network

Article

Towards Secure Searchable Electronic Health Records Using Consortium Blockchain

Muneera Alsayegh [1], Tarek Moulahi [1,*], Abdulatif Alabdulatif [2] and Pascal Lorenz [3]

[1] Department of Information Technology, College of Computer, Qassim University, Buraydah 52571, Saudi Arabia; 411200028@qu.edu.sa
[2] Department of Computer Science, College of Computer, Qassim University, Buraydah 52571, Saudi Arabia; ab.alabdulatif@qu.edu.sa
[3] MIPS-GRTC Laboratory, University of Haute Alsace, 68008 Colmar, France; pascal.lorenz@uha.fr
* Correspondence: t.moulahi@qu.edu.sa

Abstract: There are significant data privacy implications associated with Electronic Health Records (EHRs) sharing among various untrusted healthcare entities. Recently, a blockchain-based EHRs sharing system has provided many benefits. Decentralization, anonymity, unforgeability, and verifiability are all unique properties of blockchain technology. In this paper, we propose a secure, blockchain-based EHR sharing system. After receiving the data owner's authorization, the data requester can use the data provider's keyword search to discover relevant EHRs on the EHR consortium blockchain and obtain the re-encryption ciphertext from the proxy server. To attain privacy, access control and data security, the proposed technique uses asymmetric searchable encryption and conditional proxy re-encryption. Likewise, proof of permission serves in consortium blockchains as the consensus method to ensure the system's availability. The proposed protocol can achieve the specified security goals, according to the security analysis. In addition, we simulate basic cryptography and put the developed protocol into practice on the Ethereum platform. The analysis results suggest that the developed protocol is computationally efficient.

Keywords: consortium blockchain model; EHRs; searchable encryption; proxy re-encryption

Citation: Alsayegh, M.; Moulahi, T.; Alabdulatif, A.; Lorenz, P. Towards Secure Searchable Electronic Health Records Using Consortium Blockchain. *Network* **2022**, *2*, 239–256. https://doi.org/10.3390/network2020016

Academic Editor: Thang N. Dinh

Received: 20 March 2022
Accepted: 18 April 2022
Published: 20 April 2022

1. Introduction

As a replacement for the traditional manuscript patient's health record, electronic health records (EHRs) have been developed. EHRs have emerged as a result of the rapid growth of information technology and Internet technology. The recent advances in computing perspectives, such as clouds and the internet of things, provide modern health systems for doctors with greater facilities in the collection, analysis, and surveillance of healthcare information for remote patients [1]. Health information includes patient information which must not be communicated to an unreliable third party due to security concerns and any information exploitation. Although the exchange of patient data between different healthcare providers via EHR can increase the accuracy of diagnostics, the medical server can be a single weak point and can be targeted by hackers leading Distributed Denial of Service and ransomware attacks (DDOS) [2].

In addition, infringements of health data are now occurring more than once per day. Therefore, EHRs are a crucial problem for data sharing and privacy preservation. Notably, before making the diagnosis or treatment, the doctor typically wants to know the patient's medical background. Furthermore, the EHR must be able to securely and timely query historical medical data produced by different doctors in various hospitals with the consent of the patient. In short, the secure exchange of medical information is primarily hampered by [3]:

- Increasing massive data at high speeds: Medical information is large and annually increases in volumes by 20–40%. The challenges include not only how to obtain such a large amount of data from established IT systems but also how to maintain its privacy and protect its integrity while keeping third-party users highly accessible;
- Interoperability of cross-institutional data: To escape external attacks and threats, most existing healthcare systems are constructed in a closed area with a network security perimeter. Furthermore, the lack of medical information data interoperability presents a barrier for medical analytics that would require a great deal of clinical information. Besides, it poses drawbacks for patients who pursue improved care plans because their records are spread across many hospitals.

In terms of sharing and access through EHRs, emerging technology based on breakthroughs and blockchain can bring encouraging solutions to secure patient data. Blockchain requires robust safety and privacy mechanisms for the interoperability, authentication, and exchange of health information in healthcare applications to follow the stringent legal requirements of the 1996 Health Insurance Portability and Accountability Act [2]. Blockchain was revealed in 2018 [4] to facilitate life in many areas with its distributed, safe and unchangeable structure. Many countries have had great success combining blockchain technology with eHealth systems. This technology has gained significant attention in recent years in the healthcare industry especially as a solution against a single point of failure problem. Smart contracts can make only authorized devices or users connect or access documented EHR data with multiple signatures between patients and service providers. This function ensures that patients can check the validity of EHR data while preserving their actual identity confidentiality. Even so, blockchain technology is not the best option for solving any problems in the industrial sector because it protects data integrity and availability, but it does not protect the confidentiality of data sharing.

Therefore, cryptography is an appropriate solution for a secure data sharing-based blockchain, but it has a disadvantage with latency because when trying to encrypt all the data stored in the blockchain we need to decrypt it completely whenever we need specific data. To solve this problem many studies have proposed different solutions; one of them is Searchable Encryption (SE), which enables users to securely search for encrypted data without the need to decrypt all data [5]. Searchable encryption is a technology that allows users to save ciphertext documents while ensuring the functionality to search their documents with keywords. In recent years, two different types of Searchable Encryption (SE) have been widely openly discussed, namely Symmetrical Searchable Encryption (SSE) and Public Key Encryption with Keyword Search (PEKS) or Asymmetrical Searchable Encryption (ASE). The downside of the SSE method is that there are several keys used for encryption and decryption and multi-keyword search cannot be supported [6]. PEKS was initially suggested by Boneh et al. [7], which is primitive encryption that solves the above addition issues efficiently. However, the vulnerability against Keyword Guessing Attacks (KGA) is an issue that reduces the security of the PEKS scheme.

Recently, efforts have been spent on developing the PEKS scheme to solve the KGA problem, for example, in [8], in a Public-key Authenticated Encryption with Keyword Search (PAEKS) scheme a keyword is not only encrypted but also authenticated by the data owner. Another study [9] uses the method of renewing the keywords in the key server periodically to prevent the key server from being compromised. In [10] they used the smart contract as an effective solution against KGA. Besides this, Access Control (AC) in systems is typically carried out in three steps: Identification, Authentication and Authorization [11]. To implement AC mechanisms with SE methods, the proxy re-encryption (PRE) scheme can provide efficient Access Control for the patients with regard to their data. PRE is an encoding scheme allowing a third party (proxy) to modify a single party-encoded ciphertext to decode it by another party approved to do so [3].

The motivation of this paper is to develop an EHRs sharing protocol-based blockchain. It can be used to store, manage, and to exchange EHRs. The protocol should preserve

security and privacy in the method used to share medical data, in addition to taking into consideration the minimization of communication and computational cost.

In dealing with previous challenges, we proposed a secrecy and efficient blockchain protocol for EHRs sharing based on Public-key Encryption with Keyword Search (PEKS) using Elliptic-curve Diffie–Hellman (ECDH) with a Proxy Re-Encryption (PRE) scheme to preserve the data security and patient privacy. In summary, the contributions of the developed scheme are as follows.

1. To address the problem of poor AC of patients over their EHR, we suggest using a PRE-based blockchain to preserve the privacy of EHR and patients' fine-grained AC by re-encrypting the data by the patient's public key after each access by a third party (data researchers);
2. To address the problem of patient identity disclosure, we suggest storing the real identity in a private blockchain and using a unique blockchain address as a pointer to their identity;
3. To address the problem of preserving confidentiality in an EHR-sharing blockchain, we suggest using PEKS with a conjunctive keyword searchable scheme to store the encrypted index in the smart contract on a consortium Ethereum blockchain then storing the EHR in a private blockchain and periodically using a renewal key server technique to prevent compromising the key server and to solve the KGA problem.

