


Article

PHR-NFT: Decentralized Blockchain Framework with Hyperledger and NFTs for Secure and Transparent Patient Health Records

Huwida E. Said ^{1,*} , Nedaa B. Al Barghuthi ^{2,*}, Sulafa M. Badi ³, Faiza Hashim ⁴ and Shini Girija ¹

¹ College of Technological Innovation, Zayed University, Dubai P.O. Box 19282, United Arab Emirates; shini.girija@zu.ac.ae

² College of Computer Information Science, Higher Colleges of Technology, Sharjah P.O. Box 25026, United Arab Emirates

³ Faculty of Business and Law, The British University in Dubai, Dubai P.O. Box 345015, United Arab Emirates; sulafa.badi@buid.ac.ae

⁴ College of Information Technology, UAE University, Al-Ain P.O. Box 15551, United Arab Emirates; faiza.hashim@uaeu.ac.ae

* Correspondence: huwida.said@zu.ac.ae (H.E.S.); nedaa.albarghuthi@hct.ac.ae (N.B.A.B.)

Abstract: Blockchain technology holds significant promise for healthcare by enhancing the security and integrity of patient health records (PHRs) through decentralized storage and transparent access. However, it has substantial limitations, including problems with scalability, high transaction costs, privacy concerns, and intricate stakeholder access management. This study presents PHR-NFT, a novel framework that strengthens PHR privacy by utilizing Hyperledger Fabric and non-fungible tokens (NFTs) to address these issues. PHR-NFT improves privacy and communication by letting patients keep control of their medical records while permitting temporary, permission-based access by medical professionals. PHR-NFT offers a transparent solution that increases trust among healthcare stakeholders through the robust and decentralized architecture of the Hyperledger Fabric. This study demonstrates the viability and effectiveness of the PHR-NFT framework through performance evaluations focused on transaction latency, throughput, and security. This research has valuable implications for enhancing data privacy and security in healthcare practices and insightful information about blockchain-based healthcare systems.

Keywords: blockchain; Hyperledger; non-fungible tokens; patient health records tracking system; privacy



Citation: Said, H.E.; Al Barghuthi, N.B.; Badi, S.M.; Hashim, F.; Girija, S. PHR-NFT: Decentralized Blockchain Framework with Hyperledger and NFTs for Secure and Transparent Patient Health Records. *Appl. Sci.* **2024**, *14*, 10744. <https://doi.org/10.3390/app142210744>

Academic Editor: Luis Javier Garcia Villalba

Received: 3 October 2024

Revised: 3 November 2024

Accepted: 4 November 2024

Published: 20 November 2024



Copyright: © 2024 by the authors. Licensee MDPI, Basel, Switzerland. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution (CC BY) license (<https://creativecommons.org/licenses/by/4.0/>).

1. Introduction

Technological advancements in digitalization and information exchange are driving a transformation in healthcare, mainly through patient health records (PHRs) [1,2] and tele-care medicine information systems [3], which have enhanced accessibility and convenience. Despite their benefits for diagnosis and treatment, these systems face challenges related to data accessibility, security, and interoperability [4,5]. Concerns about data integrity, privacy, and the fragmented nature of medical records highlight the need for improved systems [6]. Blockchain technology has emerged as a potential solution [7,8], offering a decentralized and immutable ledger that enhances security, real-time access, and interoperability across healthcare networks [9]. Blockchain addresses privacy concerns and ensures accurate treatment by giving patients more control over their data and safeguarding transactions with smart contracts [10]. Different blockchain topologies, including public, private, and consortium models, enable tailored solutions [11]. Integration with technologies like reputation systems [12], trustworthy oracles [13], proxy re-encryption [14], and the Inter Planetary File System (IPFS) [15] further enhance blockchain-based PHR systems (BPHRSs). These systems securely encrypt and store PHRs via decentralized networks, promoting privacy, data integrity, and streamlined regulatory compliance [16–18]. This ultimately

improves the quality of patient care by providing a secure, transparent platform for health information management.

BPHRSs that make use of Quorum [19], Ethereum [20], and Hyperledger Fabric [21] provide tamper-proof, decentralized methods for handling confidential medical records. These systems have significant limitations that prevent their general implementation in the healthcare sector despite their potential security, openness, and data integrity benefits. The high cost of establishing and maintaining blockchain infrastructure is one of its fundamental limitations [22]. Due to the intricacy of blockchain technology, many healthcare organizations may find it prohibitive to invest in the necessary infrastructure and acquire the required knowledge. The lack of established data-sharing protocols between various blockchain platforms and current healthcare systems causes interoperability problems [21]. Blockchain-based patient monitoring systems have limited potential benefits if they cannot seamlessly integrate with older systems. This can impede effective data sharing and collaboration between healthcare providers. Another issue facing BPHRS is scalability, particularly given the exponential growth in data collected on medical conditions [7]. The massive volume of data created by healthcare transactions is too much for current blockchain systems to handle, which causes delays and performance bottlenecks in data processing. The immutable nature of blockchain raises privacy concerns since it makes it difficult to remove or amend sensitive information after it has been entered into the ledger, even as it ensures data integrity [19]. Privacy concerns are brought up by this lack of flexibility, especially in light of the right to be forgotten and the need to abide by laws like the General Data Protection Regulation (GDPR) [23]. Moreover, the blockchain's data ownership presents difficulties in preserving privacy and control over medical records [20,24]. Patients may not have precise control over their data, which could be dispersed across several networks and systems, compromising their right to privacy and making it more difficult for them to receive the appropriate care.

This research addresses critical gaps in existing blockchain-based personal health record systems (BPHRS) by proposing PHR-NFT. This novel solution leverages NFTs and Hyperledger Fabric to enhance healthcare data management's security, privacy, and interoperability. One of the significant issues with current BPHRS is the high cost and complexity of maintaining blockchain infrastructure, which significantly limits their scalability [21,25,26]. Additionally, these systems often struggle with seamless integration into existing healthcare infrastructures, making interoperability a substantial challenge [26,27]. Privacy concerns are also prevalent, as many blockchain platforms provide limited control to patients once their health data are stored, mainly due to the immutable nature of the blockchain [12,28,29].

Moreover, scalability remains a concern as the volume of healthcare data grows, leading to inefficiencies in existing systems [28,30,31]. Current solutions, like Ethereum-based frameworks [32,33], face challenges such as high energy consumption [34], while other platforms, like BlockMedCare, encounter difficulties in deployment and ensuring compatibility with healthcare systems [21,25,26,35]. PHR-NFT directly addresses these shortcomings by leveraging the scalable and modular architecture of Hyperledger Fabric, which reduces operational costs and simplifies deployment. By integrating NFTs, PHR-NFT enhances interoperability, enabling seamless data sharing between blockchain platforms and legacy healthcare systems. This facilitates more effective collaboration between healthcare providers. Furthermore, using NFTs helps address scalability issues by linking each health record to a unique, easily trackable token, thus avoiding bottlenecks as data volumes increase. Privacy concerns are mitigated by giving patients full ownership and control over their health data through NFTs, offering flexible and temporary access to healthcare records as needed, all while ensuring compliance with privacy regulations like GDPR [23].

PHR-NFT offers an efficient solution to the essential security and privacy needs that come with healthcare administration systems. PHR-NFT shows notable advances in several areas, including data integrity, confidentiality, availability, effective interoperability, global accessibility, data privacy, and security, compared to current blockchain-based implementations described in related work. Key benefits of PHR-NFT include enhanced data integrity through unique NFTs that create an immutable distributed ledger, ensuring unauthorized updates are difficult. The system addresses confidentiality by empowering patients to control access to their personal health information, allowing only authorized users to view their electronic health records. PHR-NFT ensures availability by distributing data across decentralized nodes, eliminating reliance on single points of failure and maintaining uninterrupted access even during node failures. Its design promotes effective interoperability by facilitating seamless communication between healthcare professionals across various systems. It allows patients to access their authorized medical records globally via NFTs issued by the Ministry of Health (MoH). NFT integration further improves data security and privacy by limiting access to critical patient data to authorized parties only, thus optimizing data security, privacy, and confidentiality throughout the healthcare ecosystem. Overall, by offering a thorough method for safe and effective patient health record administration, PHR-NFT addresses essential gaps in the literature and improves already-existing BPHRS frameworks.

The following are the key contributions of this research:

- Proposing PHR-NFT, a blockchain-based patient tracking system that uses NFTs to securely store patient data, enhancing the privacy and security of health records. Our framework adopts a patient-centric approach, allowing patients to control their NFTs and grant access permissions to authorized stakeholders based on collaborators within the network.
- Implementing patient NFTs on the Hyperledger Fabric blockchain platform. Smart contracts are utilized to automate health data sharing, ensuring that data are only shared with authorized parties after explicit patient consent.
- Conducting a comprehensive network performance analysis, evaluating key metrics, including throughput, latency, success rate, failure rate, and security.

The rest of the research paper is organized as follows: Section 2 presents the related works in blockchain-based patient records tracking systems. Section 3 outlines the methodology used in this study. Section 4 depicts the implementation of the proposed system. Section 5 concludes the paper and suggests future research directions.

2. Related Works

2.1. Blockchain-Based Patient Records Tracking Systems (BPHRS)

Blockchain technology has emerged as a leading trend for supporting distributed applications by removing the need for a reliable third party and guaranteeing stored data's integrity, validity, non-repudiation, and accountability [13,36]. Its various network types—public [18], private [20], hybrid [19], and consortium [12]—provide flexible solutions for managing PHRs, offering secure and transparent data management that enhances privacy, access control, and interoperability across healthcare systems.

