computers

MDPI

Article

Blockchain-Based Cooperative Medical Records Management System

Sultan Alyahya * and Zahraa Almaghrabi

Department of Information Systems, King Saud University, Riyadh 11451, Saudi Arabia
* Correspondence: sualyahya@ksu.edu.sa

Abstract

The effective management of electronic medical records is critical to deliver high-quality healthcare services. However, existing systems often suffer from issues such as fragmented data, lack of interoperability, and weak privacy protections, which hinder collaboration among healthcare stakeholders. This paper proposes a blockchain-based system to securely manage and share medical records in a decentralized and transparent manner. By leveraging smart contracts and access control policies, the system empowers patients with control over their data, ensures auditability of all interactions, and facilitates secure data sharing among patients, healthcare providers, insurance companies, and regulatory authorities. The proposed architecture is implemented using a private Ethereum blockchain and evaluated through a scenario-based comparison with the Prince Sultan Military Medical City system, as well as quantitative performance measurements of the blockchain prototype. Results demonstrate significant improvements in data security, access transparency, and system interoperability, with patients gaining the ability to track and control access to their records across multiple healthcare providers, while system performance remained practical for healthcare workflows.

Keywords: blockchain; medical records; healthcare; privacy; cooperation

Academic Editors: Ben Soh and Singara Singh Kasana

Received: 26 August 2025
Revised: 5 October 2025
Accepted: 9 October 2025
Published: 21 October 2025

Citation: Alyahya, S.; Almaghrabi, Z. Blockchain-Based Cooperative Medical Records Management System. *Computers* **2025**, *14*, 447. https://doi.org/10.3390/computers14100447

1. Introduction

Blockchain is a new and promising technology in the field of information technology. It is a secure, tamper-proof, distributed architectural platform that enables rapid and reliable peer-to-peer transactions. Blockchain uses a smart contract that runs when predetermined conditions are met to trigger an event [1]. Some popular examples of blockchain are bitcoin and other cryptocurrencies; now, however, blockchain has expanded beyond the financial sector to different industry sectors [2].

Healthcare is one important sector that can benefit from blockchain technology. Today, many governments across the world have made healthcare services one of their major priorities. They strive to improve healthcare quality and provide their citizens with wide access to healthcare [3]. Despite this interest and effort by governments, there are still shortcomings, including the occurrence of medical errors and the difficulty in accessing patient information, and this can cause the expenditure of more time and money to redo medical tests [4]. The loss of trust between participating parties causes a lack of cooperation, which is important for the success of the healthcare process [5]. The e-healthcare in developing countries has additional challenges, including the lack of a national standard for managing electronic medical records and the presence of barriers related to confidentiality and data privacy [6,7].

Blockchain has several features that make it a suitable solution for many issues in healthcare, such as decentralization—which does away with reliance on a centralized authority to implement distributed healthcare applications—as well as the transparency and openness of information, the ease of transactions, and the immutability of data [8]. Blockchain enables a trusting collaboration to develop among participating parties by providing a secure method of sharing health data [9].

This research aims to help improve patient medical record management, particularly in the Kingdom of Saudi Arabia, through designing and developing an effective system based on blockchain technology. It can contribute to solving the following challenges:

Privacy and security: Current medical record management systems are based on the exchange of medical information between all relevant parties: patients, providers, and insurance companies. All these parties can access patient data at any time, which makes it a challenge to protect the confidentiality of patient information [10]. For example, patients have reported concerns that sensitive test results, such as genetic screenings, may be viewed by insurance companies without their explicit consent.

Data fragmentation: Patient records are fragmented in Saudi Arabia, so patients lose control of and access to their health data in real time. Additionally, patients have to provide their medical history whenever they visit a hospital or health center for the first time. A lack of patient-driven interoperability hinders patients from accessing their health records on demand [11] (e.g., patients visiting different hospitals must repeat lab tests due to fragmented records).

Lack of collaborative process: Providing health services requires cooperation between the parties involved in the health process. This cooperation can be missing if there is a lack of strong trust between the parties that wish to share secure and reliable data [12]. For instance, disputes sometimes arise when doctors and insurance companies rely on separate, inconsistent patient records, delaying treatment approvals.

The remainder of this paper is organized as follows: Section 2 presents the related work; Section 3 describes the research methodology; and Sections 4–6 are about the requirements, design, and implementation of the system. Section 6 discusses the evaluation of the work, and Section 7 provides the conclusion.

2. Related Work

2.1. Blockchain Technology

Recently, blockchain has become one of the most popular technologies. Although it emerged in the financial sector, its application has expanded to medicine, logistics, and supply chain management systems [4,13]. Essentially, blockchain is a digital, incorruptible, and distributed ledger of all transactions [14]. Transactions in blockchain are processed without the necessity of a trusted third party or central administration to authenticate or verify the information [15].

Blockchain is a decentralized database that consists of a reliable sequence of blocks that record a complete list of transactions [16]. These blockchain blocks are structured as a peer-to-peer network. The work in a blockchain is performed in a consensus manner, where the node with the name miner is responsible for all work in the blockchain network, such as connecting the blockchain network, confirming transactions, and creating and passing new blocks to the blockchain. A block in a network is generated based on some requirement that must be fulfilled [11]. In the blockchain, transactions and information are copied to each node included in the network and must be verified to be validated [17]. Thus, blockchain is highly useful for a system in which all the parties need to access the same information.

Each block in the blockchain is signed by the responsible miner using a hash function or Merkle root hash algorithm. The hash function is worked to ensure that no duplicate

hashing exists. Information in every block cannot be changed or tampered with, and each block contains the data and hash of the previous block [1].

Based on the types of users who can access the blockchain and the way it is constructed and verified, blockchains are divided into three categories: public (permissionless), private (permissioned), and consortium (hybrid) blockchains [18]. A public blockchain is considered a fully decentralized blockchain; every peer in the blockchain network can read, write, and verify transactions and can participate in a consensus process to make decisions for blocks that get added to the blockchain [19]. Peers in private blockchains are restricted, as writing permission is given to individuals or groups of peers, while reading permission is open to all peers or can be restricted to a subset of peers in the blockchain network. Consequently, the generation of blocks allows privileged individuals or groups of peers to gain access to permission through a special invitation. A consortium (hybrid) blockchain is considered a partially private block, in which the writing permissions and block generation are determined for preselected peers, while others can access the blockchain network and read but not participate in the consensus process [20].

Blockchain uses decentralized consensus mechanisms to ensure that every peer in the blockchain network reaches an agreement [21]. Consensus mechanisms guarantee consistency and efficiency of data and transactions [22]. There are many types of consensus mechanisms that can be adapted by a blockchain [23]. PoW, PoS, Practical Byzantine Fault Tolerance (PBFT), and Delegated Proof of Stake (DPoS) are the most popular consensus protocols. They differ in some ways, such as energy and cost consumption and scalability [19].

2.2. Blockchain in Healthcare

Healthcare is one of the fields that has adopted blockchain technology [24]. It has been used in many areas, including research and clinical trials, drug supply chain management, billing processes, and medical record sharing [13].

The process of clinical trials combines multiple parties such as medical practitioners and researchers, who collaborate with each other in implementation. Essentially, each stage in the trials, starting with data collection, needs strong monitoring and high trust among the involved parties. Blockchain can help monitor and ensure that the trials meet consent regulations [25]. Benchoufi et al. [26] established an authentication system that gives subjects of clinical trials ownership of their data and provides auditing features for the clinical staff, researchers, and regulators.