The remainder of the paper is arranged as follows. Section 2 outlines existing studies linked to our study, and describes the background of this work. Section 3 presents the developed system architecture and performance analysis of the EHR consortium. In Section 4, we conduct an experimental study, and we compute the computational and communication overheads of our proposed protocol implementation in Ethereum. An overall discussion regarding the proposed protocol is given in Section 5. Finally, Section 6 is the last section of our paper.

2. Background and Related Works

This section describes the background of our study in addition to outlining the literature review.

2.1. Background

2.1.1. Electronic Health Records (EHRs)

Electronic Health Records (EHRs) are the digital format of patient data that is replacing traditional patient data collection which is a part of the rapid advancement of information technology and internet technology. In addition, health information contains highly sensitive private information, which should be shared by individuals, including health specialists, pharmacists, relatives, insurers, and other hospitals.

Jamoom et al. [12] were the first to transform paper health records into EHRs. EHR is a popular method for healthcare providers (e.g., hospitals) to store patient data. In addition, Figure 1 illustrates a typical view of EHRs. In such a system, protecting data integrity, anonymity, and confidentiality is certainly a critical issue.

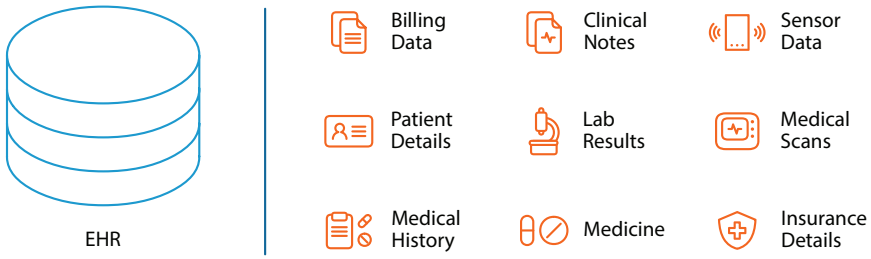

Figure 1. Overview of Electronic Health Records (EHRs) services.

On the other hand, EHRs face several privacy and security challenges ,which range from malware to Distributed Denial-of-Service (DDoS) attacks that can lead to inefficiency of patient care. Cyber-attacks can lead to major consequences which overtake security breaches and economic damage [13]. These activities illustrated the critical need to safeguard the confidentiality, integrity, availability, protection, and privacy of sharing electronic health records (EHRs) [6].

2.1.2. Blockchain Technology

The development of blockchain technology in the healthcare domain focuses on applying blockchain strategies to ensure EHRs privacy and security in various healthcare applications. Blockchain technology was initially used in Bitcoin and was created for the cryptocurrency Bitcoin by Satoshi Nakamoto in 2008 [4]. Blockchain technology offers an opportunity for recording and sharing data in a decentralized network. Blockchain can provide trust in peer-to-peer networks. The core elements of blockchain technology are a distributed ledger, consensus mechanisms and public-key encryption [2]. Any block in the blockchain consists of at least one transaction, a block validator signature and a reference of block headers to the previous block. Blockchain data structures facilitate the generation and sharing of different transactions between nodes in a peer-to-peer network inside a digital ledger. Blockchain technology allows participants to store and exchange sensitive data in real-time without exposing communication networks to malicious intent, forgery, or theft. Each transaction in the blockchain is associated with a hash, which is used to create the binary Merkle tree. The timestamp and identifier of the preceding block are stored in the block header along with the binary tree. The term "chain" refers to the blocks that are linked in chronological order and serve as a record of the ledger's state changes [14]. As a result, if a hacker tries to change the records in the blockchain, he must change not only the hash of that particular block but also the hash of any subsequent block, which is virtually impossible to do [15].

2.1.3. Types of Blockchain

The blockchain architecture defines the relation for the transaction or validation of nodes running on the network. In the case that the blockchain nodes members are known to the network, then blockchains such as Hyperledger Fabric [16] and Ripple [17] are referred to as permissioned. When an architecture is available to the public, a single node or organization, such as Ethereum and Bitcoin, may be part of the network, so this blockchain is public [2].

1. **Public blockchain network**
   The data in a public blockchain network are accessible to the public where participants can be part of the consensus without the need for permissions. Transactions with some anonymities are available to all nodes [18]. The participant, based on a consensus algorithm, may therefore verify a transaction and engage in the approval process, as in Proof of Stake (PoS) and Proof of Work (PoW) [2]. The system is fully secure by repeating synchronous public blockchains with each network miner. This architecture is employed in cryptocurrency networks such as Bitcoin and Ethereum; however, it raises privacy issues.
2. **Private blockchain (permissioned)**
   This kind of limited blockchain permits the return of an intermediary. Private blockchains strictly control the data access permission of a network. Any transaction in the network can only be verified and validated by companies or organizations with a high level of efficiency. The failure to provide a decentralized infrastructure for secure databases is a drawback of private blockchains, which are provided by public blockchains [19]. Private blockchains can be recognized correctly as conventional centralized networks but with a strong cryptographic model for network transactions to be verified and validated [2]. Each hospital keeps EHRs in its private blockchain, which offers the benefits of speed, privacy, cheap cost, and improved security [20].

3. **Consortium or federated blockchain**
   A consortium is a combination of private and public blockchains that can be thought of as partly decentralized. The nodes have the authority to be chosen ahead of time and the transaction can be made private or public [2]. In addition, the hospitals are structured to create a blockchain consortium that keeps searchable PHI indexes. The physician can find the indexes in the consortium blockchain to obtain the originals by visiting the associated private hospital blockchain [20].

2.1.4. The Blockchain Platforms

However, there are several various types of blockchain platforms, such as Bitcoin, Ethereum, Hyperledger, Ripple and Quorum, which have been proposed and applied to several security application scenarios in recent years. Through the introduction of new decentralized technologies in financial or non-financial areas, the Ethereum blockchain provides the concept of a full programming language in a blockchain setting [21]. Ethereum was one of the first blockchain platforms to implement smart contracts, and it has the most developer support. Ethereum is a decentralized forum for smart contract execution. In Ethereum, the smart contract is used to calculate some general function in a blockchain. In principle, this means that an Ethereum smart contract may be used to perform any computational operation [10]. Miners in the Ethereum network verify and authorize transactions, employ systems many times, and rapidly guess answers to a puzzle before one of them wins [22]. Each miner in the Ethereum network uses the Ethereum Virtual Machine (EVM).

2.1.5. Searchable Encryption

Encryption or cryptography is the process of securing a message over an insecure network. Traditional search methods are ineffective when dealing with encrypted data. Using Searchable Encryption (SE) is an appropriate solution [5] for this purpose. Searchable encryption is regarded as a key technology for achieving data confidentiality and retrieval functions which is an encryption technique that encrypts data in such a way that it can be searched using keywords [23]. Searchable Encryption (SE) stands for "searching without decryption" on encrypted data stored on an untrusted server or cloud [5].

Public key encryption with keyword (PEKS) enables anybody to encrypt the data with the public key of the data owner, but searches can be performed only by the private key holder [23]. Different cryptographic algorithms are used for confidential data exchange over a public network. There are several public-key cryptography algorithms available, each with its own set of strengths and weaknesses. RSA and ECC are the most extensively used public-key cryptosystems. Today, several elliptic curve protocols are in use, including ECDSA, ECIES, and ECDH. The researchers in [24] provide a comparative analysis between RSA and ECC and all comparing parameters show that our elliptic curve-based implementations outperform the RSA algorithm.

2.1.6. Searchable Encryption Vulnerability

- Keyword Guessing Attack (KGA): one of the most serious PEKS security issues is its vulnerability against off-line Keyword Guessing Attacks (KGA). An adversary can encrypt the candidates' keywords by using the public key of the receiver and identifying the ciphertext that fits the intended trapdoor. This allows the adversary to retrieve the keyword concealed in the trapdoor to breach the privacy of the users. Such attacks rely on the keywords' observations that are selected and receivers typically scan for files using well-known keywords [25].