Numerous studies [3,12,26–31] have examined the advantages of utilizing blockchain technology in patient record-tracking systems, emphasizing safe access to medical records, authorization, and authentication. Nedaa et al. [37] highlighted the growing concern regarding potential risks and vulnerabilities in blockchain-based PHR systems and the need to carefully evaluate their scope and effects on patient data. Zaabar et al. [3] proposed BPHRS-Healthblock, an architecture that enhances the security and privacy of PHRs by leveraging blockchain technology, decentralized databases, and access control mechanisms. A potential constraint of this study could be the requirement for additional verification of the scalability and interoperability of the proposed system in real healthcare environments, in addition to performance assessment parameters. Mohammed et al. [12] created smart contracts based on the Ethereum blockchain to provide patients with decentralized,

immutable, transparent, traceable, trustworthy, and secure control over their data. The proposed approach securely retrieves, stores, and distributes patient medical data by utilizing trusted reputation-based re-encryption oracles in conjunction with decentralized storage of IPFS. However, beyond the provided evaluation criteria, additional validation of the suggested solution's scalability and interoperability in various healthcare environments may be required, which could be a significant drawback of this study. Tanwar et al. [21] introduced a novel design and access control algorithm to enhance data protection while ensuring patient data privacy and security within a PHR system by eliminating central authority and single points of failure and leveraging Hyperledger blockchain technology. Despite the utilization of Hyperledger for safeguarding privacy and security, potential system flaws or vulnerabilities may remain, potentially enabling unauthorized access by hackers to patient data, thereby jeopardizing the system's integrity.

BlockMedCare, created by Azbeg et al. [25], is an IoT and Blockchain integration that allows for secure remote patient monitoring for chronic diseases. It guarantees security by integrating Blockchain and re-encryption, scalability through an off-chain IPFS database, and faster processing times with Ethereum-based proof of authority. While BlockMedCare offers benefits, it may have deployment and interoperability problems that necessitate carefully assessing compatibility with existing healthcare infrastructures. The Hyperledger blockchain-based HapiFabric system was proposed by Kordestani et al. [26] to improve the security, scalability, and dependability of medical operations. It is tailored for patient-centric telemedicine. Prioritizing the requirements of patients, HapiFabric also helps healthcare providers by minimizing needless travel and improving time management while upholding the standard of treatment. However, one limitation is the restricted accessibility of medical records across all locations. Wang et al. [28] introduced HSHB, a hybrid blockchain-based strategy for health data sharing that adapts to different sharing entities' requirements by utilizing alliances and private chains. It implements the health data access control policy to protect entities from interference and uses efficient query algorithms to obtain previous health data. Despite these advancements, HSHB may still encounter difficulties with integration and complexity of deployment into today's healthcare systems.

Furthermore, it offers patients minimal control over their information, which may raise privacy concerns. Bodur and Yaseen [30] suggested a blockchain-based strategy for sharing, accessing, and storing PHR. They used consensus techniques, including PoW, PoS, and PoA, to guarantee data confidentiality, integrity, and resilience to different types of cyberattacks. However, its emphasis on consensus techniques like PoW can lead to scalability problems and increased energy consumption. Jakhar et al. [31] proposed a BPHRS system that helps to manage healthcare data by utilizing Hyperledger Fabric for permissioned, safe, and efficient access control. This improves privacy, security, and data integrity while granting patients authority over access rules. However, it does not adequately address individual health records' interoperability and scalability challenges. Swetha et al. [32] developed the SecureMed framework, which helps manage healthcare data by using IPFS and Ethereum's blockchain to handle electronic health records (EHRs) decentralized and securely. It provides a trustless platform and smart contracts for scalability and access control. It does not, however, have the ability to protect privacy or provide individualized control over personal records. Venkatesh and Hanumantha [33] proposed a quantum blockchain-based privacy-preserving method that lowers communication and computation costs during the exchange of electronic medical records while preventing various attacks, including quantum threats like collective and coherent attacks. However, it lacks the strategy for patient-centered ownership and control of medical records, and it has issues with interoperability and scalability. Haddad et al. [34] proposed the patient-centered blockchain-based EHR management system using Ethereum and IPFS, which provides a decentralized and patient-centered approach to EHR management, giving patients complete control over their records and guaranteeing safe and scalable data sharing amongst various stakeholders without the need for centralized infrastructure. This solution may not be as effective in complying with stringent data privacy regulations like GDPR since it lacks

the sophisticated privacy capabilities necessary for fine-grained, adaptable access control and ownership management. Chinnasamy et al. [35] presented a scalable EHR sharing mechanism for cloud-based IoT in e-health that uses Ethereum and IPFS. It offers a robust access control system via smart contracts that improves data security and facilitates the effective exchange of medical records. Although the system guarantees secure data sharing and scalability, it mainly concentrates on cloud-based solutions, which may pose difficulties concerning patient ownership of data and decentralization in contrast to more patient-centered frameworks.

Most of the existing BPHRSs lack patient-centric solutions and the capacity to trace and track PHRs in a transparent and tamper-proof manner [12,31,35]. When third parties try to access patient data, current BPHRSs can jeopardize patient privacy. Furthermore, patients frequently have little control over their health data under the present systems, which makes it difficult for them to access records and communicate with medical professionals [28,29,33]. Additionally, BPHRSs are vulnerable to cybersecurity threats and data breaches, particularly when patient data are shared among networks [26,27]. There are serious privacy risks associated with these breaches since they may expose PHR to hackers [32,34]. Furthermore, current blockchain-based solutions involve considerable costs and high energy consumption [21,25,26]. The lack of procedures to enable patients to modify or delete their information is another limitation in existing systems. It runs against privacy laws like the GDPR, which upholds the right to be forgotten [23,30]. Furthermore, the confidentiality of patient information may be compromised by the usage of public blockchain networks in certain BPHRSs since health data, even when encrypted, may be accessible or traceable [19,32]. Finally, sensitive data are visible to parties not directly involved in patient care since many existing systems lack efficient access control methods [21,38].

Although current solutions offer blockchain-based security and transparency, they frequently lack thorough validation in actual healthcare settings, pose difficulties with scalability, interoperability, privacy, and patient data control, and may still leave vulnerabilities open to unauthorized access. PHR-NFT bridges these gaps by empowering patients with ownership of their health data while providing temporary access to authorized medical providers through the use of Hyperledger Fabric and NFTs. This system guarantees the integrity and traceability of patient records while improving privacy, scalability, and interoperability. Additionally, PHR-NFT uses a decentralized framework to facilitate smooth data transmission across various healthcare platforms, addressing the problem of healthcare system integration and offering a solid solution for enhancing global healthcare data management.

Table 1 indicates that compared to the existing BPHRS framework, the proposed approach yields the greatest possible benefits by guaranteeing the patient complete ownership of the NFT, assured security, and performance analysis. PHR-NFT is demonstrated to be based on the Hyperledger blockchain platform, which uses NFTs to manage patient records and incorporate security and network performance evaluations. Stakeholders can better grasp how PHR-NFT addresses healthcare data management and security issues by comparing it to and contrasting it with other blockchain-based solutions. The proposed research considers latency, send rate, number of failed transactions, failure rate, and throughput to probe deeper into the operational dynamics and efficiency of the system. These measurements provide information on the system's overall responsiveness, transaction handling capability, resilience, and real-time performance.

Table 1. Comparison with existing works.

References	Blockchain Type	NFT	Network Performance Analysis	Security Analysis
[26]	Hyperledger	×	×	×
[27]	Ethereum	×	✓	×
[12]	Ethereum	×	×	×
[28]	Komodo	×	×	×
[29]	Hyperledger	✓	×	×
[30]	Ethereum	×	×	✓
[31]	Hyperledger	×	×	✓
[32]	Ethereum	×	×	✓
[33]	Quantum	×	×	×
[34]	Ethereum	×	×	✓
[35]	Ethereum	×	×	✓
PHR-NFT	Hyperledger	✓	✓	✓

× means “Not Included” and ✓ means “Included”.

2.2. Non-Fungible Tokens (NFTs)

In blockchain terminology, an NFT is a distinct digital asset that is not tradable one-to-one for another token of the same kind [24]. NFTs are different and indivisible, each having unique traits and attributes, unlike fungible tokens, like cryptocurrencies, where each unit is identical and equivalent. The token’s metadata contains unique identifiers that provide a digital certificate of ownership and authenticity. NFTs use the decentralized ledger technology of blockchain to safely document provenance and ownership, guaranteeing transparency and unchangeability [39]. Through smart contracts and cryptographic hashing, NFTs facilitate digital asset production, ownership, and transfer with substantial uniqueness and exclusivity. Seyed et al. [40] presented a tiered conceptual framework that offers guidance on storage, decentralized authentication, verification, blockchain, and application layers for presenting intellectual property assets, specifically patents, as NFTs. This opens the door for using NFTs in real-world applications beyond digital artwork and collectibles. Zhang et al. [24] put forth a novel strategy that combines federated learning with NFTs to enable users of the Metaverse to share economic value and control ownership.

We intend to apply NFTs in PHR-NFT to revolutionize the management of patient health records by providing a robust, secure, and globally accessible system. NFTs are perfect for protecting patient data confidentiality and privacy because they offer distinct digital identities that guarantee ownership and authenticity verification [41]. NFTs are a safe way to allow authorized users to access patient records in the proposed PHR-NFT system, giving patients authority over their data while maintaining data privacy [42]. Using NFTs and blockchain technology, PHR-NFT improves system interoperability, data security, and patient tracking, resulting in a more connected and effective global healthcare environment.