In line with this, Maslove et al. [27] presented the BlockTrial, a blockchain-enabled clinical trial data management system, to increase the trustworthiness of the data collected during clinical research and ensure that the analysis of these data comply with prespecified plans. BlockTrial gives patients better control to access their data and provides useful tools for researchers to maintain a commitment to reporting requirements.

Medical drugs can be counterfeited, and their sale can lead to significant losses. Blockchain provides the ability to track supply chain operations from the manufacturer to the consumer. Tseng et al. [28] employed immutable, consensus-driven, and transparent features in blockchain to implement the Gcoin blockchain system and create transparent drug transaction data. Gcoin blockchain tracks every pill for identification in the drug supply chain to prevent counterfeit drugs from reaching the market, thus protecting public health. The billing process can be impaired by fraud, and it takes a long time to implement the different stages of the process and receive the required bills. Katuwal et al. [29] used Ethereum to make claims management easy and fast. It provides a single system that is accessible to patients, providers, and insurers, together with a real-time patient health journey review.

Blockchain is used to store, process, and share medical data in a secure and trustworthy way. Cyran [30] proposed a health data-sharing platform that protects sensitive data and maintains patient data privacy and security by applying cryptographic algorithms that enforce the privacy of transactions. Alam et al. [31] analyzed the suitability of electronic health records in blockchain for the efficient management of the COVID-19 pandemic. They reported that using blockchain technology could help manage COVID-19 pandemic issues by ensuring accurate, reliable, and secure data storage and exchange.

Patel [32] suggested a framework that uses blockchain technology to permit patients to access medical image data in a secure, private, and tamper-resistant manner. Dagher et al. [33] proposed a blockchain-based framework named Ancile for the management of electronic health records. An Ancile framework provides secure, interoperable, and efficient access to patients' records, as well as preserves their privacy. Additionally, it gives patients ownership and final control of their electronically collected health records.

Another relevant patient-centric healthcare data management system that focuses on safe privacy by using blockchain is the MediBchain proposed by Liang et al. [25]. It uses the pseudonymity of patients to hide their identities, and interaction with the system is restricted to registered parties only. The Blockchain-Based Data Sharing system (BBDS) [34] is another system that focuses on maintaining the privacy of patients through using encryption and digital signatures rather than traditional access control methods of passwords, firewalls, and intrusion detection systems to ensure efficient access control over a sensitive shared data pool in the cloud.

Recent work has continued to explore blockchain for secure healthcare record management. For example, Tahir et al. [35] proposed a blockchain-based framework emphasizing security, privacy, and interoperability in patient data exchange. While effective in enhancing data protection, the framework does not explicitly address cooperation among multiple stakeholders such as insurers and regulators. Another recent system, HealthRec-Chain [36], integrates blockchain with IPFS for scalable off-chain storage and employs smart contracts for access control. This improves storage efficiency and latency but still focuses primarily on patient–provider data sharing. More recently, Alruwaill et al. [37] propose hChain 4.0, a permissioned blockchain architecture with AES encryption together with partial homomorphic encryption, using ABAC for fine-grained permission control among authorized parties; this work advances privacy and scalability but still does not integrate all stakeholder groups (patients, providers, insurers, regulators) in cooperative workflows as our system does.

The use of medical records management systems, particularly in Saudi Arabia, has been criticized in the literature. There is a lack of a national standardized medical records management system in the kingdom due to the absence of a national regulator [6,7]. Patients have separate medical records for each healthcare provider they visit. This causes patients' data to be fragmented. Many researchers mentioned that there is a lack of sufficient mechanisms for maintaining confidentiality and data privacy [7,19].

Although there are many blockchain-based approaches applied in the domain of healthcare information systems (Table 1), we are unaware of any research allowing for a secure-collaborative medical records system that can serve the following parties together: doctors, patients, healthcare providers, and insurance companies. The process of sharing medical data between those different parties is proposed in this research. We next identify the requirements that such a solution has to fulfill.

Table 1. Comparison between blockchain-based systems in healthcare.

System	Privacy and Security	Data Fragmentation/Interoperability	Collaboration Among Stakeholders	Limitation Compared to Proposed System
BlockTrial [27]	Protects patient data integrity in clinical trials	Not designed for cross-provider records	Focuses on patients, researchers, and regulators only	Does not support general medical record sharing across hospitals, insurers, and regulators
Ancile [33]	Strong privacy-preserving access control	Provides interoperable EHR exchange	Limited to patients and healthcare providers	Lacks support for insurance companies and regulators in the cooperation model
MediBchain [25]	Pseudonymity protects patient identity	Records restricted to registered parties only	Covers patients and healthcare providers	Does not address insurer/regulator cooperation; limited interoperability
BBDS [34]	Uses encryption and digital signatures	Enables secure cloud-based sharing	Focuses mainly on patients and cloud providers	Does not provide multi-stakeholder cooperation in the healthcare ecosystem
Tahir et al. [35]	Employs smart contracts, blockchain, and IPFS for privacy and integrity	Enhances interoperability through IPFS integration	Covers mainly patients and providers	Does not address insurer/regulator cooperation; lacks full multi-stakeholder workflows
HealthRec-Chain [36]	Uses IPFS with GPG encryption and blockchain metadata for secure storage	Benchmarked for latency and throughput; supports scalable off-chain storage	Primarily patients and providers	Excludes insurers and regulators; cooperation scope limited
hChain 4.0 [37]	Combines AES, Partial Homomorphic Encryption, and ABAC for fine-grained access control	Designed for scalability in permissioned blockchain environments	Supports authorized users but not explicitly all stakeholders	Strong cryptographic model but lacks unified workflows covering patients, providers, insurers, and regulators

3. System Requirements

Our system works to achieve the auditability and traceability of patients' medical records. It has five main stakeholders—the patient, doctor, healthcare provider (which may be a public or private hospital or clinic), insurance company, and Ministry of Health. The Ministry supervises the other four stakeholders.

To begin with, in order to connect all participants to the system, the identities of all patients, doctors, insurance companies, and healthcare providers are confirmed and authenticated by the Ministry of Health in cooperation with national access in the Kingdom of Saudi Arabia. Once their identities have been confirmed, all the stakeholders can use all features of the system. By using blockchain, medical records are accessed through a smart contract and all participating parties can see the transactions in real time.

Based on our objectives and prior studies [38–41], we wished to highlight certain aspects of blockchain in healthcare. It has an effective role in providing quality medical services to patients that raise the level of healthcare. The basic requirements for the main stakeholders of the system are as follows:

- System Requirements for Patients.

  The system shall allow patients to view medical record contents.
  The system shall allow patients to create and update access policies.

- System Requirement for Doctors.

  The system shall allow doctors to update patient medical records.

- System Requirement for Insurance Companies.

  The system shall allow insurance companies to process medical insurance claims.

- System Requirements for Healthcare Providers.

  The system shall allow healthcare providers to create insurance claims.
  The system shall allow healthcare providers to create medical records for patients.

- System Requirement for Ministry of Health.

