Web Application:* The web application acts as the interface between healthcare providers, patients, and the blockchain network. Designed with usability in mind, the platform enables users to log in, view medical records, and securely share data with healthcare providers. Real-time querying of the blockchain ensures rapid access to critical patient information, such as medical histories and prescriptions. Access control is enforced by smart contracts, guaranteeing that only authorised users can interact with the data.

*3) Smart Contracts:* The system leverages Hyperledger Fabric's smart contracts, also referred to as chaincode, to implement business logic and control user access. Written in Java (as well as Go or Node.js), these smart contracts enforce user roles and permissions by verifying the identities of patients and healthcare providers through Hyperledger Fabric's identity management services. Additionally, they log all interactions with the blockchain, creating an immutable audit trail that ensures transparency, accountability, and data integrity.

### B. Blockchain Architecture Design

The blockchain architecture is designed to store critical medical data securely while optimising performance. The system utilises a distributed ledger to store patient medical histories and prescriptions. Each transaction is recorded immutably, ensuring that once data is added, it cannot be altered. The system generates a unique transaction ID for each interaction, providing a secure and traceable history of all medical data exchanges.

Hyperledger Fabric was selected for its permissioned network, which ensures that only authorised participants can access the network. This feature is particularly important in healthcare, where patient confidentiality and data security are paramount. Unlike public blockchains, which allow anyone to participate, Hyperledger Fabric restricts access to known and verified participants, providing an additional layer of security. Each participant is assigned specific roles and permissions, ensuring that only those with the necessary credentials can interact with the blockchain.

The system employs chaincode (smart contracts) written in Java to manage user roles and control data access. For example, the chaincode verifies that a patient's identity matches their medical records before granting access. Additionally, it tracks and records every transaction on the blockchain, creating an immutable audit trail that ensures the integrity and transparency of the data.

### C. Hybrid Data Storage Solution

To address blockchain's storage limitations, the system adopts a hybrid storage model. Critical and sensitive medical data are securely stored on the blockchain, leveraging its immutability and robust security features. Less sensitive information, such as metadata or general patient details, is stored in MariaDB, a relational database system. This hybrid approach alleviates the performance overhead associated with storing large volumes of data on the blockchain while ensuring the security of sensitive information. Furthermore, the system synchronises data between the blockchain and MariaDB to maintain consistency across platforms.

### D. Security, Authentication Flow and Data Integrity

The system's security is built upon Hyperledger Fabric's cryptographic mechanisms and identity management features. Authentication is managed through public-key cryptography, with each user's identity verified by a certificate authority. This ensures that only authorised individuals can access or modify patient records, effectively preventing unauthorised access. Additionally, all interactions are securely recorded using smart contracts, creating a transparent and tamper-proof audit trail.

Hyperledger Fabric's consensus mechanism ensures that all nodes agree on the state of the ledger, safeguarding against malicious actors attempting to alter patient data. This is critical for maintaining the integrity of healthcare information, where accuracy is paramount for effective treatment decisions.

The system's authentication process begins with a user logging into the web application, which interfaces with the blockchain through smart contracts. The smart contract verifies the user's credentials against the blockchain's identity management system. Once authenticated, the user can query the blockchain to retrieve or update medical records. Each interaction is recorded as a transaction, validated by the blockchain's consensus mechanism, and subsequently added to the ledger.

## IV. Results and Discussion

This section presents the results from the prototype implementation of a Blockchain-Based Healthcare Information System and discusses the implications of these findings in the context of existing healthcare information management. It includes an evaluation of the system's performance, security, and usability, with particular focus on the insights gained through User Experience (UX) Testing. The results provide a comprehensive view of the system's effectiveness in securely managing electronic medical records (EMRs) and its potential to enhance healthcare workflows. The findings also highlight areas for future development, including system scalability, performance optimisation, and user adoption strategies.