3. Methodology

3.1. Usecase Scenario

In this section, we present our use-case scenario consisting of Patient A, who registers at Hospital X, which has been approved by the MoH, and asks Insurance Company I1 for access to their medical information. After the insurance provider has verified the request, Hospital X authorizes it by processing Patient A’s Emirates ID. Lab tests are ordered during a consultation, and the additional requests are reviewed and approved by Insurance Company I1. Prescriptions, lab data, and consultation reports are all stored on the blockchain by Hospital X. The validity and integrity of the saved data are then ensured by the MoH, which uses Patient A’s Emirates ID as the key to validate the information. Following validation, MoH provides an NFT as a digitally authenticated certificate certifying Patient A’s medical records. Authorized healthcare providers can securely access this NFT during the patient’s

visit and for a limited time afterward, ensuring patient-centric control over data access. With the approval of Patient A, the patient’s information can also be safely accessed by other healthcare facilities across the globe that accept the MoH-approved NFT, ensuring data integrity, privacy, and interoperability.

3.2. PHR-NFT System Workflow

The workflow of the PHR-NFT system (see Figure 1) begins with the registration of healthcare organizations by the MoH on the blockchain network. The hospital (H) works with the MoH to safely log all transactions on the blockchain, including prescriptions and test results. The MoH confirms the recorded information using the patient’s Emirates ID to guarantee data authenticity and accuracy. The MoH provides the patient with a non-fungible certificate (NFC) that serves as a representation of their certified medical records after successful verification. Hospitals worldwide can accept this NFC, which acts as a digital token for the patient’s approved medical data and has built-in authentication to ensure dependability. With the patient’s consent, authorized healthcare practitioners can safely access the patient’s records via the blockchain. The blockchain is used to build and store smart contracts, which define conditions such as the requirement for patient consent before document access is granted. Each institution is limited to tracking and accessing patient records to protect privacy and security. Doctors can quickly access pertinent information for proper care by accessing the patient’s records during appointments and a prearranged follow-up period. Moreover, the patient controls their data sharing by allowing other insurance companies access to their medical records from the blockchain only with express authorization. This process guarantees safe and effective patient data administration, with strict privacy regulations and simplified access for insurance companies and healthcare providers.

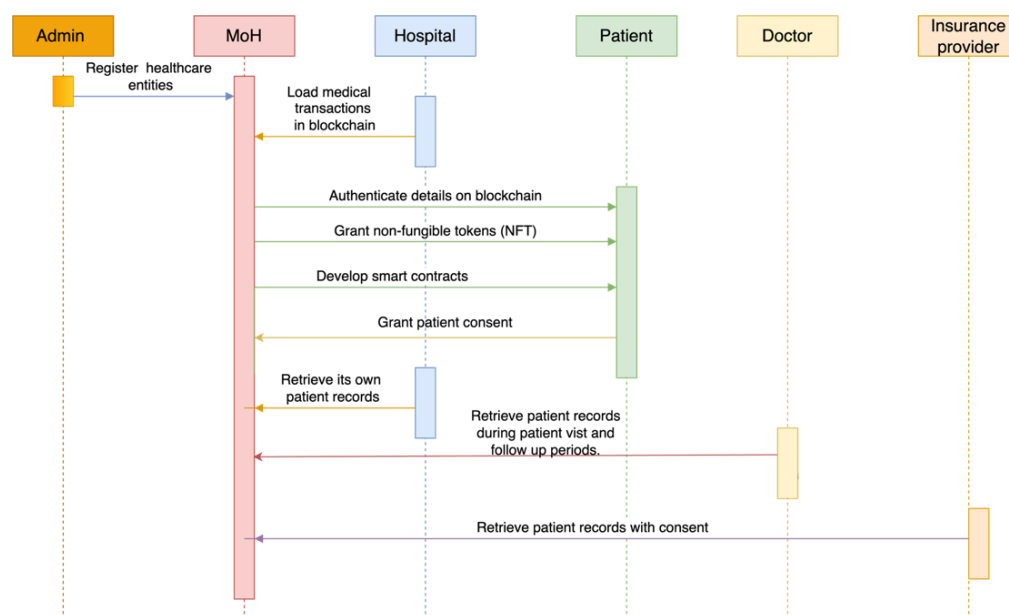


Figure 1. PHR-NFT system workflow.

3.3. PHR-NFT System Architecture

Figure 2 depicts the proposed BPHRS, PHR-NFT, which uses NFT and Hyperledger technology. Integrating NFTs with Hyperledger-based patient data monitoring systems creates a safe, decentralized network for the administration of medical records in the healthcare industry. It consists of two layers: the user layer and the blockchain network layer.

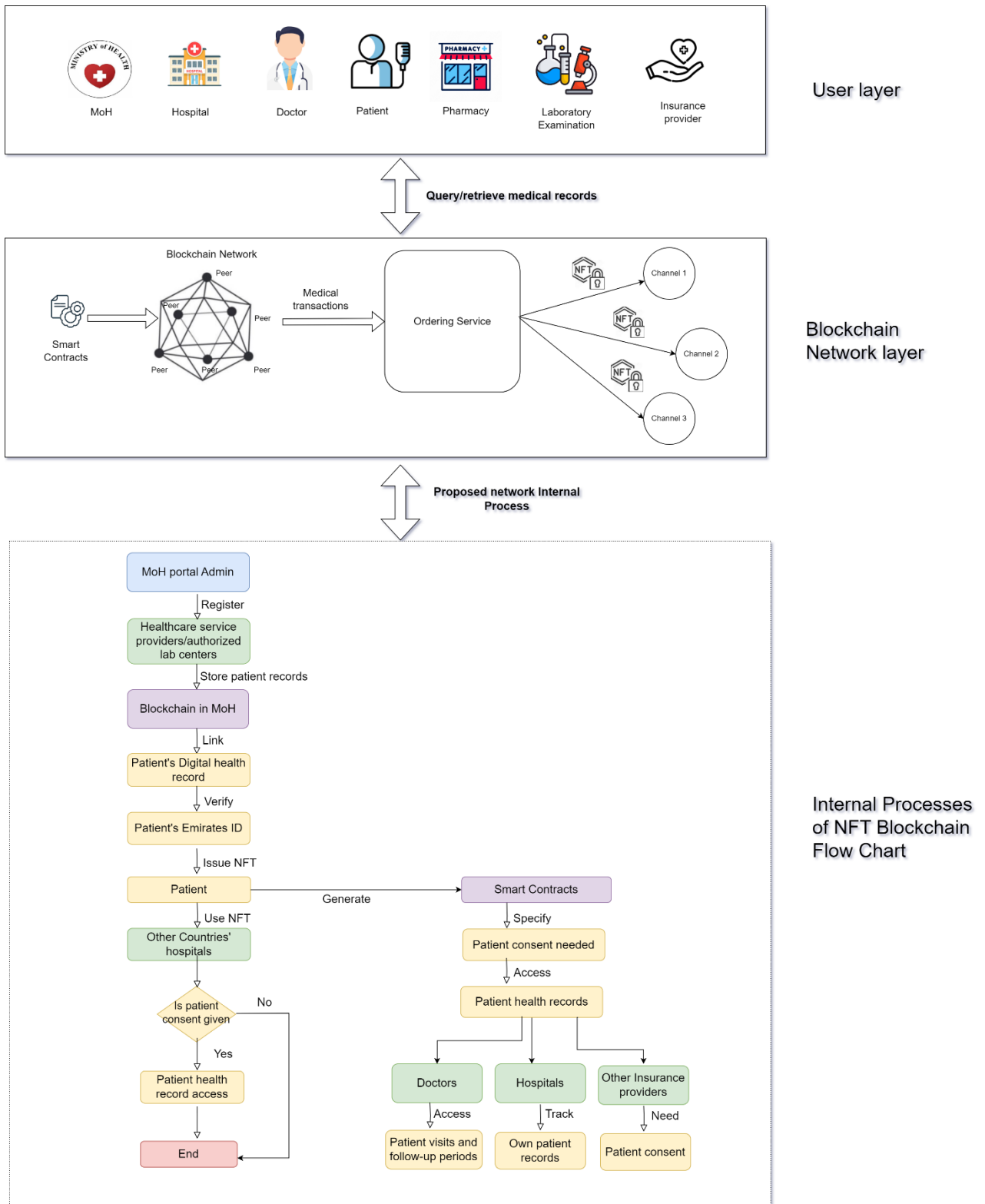


Figure 2. PHR-NFT system architecture.

3.3.1. User Layer

The system serves many users, including patients, physicians, hospitals, MoH, doctors, pharmacies, insurance providers, and labs. PHRs can be gathered and occasionally shared by doctors and patients. Using NFTs, the system gives patients control and authority over their medical records. Doctors wishing to view or amend a patient’s medical record

must undergo an authentication process. The safe and controlled exchange of medical information is ensured by the fact that only authorized individuals can access these records.

3.3.2. Blockchain Network Layer

The blockchain layer serves as the foundational network infrastructure for sharing electronic health records (EHRs) within the healthcare ecosystem. The proposed PHR-NFT framework leverages blockchain technology to create and manage patient health records using NFTs. This layer integrates multiple components and mechanisms designed to ensure secure, decentralized, and efficient data management and sharing.

Blockchain Type

The proposed framework utilizes a consortium blockchain network, which is shared and maintained by a selected group of organizations; access to this network necessitates prior registration, ensuring that only authorized entities can participate. In this study, multiple hospitals, laboratories, pharmacies, and insurance companies serve as network participants. The MoH oversees the network and manages transaction tracking and participant registration. Despite this oversight, the sharing of records occurs peer-to-peer, maintaining a decentralized environment that ensures secure and efficient data exchange among the stakeholders. Equation (1) represents the consortium blockchain network in the proposed framework:

$$BN = \{MoH, P, SC, T_{xn}, R_{NFT}, \pi, Peers, DS, TS\} \quad (1)$$

where BN is the consortium blockchain network; P is the set of participants (hospitals, labs, pharmacies, insurance companies); MoH manages the network; T_{xn} is the set of transactions, such that $T_{xn} = \{t_1, t_2, t_3, \dots, t_n\}$; SC is the set of smart contracts in the network, such that $SC = \{add_patient, update_patient, query_patient, patient_NFT\}$; R_{NFT} is the set of patient record NFTs; π is the set of permissions and access control policies; Peers are the peer nodes participating in the network, such that $Peers = \{H1: p1, p2, \dots, pn; H2: p1, p2, \dots, pn; H3: p1, p2, \dots, pn, Lab1: p1, p2\}$; DS is the digital signature for security and authenticity; and TS is the timestamp of transactions and record updates.