  The system shall allow the Ministry of Health to view medical records for patients

In addition to these functional requirements, the system must also satisfy several non-functional requirements that ensure its performance, security, and availability in practical healthcare settings:

- Performance (Latency): The system shall maintain an average patient record retrieval latency below 100 ms under up to 100 concurrent requests.
- Performance (Throughput): The system shall sustain at least 200 requests per second with 300 concurrent users.
- Security: The system shall ensure confidentiality of medical records using asymmetric encryption, with access controlled through one-time tokens that expire after use.
- Availability: The system shall provide continuous access to medical records through blockchain replication, ensuring resilience against individual service failures.

4. System Design

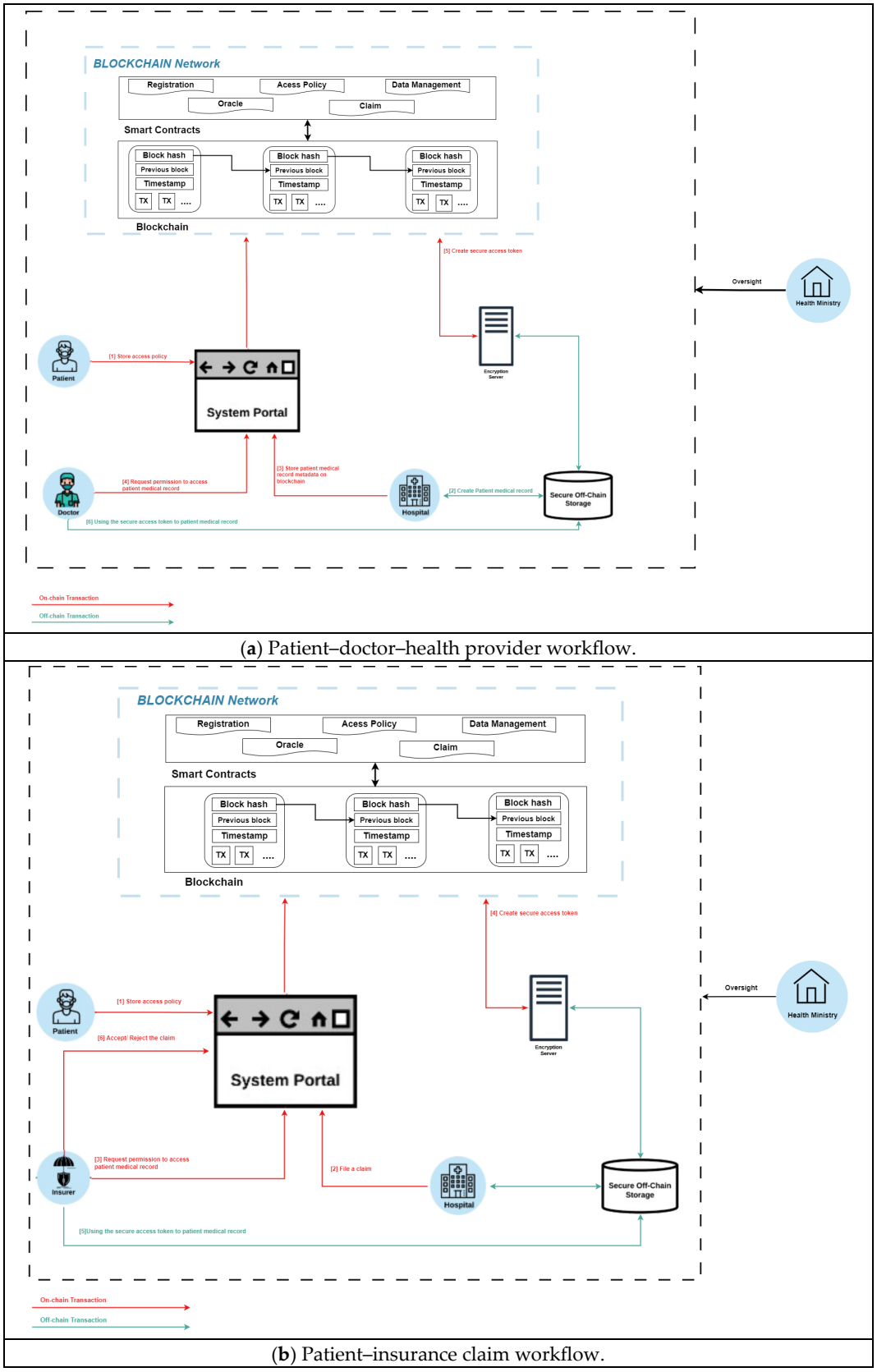
Building on the requirements identified in the previous section, this section presents the workflow of our blockchain-based health record system and also discusses the potential threats associated with the system.

4.1. System Workflow

The patient–doctor–health provider workflow is presented in Figure 1a. It depicts the interactions that occur among the various components.

The steps involved in the workflow are as follows:

- Step 1: The patient generates access policies for the blockchain, and this enables the system to evaluate access requests without the need to approach the patient directly. Access requests are automatically granted or rejected.
- Step 2: When the patient consults a healthcare provider, the healthcare provider creates the patient's medical record and stores it in the database.
- Step 3: The healthcare provider stores the reference to this record on the blockchain network in order to ensure the integrity of patient data and enable other parties in the system to access the medical record.
- Step 4: To complete the treatment process, the doctor requests permission to access the patient's record using the patient's address on the blockchain. The request is processed through the access policy in the smart contract, which considers the request and checks the patient's access policies.
- Step 5: To grant access to the doctor, the request is redirected to the encryption server. This generates a secure access token for the doctor. This process is completed using a smart contract named Registration.
- Step 6: The doctor, using the secure access token, can review the patient's medical record and add details about the patient's visit.



(**a**) Patient–doctor–health provider workflow.

(**b**) Patient–insurance claim workflow.

Figure 1. System's Workflows (patient–doctor–health provider workflow and patient–insurance claim workflow).

Furthermore, the steps to be followed when a patient requires insurance approval for a treatment plan are illustrated in Figure 1b and listed below:

- Step 1: The patient generates access policies for the blockchain.
- Step 2: The healthcare provider files the patient's insurance claim, which is then stored in the smart contract on the blockchain network named Claim. Subsequently, the insurance company is notified.
- Step 3: The company requests permission to access the patient's record by employing the methods delineated in Step 4 in patient–doctor–health provider workflow section.
- Step 4: To grant access to the insurance company, the request is redirected to the encryption server. This generates a secure access token for the insurance company. This process is completed using a smart contract named Registration.
- Step 5: The healthcare provider uses the secure access token to access the patient's medical record.
- Step 6: The healthcare provider evaluates the claim made by its medical staff based on the data in the patient's medical record and then either accepts or rejects it.

The above-mentioned operations are executed under the supervision of the Ministry of Health in the Kingdom of Saudi Arabia, thus ensuring their integrity. Further details about the workflow, including a process description of each requirement identified in the previous section, can be accessed through our design repository shown this link (https://github.com/salyahya99/Blockchain-Paper-System-Design, accessed on 1 October 2025).

As outlined in our system design repository, the system combines one-time access tokens with asymmetric encryption. After registering, a patient defines an access policy that controls who may access his/her records; this policy can be modified or revoked at any time. Based on the policy, a smart contract issues a one-time access token whenever an authorized party (e.g., doctor or insurer) requests access. Each token is valid for a single use and expires immediately afterward, preventing reuse or unauthorized access. In addition, the contents of each medical file are encrypted with the authorized party's public key (RSA), ensuring that only the holder of the corresponding private key can decrypt the data. This mechanism ensures that even if storage is compromised, unauthorized entities cannot read the records. All token requests and key releases are immutably recorded on the blockchain, providing a transparent audit trail that enforces privacy and accountability.