2.1.7. Access Control Based Blockchain

Another line of research looked at how to handle the access control and the privacy of EHR sharing on the blockchain when third-party organizations or individuals other than hospitals' or patients' attempts to obtain patient data, patient privacy may be compromised.

Recently, fine-grained access control of encrypted data can be achieved using many methods such as attribute-based encryption (ABE) and proxy re-encryption (PRE).

- Proxy re-Encryption scheme: a cryptographic-based technique that re-encrypts ciphertext by using a semi-trusted proxy server with a user public key into ciphertext encrypted with another user's public key [6]. A proxy re-encryption scheme ensures access is denied after a specific time frame. In comparison to existing schemes, the proposed protocol ensures fine-grained access control, flexible client revocation, and lower storage and encryption time costs [6]. As shown in Figure 2, Alice sends a message via a semi-trusted proxy server to Bob without the need to share the private key of Alice with any entity while ensuring the message's privacy.

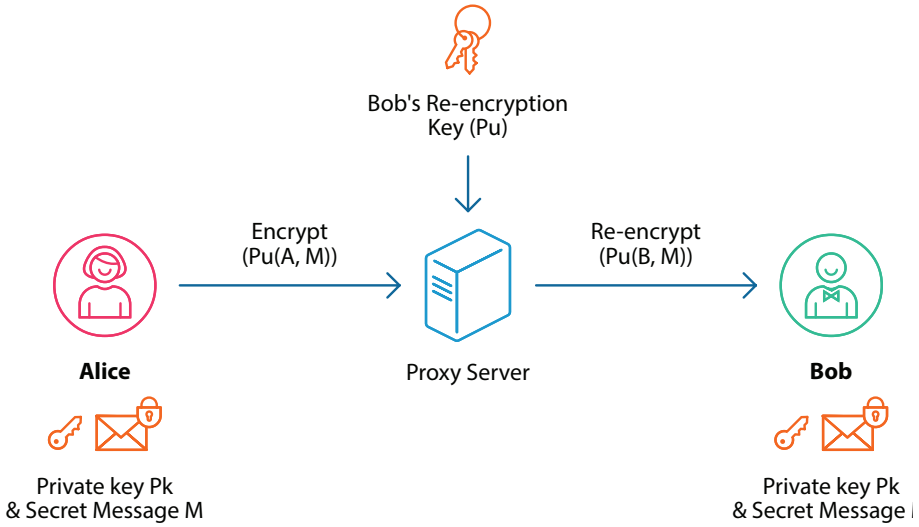

Figure 2. Overview of proxy re-encryption scheme.

2.2. Relate Works

2.2.1. Blockchain-Based Healthcare Applications

In recent years, blockchain has received a lot of attention in areas such as data storing, data sharing, and data confidentiality. Many studies have used this technology to address problems in existing EHRs. Existing deployments of IT infrastructure in a medical facility usually involve private structures that impose limitations on scalability and information sharing [26] where it is important to choose a suitable type of blockchain (private or public) for medical data sharing. Jin et al. in [3,27] presented a review of security and privacy-preserving EHRs which explain different blockchain architectures based on sharing EHRs. They review a comparison of current EHRs schemas-based blockchains with security metrics and functionality.

Recently, blockchain is becoming a major technology that will change the way we share information with increasing confidence in distributed environments without the need for authorization. Reyna et al. [28] present a blockchain technology survey that evaluates the unique characteristics of blockchain and discover the research gaps, classify and review the various ways that IoT and blockchain can be integrated, and also review existing networks and frameworks for blockchain-IoT and assessment results with a comparison of various blockchains in IoT devices. There are many EHRs schemes based on blockchain provided. For example this study [29] designed MedRec, an Ethereum-based medical data-sharing platform that allows for the decentralized safe integration of medical data across medical organizations. Nonetheless, to preserve blockchain stability, its consensus technique PoW requires a high computing load. A design that is similar to this is proposed in [30]. Xue et al. [31] proposed the MDSM medical blockchain system, which uses an upgraded DPoS consensus method to reduce node computation burden and improve data sharing security and efficiency. For COVID-19 pandemic management, smart contracts and

blockchain were also used [32,33]. The idea of these studies is tracking the tests through automated medical passports and certificates of immunity.

2.2.2. Blockchain Enabled Searchable Encryption

A blockchain-based symmetric searchable encryption (SSE) system for electronic medical record sharing was proposed [10] to enhance data searchability. In this case, SSE with AES will help dynamic searchable symmetric key encryption and address key sharing problems, but the multi-keyword search cannot be supported [6]. Regarding this, in [34], a trustworthy and private keyword searchable privacy protection method based on blockchain is developed, which employs searchable encryption to enable an encrypted data search. Tian et al. [35] proposed a blockchain privacy protection strategy based on searchable symmetric encryption, which ensured both sides' fairness.

However, most techniques only offer single-keyword searches and cannot be used for file updates, limiting the scheme's imperfection. The authors of [36] developed a blockchain-enabled public key encryption system with multi-keyword search (BPKEMS) to solve these issues, and their approach also enables file updates. However, the security issue related to using PEKS schemes is a keyword guessing attack (KGA). To address keyword guessing attack (KGA) issues, the authors of [37] present certificateless searchable public-key authenticated encryption scheme with a designated tester (CL-dPAEKS). Public-key Authenticated Encryption with Keyword Search (PAEKS) in [8] provides a different approach to solve the same problem. Besides that, the authors of [9] present SEPSE to resolve online and offline keyword guessing and also the single point of failure problem. SEPSE uses PEKS, which supports key renewal to replace a new key on each key server regularly to avoid the key compromise. SEPSE is based on threshold blind BLS signature and we can decrease the computing time for enhanced performance by using ECC encryption techniques [38].

2.2.3. Blockchain-Based Access Control Schemes

Another research direction looked at how to overcome the access control and privacy concerns of EHR sharing on the blockchain; when third-party organizations or individuals other than hospitals or patients attempt to obtain patient data, patient privacy may be compromised. Recently, the use of ciphertext-policy attribute-based encryption (CP-ABE) in access control methods for secure data sharing has received a lot of attention. The authors of [39] proposed BMAC, a Blockchain-based Multi-authority Access Control mechanism for the secure sharing of EHRs.

Wang et al. [40] suggested an encryption system based on an attribute based on the smart Ethereum contract. In this method, the data owner is able to distribute data users' keys which removes the key misuse phenomenon and assures private data protection. To implement fine-grained access control policies, the authors of [41] introduce a blockchain-based system for secure mutual authentication, called BSeIn. The proposed model includes a combination of multi-receiver encryption, message authentication code, and attribute signature. This model provides privacy and security assurances including anonymous authentication, auditability, and secrecy. On another side, proxy re-encryption (PRE) supports an efficient fine-grained access control for the patients' data. PRE is an encoding scheme allowing a third party (proxy) to modify a single party-encoded ciphertext to decode it by another party approved to do so. In this case, a two-party proxy key allows a semi-confident intermediate proxy to convert ciphertext, avoiding sender-side decryption and the re-encryption of data [3].

2.2.4. Blockchain-Based Searchable Encryption and Access Control Schemes

This section presents how searchable encryption and access control can work together. To obtain strong conceptions of confidentiality, various technologies must be combined. The integration between PEKS and PRE schemes present in [42] can provide an efficient EHRs sharing protocol based on two types of blockchain: private blockchain for stored

data and public blockchain for storing an EHR index. According to this research [35], the EHR data ciphertext is stored in the cloud, and the EHR data keyword index is stored on the blockchain. Fine-grained access control of cloud data is achieved via the attribute encryption approach, and attribute signature technology is employed to validate the authenticity of the EHR data source. The authors of [43], a new cryptographic primitive called conjunctive keyword search with designated tester and timing, allowed the proxy re-encryption method (Re-dtPECK), which is a time-dependent SE scheme. In this scheme, the duration of time for the delegate to scan and decrypt the delegator's encrypted documents can be regulated. This scheme supports conjunctive keyword search and prevents keyword guessing attacks.