Smart Contracts

Smart contracts are integral programs that enable the blockchain network to function effectively by automating specific operations. They are self-executing contracts, with the terms of the agreement directly written into code, and they are automatically triggered when predefined conditions are met. In the proposed framework, the smart contracts described below are utilized.

Add_Patient Smart Contract

The Add_patient smart contract is pivotal to integrating new patient records into the blockchain network, ensuring patient data are securely recorded and assigned a unique identifier for future reference. Upon registering a new patient in the network, an NFT is created and assigned to the patient, which acts as their unique digital identity, encapsulating their health records. Access rights are granted to the patient, empowering them with control over their medical data and ensuring their health information's secure, decentralized management.

Update_Patient Smart Contract

This contract allows authorized entities to update existing patient NFTs. Before any modifications are made, explicit consent from the patient is obtained to access their NFT. This protocol guarantees that alterations to patient information undergo a rigorous logging and tracking process, preserving the absolute integrity and uniformity of the data.

Query_Patient Smart Contract

This contract facilitates the seamless retrieval of patient records stored on the blockchain, granting authorized users efficient access to patient information while rigorously enforcing access control policies. Before any retrieval, the patient’s consent is diligently sought through their NFT, ensuring a secure and transparent process.

Smart Contract for NFT

This contract is responsible for creating and managing NFTs for patient records, assigning a unique digital identity to each patient’s health record, and ensuring secure and verifiable ownership and access control. When a new patient is registered in the network, an NFT is created for the patient, which is represented in Equation (2):

$$T_{add} = \{P_{ID}, NFT_P, \pi, DS, TS, C_{set}\} \tag{2}$$

where T_{add} is the Add_patient Transaction, which is the operation of adding a new patient; P_{ID} is the unique identifier assigned to the patient; NFT_P is the non-fungible token created for the patient, which includes the patient identifier, health record data, digital signature, and timestamp such as $NFT_P = \{P_{ID}, R, \sigma, TS\}$, where R is the patient record, σ is the digital signature, and TS is the timestamp for creating the NFT; π is the access rights granted to the patient, defining who can access or modify their health data; DS is the digital signature that ensures the authenticity and integrity of the data; TS is the timestamp indicating when the patient was registered to the blockchain; C_{set} denotes the set of collaborators. When a request for patient NFT access is initiated, the requesting node undergoes verification within the collaborator set. If the node is found within this set, permission is promptly granted.

4. Performance Evaluation

In this section, we evaluate the performance of our proposed framework based on standard critical metrics used in the literature [21,43], such as throughput, latency, transaction failure, and security performance (Table 2). The performance analysis provides valuable insights into the scalability and reliability of our framework under different workload conditions (the implementation code will be provided upon request to the authors).

Table 2. Performance matrix.

Performance Matrix	Explanation
Throughput	Throughput indicates the overall transaction processing capacity (in TPS), considering successful transactions per second. Higher throughput values reflect higher transaction processing efficiency.
Latency	Latency measures the time it takes for a transaction to be processed and confirmed. Lower latency values are preferable as they indicate quicker transaction confirmations in the network.
Scalability	Scalability tests the network performance with an increasing number of transactions.
Fail Transaction	This denotes the number of failed transactions during processing. Minimizing failed transactions is essential for a robust blockchain network.
Security Analysis	Security analysis of the deployed network based on the threat model.

Threat Model

Security analysis is crucial for assessing the robustness of the proposed network. This research addresses **Denial of Service (DoS) attacks**, representing a significant and prevalent threat to distributed networks. In the context of a DoS attack, a malicious actor seeks to flood the network with unauthorized transactions, thereby exhausting system resources and rendering services unavailable to legitimate users, ultimately disrupting network operations. Our threat model assumes that the attacker can generate a substantial volume of transactions at a rapid pace, effectively overwhelming the **ordering service** within the blockchain network. The attacker aims to induce service degradation by imposing sufficient

load to provoke transaction delays, high failure rates, or even the total cessation of network functionality. The failure rate is defined as follows:

$$\text{Failure rate}(\%) = \frac{\text{Failed Transactions}}{\text{Total Transactions}} \times 100$$

5. Experimental Environment

We conducted our experiments using Hyperledger Fabric (HLF) version 2.4, an enterprise consortium blockchain framework. The blockchain network was deployed on a system with the specifications shown in Table 3.

Table 3. Hardware and software specifications of the experiment.

Hardware Specifications	Software Specifications
Operating System: Ubuntu 20.04 LTS CPU: 12th Gen Intel® Core™ i9-12950HX×24	Hyperledger Fabric v2.x Docker Engine v24.0.5 Docker Compose v1.29.2 Hyperledger Caliper v0.6.0 Npm v5.x Git 2.9+ Go 1.11 Python v2.7.x Visual Studio v17.11

Docker Engine version 24.0.5 and Docker Composer version 1.29.2 are used in blockchain development, providing the development environment to set up the container and docker image on the virtual machine. Docker Composer offers the runtime environment for Docker Engine. The performance of the deployed network is precisely assessed using Hyperledger Caliper [44]. Hyperledger Caliper, a Linux-based open-source benchmarking tool, is used to evaluate the performance of the blockchain-based platform with utmost accuracy. In the deployed network, the performance is measured in terms of transaction latency and throughput. We deployed five worker nodes for the network test and ran the experiments five times, taking the average for the performance measures.

5.1. Implementing NFTs in the Hyperledger Fabric Network to Tokenize the Patient Record

The NFT for patient records was implemented using the Go programming language within the HLF network's chain code directory. The chain code files described below encapsulated the core logic for handling patient records and access permissions.

- **patient-contract.go:** The patient-contract.go file contains the main logic for managing patient records as NFTs and defines their structure and behavior, including metadata attributes such as the patient ID, medical history, and associated access controls.
- **token.go:** The token.go file complements the patient-contract.go file by implementing the NFT token functionality, including token minting, transfer, and access permission management.

A predefined set of collaborators was established to ensure secure and authorized access to patient NFTs. This collaborator set comprises registered healthcare professionals across multiple institutions, including hospitals and laboratories.

- **Hospitals** (e.g., hospital1, hospital2, hospital3): registered doctors within these hospitals are designated as collaborators, enabling them to request access permission for specific patient records within their respective institutions.
- **Laboratories** (e.g., lab1, lab2): similarly, lab scientists affiliated with designated laboratories are included in the collaborator set, allowing them controlled access to patient data for diagnostic and research purposes.

The NFT implementation incorporates a robust access control mechanism where authorized collaborators can request access permissions for specific patient records. Access requests trigger a permission verification process within the chain code, ensuring only validated collaborators can retrieve or update patient information. Algorithm 1 presents a comprehensive, step-by-step guide for implementing NFTs, outlining the specific procedures and methods involved in the process.

Algorithm 1: HLF Network Setup and Patient NFT Access Control

```

//Setup HLF Network
1 InitializeHLFnetwork(version = 2.4, nodeVersion = 14.17.0)
2 configureEntities(entities = ["hospital1", "hospital2", hospital3", "lab1", "lab2", "MoH"])
//Deploy chain codes
3 deployChaincodes(chaincodes = ["doctor_contract.go", "patient_contract.go",
"patient_checkup.go", "patient_health.data.go", "token_contract.go"])
4 deployPatientNFT(tokenContract = "token_contract.go")
//Create collaborator set for access permission for patient NFT
5 createCollaboratorSet(collaborators = ["registered doctors in hospital1/hospital2/hospital3",
"lab scientists in lab1/lab2"])
//Request access permission for patient NFT
6 searchPatients(criteria)
7 requestAccessPermission(healthcare_entity, patient)
8 If (healthcare_entity in collaborators) then
9   sendAccessRequest(patientID)
//For Patient:
10   AccessRequestReceived(healthcare_entity ID)
11   PermissionRevoked(healthcare_entity ID)
//For healthcare_entity
12   RecordViewed(patientID) or RecordUpdate(patientID)
13   updatePatientNFT(patientID, accessGranted)
14   commitTransactionToBlockchain(transaction)
15 else
16   Reject access request for patient data
17   logUnauthorizedAccessAttempt(healthcare_entity ID)
18 end if
19 recordTransactions(transactionHistory, CouchDB)

```

5.2. Experimental Results and Discussion

In this section, we detail the experiments conducted on the deployed HLF network, which comprises three hospitals, two laboratories, and the MoH acting as the network administrator. We simulated a real-world healthcare scenario for sharing patient records in a healthcare federation with the participants in the network above. The main operational functionalities include querying and updating patient records for existing or registered patients and creating patient NFTs for newly registered patients. The network architecture includes multiple peers, orderers, and endorsers distributed across the participating entities. Table 4 shows the deployed network configuration in terms of resource utilization.

Table 4. Network configuration.

Name	CPU% (max)	CPU% (avg)	Memory (max) [GB]	Memory (avg) [GB]	Traffic In [MB]	Traffic Out [MB]	Disc Write [MB]
Total	74.96	31.19	5.3433	4.8441	284.6892	273.69	765.9

The maximum CPU utilization recorded is 74.96%, which indicates the peak load on the CPU during the observed period, potentially reflecting high computational demand or processing requirements. The average CPU utilization is 31.19%, which signifies the

typical workload on the CPU over the monitoring interval. A lower average compared to the maximum suggests fluctuations in the CPU demand. The maximum memory usage observed is 5.3433 GB (gigabytes), which reflects the peak memory consumption during the monitoring period, highlighting the maximum memory capacity required by the blockchain network. The average memory usage is 4.8441 GB, representing the typical memory utilization over time, providing insights into the network's memory requirements for regular operation. "Traffic in" denotes the inbound network traffic, measuring the volume of data that the network receives in megabytes (MB). The observed value of 284.6892 MB indicates the amount of data the network processed from external sources. "Traffic out" represents the outbound network traffic, indicating the volume of data transmitted by the network to external destinations. The value of 273.69 MB reflects the amount of data sent out by the network. Disc write captures the maximum disk writing activity observed in megabytes (MB). The recorded value of 765.9 MB indicates that the peak data rate was written to disk during the monitoring period.