4.2. Threats Modeling

While access control policies provide a foundation for secure medical record management, it is important to analyze potential attack scenarios. One threat is the compromise of a private key. If an attacker obtains a patient's or doctor's private key, he may impersonate the legitimate user and gain unauthorized access. To mitigate this risk, the system requires periodic re-authentication through the Ministry of Health and records every transaction on the blockchain, enabling the rapid detection and revocation of suspicious activity. Another concern is collusion among stakeholders, for example, between an insurance company and a healthcare provider seeking to exploit patient data. In our system, such collusion is deterred because all access requests and record modifications are immutably logged. Any irregular pattern of access can be audited by Ministry of Health.

Finally, insider threats can be a challenge, as authorized users may misuse their legitimate access rights. The blockchain's immutable audit trail serves as both a deterrent and a mechanism for accountability, ensuring that malicious actions can be traced to specific individuals.

5. System Implementation

A private blockchain approach can be implemented by the Ethereum platform. Remix IDE is used to create and deploy the required smart contracts for the system; it writes Solidity contracts. The main smart contracts involved in our system are Registration, Data-

Management, AccessManagement, and Claim. The Registration smart contracts contain all the data and operations related to the Registration functions in the system and assumes that they are the responsibility of the Ministry of Health. The DataManagement smart contract contains all the data and operations related to data management in the system, and it saves data on the blockchain related to patient records.

The Claim smart contract contains all the operations for managing insurance claims (i.e., creation, acceptance, and rejection of claims). The AccessManagement smart contract contains all the operations for processing access requests and creating a patient's access policy. In other words, it manages the access to patient data that is held in off-chain storage.

Table 2 summarizes the deployment environment of the proposed system. It provides information regarding the blockchain platform, consensus mechanism, number of nodes, hardware specification, and development tools used during implementation. With regard to block confirmation time, Ganache mines blocks instantly by default, so confirmation delays are negligible.

Table 2. Deployment parameters.

Parameter	Setting
Blockchain Platform	Ethereum (Ganache CLI local test network)
Consensus Mechanism	Proof of Authority (PoA, Ganache default)
Number of Nodes	10
Hardware Specification	Intel Core i7, 16 GB RAM, Windows 11 laptop
Development Tools	Remix IDE, Solidity 0.8.x, MetaMask

Code snippets of the smart contracts are provided in Figures A1–A4 in the Appendix A while implementation of the main functions of the system is detailed below.

Create Access Policies Function

After a patient registers and logs into the system, the system allows the patient to add access policies that control the access to their medical records. As depicted in Figure 2, the patient determines the appropriate role, such as doctor or insurance company, and type of access, which can be for one visit to a healthcare provider or an entire medical record.

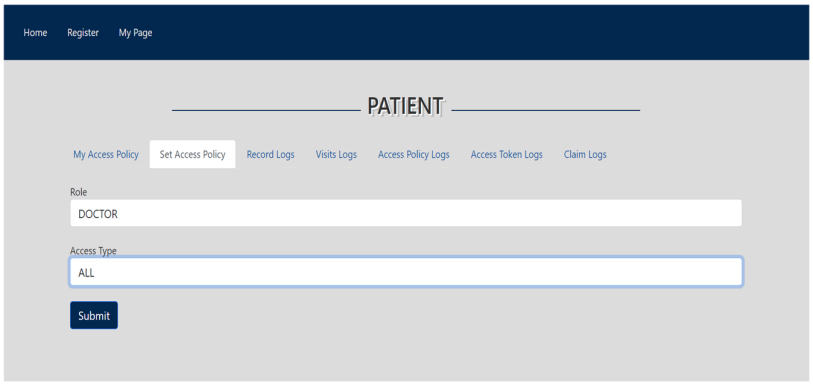


Figure 2. Setting access policy: Patients can define access policies by selecting the role (e.g., doctor, insurance company) and specifying the scope of access, such as a single visit or the entire medical record.

View Medical Record Contents Function

Through this function, patients can view their medical records, which contain the details of all the visits to doctors and healthcare providers in the Kingdom of Saudi Arabia. Patients can also view all the attachments included for each visit (Figure 3). The interface

displays previous visits, associated diagnoses, attached X-ray images, and prescribed medications, visible only to the patient.

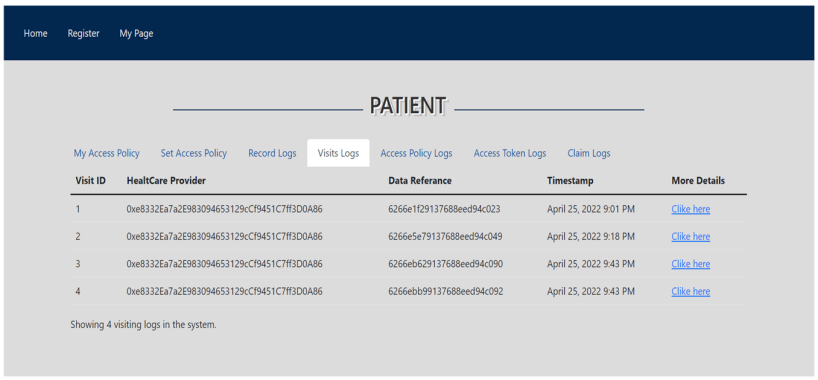


Figure 3. Visit logs page: Patients can view details of their past visits, including clinic and doctor information, diagnoses, treatment plans, prescriptions, and attached medical files such as X-ray images or lab reports.

Create Medical Insurance Claim Function

As part of the Claims smart contract, the function "create a medical insurance claim" is provided to the healthcare provider. As illustrated in Figure 4, the "Create Claim" page allows healthcare providers to submit insurance claims on behalf of patients, attaching visit details and supporting documents; this workflow demonstrates how claim creation is integrated with the blockchain-based access controls and the Claim smart contract.

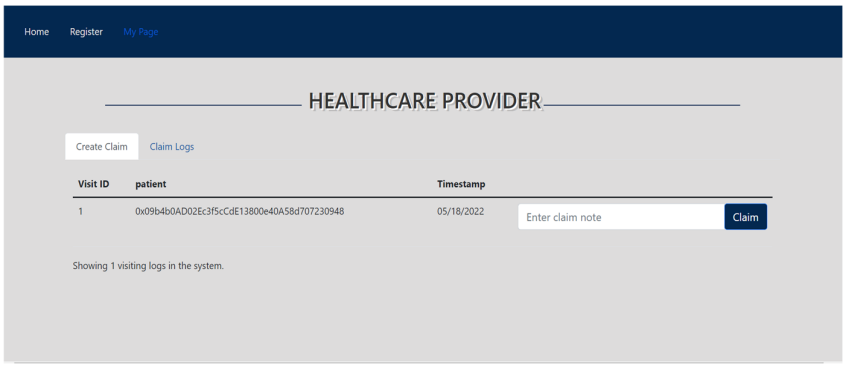


Figure 4. Creating claim page: Healthcare providers can submit insurance claims on behalf of patients, including visit details and supporting medical documentation required for claim approval.