The authors of [44] introduced a blockchain-based attribute-based searchable encryption scheme with a verifiable ciphertext. The scheme uses the PRE technique to enforce user attribute revocation when the user's attributes or the ciphertext access structure need to be modified, and the authority center is in control of the overall attribute revocation procedure. However, to securely find keywords on the blockchain consortium, the authors of [45] use public encryption with the methods of keyword searchable PEKS. In the decoding phase, proxy re-encryption technology is used to provide secure access to patient data for third-party users. Besides, the authors of [46] proposed a blockchain-based EHR sharing protocol that is both secure and private. To achieve data protection, privacy preservation, and access control are needed. The scheme primarily uses searchable encryption and conditional proxy re-encryption. Finally, to the best of our knowledge, we still need to develop an efficient sharing EHR protocol using PEKS with PRE schemes based on blockchain to solve the KGA problem with low computational and communication costs.

3. System Model

3.1. Problem Statement

EHRs are important, sensitive, and private data that must always be kept secure and available. Intentional or unintended security risks may compromise healthcare systems. EHRs contain confidential data for medical diagnosis and care, so it must be exchanged regularly by various parties. If unauthorized people can access patient records then the data's confidentiality and availability are compromised. The security goal of the healthcare industry is to ensure the availability, confidentiality, and integrity of their services. Besides that, access to EHRs should be restricted to protect the data's security and privacy by preventing unauthorized entities from changing the meaning of the EHR. However, all systems that interact with the patients must respect their privacy and the data owners (patients) must have full control of their EHRs. Recently, several studies have proposed blockchain technology as a practical solution that can protect data integrity and availability but it does not protect data sharing confidentiality since any transaction in the blockchain is visible to the public [2,47]. Besides, access authorization is needed to protect the privacy of EHRs and the interoperability can assist patients in managing their EHR access rights [46,48].

3.2. The Proposed Protocol

The proposed protocol is divided into three phases and each phase relies on the previous phase as shown in Figure 3.

Phase 1:

Is called the registration phase, this step aims to preserve the patient's privacy and for them to gain full access control over her/his data. The input of this step is the real identity of a patient, and the output is producing the patient's blockchain address which will be used asa visit card to avoid the patient's identity beuing disclosed. In this step, the system manager produces the pair of patient's and doctor's private and public keys. The system manager also generates the keyword from the key server as the output of this phase.

Phase 2:

With data storage, the aim is to encrypt EHRs with the patient's identity and send it to a private blockchain and encrypt the index of a doctor's public key using Public Key encryption with a conjunctive Keyword Searchable (PKES) scheme and send it to a smart contract in the consortium blockchain. The inputs of this step are the patient's address and his/her EHR, and the outputs are storing the encrypted EHRs and the secure encrypted index.

Phase 3:

With data sharing, the aim is to provide a secure EHR sharing based blockchain for the data users under the patient's control; this step receives the trapdoor from the third party, in which is contained the private key of a patient, and the keyword. The outputs sent ordered EHRs to the third party and implements proxy re-encryption (PRE) by the system manager to re-encrypt the index by the patient's private key after each decryption and to renew the keyword set after an epoch similar to [9].

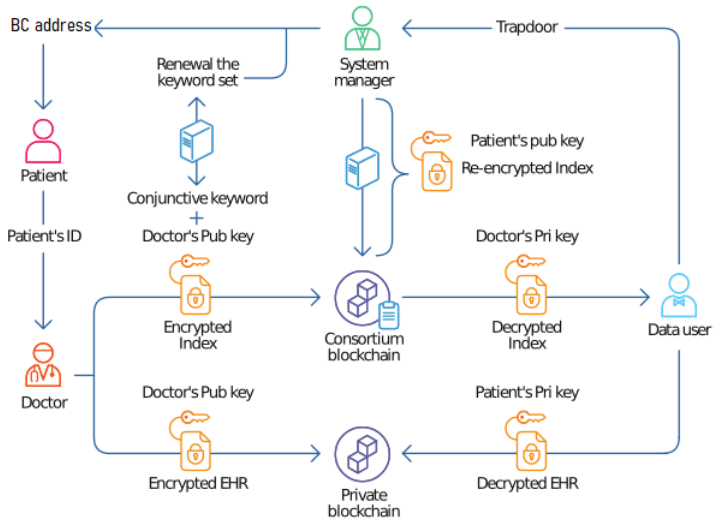

Figure 3. Overview of the proposed protocol.

3.3. System Model Design

In Table 1, several symbolic notations are presented to ease the following description.

Table 1. Proposed protocol symbolic notations.

Symbolic	Description
$\mathcal{SM}$	System manager
λ	System parameter
U_{pi}	Patient of the system
U_{ui}	User data
Sk_{pi},Pk_{pi}	The pair of patient's private and public keys
Sk_d,Pk_d	The pair of doctor's private and public keys
ω	Keyword set
$c\omega$	The ciphertext of the keyword
K_{si}	Key server
$\mathcal{Q}$	Keyword query
e	An epoch (predetermined time frame)
T_Q	The Trapdoor
Id_p	Patient's identity
C_m	Encrypted plaintext
$\acute{C}_m$	Re-encryption plaintext
RK_i	Re-encryption secure index

3.3.1. Phase 1: Registration Process

In this phase, firstly, before seeing a doctor, patients must register with the hospital's blockchain network, and the system manager provides the patient with an Ethereum address which is unique and is equal to the visit cards of patients. Secondly, the system manager produces the pair key (public key, private key) for the patient and the doctor. Thirdly, the system manager generates new keywords from the key server.

In this step, the preparation of the data samples was made by registering the patients, doctors, and data users (third parties) to produce the blockchain accounts for them. We use four entities in the system: medical service provider (doctor), system manager, data owner (patient) and finally data users (third parties). In this paper, the public key encryption with conjunctive keyword search features are used to permit any third party to search a document containing several keywords while using an encryption public key. This phase runs as follows.

- $KeyGen(\lambda)$: a security parameter λ as an input and a pair of the public and private keys (Sk,Pk) as an output for a given doctor and patients;
- $PEKS$ (Pk_{pi}, ω): a patient public key Pk_{pi} and a selected set of keywords ω = (ω_1,..., ω_n) as inputs. The public key of the patient to generate a searchable encryption $c\omega$ for ω;
- $Trapdoor$ (Sk_{pi}, $\mathcal{Q}$): The private key of a patient Sk_{pi} and the keyword query Q = (Ω_1,..., Ω_n) as inputs. The trapdoor T_Q is computed for the conjunctive search of a possible keyword query;
- $KeyRenew$ (ω,e): Each key server K_{si} (here 2 $[1; n]$) can update its secret share without affecting the secret shared by all key servers to produce a new keyword $\hat{\omega}$. It needs to be executed only once in an epoch (A period, often known as an epoch, is a definite and predetermined time frame).

3.3.2. Phase 2: Data Storage

In this step, firstly the doctor produces the encrypted patient's personal information and his/her EHRs with the patient's identity and sent it to the private blockchain which works as a medical server. Secondly, the doctor encrypts the index with a public key encryption using the ECDH algorithm and stores it in the smart contract-based consortium blockchain, then requests the keyword set from the key server and then encrypts the keyword set and the patient private key. Secondly, the doctor sends the encrypted EHRs to the private blockchain and the secure index (encrypted keyword and patient's private key) is stored in the smart contract-based consortium Ethereum blockchain.