5.2.1. Network Performance

In this section, we investigated the scalability performance of our test network with increasing transaction load, ranging from 100 to 1100 transactions per round (i.e., a single iteration of testing), using the Hyperledger Caliper analysis tool. Scalability refers to the network's ability to handle growing transactions without significant performance degradation. The experiments ran five tests for each transaction load setting, and the latency metrics (maximum, minimum, and average) were recorded and analyzed. Figure 3 represents the maximum, minimum, and average latency observed across different transaction loads (100, 200, 300, 400, . . . , 1100). The plot illustrates how latency metrics change with increasing transaction volumes. Analyzing maximum, minimum, and average latencies helps identify performance trends and informs optimization strategies such as capacity planning, resource allocation, and workload distribution. The maximum latency metric indicates the peak response time observed during a round of transactions. It represents the upper bound of transaction execution times and is crucial for identifying potential performance bottlenecks or outliers. Conversely, minimum latency represents the fastest response time achieved during a round of transactions. It provides insights into the best-case performance scenario and highlights the efficiency of the blockchain network under optimal conditions. The average latency metric summarizes the network's overall performance by calculating the mean response time across all transactions in a round. It serves as a baseline indicator of transaction processing efficiency and system responsiveness. As transaction loads increase, latency metrics typically exhibit non-linear behavior. Initially, latency may remain relatively stable but can increase sharply beyond a certain threshold due to resource saturation or contention.

Figure 4 illustrates the network throughput and send rate relationship across transaction volumes. The send rate refers to the rate at which transactions are submitted to the blockchain network. It corresponds to the frequency of transaction submissions during each experimental round. We systematically varied the transaction loads, ranging from 100 to 1100 transactions per round, to assess the network's scalability and performance under increasing workloads. As the number of invoked transactions increases (from 100 to 1100), the network throughput demonstrates a linear increase in Figure 4. This suggests the network's capacity to process transactions scales proportionally with transaction volume. Higher send rates (faster transaction submissions) correlate with increased network throughput, highlighting the importance of transaction rate management in optimizing network performance. Network throughput is proportional to latency. Network throughput tends to increase due to faster transaction processing and reduced queuing delays, while latency rises slower, as depicted in Figure 5.

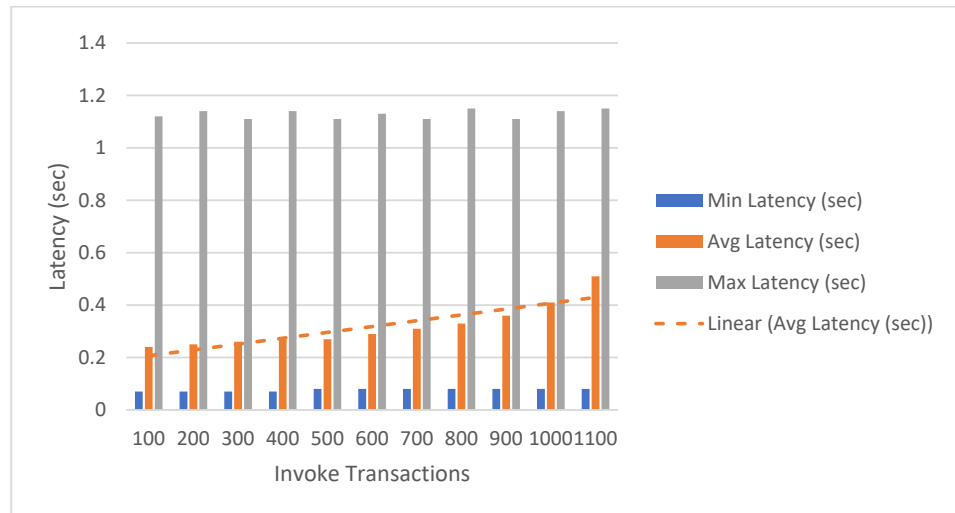


Figure 3. Maximum, minimum, and average latency.

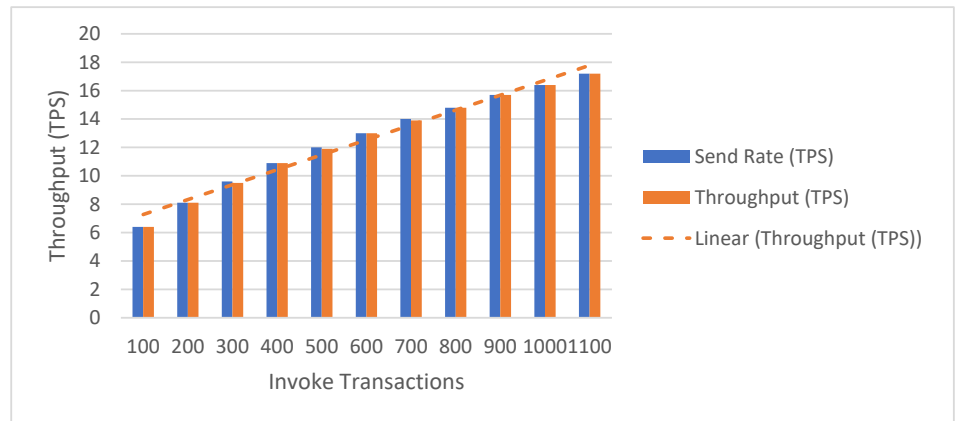


Figure 4. Throughput paired with network send rate.

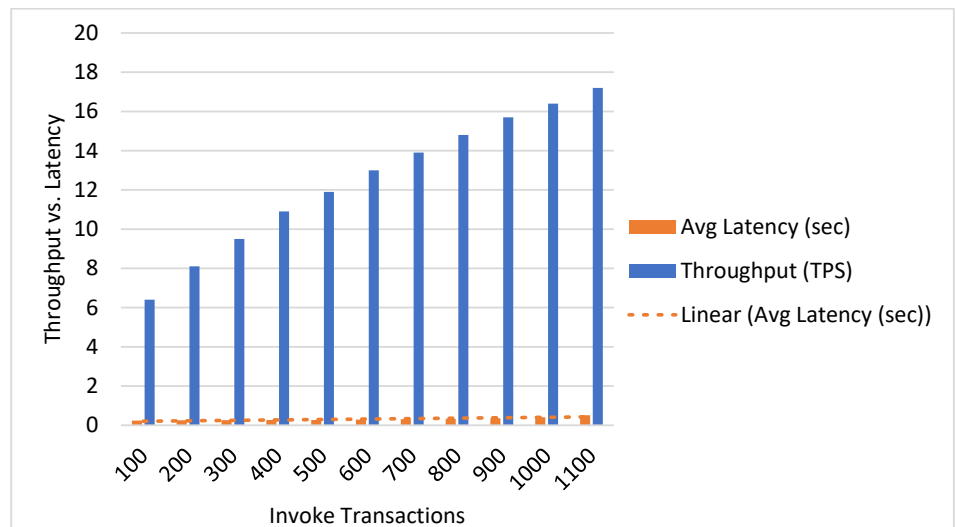


Figure 5. Network throughput vs. transaction latency.

Next, we analyze the total execution time. The total transaction execution time is the cumulative duration required to process and commit all transactions within a given workload. It includes transaction initiation, endorsement, ordering, validation, and ledger

update processes. Figure 6 illustrates the relationship between the total transaction execution time and the number of invoked transactions (ranging from 100 to 1100). As the number of invoked transactions increases from 100 to 1100, there is linear growth in the total transaction execution time. This suggests that transaction processing time scales proportionally with transaction volume, reflecting the network's ability to handle larger workloads. The linear increase in execution time indicates that the transaction volume influences the blockchain network's processing capacity. Higher transaction loads require more computational resources and time to process transactions, leading to longer execution times.

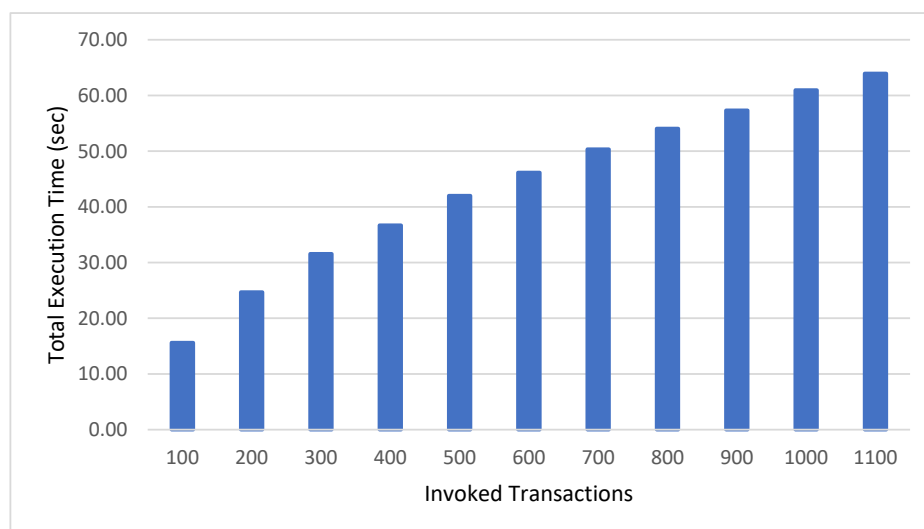


Figure 6. Total execution time.

