applied sciences

MDPI

Article

An Adaptive Biomedical Data Managing Scheme Based on the Blockchain Technique

Ahmed Faeq Hussein [1,*], Abbas K. ALZubaidi [2], Qais Ahmed Habash [1] and Mustafa Musa Jaber [3]

[1] Biomedical Engineering Department, Al-Nahrain University, Baghdad 10072, Iraq; qah@eng.nahrainuniv.edu.iq

[2] Biomedical Engineering Division, University of Saskatchewan, Saskatchewan S7N 5A2, Canada; aba658@mail.usask.ca

[3] Department of Computer Science, Dijlah University College, Baghdad 10072, Iraq; mustafa.musa@duc.edu.iq

* Correspondence: a.f.hussein@eng.nahrainuniv.edu.iq

Received: 10 May 2019; Accepted: 17 June 2019; Published: 19 June 2019

Abstract: A crucial role is played by personal biomedical data when it comes to maintaining proficient access to health records by patients as well as health professionals. However, it is difficult to get a unified view pertaining to health data that have been scattered across various health centers/hospital sections. To be specific, health records are distributed across many places and cannot be integrated easily. In recent years, blockchain has arisen as a promising solution that helps to achieve the sharing of individual biomedical information in a secure way, whilst also having the benefit of privacy preservation because of its immutability. This research puts forward a blockchain-based managing scheme that helps to establish interpretation improvements pertaining to electronic biomedical systems. In this scheme, two blockchains were employed to construct the base, whereby the second blockchain algorithm was used to generate a secure sequence for the hash key that was generated in first blockchain algorithm. This adaptive feature enables the algorithm to use multiple data types and also combines various biomedical images and text records. All data, including keywords, digital records, and the identity of patients, are private key encrypted with a keyword searching function so as to maintain data privacy, access control, and a protected search function. The obtained results, which show a low latency (less than 750 ms) at 400 requests/second, indicate the possibility of its use within several health care units such as hospitals and clinics.

Keywords: blockchain; biomedical data managing; DWT; keyword search; data sharing

1. Introduction

The blockchain can be regarded as a chain of blocks that have already been time-labeled and stay connected by employing encryption features (cryptographic hashes). A block can include the communications of various users, which are publicly offered to all users within the network. Furthermore, each block embraces the hash of the earlier block as well as the traditional transaction data, which results in the generation of an immutable and secured, append-only chain. There is a continuous increase in chain length with the addition of each new block to the end of the chain [1].

The blockchain infrastructure is usually based on a peer-to-peer interaction, wherein both network users (transactions participators) as well as the blockchain "miners" (those that enable communications with a distributed ledger) are involved. The storing of the ledger is done in a decentralized node network, which is generated via cryptographic routes that have been computed by all the miners present in the network [2]. Furthermore, highly reliable storage capabilities are provided by the blockchain ledger since digital signatures, consensus mechanisms, and hash chains are employed for its creation, because of such unconventional features, blockchain technology offers many facilities, including information traceability, security, and non-repudiation, while at the same time keeping all information within a public decentralized way, thus maintaining privacy [3]. Figure 1 depicts the blockchain structure overview.

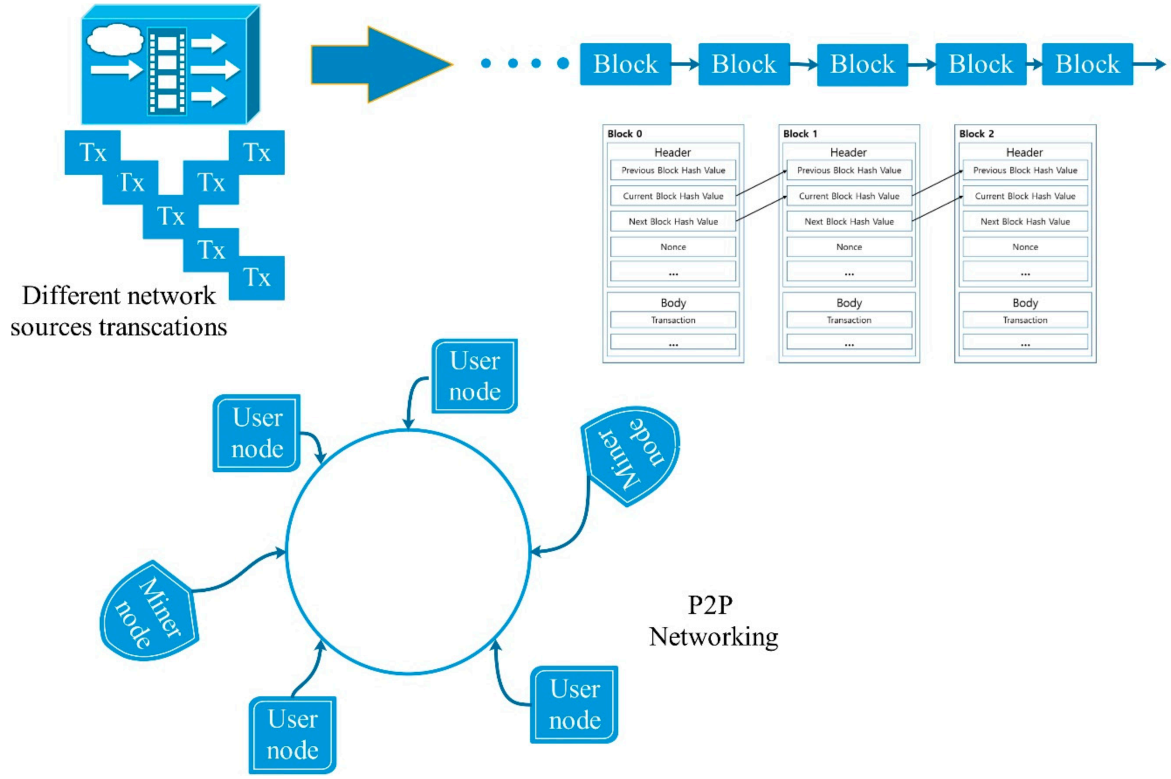


Figure 1. The overview of the blockchain structure.