In this phase, the doctor first logs in to the Ethereum blockchain with the patient's address. Secondly, the encrypted patient information and his/her EHR with their identity are stored in a private blockchain. Thirdly, he encrypts the secure index (encrypted keyword and patient's private key) with the doctor's public key using the public-key encryption algorithm, which is the ECDH algorithm in this case, and stores it in the smart contract-based consortium Ethereum blockchain. This phase runs the following algorithm:

- $PEKS$ (Pk, ω, ID_{pi}): Given the patient public key Pk_p, select a keyword set ω = (ω_1, ω_2,..., ω_n) as input and return it to the patient identity ID_{pi} as a pointer for the EHR's location in the private blockchain;
- $EncryptEHR$ (m, Pk_p): It takes the patient's public key Pk_p and plaintext m as an input and returns ciphertext C_m;
- $Encryptindex$(ω,Sk,Pk): It takes the keyword set and the patient's private key and encrypts it with the patient's public key then returns the index ciphertext.

3.3.3. Phase 3: Data Sharing

When a data researcher, such as a physician, insurance provider, or some other third party, uses a certain keyword search and the private key of the patient to create a trapdoor then the smart contract performs the test algorithm for data retrieval. After the authentic

EHR ciphertext search is completed by the system manager, the EHR delivers to third-party users and acts as an aid to proxy re-encryption of the original ciphertext by running the ReKeyGen algorithms to generate the proxy re-encryption key and re-encrypt the ciphertext using patient's public key.

In this phase, firstly, the third party (data user) send sends the request to the Ethereum smart contract to display the patient's EHRs using the trapdoor (patient's private key + keyword set). Secondly, the EHRs' index will decrypt and re-encrypt using the ECC algorithm's public key of the patient. Thirdly, the original EHRs will be sent to a third party and the encrypted EHRs index will be restored in the smart contract.

- $Test(c, \omega, Pk, T_Q)$: The function inputs are searchable keyword encryption c, a public key Pk and a trapdoor T_Q. If Q is included in $c\omega$ the server outputs "yes", otherwise "no";
- $ReKeyGen(\omega, sK_{pi}, pK_{pi})$: The input is the set of keywords from Ksi and the patient's private key sK_{pi}. This process generates a secure re-encryption index using the patient's public key pK_{pi};
- $ReEnc(C_m, RK_i)$: The function inputs are ciphertext C_m and re-encryption secure index (RK_i) and the output is a re-encryption ciphertext $\acute{C}_m$;
- $Dec(\acute{C}_m, Sk_a)$: The function inputs are the re-encryption ciphertext $\acute{C}_m$ and a patient private key and the output is the plaintext (m).

4. Experimental Results

We compared the security features of our proposed protocol to [9,10,42]. The results are presented in this section. The proposed protocol in [10] has presented a blockchain paradigm with a secure search using Ethereum smart contracts and a symmetric searchable encryption, as shown in Table 2. This paradigm also hides the original patient identity to protect privacy, but it does not provide the patient with access control. A blockchain concept with ASE is presented in [9]. This study provides an efficient PEKS scheme based on a blockchain resistance KGA problem with secure data sharing and it ensures the authentication via employing the smart contract. However, this solution does not ensure data privacy and does not provide access control mechanisms. Furthermore, this study [49] presents a system for managing a private blockchain based on personal data that is built on Hyperledger Fabric. The proposed system provides fine-grained access control via an access control policy which ensures that any access token expires after a set period of time and must be refreshed. This system can provide pseudo-anonymity for data owners using public-key cryptography as identitiers. However, this system does not provide secure data sharing because it retrieves the requested data from the resource server using the data pointer without encryption. Moreover, because it does not use searchable encryption techniques, it does not prevent the KGA problem. Finally, while the proposed protocol in [42] is comparable to our proposed protocol, which presents a blockchain scheme for sharing EHR using PEKS and PRE to provide access control, secure searching of data, authentication and preserving patient privacy using pseudo-anonymity, it does not address the KGA issue.

The comparison shows that our proposed protocol has more security features than related schemes [9,10,42,49]. It emphasizes the fact that our protocol achieves the maximum desired security properties and is more resistant to KGA than related protocols.

The cryptography primitives are implemented in JavaScript on a PC with an Intel CPU Intel(R) Core (TM) i7-7500U and RAM 8 GB running Windows 10. On Windows 10, Ganache framework is used to create a private test blockchain. Using the Solidity programming language, the data are written into smart contracts and embedded in Ethereum. The smart contracts' test framework is truffle 5.0.5 and the compiler of solidity is solc 0.5.16. The Nodejs Web3js package is applied to connect with blockchain smart contracts and evaluate the execution time (time cost) of the transactions. This is due to the inability of solidity to compute the required time to publish smart contracts to the blockchain. Nodejs is a server-side development platform that allows JavaScript to execute. Table 3 shows the

specific configurations. Figure 4 shows the front-end of the webpage including the patient's address and adding an EHR button to save data by a doctor.

Table 2. Comparison of security properties.

Properties	[10]	[9]	[42]	[49]	Proposed Protocol
Blockchain based	✓	✓	✓	✓	✓
Access control	-	-	✓	✓	✓
Secure search	✓	✓	✓	-	✓
Public key encryption	-	✓	✓	✓	✓
Authentication	✓	✓	✓	✓	✓
Privacy preservation	✓	-	✓	✓	✓
KGA resistance	-	✓	-	-	✓

Table 3. Configurations of Ethereum test blockchain.

Component	Description
Operating system	Windows 10
CPU	Intel(R) Core (TM) i7-7500U CPU @ 2.70 GHz
RAM	8 GB
Program language	Solidity & JavaScript & HTML
Solidity compiler	Solc 0.5.16
Test framework	PTruffle 5.0.5
Interactive platform	Web3 1.0.0-beta.55
Ethereum platform	Ganache v 5.4

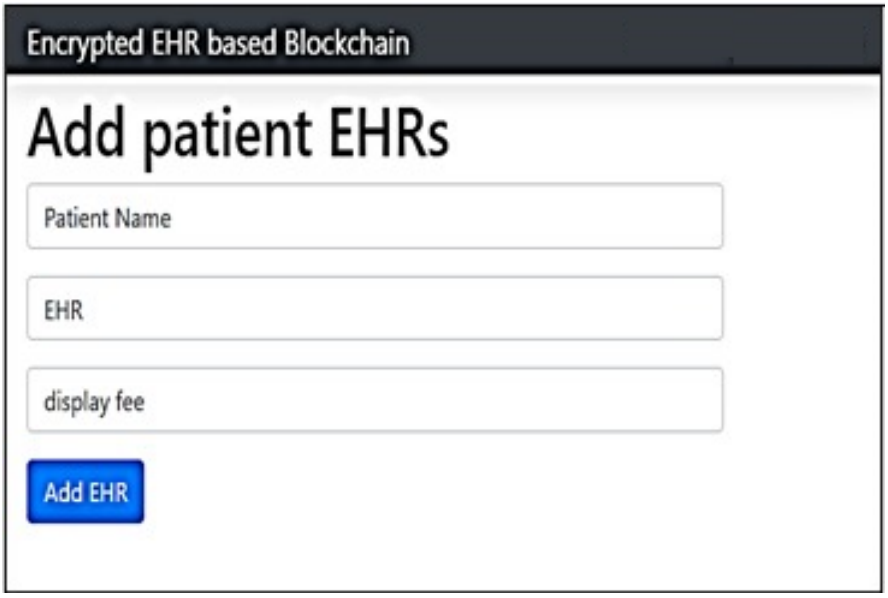

Figure 4. Front-end of our proposed protocol.

In Figure 5, we show the encryption algorithms' computational time in milliseconds with a different record size similar to the results of [31]. We varied the record size from 16 bits, 64 bits, 128 bits, 256 bits, to 512 bits and we measured the time of encrypting and uploading the record to the blockchain. For each record size, we conducted the experiment five times and next took the average of them. We can see that the greater the record size length the more computational time needed. The record size depends on the patient and their information.