5.2.2. Chain Code Performance Comparison

This section analyzed the network for chain code operations (Update Patient, Query Patient, Create Patient). We examined the success rate, failure rate, send rate, latency, and throughput associated with each operation. Figure 7 illustrates a comparative analysis of chain codes for transaction load 1000 TPS. Figure 7a shows that the average latency for Create Patient transactions is 92.13 ms, significantly higher than that of the Update and Query Patients transactions. The high latency of the Create Patient operation is due to several factors involving more complex transaction logic and resource-intensive processes compared to Query Patient and Update Patient operations. Creating a new patient record requires more computational resources, NFT creation, database writes, and validation steps, contributing to longer transaction processing times and potentially higher resource consumption.

Similarly, Figure 7b compares the throughput of different chain code operations within the blockchain network. Query Patient transactions exhibit a higher throughput of 26.8 transactions per second (TPS) compared to Update Patient transactions. However, Create Patients with high latency experience the lowest throughput. This highlights the impact of latency on transaction processing efficiency, emphasizing the importance of optimizing latency for improved network performance. Subsequently, Create Patient shows a lower success rate than both the chain codes (which exhibit a 100% success rate), as depicted in Figure 7c. The Create Patient success rate is 45.1% due to the 549 failed transactions; see Figure 7d. Creating a new patient record typically involves multiple data fields, creating NFTs, and more validation steps compared to updating or querying. This increases the chances of failure during the process due to incorrect or incomplete data submissions.

Next, we analyzed the Query Patient operation to retrieve a patient's record in Hospital 1. We compared the patient record retrieval performances of Hospital 1 and Hospital 2, and Figure 8 presents a comparative analysis of the results. The study revealed a minor increase

in the throughput of Hospital 2 compared to Hospital 1; however, this difference is relatively small because the simulation was conducted within the same system environment. The factors that influence the performance variations include variations in the number and distribution of peer nodes across organizations, the configuration and deployment of chain codes within each hospital’s blockchain network, differences in the network bandwidth availability and utilization, the time taken for a patient to authorize access to their NFT, and delays in communication and data transfer between the network participants. These factors collectively impact transaction processing, network efficiency, validation times, data transfer speeds, transaction latency, throughput, and overall system responsiveness.

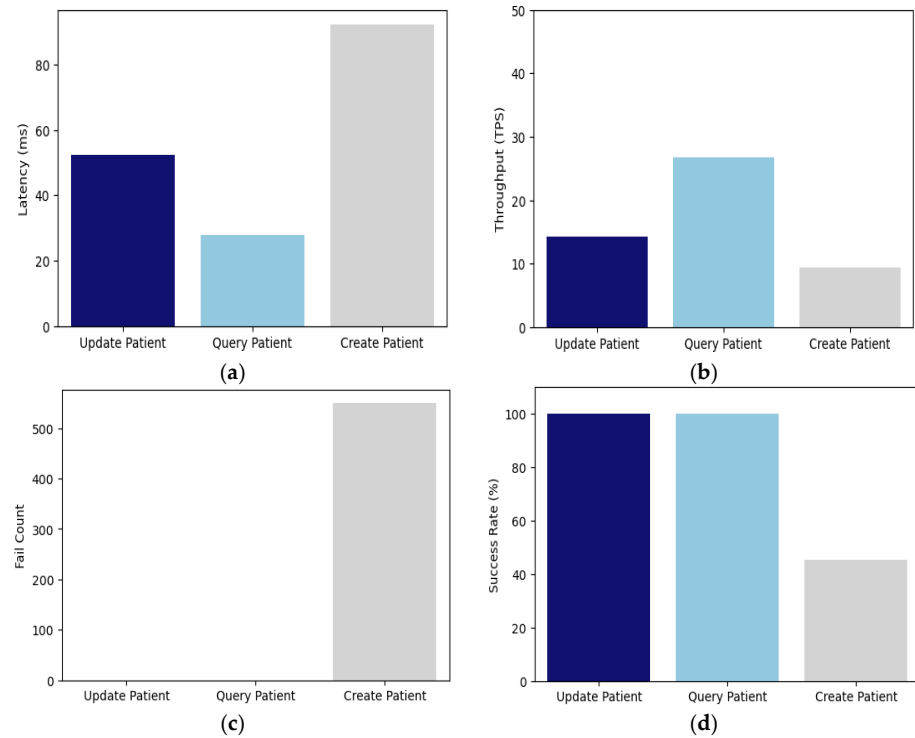


Figure 7. Comparing Create Patient, Update Patient, and Query Patient chain codes. (a) Latency comparison, (b) throughput comparison, (c) fail count comparison and (d) success rate comparison.

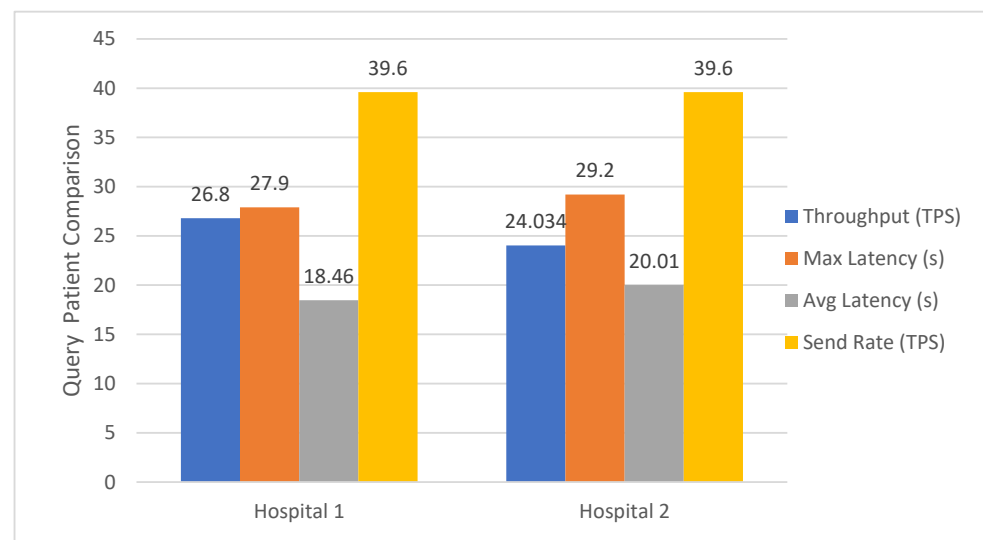


Figure 8. Patient record retrieval from Hospital 1 and Hospital 2.

5.2.3. Security Analysis

This section presents the security analysis of our proposed network. We conducted simultaneous transactions in the network, varying the number of workers and transaction loads to assess the network's susceptibility to DoS attacks. Specifically, we aimed to evaluate the risk of the order service becoming unavailable due to processing a large volume of transactions. These simulating conditions could be exploited in a DoS attack scenario. We checked the failure rate in the network under the given workload.

Figure 9 illustrates the impact of varying the number of workers (or nodes) on the total number of failed transactions under a transaction load of 8000 TPS. Our testing involved deploying 50, 80, and 100 workers to initiate 8000 transactions simultaneously. The results indicate a concerning trend: as the number of workers increases, the network becomes more vulnerable to DoS attacks, resulting in a higher rate of transaction failures.

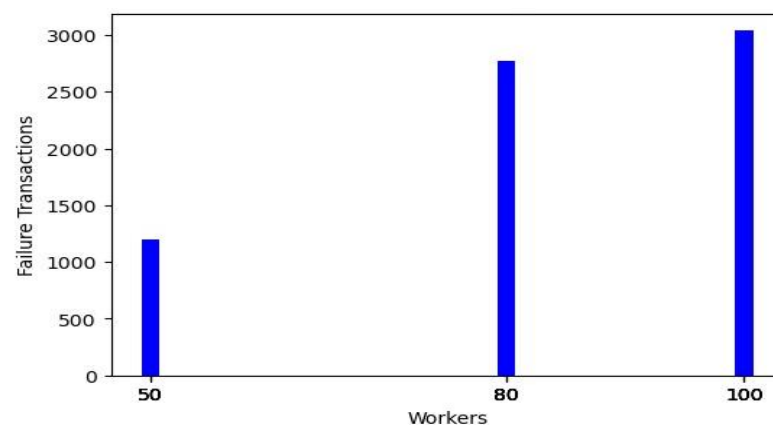


Figure 9. Transaction failure by varying worker nodes (transaction load = 8000).

In our subsequent test, we evaluated our network's performance under varying transaction loads ranging from 6000 TPS to 8000 TPS, with different numbers of workers. Figure 10 illustrates that our network demonstrated resilience when processing up to 6000 TPS across 50, 80, and 100 workers, achieving a 100% success rate. However, the network's stability was compromised as the transaction load increased to 6500 TPS. At this point, the network became susceptible to DoS attacks, resulting in network congestion and rendering the orderer service unavailable. Consequently, transaction failures began occurring once the transaction load reached 6500 TPS, underscoring the importance of optimizing the network capacity and implementing robust security measures to safeguard against potential disruptions and attacks at higher transaction volumes.

Subsequently, we computed a correlation matrix (Table 5) to analyze the relationships between the variables (workers, total transactions, send rate, latency, throughput, failed transactions, and failure rate (%)) using the experimental data. The correlation matrix provides insight into the strength and direction of the associations between these key performance metrics and the behavior and interdependencies within our experimental network environment.

The key findings of the correlation matrix are outlined below:

- **Workers vs. Other Variables:** Workers have a negative correlation with the send rate (-0.49), throughput (-0.32), latency (-0.13), failed transactions (0.28), and failure rate (%) (0.30). More workers are associated with a lower send rate, throughput, and latency and a slightly higher failed transaction number and failure rate.
- **Total Transactions vs. Other Variables:** The total transactions have a positive correlation with the failed transactions (0.89) and failure rate (%) (0.88) and a negative correlation with the send rate (-0.37) and throughput (-0.17). Higher total transactions are strongly associated with more failed transactions and a higher failure rate, showing weaker negative associations with the send rate and throughput.