### A. System Implementation Results

The developed system is a web application integrated with Hyperledger Fabric, a permissioned blockchain, to facilitate the secure sharing of Electronic Medical Records (EMRs). Both patients and healthcare providers can register and access the system. Patients are identified using their Thai 13-digit ID number during registration. Once logged in, they can securely upload and store medical records, such as medical certificates or treatment data, on the blockchain, ensuring safe and controlled access.

The implementation demonstrated that blockchain technology significantly enhances data security, access control, and transparency in healthcare. By decentralising medical data storage, it reduced the risk of unauthorised access and tampering. The blockchain's immutable nature ensured that any modifications to records were securely logged, providing full accountability. However, performance issues were observed, particularly slower transaction speeds during periods of high usage. To address this, a hybrid storage model, incorporating MariaDB for non-critical data, improved system performance. Security remained robust, with cryptographic protections and Hyperledger Fabric's consensus mechanism ensuring authorised access. Additionally, smart contracts enabled secure data sharing, giving patients greater control over who could access their records.

### B. Main Features of the System

The main features of the system included:

*1) User-friendly Interface:* The web interface was intuitive, allowing users to easily upload and access their medical records. Patients could review their treatment history, drug allergy details, and medical certificates in real time.

*2) Blockchain Integration:* Critical data, such as medical histories, were stored securely on the blockchain using Hyperledger Fabric's cryptographic and consensus mechanisms, ensuring data integrity and security.

*3) Hybrid Storage:* To optimise performance, the system employed a hybrid data storage model, storing sensitive data on the blockchain while non-sensitive data was kept in a traditional relational database, MariaDB. This approach addressed blockchain's limitations in terms of storage capacity and performance.

*4) Smart Contracts:* The system used smart contracts to enforce access control, allowing only authorised users (doctors, medical staff, and patients) to view or modify the records. The smart contracts also recorded every transaction made, providing a transparent and immutable audit trail of interactions with the data.

### C. System Performance and Security

The implementation demonstrated that using blockchain technology in healthcare offers significant improvements in data security, access control, and transparency. By decentralising medical data storage, the system mitigated the risk of unauthorised access or tampering. The blockchain's immutable nature ensured that any changes to patient records were securely logged and could not be altered, thereby providing full accountability for all medical interactions.

However, performance limitations were observed, particularly in terms of processing speed when handling larger volumes of transactions. Blockchain's inherently slower transaction times, compared to traditional relational databases, were noted, particularly during peak usage periods. The integration of a hybrid storage model helped alleviate some of these concerns by offloading non-critical data to the MariaDB database, which allowed the system to maintain adequate performance levels.

In terms of security, the blockchain-based system provided strong data protection through cryptographic techniques. The consensus mechanism employed by Hyperledger Fabric ensured that only authorised participants could access the network, and the use of smart contracts further guaranteed secure data sharing between stakeholders. Patients also benefited from increased control over their medical records, as they could directly manage who could access their data.

### D. Prototype User Interface Design

The design of the Blockchain-Based Healthcare Information System focuses on providing an intuitive and secure interface that allows patients and healthcare providers to interact seamlessly with the blockchain-based backend system. Below are the key screens developed in the prototype, which demonstrate the core functionalities of the system: landing page, registration page, and medical record page.

*1) Landing Page:* Fig. 1 shows the Landing Page, the gateway to the Blockchain-Based Healthcare Information System. It features a clean, user-friendly interface for both patients and healthcare providers, offering clear options for logging in or registering with role-specific paths for easy navigation. The design emphasizes security and decentralised medical record management, assuring users that their healthcare data is securely handled. The page is crafted to ensure a smooth entry into the system, prioritising accessibility and ease of use.