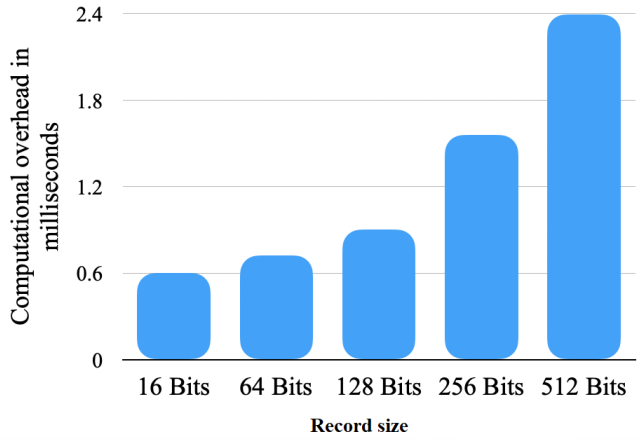

Figure 5. Encryption algorithms' computational time in milliseconds with different record sizes. We vary the record size (16 bits, 64 bits, 128 bits, 256 bits, and 512 bits) and measure the time of encrypting and uploading the record to the blockchain. For each record size, we conduct the experiment 5 times and take the average.

In Figure 6, we give the encryption algorithms' computational time in milliseconds with different records sizes. This time, we varied the key size from 256 bits, 384 bits, to 512 bits and for each size, we measured the time of encrypting and uploading the record to the blockchain. For each record size, we conducted the experiment five times and next took the average. We can deduce that the greater the key size length the longer the computational time is. The key size with a maximum length ensures acceptable protection against attacks but it needs more computational time.

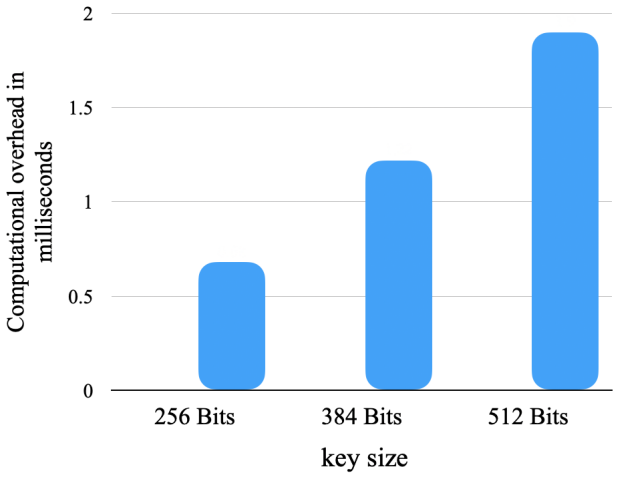

Figure 6. Encryption algorithms' computational time in milliseconds with different key size. We vary the key size (256 bits, 384 bits, and 512 bits) and measure the time for encrypting and uploading the record to the blockchain. For each key size, we conduct the experiment 5 times and next take the average.

Figure 7 outlines the encryption algorithms' gas consumption with different record sizes. We varied the record size (16 bits, 64 bits, 128 bits, 256 bits, and 512 bits) and measured the consumed gas for uploading the record to the blockchain. For each record size, we conducted the experiment 5 times and next took the average. We can notice that there is no big variation of the consumed gas when varying the record size because it is depending on the operation itself. For example, there is a slight augmentation of consumed gas between a record with 256 bits compared to a record with 128 bits. Although the record size is

doubled, we only need $3.72 \cdot 10^{-6}$ more gas. The growth of the record size has an impact on gas consuming similar to the results of [32].

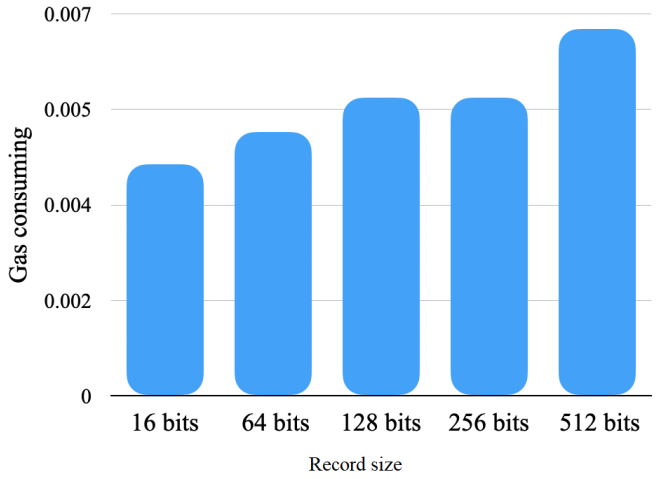

Figure 7. Encryption algorithms' consuming gas in *eth* with different records sizes. We vary the record size (16 bits, 64 bits, 128 bits, 256 bits, and 512 bits) and measure the consumed gas for uploading the record to the blockchain. For each record size, we conduct the experiment 5 times and next take the average.

Finally, Figure 8 shows the encryption algorithms' consuming gas in *eth* with different key size. We varied the key size from 256 bits, 384 bits, to 512 bits and we measured the consumed gas for uploading the record to the blockchain. For each key size, we conducted the experiment five times and next took the average. We can see that there is no effect on the consumed gas. In fact, the record size to be uploaded to the blockchain is still always the same.

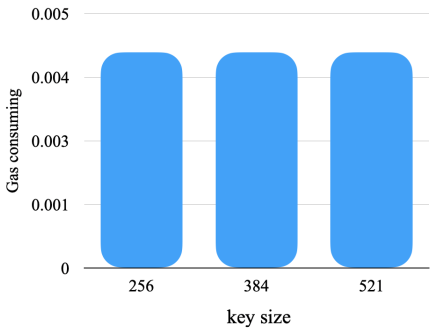

Figure 8. Encryption algorithms' consuming gas in *eth* with different key size. We vary the key size (256 bits, 384 bits, and 512 bits) and measure the consumed gas for uploading the record to the blockchain. For each key size, we conduct the experiment 5 times and next take the average.

5. Discussion

In the previous section, we explored the function, efficiency, and comparative analyses of our protocol to existing work. The characteristics of the implementation section includeprivacy preservation, integrity, secure search, authentication, access control, and KGA defense.

5.1. Our Protocol Ensures EHR Sharing Integrity and Confidentiality

Before sending EHRs to a private blockchain, the doctor encrypts it with the patient's public key, the doctor's public key, and a set of keywords retrieved from the EHR. As a result, without the patient's private key and keywords, the ciphertext cannot be decrypted.

Under the ECDH assumption, the private key is secure. Furthermore, only the institution authorized by the patient has access to the data on the private blockchain. In fact, the system manager uses the public key and keyword of the doctor to construct a re-encryption key. As a result, the ciphertext can only be decrypted by the intended third party, enhancing data confidentiality. Furthermore, each block's signatures ensure data integrity.

5.2. Our Protocol Ensures Access Control

In our proposed protocol, the patient transmits his or her private key along with the keyword as a trapdoor to enable the third party to query the consortium blockchain using smart contracts. It is used to find matched keywords that have been encrypted with the doctor's public key. As a result, the patient has control over the data search. Meanwhile, following each EHR request, the system management produces a re-encryption key and transfers it to a private blockchain for proxy re-encryption. Only an authorized third party can decrypt the re-encrypted ciphertext in this manner. As a result, the patient has control over who can access his or her data.

5.3. The Developed Protocol Ensures Authentication

Different nodes and their legality are distinguished by the EHR consortium blockchain network. The private key of a user and the keyword are used to establish the re-encryption key. The EHR ciphertext that is saved in a selected place and encrypted with the public key of a doctor can only be re-encrypted. Furthermore, a specific ciphertext can only be decrypted by an authorized third party with a patient's private key and keyword.

5.4. The Developed Protocol Ensures Secure Search

In a consortium blockchain based on smart contracts, the keywords and the patient's private key for searching are encrypted by the doctor's public key. For searching the target EHR, the third party must obtain a searching trapdoor from the patient. As a result, other entities cannot see the search keywords or the search result during the third-party search procedure. Meanwhile, even if the attackers obtain the keyword or the patient's private key, they are unable to determine the relationship between the encrypted keyword and the patient's private key.