- Send Rate vs. Other Variables:** The send rate has a negative correlation with the workers (−0.49), latency (−0.50), failure rate (%) (−0.47), and a positive correlation with the throughput (0.46). A higher send rate is associated with fewer workers, lower latency, a lower failure rate, and higher throughput.
- Latency vs. Other Variables:** Latency has a negative correlation with the send rate (−0.50) and throughput (−0.51) and a positive correlation with the failed transactions (0.20) and failure rate (%) (0.21). Lower latency is associated with a higher send rate, throughput, and slight increases in failed transactions and the failure rate.
- Throughput vs. Other Variables:** The throughput has a positive correlation with the send rate (0.46) and a negative correlation with the latency (−0.51), workers (−0.32), and failure rate (%) (−0.32). Higher throughput is associated with a higher send rate, a lower latency and failure rate, and fewer workers.
- Failed Transactions vs. Other Variables:** Failed transactions have a strong positive correlation with the total transactions (0.89), indicating that as the number of transactions increases, the number of failed transactions also increases.
- Failure Rate (%) vs. Other Variables:** The failure rate (%) has a strong positive correlation with failed transactions (0.99) and total transactions (0.88), indicating that it closely tracks the number of failed transactions and total transactions.

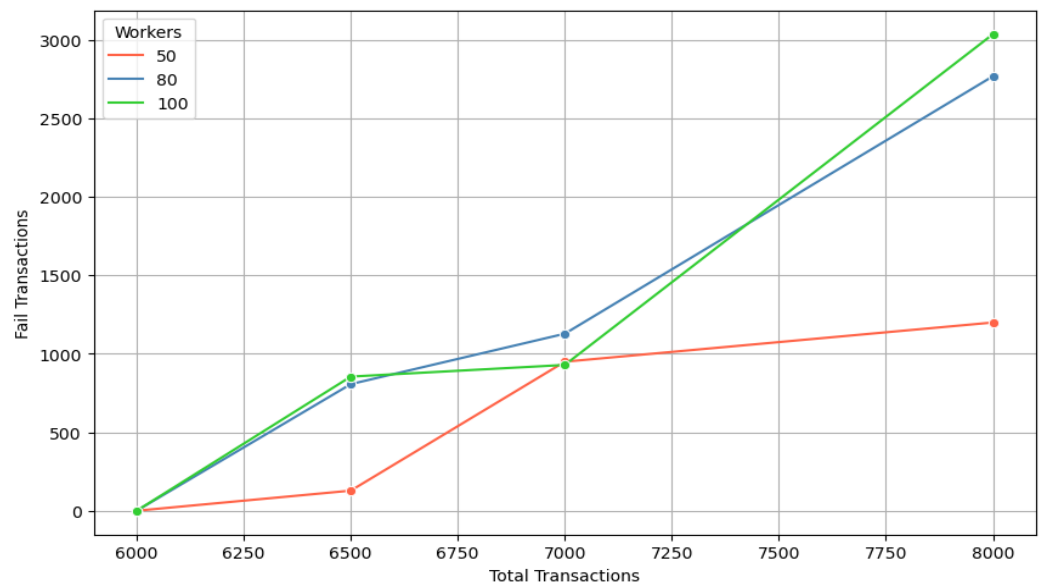


Figure 10. Fail transaction rates across the configuration.

Table 5. Correlation matrix.

	Workers	Total Transactions	Send Rate	Latency	Throughput	Fail Transactions	Failure Rate (%)
Workers	1.00	−0.00	−0.49	−0.13	−0.32	0.28	0.30
Total Transactions	−0.00	1.00	−0.37	0.34	−0.17	−0.17	0.88
Send Rate	−0.49	−0.37	1.00	−0.50	0.46	0.46	−0.47
Latency	−0.13	0.34	−0.50	1.00	−0.51	−0.51	0.21
Throughput	−0.32	−0.17	0.46	−0.51	1.00	−0.2	−0.33
Fail Transactions	0.28	0.89	−0.44	0.20	−0.28	1.00	1.00
Failure Rate (%)	0.30	0.88	−0.47	0.21	−0.33	1.00	1.00

6. Conclusions

This study provides a decentralized, safe, and user-friendly approach to BPHRSs by utilizing NFT and Hyperledger blockchain in patient record tracking systems. The PHR-NFT system outperforms existing BPHRS by using NFTs to enhance patient data ownership,

privacy, security, integrity, and interoperability, effectively addressing confidentiality and data management constraints. Patients can use a permission-based system, which ensures data ownership and control, to provide others with temporary access to their data. Data accountability and integrity are ensured with NFTs by monitoring all activity related to patient records and verifying ownership. The performance evaluation demonstrates the practicality and efficiency of PHR-NFT in terms of throughput, latency, transaction failure rates, and security against DoS attacks. The non-linear behavior of transaction delay with increasing transaction loads highlights the significance of effective resource allocation and transaction rate management. Performance varies throughout healthcare organizations due to network bandwidth, chain code configuration, and peer node dispersion. Furthermore, the system's ability to withstand DoS attacks is critical, underscoring the necessity of robust security protocols.

However, the research also has certain shortcomings, especially regarding scalability. Peer node distribution and resource management become more complex as network users rise, potentially increasing a system's susceptibility to attacks. The adoption of NFTs may be costly due to infrastructure expenses and inefficient, compounded by a shortage of technical experts skilled in NFT technology within the healthcare industry. Subsequent research endeavors focus on integrating artificial intelligence and machine learning components to automate healthcare diagnosis determinations. The widespread adoption of NFTs and blockchain technology in the healthcare sector will require the development of comprehensive industry standards and regulations, ultimately supporting the creation of an effective and compliant healthcare data ecosystem. Further, more studies are needed to solve scaling issues and improve system performance, even if PHR-NFT offers potential ways to strengthen PHR security and privacy.

Future PHR-NFT enhancements will apply modern penetration testing methods to strengthen security and privacy and guarantee cyberattack resistance. One improvement will be more detailed NFT-based access controls, which will provide accurate patient data management while maximizing blockchain scalability. Furthermore, privacy-preserving algorithms will be researched to guarantee adherence to laws like the GDPR, thereby enhancing patient privacy and maintaining data integrity. As a result of these enhancements, PHR-NFT will become a more reliable and flexible solution for safe patient health record management.

Author Contributions: Conceptualization, H.E.S., N.B.A.B. and S.M.B.; Methodology, H.E.S., N.B.A.B., S.M.B. and F.H.; Formal analysis, H.E.S., N.B.A.B., S.M.B. and F.H.; Data curation, N.B.A.B.; Writing—original draft, H.E.S., S.M.B., F.H. and S.G.; Writing—review & editing, H.E.S., N.B.A.B., S.M.B. and S.G.; Supervision, H.E.S. and N.B.A.B.; Project administration, H.E.S.; Funding acquisition, H.E.S. and S.M.B. All authors have read and agreed to the published version of the manuscript.

Funding: This research was funded by Zayed University, Grant R21063.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The data presented in this study are available on request from the corresponding author.

Conflicts of Interest: The authors declare no conflict of interest.

References

1. Chen, L.; Lee, W.-K.; Chang, C.-C.; Choo, K.-K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. *Future Gener. Comput. Syst.* **2019**, *95*, 420–429. [[CrossRef](#)]
2. Chen, Z.; Xu, W.; Wang, B.; Yu, H. A blockchain-based preserving and sharing system for medical data privacy. *Future Gener. Comput. Syst.* **2021**, *124*, 338–350. [[CrossRef](#)]
3. Zaabar, B.; Cheikhrouhou, O.; Jamil, F.; Ammi, M.; Abid, M. HealthBlock: A secure blockchain-based healthcare data management system. *Comput. Netw.* **2021**, *200*, 108500. [[CrossRef](#)]