Update Patient Medical Record Function

The system permits the doctor to update the patient's medical record. The information includes the patient's condition, treatment plan, prescription, and any attachment. As illustrated in Figure 5, the "Add Visit" page allows doctors to record new medical encounters, including fields for diagnosis, treatment, and attached documents (e.g., lab results or X-rays). This interface demonstrates how new records are securely entered into the system while access control policies are enforced in the background.

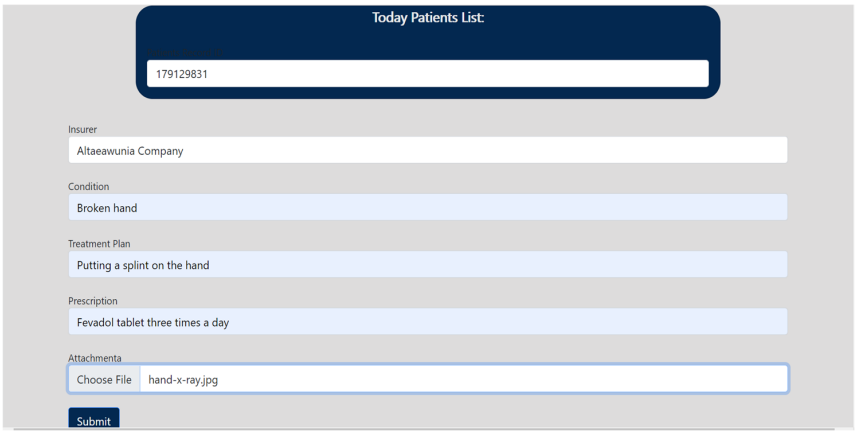


Figure 5. Adding visit page: Doctors can update patient medical records by entering information about the patient's condition, treatment plan, prescribed medications, and uploading relevant attachments.

Processing Medical Insurance Claim Function

For an insurance company, the system provides an option to process the medical insurance claim. Once the insurance company receives a new claim, it requests access to the patient's medical records, which can include specific details of a visit. Based on the access policies of the client, the system will either release the access token or not. After the insurance company is granted access to the medical records and assesses the claim, it can accept or reject the claim.

Figure 6 presents the insurer's claim-processing interface, where authorized insurance staff review submitted claims, access patient records (subject to patient policies), and accept or reject claims. All claim actions are logged immutably for audit.

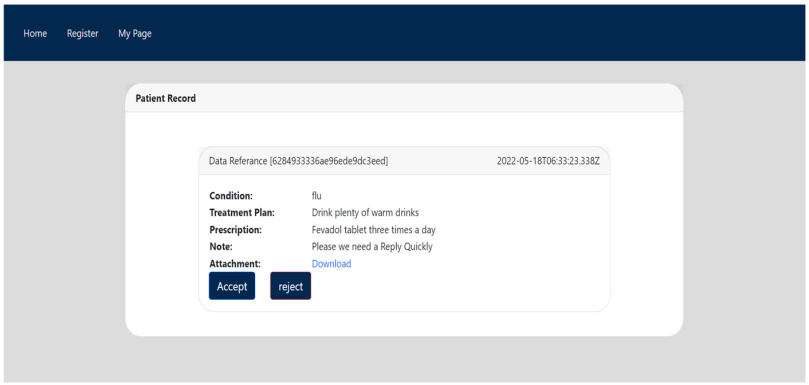


Figure 6. Processing medical insurance claim page: insurance companies can review submitted claims, access authorized patient records, and make decisions to accept or reject claims based on the medical data provided.

6. Evaluation

6.1. Qualitative Evaluation

The scenario-based method was used to evaluate our system as it reduces the effort and expense associated with more immersive methods by providing specific focal points for evaluation [42]. In addition, the method provides a common tractable language for parties involved in the evaluation process: designers, users, and evaluators [43]. We chose the medical record system of the Prince Sultan Military Medical City to conduct comparisons. It is commonly seen as one of the best hospitals affiliated with the Ministry of Health in the Kingdom of Saudi Arabia and has an advanced and competitive system. It would allow the application of scenarios that would facilitate a comparison between the classic and

the blockchain-based systems for the management of medical records for patients. The following sections present the three scenarios, and the analysis of the scenarios is shown in Tables 3–5.

Scenario 1: Reviewing Previous Patient Visits

Classic Health Record System Version of Scenario 1:

1. Patient logs into the health provider system with username and password.
2. Patient makes a "visit notice" request.
3. System retrieves date of visit, clinic type, and patient number and name.

Blockchain Health Record System Version of Scenario 1:

1. Patient logs into the "tracking and auditing medical record system" with wallet address.
2. Patient makes "view visit log" request to blockchain.
3. System retrieves visits added in patient's medical record.
4. Patient views his/her visit log to see what information has been added to the medical record and by whom.

Analysis of Scenario One

Table 3. Analysis of Scenario 1.

Classic Health Record System	Blockchain Health Record System
Patients can see basic information, such as the name of the clinic and date of the visit, and can access X-rays and test results. Patients cannot see other information, such as the doctor's notes. Patients can access information associated with this hospital only.	Patients can access their medical record, which includes the entire history of visits to any healthcare provider in any city in Saudi Arabia. The visit history contains information about doctors, healthcare providers, diagnoses and health conditions, and treatment plans, and any attachments to the records can be viewed. This enables patients to track information in their medical record.
Information added to a patient's medical record by a doctor can be modified or deleted.	Information added to a patient's medical record, especially visit content added by any doctor, cannot be modified or deleted.

Scenario 2: Viewing the Patient's History

Classic Health Record System Version of Scenario 2:

1. Doctor logs onto the health provider system with username and password.
2. Doctor clicks on "today's patient list" in the health provider system.
3. Doctor selects intended patient from the patient list.
4. System retrieves medical records of patient associated with this hospital only.

Blockchain Health Record System Version of Scenario 2:

1. Doctor logs onto the "tracking and auditing medical record system" with wallet address.
2. Doctor clicks on "patient history" in the system.
3. Doctor chooses intended patient from the list.
4. Doctor makes an "access patient history" request to the system.
5. Based on the access policies of the patient, the request is accepted and the access token is released or the request is denied.
6. System retrieves encoded patient medical record content.
7. Confidential medical record contents are decrypted via the doctor's private key.
8. Doctor views details of patient's history from all healthcare providers.

Analysis of Scenario Two

Table 4. Analysis of Scenario 2.

Classic Health Record System	Blockchain Health Record System
Doctor can access patient's medical record at any time without any access control or awareness on the part of the patient.	Doctor needs an access token to access patient's medical records. The token is accepted or rejected based on access policies determined by the patient.
Doctor can only view data on previous visits by the patient to a doctor in the same healthcare provider's system.	Doctor can view details of the patient's history regardless of the type of patient or the healthcare provider who treated the patient. Doctor can see all of the details of the patient's medical conditions and all previous treatments and medications from all healthcare providers that the patient has consulted. This information is encrypted asymmetrically and decrypted through the doctor's private key.

Scenario 3: Processing of Medical Insurance Claim

Classic Health Record System Version of Scenario 3:

1. Insurance company logs into the claims system.
2. System retrieves the patient's medical claims.
3. Insurance company selects the claim and adds a response to the claim, which is either an acceptance or rejection of the claim.