5.5. The Developed Protocol Ensures Privacy Preservation

A user transmits and receives data by using a blockchain account during the data transmission. The user account in the blockchain is private and cannot be linked to a real person. As a result, blockchain anonymity has the ability to protect public data from revealing an entity's real identity. Furthermore, no information about the patient will be revealed throughout the keyword search procedure. The private blockchain cannot derive the patient's true identity from the EHR's encrypted text and re-encryption key through proxy re-encryption.

5.6. The Developed Protocol Ensures KGA Resistance

As previously mentioned, a set of keywords are required to build the secret trapdoor, and a significant aspect of KGA's success is that the keywords must be selected and embedded in a small space and chosen from well-known phrases for searching purposes. This means that the used number of keywords by the user is limited, and many other terms are considered predetermined. As a result, when the keywords are determined, a user can request her or his frequently used terms from key servers. Our proposed protocol avoids the KGA problem by supporting key renewal on each key server, with secret shares on key servers renewed on a regular basis to prevent key compromise.

6. Conclusions

This paper investigated how to preserve the privacy and security of sharing EHRs on the two types of blockchain networks. The private blockchain is for storing encrypted

EHRs and patients' identities, using a consortium blockchain-based smart contract to store an encrypted index using public-key encryption by implementing an ECDH algorithm with a conjunctive keyword search. We examined the performance of the blockchain-based EHR-sharing protocol in terms of patient access control, integrity, confidentiality, authentication, secure searches, and the index protection from the KGA problem. We examined the proposed protocol with different record sizes and with different key encryption sizes to measure the time computational and gas consumption used. The results show the growth in record length and key size has a significant impact on the encryption algorithm's computational and communication costs. To better understand the benefits and drawbacks of sharing EHRs in the blockchain, we could benefit from using accurate patient data in our research but the high costs of deploying our proposed protocol in a real blockchain environment such as Ethereum constrained our work.

Author Contributions: Conceptualization, T.M.; methodology, M.A.; software, M.A.; validation, M.A.; formal analysis, T.M.; investigation, T.M.; resources, A.A.; data curation, M.A.; writing—original draft preparation, A.A.; writing—review and editing, P.L.; visualization, T.M.; supervision, T.M.; project administration, P.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No used data.

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

References

1. Chaudhary, K.; Kant, U.; Kumar, P. A View on the Blockchain as a Solution to the Healthcare Industry: Challenges and Opportunities. In Proceedings of the International Conference on Computational Intelligence, Security and Internet of Things, Agartala, India, 13–14 December 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 160–169.
2. Hussien, H.M.; Yasin, S.M.; Udzir, N.I.; Zaidan, A.A.; Zaidan, B.B. A Systematic Review for Enabling of Develop a Blockchain Technology in Healthcare Application: Taxonomy, Substantially Analysis, Motivations, Challenges, Recommendations and Future Direction. *J. Medical Syst.* **2019**, *43*, 320:1–320:35. [CrossRef] [PubMed]
3. Jin, H.; Luo, Y.; Li, P.; Mathew, J. A Review of Secure and Privacy-Preserving Medical Data Sharing. *IEEE Access* **2019**, *7*, 61656–61669. [CrossRef]
4. Sidhu, J. Syscoin: A Peer-to-Peer Electronic Cash System with Blockchain-Based Services for E-Business. In Proceedings of the 26th International Conference on Computer Communication and Networks, ICCCN 2017, Vancouver, BC, Canada, 31 July–3 August 2017; pp. 1–6.
5. Chamili, K.; Nordin, M.J.; Ismail, W.; Radman, A. Searchable encryption: a review. *Int. J. Secur. Its Appl.* **2017**, *11*, 79–88. [CrossRef]
6. Chenthara, S.; Ahmed, K.; Wang, H.; Whittaker, F. Security and Privacy-Preserving Challenges of e-Health Solutions in Cloud Computing. *IEEE Access* **2019**, *7*, 74361–74382. [CrossRef]
7. Boneh, D.; Crescenzo, G.D.; Ostrovsky, R.; Persiano, G. Public Key Encryption with Keyword Search. In *Lecture Notes in Computer Science, Proceedings of the Advances in Cryptology—EUROCRYPT 2004, International Conference on the Theory and Applications of Cryptographic Techniques, Interlaken, Switzerland, 2–6 May 2004*; Cachin, C., Camenisch, J., Eds.; Springer: Berlin/Heidelberg, Germany, 2004; Volume 3027, pp. 506–522.
8. Chi, T.; Qin, B.; Zheng, D. An Efficient Searchable Public-Key Authenticated Encryption for Cloud-Assisted Medical Internet of Things. *Wirel. Commun. Mob. Comput.* **2020**, *2020*, 8816172:1–8816172:11. [CrossRef]
9. Zhang, Y.; Xu, C.; Ni, J.; Li, H.; Shen, X.S. Blockchain-Assisted Public-Key Encryption with Keyword Search Against Keyword Guessing Attacks for Cloud Storage. *IEEE Trans. Cloud Comput.* **2021**, *9*, 1335–1348. [CrossRef]
10. Chen, L.; Lee, W.; Chang, C.; Choo, K.R.; Zhang, N. Blockchain based searchable encryption for electronic health record sharing. *Future Gener. Comput. Syst.* **2019**, *95*, 420–429. [CrossRef]
11. 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]
12. Jamoom, E.; Yang, N.; Hing, E. *Adoption of Certified Electronic Health Record Systems and Electronic Information Sharing in Physician Offices: United States, 2013 and 2014*; US Department of Health and Human Services, Centers for Disease Control and Prevention, National Center for Health Statistics: Hyattsville, MD, USA, 2016.