4. Chelladurai, M.U.; Pandian, S.; Ramasamy, K. A blockchain based patient centric electronic health record storage and integrity management for e-Health systems. *Health Policy Technol.* **2021**, *10*, 100513. [[CrossRef](#)]
5. Shamshad, S.; Minahil; Mahmood, K.; Kumari, S.; Chen, C.-M. A secure blockchain-based e-health records storage and sharing scheme. *J. Inf. Secur. Appl.* **2020**, *55*, 102590. [[CrossRef](#)]
6. Li, H.; Yang, X.; Wang, H.; Wei, W.; Xue, W. A controllable secure blockchain-based electronic healthcare records sharing scheme. *J. Healthc. Eng.* **2022**, *2022*, 2058497. [[CrossRef](#)]
7. Ismail, L.; Materwala, H. BlockHR: A blockchain-based framework for health records management. In Proceedings of the 12th International Conference on Computer Modeling and Simulation, Brisbane, QLD, Australia, 22–24 June 2020; pp. 164–168.
8. Wu, H.; Dwivedi, A.D.; Srivastava, G. Security and privacy of patient information in medical systems based on blockchain technology. *ACM Trans. Multimedia Comput. Commun. Appl.* **2021**, *17*, 1–17. [[CrossRef](#)]
9. Ismail, L.; Materwala, H.; AB Khan, M. Performance evaluation of a patient-centric blockchain-based healthcare records management framework. In Proceedings of the IECC 2020: 2020 2nd International Electronics Communication Conference, Singapore, 8–10 July 2021.
10. Liu, X.; Wang, Z.; Jin, C.; Li, F.; Li, G. A blockchain-based medical data sharing and protection scheme. *IEEE Access* **2019**, *7*, 118943–118953. [[CrossRef](#)]
11. Houtan, B.; Hafid, A.S.; Makrakis, D. A survey on blockchain-based self-sovereign patient identity in healthcare. *IEEE Access* **2020**, *8*, 90478–90494. [[CrossRef](#)]
12. Madine, M.M.; Battah, A.A.; Yaqoob, I.; Salah, K.; Jayaraman, R.; Al-Hammadi, Y.; Pestic, S.; Ellahham, S. Blockchain for giving patients control over their medical records. *IEEE Access* **2020**, *8*, 193102–193115. [[CrossRef](#)]
13. Al Mamun, A.; Azam, S.; Gritti, C. Blockchain-based electronic health records management: A comprehensive review and future research direction. *IEEE Access* **2022**, *10*, 5768–5789. [[CrossRef](#)]
14. Wang, S.; Zhang, D.; Zhang, Y. Blockchain-based personal health records sharing scheme with data integrity verifiable. *IEEE Access* **2019**, *7*, 102887–102901. [[CrossRef](#)]
15. Sun, J.; Yao, X.; Wang, S.; Wu, Y. Blockchain-based secure storage and access scheme for electronic medical records in IPFS. *IEEE Access* **2020**, *8*, 59389–59401. [[CrossRef](#)]
16. Liu, J.; Li, X.; Ye, L.; Zhang, H.; Du, X.; Guizani, M. BPDS: A blockchain-based privacy-preserving data sharing for electronic medical records. In Proceedings of the GLOBECOM 2018—2018 IEEE Global Communications Conference, Abu Dhabi, United Arab Emirates, 9–13 December 2018; pp. 1–6.
17. Tith, D.; Lee, J.S.; Suzuki, H.; Wijesundara, W.M.A.B.; Taira, N.; Obi, T.; Ohyama, N. Application of blockchain to maintaining patient records in electronic health records for enhanced privacy, scalability, and availability. *Healthc. Inform. Res.* **2020**, *26*, 3. [[CrossRef](#)] [[PubMed](#)]
18. Daraghmi, E.-Y.; Daraghmi, Y.-A.; Yuan, S.-M. MedChain: A design of blockchain-based system for medical records access and permissions management. *IEEE Access* **2019**, *7*, 164595–164613. [[CrossRef](#)]
19. Balakumar, S.; Kavitha, A.R. Quorum-based blockchain network with IPFS to improve data security in IoT network. *Stud. Inform. Control.* **2021**, *30*, 85–98. [[CrossRef](#)]
20. Sammeta, N.; Parthiban, L. Hyperledger blockchain enabled secure medical record management with deep learning-based diagnosis model. *Complex Intell. Syst.* **2021**, *8*, 625–640. [[CrossRef](#)]
21. Tanwar, S.; Parekh, K.; Evans, R. Blockchain-based electronic healthcare record system for healthcare 4.0 applications. *J. Inf. Secur. Appl.* **2019**, *50*, 102407. [[CrossRef](#)]
22. Rajput, A.R.; Li, Q.; Ahvanooy, M.T. A blockchain-based secret-data sharing framework for personal health records in emergency conditions. *Healthcare* **2021**, *9*, 206. [[CrossRef](#)]
23. Meier, P.; Beinke, J.H.; Fite, C.; Brinke, J.S.T.; Teuteberg, F. Generating design knowledge for blockchain-based access control to personal health records. *Inf. Syst. E-Business Manag.* **2020**, *19*, 13–41. [[CrossRef](#)]
24. Zhang, Q.; Xiong, Z.; Zhu, J.; Gao, S.; Yang, W. A Privacy-preserving Auction Mechanism for Learning Model as an NFT in Blockchain-Driven Metaverse. *ACM Trans. Multimedia Comput. Commun. Appl.* **2024**, *20*, 1–24. [[CrossRef](#)]
25. Azbeg, K.; Ouchetto, O.; Andaloussi, S.J. BlockMedCare: A healthcare system based on IoT, Blockchain and IPFS for data management security. *Egypt. Inform. J.* **2022**, *23*, 329–343. [[CrossRef](#)]
26. Kordestani, H.; Barkaoui, K.; Zahran, W. HapiFabric: A Teleconsultation Framework Based on Hyperledger Fabric. In *European, Mediterranean, and Middle Eastern Conference on Information Systems*; Springer International Publishing: Cham, Switzerland, 2020; pp. 399–414.
27. Bisht, A.; Das, A.K.; Niyato, D.; Park, Y. Efficient Personal-Health-Records Sharing in Internet of Medical Things Using Searchable Symmetric Encryption, Blockchain, and IPFS. *IEEE Open J. Commun. Soc.* **2023**, *4*, 2225–2244. [[CrossRef](#)]
28. Wang, T.; Wu, Q.; Chen, J.; Chen, F.; Xie, D.; Shen, H. Health data security sharing method based on hybrid blockchain. *Future Gener. Comput. Syst.* **2023**, *153*, 251–261. [[CrossRef](#)]
29. Rai, S.; Chaurasia, B.K.; Gupta, R.; Verma, S. Blockchain-based NFT for healthcare system. In Proceedings of the 2023 IEEE 12th International Conference on Communication Systems and Network Technologies (CSNT), Bhopal, India, 8–9 April 2023; pp. 700–704.
30. Bodur, H.; Al Yaseen, I.F.T. An Improved blockchain-based secure medical record sharing scheme. *Clust. Comput.* **2024**, *27*, 7981–8000. [[CrossRef](#)]

31. Jakhar, A.K.; Singh, M.; Sharma, R.; Viriyasitavat, W.; Dhiman, G.; Goel, S. A blockchain-based privacy-preserving and access-control framework for electronic health records management. *Multimedia Tools Appl.* **2024**, *83*, 84195–84229. [CrossRef]
32. Swetha, M.S.; Muneshwara, M.S.; Madihalli, A.T.; Bhardwaj, A.; Ananya; Solanki, V.K. A Novel Approach on Medical Health Record Management System Using Blockchain. In *The International Conference on Intelligent Systems & Networks*; Springer Nature: Singapore, 2024; pp. 678–687.
33. Venkatesh, R.; Hanumantha, B.S. Electronic medical records protection framework based on quantum blockchain for multiple hospitals. *Multimedia Tools Appl.* **2023**, *83*, 42721–42734. [CrossRef]
34. Haddad, A.; Habaebi, M.H.; Suliman, F.E.M.; Elsheikh, E.A.; Islam, M.R.; Zabidi, S.A. Generic patient-centered block-chain-based EHR management system. *Appl. Sci.* **2023**, *13*, 1761. [CrossRef]
35. Chinnasamy, P.; Albakri, A.; Khan, M.; Raja, A.A.; Kiran, A.; Babu, J.C. Smart contract-enabled secure sharing of health data for a mobile cloud-based e-health system. *Appl. Sci.* **2023**, *13*, 3970. [CrossRef]
36. Zaghoul, E.; Li, T.; Mutka, M.W.; Ren, J. Bitcoin and Blockchain: Security and Privacy. *IEEE Internet Things J.* **2020**, *7*, 10288–10313. [CrossRef]
37. Al Barghuthi, N.; Said, H.E.; Badi, S.M.; Girija, S. Security Risk Assessment of Blockchain-Based Patient Health Record Systems. In *Information Systems. EMCIS 2022. Lecture Notes in Business Information Processing*; Papadaki, M., da Cunha, P.R., Themistocleous, M., Christodoulou, K., Eds.; Springer: Cham, Switzerland, 2023; Volume 464. [CrossRef]
38. Kumari, D.; Parmar, A.S.; Goyal, H.S.; Mishra, K.; Panda, S. HealthRec-Chain: Patient-centric blockchain enabled IPFS for privacy-preserving scalable health data. *Comput. Netw.* **2024**, *241*, 110223. [CrossRef]
39. Turki, M.; Cheikhrouhou, S.; Dammak, B.; Baklouti, M.; Mars, R.; Dhahbi, A. NFT-IoT pharma chain: IoT drug traceability system based on blockchain and nonfungible tokens (NFTs). *J. King Saud Univ.-Comput. Inf. Sci.* **2023**, *35*, 527–543. [CrossRef]
40. Bamakan, S.M.H.; Nezhadsistani, N.; Bodaghi, O.; Qu, Q. A decentralized framework for patents and intellectual property as nft in blockchain networks. *Res. Sq.* **2021**, *in press*.
41. Said, H.E.; Al Barghuthi, N.B.; Badi, S.M.; Hashim, F.; Girija, S. Developing a Decentralized Blockchain Framework with Hyperledger and NFTs for Secure and Transparent Patient Health Records. In *Proceedings of the Third International Conference on Innovations in Computing Research (ICR'24)*, Athens, Greece, 12–14 August 2024; Springer Nature: Cham, Switzerland, 2024.
42. Said, H.E.; Al Barghuthi, N.B.; Badi, S.M.; Girija, S. Design of a Blockchain-Based Patient Record Tracking System. In *Proceedings of the International Conference on IoT and Health, Istanbul, Türkiye, 20–21 October 2024*; Springer Nature: Cham, Switzerland, 2024; pp. 145–161. Available online: https://link.springer.com/chapter/10.1007/978-3-031-52787-6_12 (accessed on 1 March 2024).
43. Shuaib, K.; Abdella, J.; Sallabi, F.; Serhani, M.A. Secure decentralized electronic health records sharing system based on blockchains. *J. King Saud Univ.-Comput. Inf. Sci.* **2022**, *34*, 5045–5058. [CrossRef]
44. Hyperledger-Caliper. Available online: <https://hyperledger.github.io/caliper/v0.6.0/getting-started/> (accessed on 1 March 2024).

Disclaimer/Publisher’s Note: The statements, opinions and data contained in all publications are solely those of the individual author(s) and contributor(s) and not of MDPI and/or the editor(s). MDPI and/or the editor(s) disclaim responsibility for any injury to people or property resulting from any ideas, methods, instructions or products referred to in the content.