Blockchain Health Record System Version of Scenario 3:

1. Insurance company logs onto the "Tracking and Auditing Medical Record System" with wallet address.
2. Insurance company clicks on "New Claims" in the system.
3. Insurance company chooses a medical claim from the list.
4. Insurance company makes an "Access Patient Medical Record" request to the system.
5. Based on the access policies of the patient, the system accepts the request and releases the access token or denies the request.
6. System retrieves encoded patient medical record content related to the visit that led to the medical claim.
7. Confidential patient medical record contents are decrypted via the insurance company's private key.
8. Insurance company selects either the "Accept" or "Reject" option for the medical claim.

Analysis of Scenario Three

Table 5. Analysis of Scenario 3.

Classic Health Record System	Blockchain Health Record System
The content of a claim, including the medical data associated with the claim, can be accessed at any time by the insurance company without the patient's knowledge.	The insurance company needs an access token to access a patient's medical record when evaluating medical claims. The release of this access token is based on access policies determined by the patient.
To process the medical claim, the insurance company may require special information related to the claim. It may need to contact the healthcare provider to obtain the information. This process may require time and effort.	When access is granted, the insurance company can easily access details of the visit and all of the attachments related to it.

6.2. Quantitative Evaluation

To complement the scenario-based qualitative evaluation, we conducted quantitative measurements focusing on three representative operations that reflect different workload types: Patient views history (read operation), Doctor adds visit (write operation), and Insurer processes claim (mixed read/write operation). The results, summarized in Table 6, compare latency at 100 concurrent users and throughput at 300 concurrent users between the classic system and the blockchain-based system.

Table 6. The quantitative evaluation (latency and throughput measurements).

Operation	Latency (100 Users)		Throughput (300 Users)	
	Classic	Blockchain	Classic	Blockchain
Patient views history (Read)	28 ms	46 ms	582 req/s	458 req/s
Doctor adds visit (Write)	38 ms	63 ms	476 req/s	348 req/s
Insurer processes claim (Mixed)	42 ms	67 ms	441 req/s	327 req/s

For comparison, we implemented a simplified classic system using the same API endpoints but backed by a centralized relational database (PostgreSQL) without blockchain components. This baseline allows us to measure the additional cost introduced by blockchain consensus and encryption while keeping the application logic identical.

For the read operation (Patient views history), the blockchain system increased average latency from 28 ms to 46 ms, while throughput decreased from 582 to 458 requests per second. In the write operation (Doctor adds visit), latency rose from 38 ms to 63 ms, and throughput declined from 476 to 348 requests per second. Finally, in the mixed operation (Insurer processes claim), latency increased from 42 ms to 67 ms, and throughput dropped from 441 to 327 requests per second.

These results indicate that read-heavy operations (such as patient history retrieval) remain close to the performance of a traditional hospital system, while write-intensive operations (adding visits, processing claims) incur more noticeable overhead due to transaction validation and ledger updates. Overall, the blockchain system demonstrated 15–25 ms additional latency and approximately 20–30% lower throughput compared to the classic system, but still maintained performance levels that are practical for healthcare workflows. Because our deployment relies on a Ganache local test, the results reflect controlled experimental conditions rather than production benchmarks. Nevertheless, they clearly illustrate the performance trade-offs introduced by blockchain consensus and encryption compared to a classic system.

Furthermore, most of the prominent blockchain-based healthcare systems reviewed in Table 1 do not report performance metrics. Earlier works such as BlockTrial [27], Ancile [33], MediBchain [25], BBDS [34], and Tahir et al. [35] primarily emphasize architectural or security aspects without quantitative benchmarking. However, more recent proposals such as HealthRec-Chain [36] and hChain 4.0 [37] include latency and throughput measurements, though typically in permissioned or off-chain storage settings that differ from our experimental environment. Our evaluation therefore complements this literature by adding indicative performance results for a cooperation-oriented architecture that supports patients, providers, insurers, and regulators simultaneously.

7. Conclusions

This research project aimed to study the design and development of an efficient system based on blockchain technology to track and audit electronic medical records. The project demonstrated how blockchain technology can support healthcare through effective medical

records management that includes the reduction in medical errors and the promotion of reliable cooperation between the participating parties.

The evaluation of the proposed system was carried out in two complementary ways. First, a scenario-based comparison with the Prince Sultan Military Medical City system demonstrated the advantages of the blockchain-based approach in terms of transparency, auditability, and patient control over medical records. Second, quantitative performance measurements of the blockchain prototype, implemented on a private Ethereum network, showed that the system can handle core operations such as record retrieval, record updates, and insurance claim submission with practical latency and throughput for healthcare workflows. Together, these results confirm both the conceptual and technical feasibility of adopting blockchain for patient-centric medical record management.

While the system demonstrates clear advantages, several limitations remain that should be acknowledged. First, scalability is a challenge. Blockchain introduces computational overhead due to consensus and cryptographic operations, which may affect transaction throughput and latency under high workloads. Although our evaluation demonstrates feasibility under moderate concurrency, further work is needed to optimize consensus protocols or integrate layer-2 solutions for large-scale deployment.

Second, user adoption presents practical difficulties. Patients, providers, and insurers may be unfamiliar with blockchain-based workflows, which differ significantly from legacy systems. Designing intuitive interfaces, reducing technical complexity, and providing training will be necessary to foster trust and acceptance among all stakeholders.

Third, integration with legacy healthcare systems remains a major hurdle. Most hospitals and insurance companies rely on proprietary or heterogeneous platforms. Seamless data migration and interoperability between blockchain and existing electronic health record (EHR) systems will require additional middleware, standardized APIs, or cross-chain solutions.

For future work, it is important to explore consensus optimization and off-chain scaling approaches to improve system scalability, usability studies to evaluate and enhance user adoption, and middleware solutions for legacy system integration. These directions will strengthen the system's applicability in real-world healthcare environments.

The future research for this study could also be enhanced in several ways. In the proposed system, we used basic access policies appropriate to the current state of the system. Developing more detailed access policies would strengthen the system further. For example, access rules could be tailored to the type of clinic or medical specialty, the sensitivity level of specific medical data (e.g., mental health records vs. routine lab results), or the urgency of care in emergency situations. Policies could also adapt based on time-limited access (e.g., for a single consultation) or role-based permissions (e.g., distinguishing between primary physicians, specialists, and insurance staff). By introducing these finer-grained policies, patients would gain greater flexibility and control over their records, while still ensuring that healthcare providers and insurers can access the information necessary to deliver care and process claims.

Author Contributions: Conceptualization, S.A. and Z.A.; methodology S.A. and Z.A.; software, Z.A.; validation, S.A. and Z.A.; formal analysis S.A. and Z.A.; investigation S.A. and Z.A.; writing—original draft preparation, S.A. and Z.A.; writing—review and editing, S.A.; visualization, S.A. and Z.A.; supervision, S.A.; project administration S.A.; funding acquisition, S.A. All authors have read and agreed to the published version of the manuscript.

Funding: Ongoing Research Funding Program- (ORF-2025-1364), King Saud University, Riyadh, Saudi Arabia.

Data Availability Statement: The original contributions presented in this study are included in the article. Further inquiries can be directed to the corresponding authors.

Acknowledgments: The authors would like to extend their sincere appreciation to the Deanship of Scientific Research at King Saud University for its funding this research (Ongoing Research Funding Program- (ORF-2025-1364)).