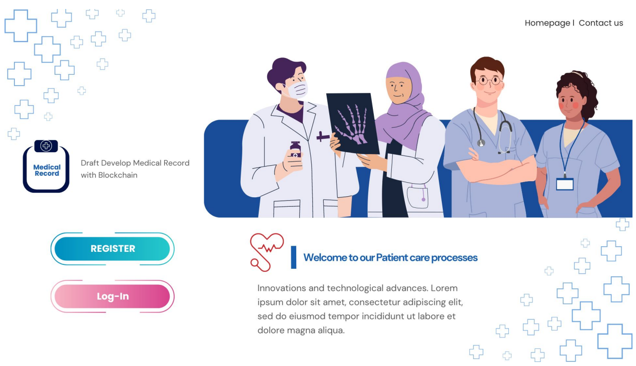


Fig. 1. Landing page.

*2) Registration Page:* Fig. 2 shows the Registration Page, where new users (patients or healthcare providers) can create an account and securely access the healthcare platform. The page collects personal and authentication details, such as name and email, while leveraging blockchain identity management for secure user verification. It employs a role-based access system, assigning distinct roles to patients and healthcare providers to control permissions. This ensures that only authorised users can view or manage sensitive medical records. Overall, the Registration Page establishes a secure foundation for verified and authenticated interactions within the system.

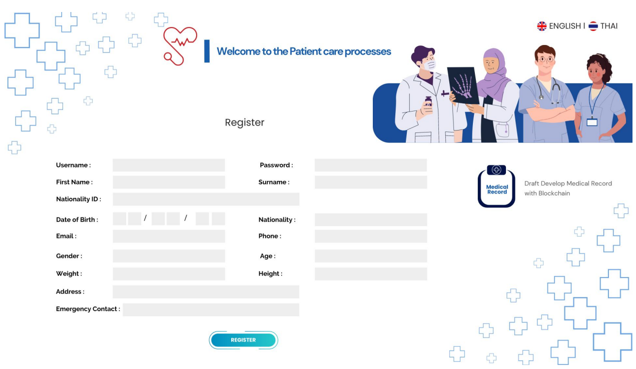


Fig. 2. Registration page.

*3) Medical Record Page:* Fig. 3 displays the Medical Record Page, the main interface where patients and healthcare providers manage Electronic Medical Records (EMR). Patients can securely view their complete medical history, while healthcare providers can upload and update records. These records are encrypted and stored on the blockchain, with access controlled by smart contracts, ensuring that only authorised users can view or modify the data. All interactions are logged for transparency and auditability, making the system both secure and efficient for enhancing patient care and experience.

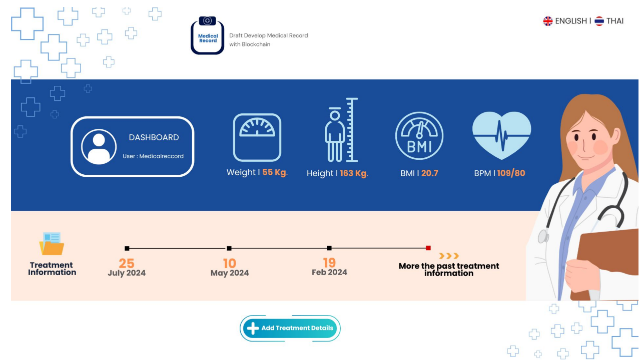


Fig. 3. Medical record page.

## E. User Experience (UX) Testing

*1) Testing Participants:* The UX testing involved healthcare providers, including doctors and medical administrators, as the sole participants. They were tasked with logging into the system, uploading treatment records, querying medical histories, and managing access permissions for patient data. Synthesised patient profiles were used to simulate realistic medical interactions, ensuring the evaluation aligned with real-world use cases.