13. Ahmed, M.; Ullah, A.S.B. False data injection attacks in healthcare. In Proceedings of the Australasian Conference on Data Mining, Melbourne, VIC, Australia, 19–20 August 2017; pp. 192–202.
14. Wang, Q.; Su, M. Integrating blockchain technology into the energy sector—From theory of blockchain to research and application of energy blockchain. *Comput. Sci. Rev.* **2020**, *37*, 100275. [CrossRef]
15. Sookhak, M.; Jabbarpour, M.R.; Safa, N.S.; Yu, F.R. Blockchain and smart contract for access control in healthcare: A survey, issues and challenges, and open issues. *J. Netw. Comput. Appl.* **2021**, *178*, 102950. [CrossRef]
16. Androulaki, E.; Barger, A.; Bortnikov, V.; Cachin, C.; Christidis, K.; Caro, A.D.; Enyeart, D.; Ferris, C.; Laventman, G.; Manevich, Y.; et al. Hyperledger fabric: a distributed operating system for permissioned blockchains. In Proceedings of the Thirteenth EuroSys Conference, EuroSys 2018, Porto, Portugal, 23–26 April 2018; Oliveira, R., Felber, P., Hu, Y.C., Eds.; ACM: New York, NY, USA, 2018; pp. 30:1–30:15.
17. Chase, B.; MacBrough, E. Analysis of the XRP Ledger Consensus Protocol. *arXiv* **2018**, arXiv:1802.07242.
18. Raghav, N.; Bhola, A. Blockchain Based Privacy Preservation In Healthcare: A Recent Trends And Challenges. *Psychol. Educ. J.* **2021**, *58*, 5315–5324.
19. Feng, L.; Zhang, H.; Tsai, W.; Sun, S. System architecture for high-performance permissioned blockchains. *Front. Comput. Sci.* **2019**, *13*, 1151–1165. [CrossRef]
20. Zhang, A.; Lin, X. Towards Secure and Privacy-Preserving Data Sharing in e-Health Systems via Consortium Blockchain. *J. Med. Syst.* **2018**, *42*, 140:1–140:18. [CrossRef] [PubMed]
21. Wood, G. Ethereum: A secure decentralised generalised transaction ledger. *Ethereum Proj. Yellow Pap.* **2014**, *151*, 1–32.
22. Andola, N.; Prakash, S.; Venkatesan, S.; Verma, S. SHEMB: A secure approach for healthcare management system using blockchain. In Proceedings of the 2019 IEEE Conference on Information and Communication Technology, Allahabad, India, 6–8 December 2019; pp. 1–6.
23. Zhang, R.; Xue, R.; Liu, L. Searchable Encryption for Healthcare Clouds: A Survey. *IEEE Trans. Serv. Comput.* **2018**, *11*, 978–996. [CrossRef]
24. Alese, B.K.; Philemon, E.; Falaki, S.O. Comparative analysis of public-key encryption schemes. *Int. J. Eng. Technol.* **2012**, *2*, 1552–1568.
25. Byun, J.W.; Rhee, H.S.; Park, H.; Lee, D.H. Off-Line Keyword Guessing Attacks on Recent Keyword Search Schemes over Encrypted Data. In *Lecture Notes in Computer Science, Proceedings of the Secure Data Management, Third VLDB Workshop, SDM 2006, Seoul, Korea, 10–11 September 2006*; Jonker, W., Petkovic, M., Eds.; Springer: Berlin/Heidelberg, Germany, 2006; Volume 4165, pp. 75–83. [CrossRef]
26. Nepal, S.; Ranjan, R.; Choo, K.R. Trustworthy Processing of Healthcare Big Data in Hybrid Clouds. *IEEE Cloud Comput.* **2015**, *2*, 78–84. [CrossRef]
27. Griggs, K.N.; Ossipova, O.; Kohlios, C.P.; Baccarini, A.N.; Howson, E.A.; Hayajneh, T. Healthcare Blockchain System Using Smart Contracts for Secure Automated Remote Patient Monitoring. *J. Med. Syst.* **2018**, *42*, 130:1–130:7. [CrossRef]
28. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On blockchain and its integration with IoT. Challenges and opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
29. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. MedRec: Using Blockchain for Medical Data Access and Permission Management. In Proceedings of the 2nd International Conference on Open and Big Data, OBD 2016, Vienna, Austria, 22–24 August 2016; Awan, I., Younas, M., Eds.; IEEE Computer Society: Washington, DC, USA, 2016; pp. 25–30.
30. Rifi, N.; Rachkidi, E.; Agoulmine, N.; Taher, N.C. Towards using blockchain technology for eHealth data access management. In Proceedings of the 2017 Fourth International Conference on Advances in Biomedical Engineering (ICABME), Beirut, Lebanon, 19–21 October 2017; pp. 1–4.
31. Xue, T.F.; Fu, Q.C.; Wang, C.; Wang, X. A medical data sharing model via blockchain. *Acta Autom. Sin.* **2017**, *43*, 1555–1562.
32. Marbouh, D.; Abbasi, T.; Maasmi, F.; Omar, I.A.; Debe, M.S.; Salah, K.; Jayaraman, R.; Ellahham, S. Blockchain for COVID-19: review, opportunities, and a trusted tracking system. *Arab. J. Sci. Eng.* **2020**, *45*, 9895–9911. [PubMed]
33. Hasan, H.R.; Salah, K.; Jayaraman, R.; Arshad, J.; Yaqoob, I.; Omar, M.A.; Ellahham, S. Blockchain-Based Solution for COVID-19 Digital Medical Passports and Immunity Certificates. *IEEE Access* **2020**, *8*, 222093–222108. [CrossRef] [PubMed]
34. Cai, C.; Yuan, X.; Wang, C. Towards trustworthy and private keyword search in encrypted decentralized storage. In Proceedings of the IEEE International Conference on Communications, ICC 2017, Paris, France, 21–25 May 2017; pp. 1–7.
35. Xiaodong, Y.; Ting, L.; Rui, L.; Meiding, W. Blockchain-based secure and searchable EHR sharing scheme. In Proceedings of the 2019 4th International Conference on Mechanical, Control and Computer Engineering (ICMCCE), Hohhot, China, 24–26 October 2019; pp. 822–8223.
36. Chen, Z.; Wu, A.; Li, Y.; Xing, Q.; Geng, S. Blockchain-Enabled Public Key Encryption with Multi-Keyword Search in Cloud Computing. *Secur. Commun. Netw.* **2021**, *2021*, 6619689:1–6619689:11.
37. Yang, X.; Chen, G.; Wang, M.; Li, T.; Wang, C. Multi-Keyword Certificateless Searchable Public Key Authenticated Encryption Scheme Based on Blockchain. *IEEE Access* **2020**, *8*, 158765–158777.
38. Prasanna, B.; Akki, C. Dynamic Multi-Keyword Ranked Searchable Security Algorithm Using CRSA and B-Tree. *Int. J. Comput. Sci. Inf. Technol.* **2015**, *6*, 826-832.
39. Qin, X.; Huang, Y.; Yang, Z.; Li, X. A Blockchain-based access control scheme with multiple attribute authorities for secure cloud data sharing. *J. Syst. Archit.* **2021**, *112*, 101854.

40. Wang, S.; Zhang, Y.; Zhang, Y. A Blockchain-Based Framework for Data Sharing With Fine-Grained Access Control in Decentralized Storage Systems. *IEEE Access* **2018**, *6*, 38437–38450. [CrossRef]
41. Lin, C.; He, D.; Huang, X.; Choo, K.R.; Vasilakos, A.V. BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0. *J. Netw. Comput. Appl.* **2018**, *116*, 42–52.
42. Shamshad, S.; Rana, M.; Mahmood, K.; Kumari, S.; Chen, C. A secure blockchain-based e-health records storage and sharing scheme. *J. Inf. Secur. Appl.* **2020**, *55*, 102590. [CrossRef]
43. Yang, Y.; Ma, M. Conjunctive Keyword Search With Designated Tester and Timing Enabled Proxy Re-Encryption Function for E-Health Clouds. *IEEE Trans. Inf. Forensics Secur.* **2016**, *11*, 746–759. [CrossRef]
44. Niu, S.; Chen, L.; Liu, W. Attribute-Based Keyword Search Encryption Scheme with Verifiable Ciphertext via Blockchains. In Proceedings of the 2020 IEEE 9th Joint International Information Technology and Artificial Intelligence Conference (ITAIC), Chongqing, China, 11–13 December 2020; Volume 9, pp. 849–853.
45. Niu, S.; Li, W.; Liu, W. Electronic Health Record Data Sharing Cryptographic Algorithm Based on Blockchain. In Proceedings of the International Conference on Artificial Intelligence and Security, Hohhot, China, 19–23 July 2020; Springer: Berlin/Heidelberg, Germany, 2020, pp. 363–375.
46. Wang, Y.; Zhang, A.; Zhang, P.; Wang, H. Cloud-Assisted EHR Sharing with Security and Privacy Preservation via Consortium Blockchain. *IEEE Access* **2019**, *7*, 136704–136719. [CrossRef]
47. Shen, M.; Zhu, L.; Xu, K. *Blockchain: Empowering Secure Data Sharing*; Springer: Berlin/Heidelberg, Germany, 2020.
48. Fan, Y.; Wang, J.; Hong, Z.; Lei, X.; Xia, F.; Ma, J.; Peng, C.; Sun, X. A Blockchain-Based Data-Sharing Architecture. In Proceedings of the International Conference on Blockchain and Trustworthy Systems, Guangzhou, China, 7–8 December 2019; Springer: Berlin/Heidelberg, Germany, 2019; pp. 636–647.
49. Truong, N.B.; Sun, K.; Lee, G.M.; Guo, Y. Gdpr-compliant personal data management: A blockchain-based solution. *IEEE Trans. Inf. Forensics Secur.* **2019**, *15*, 1746–1761. [CrossRef]