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

Appendix A. Code Snippets of the Smart Contracts

```
function patientRegister(uint256 _id, bytes memory _offChainRef) public {
    require(
        patient[msg.sender].status == STATUS.NULL,
        "Registration: Patient registered before"
    );

    patient[msg.sender].wallet = msg.sender;
    patient[msg.sender].id = _id;
    patient[msg.sender].status = STATUS.PENDING;
    patient[msg.sender].timestamp = block.timestamp;
    patient[msg.sender].offChainRef = _offChainRef;
    role[msg.sender] = ROLE.PATIENT;
    patients.push(msg.sender);

    emit patientRegisterLog(msg.sender, _offChainRef, block.timestamp);
}
function doctorRegister(
    uint256 _id,
    bytes memory _publicKey,
    address _hospital,
    bytes memory _offChainRef
) public {
    require(
        doctor[msg.sender].status == STATUS.NULL,
        "Registration: Doctor registered before"
    );

    doctor[msg.sender].wallet = msg.sender;
    doctor[msg.sender].hospital = _hospital;
    doctor[msg.sender].id = _id;
    doctor[msg.sender].status = STATUS.PENDING;
    doctor[msg.sender].publicKey = _publicKey;
    doctor[msg.sender].offChainRef = _offChainRef;
    doctor[msg.sender].timestamp = block.timestamp;
    role[msg.sender] = ROLE.DOCTOR;
    doctors.push(msg.sender);

    emit doctorRegisterLog(msg.sender, _offChainRef, block.timestamp);
}
```

Figure A1. Registration smart contract.

```
function createAcessPolicy(Registration.ROLE _role, ACCESS_TYPE _accessType)
    public
    onlyPatient
{
    bytes32 accessSignature = accessPolicySign(
        msg.sender,
        _role,
        _accessType
    );

    require(
        !accessPolicy[accessSignature].status,
        "AccessManagement: Access policy is aleady exist"
    );

    if (accessPolicy[accessSignature].timestamp > 0) {
        accessPolicy[accessSignature].status = true;
        accessPolicy[accessSignature].timestamp = block.timestamp;
    } else {
        accessPolicy[accessSignature].role = _role;
        accessPolicy[accessSignature].accessType = _accessType;
        accessPolicy[accessSignature].patient = msg.sender;
        accessPolicy[accessSignature].status = true;
        accessPolicy[accessSignature].timestamp = block.timestamp;
        accessPolicies.push(accessSignature);
    }
    emit accessPolicyLog(
        msg.sender,
        accessSignature,
        true,
        block.timestamp
    );
}
```

Figure A2. Access Management smart contract.

```
function createMedicalRecord(address _patient, uint256 _recordId)
    public
    onlyOwner
{
    require(
        !hashRecord[_patient],
        "DataManagement: record has been created before"
    );

    (, , Registration.STATUS status, , ) = registration.patient(_patient);

    require(
        status == Registration.STATUS.APPROVED,
        "DataManagement: patient should be approved"
    );

    record[_recordId].patient = _patient;
    record[_recordId].timestamp = block.timestamp;
    recordList[_patient] = _recordId;
    hashRecord[_patient] = true;
    records.push(_recordId);

    emit createMedicalRecordLog(_patient, _recordId, block.timestamp);
}

function updateMedicalRecord(
    uint256 _recordId,
    address _insurer,
    bytes memory _offChainData
) public onlyDoctor {
    require(
        record[_recordId].timestamp != 0,
        "DataManagement: record is not exist"
    );

    (, , , Registration.STATUS insurer_status, , ) = registration.insurer(
        _insurer
    );

    require(
        insurer_status == Registration.STATUS.APPROVED,
        "DataManagement: insurer should be approved"
    );
```

Figure A3. Data management smart contract.

```
function createClaim(uint256 _claimId) public {
    require(
        claim[_claimId].status == STATUS.NULL,
        "Claim: claim is already exist"
    );

    (
        uint256 recordId,
        address hospital,
        address insurer,
        ,
        uint256 timestamp,
        address doctor
    ) = dm.visit(_claimId);

    require(timestamp != 0, "Claim: no visiting available");

    (address patient, ) = dm.record(recordId);

    require(
        hospital == msg.sender,
        "Claim: only patient hospital can create claim"
    );

    claim[_claimId].patient = patient;
    claim[_claimId].visitId = _claimId;
    claim[_claimId].insurer = insurer;
    claim[_claimId].doctor = doctor;
    claim[_claimId].hospital = msg.sender;
    claim[_claimId].status = STATUS.PENDING;
    claim[_claimId].timestamp = block.timestamp;

    claims.push(_claimId);

    emit claimLog(
        _claimId,
        patient,
        insurer,
        _claimId,
        STATUS.PENDING,
        block.timestamp,
        msg.sender
    );
}
```

Figure A4. Claim smart contract.

References

1. Mohanta, B.K.; Panda, S.S.; Jena, D. An overview of smart contract and use cases in blockchain technology. In Proceedings of the 2018 9th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Bengaluru, India, 10–12 July 2018; pp. 1–4. [CrossRef]
2. Golosova, J.; Romanovs, A. Overview of the blockchain technology cases. In Proceedings of the 2018 59th International Scientific Conference on Information Technology and Management Science of Riga Technical University (ITMS), Riga, Latvia, 10 October 2018; pp. 1–6.
3. Ruben, R.J. Special communication. *Int. J. Pediatr. Otorhinolaryngol.* **2000**, *54*, 77. [CrossRef] [PubMed]
4. John, S.; Ravichandran, N.; Khan, M.F. Electronic medical record for deliverance of effective healthcare delivery: Ethical issues and challenges of digitalization in clinical information and electronic medical records (EMR) management. *IOSR J. Bus. Manag.* **2018**, *20*, 106–112.