*2) Key Findings:* The key findings from the UX testing highlight the system's usability, efficiency, and security, as well as areas for improvement. These findings were based on the feedback from healthcare providers as they interacted with the system during various tasks:

- Ease of Use: Participants found the *landing page* intuitive, with clear navigation options for login and registration. The *medical record page* was effective in facilitating tasks such as uploading and retrieving medical records, which streamlined workflows and reduced administrative complexity.
- Efficiency: Real-time access to blockchain-stored data ensured healthcare providers could quickly retrieve treatment histories and prescription details, which was particularly beneficial for emergency care simulations. The hybrid storage model improved responsiveness when accessing non-critical data, as confirmed by positive feedback during high-usage scenarios.
- Security Perception: Healthcare providers appreciated the robust security features, including blockchain's encryption and immutable audit trails, which reassured them of the system's reliability for handling sensitive information.
- Challenges: A minor learning curve was observed among participants unfamiliar with blockchain technology, particularly during the initial onboarding phase. Slower transaction speeds were noted during simulated peak loads, indicating a need for further optimisation.

Suggestions for Improvement: Based on the key findings, several suggestions for improving the system were made to enhance its usability, performance, and scalability:

- Enhanced Onboarding: Developing tutorials or quick-start guides tailored to healthcare providers could improve initial system adoption.

- Performance Optimisation: Continued refinement of the hybrid storage model and transaction speeds is recommended to enhance usability during high-demand periods.

Conclusion: The UX testing demonstrated the system's potential to streamline healthcare workflows and securely manage medical records for healthcare providers. By leveraging synthesised patient data, the evaluation provided realistic insights into the system's usability and security features while avoiding ethical concerns associated with direct patient involvement. These findings highlight the system's readiness for broader adoption, with ongoing refinements aimed at improving scalability and performance.

### F. Discussion

The prototype Blockchain-Based Healthcare Information System demonstrated significant improvements in the security and accessibility of Electronic Medical Records (EMRs) for healthcare providers. By leveraging blockchain technology and a hybrid storage model, the system ensured secure management of sensitive data while addressing performance limitations associated with blockchain's storage capacity. Feedback from healthcare providers during UX testing highlighted several strengths and areas for improvement.

*1) Scalability:* As the system grows, increasing data volumes may impact performance, particularly during peak usage periods. The integration of a hybrid storage model helped alleviate some performance issues, but future work should focus on refining consensus mechanisms and exploring advanced storage solutions such as distributed file systems or cloud integration.

*2) User Adoption:* The user-friendly interface was positively received by healthcare providers, who found the system intuitive and effective for managing medical records. However, a minor learning curve was noted, particularly for users unfamiliar with blockchain technology. Developing onboarding materials and tailored training programs could facilitate smoother adoption.

*3) Legal and Ethical Implications:* Although the system used synthesised patient data to evaluate its functionality, real-world implementation would need to address compliance with data privacy laws such as GDPR and HIPAA. Smart contracts for access control must be carefully designed to align with regulatory frameworks while ensuring secure and transparent data sharing.

These findings underscore blockchain's promise as a transformative technology in healthcare. The system's robust security features and transparent data management have the potential to streamline workflows and improve interoperability among healthcare providers. Nevertheless, addressing scalability, enhancing user adoption strategies, and ensuring regulatory compliance remain critical for widespread implementation. Future research should focus on scaling the system to support national healthcare networks and refining its performance for handling greater data volumes. Additionally, expanding UX testing to include diverse healthcare settings could provide deeper insights into its adaptability and effectiveness.

## V. Conclusion

In the proposed solution, Hyperledger Fabric was chosen over the Ethereum platform for several reasons. One significant advantage is that Ethereum imposes transaction execution fees, whereas Hyperledger Fabric is an open-source platform that does not charge such fees, making it a more cost-effective choice for healthcare applications. Additionally, Hyperledger Fabric offers robust security features, which are crucial for handling sensitive medical data.

This study is pioneering in its design and development of a prototype for managing Electronic Medical Records (EMRs) using blockchain technology, specifically in the form of a Blockchain-Based Healthcare Information System. At present, most hospitals rely on centralised systems to store patient data, typically using conventional Relational Database Management Systems (RDBMS). However, this centralised approach poses significant challenges in sharing medical records, treatment histories, and other critical information between hospitals. The research serves as a proof of concept, demonstrating the benefits of blockchain in this context. Blockchain technology was found to provide a high level of security and protection for sensitive information, ensured through consensus mechanisms and collaboration among stakeholders.

Despite its advantages, the research identified some limitations of blockchain technology, such as restricted storage capacity and the need for continuous software updates across nodes or peers. To address these issues, a hybrid approach was adopted, combining blockchain with MariaDB. Critical data was stored on the blockchain, while general information was maintained in the MariaDB system. This approach mitigated performance issues and improved overall system efficiency.

User feedback from healthcare providers during system evaluation highlighted the system's usability and its potential to streamline healthcare workflows. The integration of a user-friendly interface with blockchain's secure backend ensures effective data management while maintaining accessibility. However, minor challenges, such as transaction speeds during peak usage and onboarding support for first-time users, should be addressed in future iterations.

Future research should focus on scaling blockchain-based healthcare systems for larger networks, such as national-level infrastructures, while optimising performance to handle greater data volumes. Enhancing storage solutions through the integration of distributed file systems, such as IPFS, or cloud storage could address blockchain's inherent limitations. Additionally, exploring alternative blockchain platforms may provide valuable insights into how different technologies perform in healthcare applications. Expanding evaluations to include diverse healthcare settings will further validate the system's adaptability and effectiveness.

In conclusion, the Blockchain-Based Healthcare Information System demonstrates blockchain's potential to revolutionise healthcare data management. By addressing current limitations and leveraging innovative solutions, the system has the capacity to enhance data security, improve interoperability, and streamline workflows, contributing to better healthcare outcomes for all stakeholders.

## Disclosure and Conflicts of Interest

The author declares no conflicts of interest and has no financial interests to disclose. The author certifies that this submission is original work and is not currently under review by any other publication.

## References


[1] J. Ishizaki, M. Yoshioka, and H. Nishimura, "Analysis and categorization for the standardization of medical referral document information," in *2020 9th International Congress on Advanced Applied Informatics (IIAI-AAI)*, 2020, pp. 808–809.

[2] E. Li, J. Clarke, A. L. Neves, H. Ashrafian, and A. Darzi, "Electronic health records, interoperability and patient safety in health systems of high-income countries: A systematic review protocol," *BMJ Open*, vol. 11, no. 7, 2021.

[3] T. Chintavoarn, C. Junma, and A. Thamchalai, "The guidelines for improving the effectiveness of the health link health information exchange system," *Journal of Arts Management*, vol. 7, no. 4, p. 1725–1740, Dec. 2023.

[4] T. Waroonkun and S. Prugsiganont, "Preventing the spread of covid-19 through environmental design in thai community hospitals," *Frontiers in Built Environment*, vol. 8, 2022.

[5] V. Aumpanseang, K. Suthiwartnarueput, and P. Pornchaiwiseskul, "Determinants affecting the health information sharing management and practice for patient referral in thailand: The perceptions of patients and healthcare professionals," *Perspect Health Inf Manag*, vol. 19, no. 4, p. 1b, Oct. 2022.

[6] S. Sawang, C. Y. Chou, and B. Q. Truong-Dinh, "The perception of crowding, quality and well-being: a study of vietnamese public health services," *Journal of Health Organization and Management*, vol. 33, no. 4, pp. 460–477, Jan 2019.

[7] S. Prugsiganont and T. Waroonkun, "Identifying built environment solutions, in thai community hospital outpatient clinics, to prevent the spread of covid-19," *IOP Conference Series: Earth and Environmental Science*, vol. 1101, no. 6, p. 062035, nov 2022.

[8] B. K. Seo, "Patient waiting: care as a gift and debt in the thai healthcare system," *Journal of the Royal Anthropological Institute*, vol. 22, no. 2, pp. 279–295, 2016.

[9] M. N. M. Bhutta, A. A. Khwaja, A. Nadeem, H. F. Ahmad, M. K. Khan, M. A. Hanif, H. Song, M. Alshamari, and Y. Cao, "A survey on blockchain technology: Evolution, architecture and security," *IEEE Access*, vol. 9, pp. 61 048–61 073, 2021.