5. Liang, X.; Zhao, J.; Shetty, S.; Liu, J.; Li, D. Integrating blockchain for data sharing and collaboration in mobile healthcare applications. In Proceedings of the 2017 IEEE Annual International Symposium on Personal, Indoor and Mobile Radio Communications (PIMRC), Montreal, QC, Canada, 8–13 October 2017; pp. 1–5. [CrossRef]
6. Alshahrani, A.; Stewart, D.; MacLure, K. A systematic review of the adoption and acceptance of eHealth in Saudi Arabia: Views of multiple stakeholders. *Int. J. Med. Inform.* **2019**, *128*, 7–17. [CrossRef]
7. Jabali, A.K.; Jarrar, M. Electronic health records functionalities in Saudi Arabia: Obstacles and major challenges. *Glob. J. Health Sci.* **2018**, *10*, 50. [CrossRef]
8. Prokofieva, M.; Miah, S.J. Blockchain in healthcare. *Australas. J. Inf. Syst.* **2019**, *23*, 1–22. [CrossRef]
9. Dubey, R.; Gunasekaran, A.; Bryde, D.J.; Dwivedi, Y.K.; Papadopoulos, T. Blockchain technology for enhancing swift-trust, collaboration and resilience within a humanitarian supply chain setting. *Int. J. Prod. Res.* **2020**, *58*, 3381–3398. [CrossRef]
10. Acharya, S.; Coats, B.; Saluja, A.; Fuller, D. Secure electronic health record exchange: Achieving the meaningful use objectives. In Proceedings of the 2013 46th Hawaii International Conference on System Sciences, Wailea, Maui, 7–10 January 2013; pp. 2555–2564. [CrossRef]
11. Zubaydi, H.D.; Chong, Y.W.; Ko, K.; Hanshi, S.M.; Karuppayah, S. A review on the role of blockchain technology in the healthcare domain. *Electronics* **2019**, *8*, 679. [CrossRef]
12. Haleem, A.; Javaid, M.; Singh, R.P.; Suman, R.; Rab, S. Blockchain technology applications in healthcare: An overview. *Int. J. Intell. Netw.* **2021**, *2*, 130–139. [CrossRef]
13. Golosova, J.; Romanovs, A. The advantages and disadvantages of the blockchain technology. In Proceedings of the 2018 IEEE 6th Workshop on Advances in Information, Electronic and Electrical Engineering (AIEEE), Vilnius, Lithuania, 8–10 November 2018; pp. 1–6. [CrossRef]
14. Lapointe, C.; Fishbane, L. The blockchain ethical design framework. *Innov. Technol. Gov. Glob.* **2019**, *12*, 50–71. [CrossRef]
15. Halaburda, H. Blockchain revolution without the blockchain. *Commun. ACM* **2018**, *61*, 27–29. [CrossRef]
16. Tasatanattakool, P.; Techapanupreeda, C. Blockchain: Challenges and applications. In Proceedings of the 2018 International Conference on Information Networking (ICOIN), Chiang Mai, Thailand, 10–12 January 2018; pp. 473–475. [CrossRef]
17. Agbo, C.C.; Mahmoud, Q.H.; Eklund, J.M. Blockchain technology in healthcare: A systematic review. *Healthcare* **2019**, *7*, 56. [CrossRef] [PubMed]
18. Puthal, D.; Malik, N.; Mohanty, S.P.; Kougianos, E.; Das, G. Everything you wanted to know about the blockchain: Its promise, components, processes, and problems. *IEEE Consum. Electron. Mag.* **2018**, *7*, 6–14. [CrossRef]
19. El Mahalli, A. Electronic health records: Use and barriers among physicians in eastern province of Saudi Arabia. *Saudi J. Health Sci.* **2015**, *4*, 32–41. [CrossRef]
20. Nguyen, T.D.; Vu, H.D.; Webster, J.G.; Nimunkar, A.J. A web-based electronic medical records and hospital information system for developing countries. *J. Health Inform. Dev. Ctries.* **2011**, *5*, 155–170.
21. Zheng, Z.; Xie, S.; Dai, H.N.; Chen, X.; Wang, H. Blockchain challenges and opportunities: A survey. *Int. J. Web Grid Serv.* **2018**, *14*, 352–375. [CrossRef]
22. Li, X.; Jiang, P.; Chen, T.; Luo, X.; Wen, Q. A survey on the security of blockchain systems. *Futur. Gener. Comput. Syst.* **2020**, *107*, 841–853. [CrossRef]
23. Yahaya, S.; Jilantikiri, L.; Hassan, K.; Akande, K.; Yahaya, A. Development of an automated healthcare record management system. *Adeleke Univ. J. Eng. Technol.* **2019**, *4*, 79–90.
24. Rakic, D. Blockchain technology in healthcare. ICT4AWE 2018. In Proceedings of the 4th International Conference on Information and Communications Technologies for Ageing Well and e-Health (ICT4AWE 2018), Madeira, Portugal, 22–23 March 2018; pp. 13–20. [CrossRef]
25. Liang, X.; Yan, Z.; Zhang, P. Security, privacy, and anonymity in computation, communication, and storage. In Proceedings of the 10th International Conference on Security, Privacy and Anonymity in Computation, Communication and Storage (SpaCCS 2016), Zhangjiajie, China, 16–18 November 2016; pp. 155–167. [CrossRef]
26. Benchoufi, M.; Porcher, R.; Ravaud, P. Blockchain protocols in clinical trials: Transparency and traceability of consent. *F1000Research* **2017**, *6*, 66. [CrossRef]
27. Maslove, D.M.; Klein, J.; Brohman, K.; Martin, P. Using blockchain technology to manage clinical trials data: A proof-of-concept study. *JMIR Med. Inform.* **2018**, *6*, e11949. [CrossRef]
28. Tseng, J.H.; Liao, Y.C.; Chong, B.; Liao, S.W. Governance on the drug supply chain via gcoin blockchain. *Int. J. Environ. Res. Public Health* **2018**, *15*, 1055. [CrossRef]
29. Katuwal, G.J.; Pandey, S.; Hennessey, M.; Lamichhane, B. Applications of blockchain in healthcare: Current landscape & challenges. *arXiv* **2018**, arXiv:1812.02776. [CrossRef]
30. Cyran, M.A. Blockchain as a foundation for sharing healthcare data. *Blockchain Healthc. Today* **2018**. [CrossRef]
31. Alam, S.; Reegu, F.A.; Daud, S.M.; Shuaib, M. Blockchain-based electronic health record system for efficient COVID-19 pandemic management. *Preprints* **2021**, 1–5. [CrossRef]

32. Patel, V. A framework for secure and decentralized sharing of medical imaging data via blockchain consensus. *Health Inform. J.* **2019**, *25*, 1398–1411. [CrossRef] [PubMed]
33. Dagher, G.G.; Mohler, J.; Milojkovic, M.; Marella, P.B. Ancile: Privacy-preserving framework for access control and interoperability of electronic health records using blockchain technology. *Sustain. Cities Soc.* **2018**, *39*, 283–297. [CrossRef]
34. Xia, Q.; Sifah, E.B.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information* **2017**, *8*, 44. [CrossRef]
35. Tahir, N.U.A.; Rashid, U.; Hadi, H.J.; Ahmad, N.; Cao, Y.; Alshara, M.A.; Javed, Y. Blockchain-based healthcare records management framework: Enhancing security, privacy, and interoperability. *Technologies* **2024**, *12*, 168. [CrossRef]
36. 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]
37. Alruwaill, M.N.; Mohanty, S.P.; Kougianos, E. hChain 4.0: A Secure and Scalable Permissioned Blockchain for EHR Management in Smart Healthcare. *arXiv* **2025**, arXiv:2505.13861. [CrossRef]
38. Zain, B.; Shawkat Ali, A.B.M.; Sakzad, A. Blockchain-Powered Fraud Prevention in Health Insurance Industry. In Proceedings of the 6th ACM International Symposium on Blockchain and Secure Critical Infrastructure, Singapore, 1–5 July 2024.
39. Hsiao, C.J.; Marsteller, J.A.; Simon, A.E. Electronic medical record features and seven quality of care measures in physician offices. *Am. J. Med. Qual.* **2014**, *29*, 44–52. [CrossRef]
40. Brasil, L.M.; Abreu, C.G.; Vieira, A.G.; Machado, M.A.; Almeida, V.S.; Rodrigues, R.M. System of web-based electronic medical record. *Rev. Eletrônica Sist. Informação* **2007**, *6*. [CrossRef]
41. Sarfraz, M.; Al-Hussainan, A.F.; Mohammad, F.; Al-Azmi, H. An electronic medical record system. *Int. J. Extrem. Autom. Connect. Healthc.* **2019**, *2*, 68–102. [CrossRef]
42. Stiemerling, O.; Cremers, A.B. The use of cooperation scenarios in the design and evaluation of a CSCW system. *IEEE Trans. Softw. Eng.* **1998**, *24*, 1171–1181. [CrossRef]
43. Haynes, S.R.; Purao, S.; Skattebo, A.L. Scenario-based methods for evaluating collaborative systems. *Comput. Support. Coop. Work* **2009**, *18*, 331–356. [CrossRef]