[10] Q. Xia, E. B. Sifah, A. Smahi, S. Amofa, and X. Zhang, "Bbds: Blockchain-based data sharing for electronic medical records in cloud environments," *Information*, vol. 8, no. 2, 2017.

[11] A. Azaria, A. Ekblaw, T. Vieira, and A. Lippman, "Medrec: Using blockchain for medical data access and permission management," in *2016 2nd International Conference on Open and Big Data (OBD)*, 2016, pp. 25–30.

[12] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "Omniphr: A distributed architecture model to integrate personal health records," *Journal of Biomedical Informatics*, vol. 71, pp. 70–81, 2017.

[13] P. Zhang, D. C. Schmidt, J. White, and G. Lenz, "Chapter one - blockchain technology use cases in healthcare," in *Blockchain Technology: Platforms, Tools and Use Cases*, ser. Advances in Computers, P. Raj and G. C. Deka, Eds. Elsevier, 2018, vol. 111, pp. 1–41.

[14] H. M. Hussien, S. M. Yasin, S. N. I. Udzir, A. A. Zaidan, and B. B. Zaidan, "A systematic review for enabling of develop a blockchain technology in healthcare application: Taxonomy, substantially analysis, motivations, challenges, recommendations and future direction," *Journal of Medical Systems*, vol. 43, no. 10, p. 320, Sep 2019.

[15] R. Saranya and A. Murugan, "A systematic review of enabling blockchain in healthcare system: Analysis, current status, challenges and future direction," *Materials Today: Proceedings*, vol. 80, pp. 3010–3015, 2023, sI:5 NANO 2021.

[16] A. Haleem, M. Javaid, R. P. Singh, R. Suman, and S. Rab, "Blockchain technology applications in healthcare: An overview," *International Journal of Intelligent Networks*, vol. 2, pp. 130–139, 2021.

[17] K. Fan, S. Wang, Y. Ren, K. Yang, Z. Yan, H. Li, and Y. Yang, "Blockchain-based secure time protection scheme in iot," *IEEE Internet of Things Journal*, vol. 6, no. 3, pp. 4671–4679, 2019.

[18] K. Wisessing, P. Ekthammabordee, T. Surasak, S. C.-H. Huang, and C. Preuksakarn, "The prototype of thai blockchain-based voting system," *International Journal of Advanced Computer Science and Applications*, vol. 11, no. 5, 2020.

[19] A. Dubovitskaya, Z. Xu, S. Ryu, M. Schumacher, and F. Wang, "Secure and trustable electronic medical records sharing using blockchain," *AMIA Annu Symp Proc*, vol. 2017, pp. 650–659, Apr. 2018.

[20] X. Yue, H. Wang, D. Jin, M. Li, and W. Jiang, "Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control," *J Med Syst*, vol. 40, no. 10, p. 218, Aug. 2016.

[21] Z. Ke and N. Park, "Performance modeling and analysis of hyperledger fabric," *Cluster Computing*, vol. 26, no. 5, pp. 2681–2699, Oct 2023.

[22] C. Melo, G. Gonçalves, F. A. Silva, and A. Soares, "A comprehensive hyperledger fabric performance evaluation based on resources capacity planning," *Cluster Computing*, vol. 27, no. 9, pp. 12 395–12 410, Dec 2024.

[23] M. Kuzlu, M. Pipattanasomporn, L. Gurses, and S. Rahman, "Performance analysis of a hyperledger fabric blockchain framework: Throughput, latency and scalability," in *2019 IEEE International Conference on Blockchain (Blockchain)*, 2019, pp. 536–540.

[24] P. Thakkar, S. Nathan, and B. Viswanathan, "Performance benchmarking and optimizing hyperledger fabric blockchain platform," in *2018 IEEE 26th International Symposium on Modeling, Analysis, and Simulation of Computer and Telecommunication Systems (MASCOTS)*, 2018, pp. 264–276.