With regards to the access and management of authorizations, three kinds of blockchains can be considered: Unrestricted, consortium, and private. An unrestricted (or permissionless) blockchain must be highly distributed, wherein any person can contribute via a miner. Even though this warrants maximum immutability, the efficiency is limited because of the collaborative achievement of consensus with the help of the highly extended miner network. While in a private blockchain where miners process blocks for a single organization, efficiency can be maximized and immutability can be altered. A consortium (or federated) blockchain can offer productivity like a private one, while a moderately distributed miner network is integrated, including nodes offered by the nominated organizations [4,5].

The healthcare industry has various unique requirements in terms of privacy and security due to the need for additional legal compliance to safeguard the medical information of patients. In the age of the Internet, where cloud storage as well as the adoption of mobile health devices has facilitated the sharing of data and records, the number of malicious attacks and the possibility of private information becoming compromised during sharing have increased significantly. It has now become easy to obtain health information; patients use smart modules and consult multiple doctors, thus increasing the concerns regarding sharing and secrecy of this information. Furthermore, patients can get their medical history records easily through a widely accessible network without the need to request permission from every provider [6]. Healthcare utilities face the need for unique requirements with regards to interoperability, the transfer of biomedical data, authentication, data sharing, and the considerations regarding e-Health (mobile health) [7].

E-Health refers to the provision of health facilities by employing digital technology. In the e-Health area, research trends have been concentrated on employing electronic health records to perform tasks related to diagnoses and patient monitoring. Typically, a patient may be involved with various providers of healthcare services, including specialists, primary care physicians, and therapists [8]. Thus, in the industry and research community, health record exchanging/sharing has been garnering attention as well as causing concern pertaining to privacy preservation and data security. Recently, the Blockchain technique has been employed in numerous applications to manage and control biomedical information in the internet of medical things (IoMT) for remote and urban areas [9].

For a particular patient, a single disease could be produced by or may be linked to an additional pathema(s). In this case, reliability and interpretation accuracy are based on the patient's supplementary health information provided to the doctor. The doctor may get some information pertaining to the related sickness by asking the patient [10]. However, this process cannot always be deemed as effective for diagnosis for two reasons: i) If events occurred long before, there is a chance that the patient will not remember the details, for example, the medical examinations or medicines he/she had taken at that time, thus potentially impacting the treatment accuracy or diagnosis he/she receives; ii) most patients have limited medical knowledge and fail to describe the diagnosis or treatments they have received professionally, which can impact the current doctor's judgment. Thus, the present physician may fail to deduce precise information when carrying out the diagnosis [11].

To resolve the above-mentioned issues, we have put forward a new scheme for a secure and privacy preserving blockchain within the setting of a hospital/medical care unit. The biomedical data are stored in the private blockchain, which offers benefits in terms of better privacy preservation, a fast transaction, a better security performance, and cost-effectiveness. Moreover, hospitals have been set up in a way that allows for the formulation of a consortium blockchain, which gives the possibility of storing searchable indexes pertaining to data elements. Doctors can easily visit the corresponding hospital's private blockchain to search the consortium blockchain for indexes pertaining to the data of interest as well as having access to original patient records. Moreover, the algorithm has the ability to digest different forms of biomedical data such as images, patient's records, patient's bio-signals, etc. Additionally, the system performance can be increased and make defense against a cyber-attack more robust by employing the adaptive technique for public encryption with keyword search (PEKS) and double key encryption.

2. Literature Review

Over recent years, there has been a peak in interest in the blockchain technique in terms of establishing privacy and security in e-Health because of the associated benefits in data managing, i.e., integrated autonomy and the immutability features of the blockchain.

Q. Xia et al. [12] put forward a framework for data sharing, which is based on blockchain health data sharing to address challenges pertaining to access control for sensitive data stored in the cloud. The system was designed considering a permissioned blockchain, which gives access to those verified users who are invited. Yue et al. [13] also put forward a three-layer system made up of data usage, data storage, and data managing layers. Unlike the aforementioned works in which the cloud is used as the storage infrastructure, this framework suggests that the secluded blockchain can also act as a cloud. In [14], transactions are employed so as to conduct instructions, such as querying, storing, and data sharing. The authors integrated blockchain and off-blockchain storage to develop a private data administration platform focusing on confidentiality. The latest health care/biomedical applications pertaining to blockchain technologies have been studied by Kuo et al. [15]. They also described the potential challenges and proposed solutions that integrate blockchain technologies into the health care/biomedical domains. A new blockchain-based scheme was put forward by Hussein et al. [16] to secure and manage medical records. The proposed algorithm employs the genetic algorithm as well as discrete wavelet transform to increase the security and robustness.

The state-transition functions of the contract are employed to carry out policies, which allow for the imposing of data interchange only for those transactions that are legitimate. Instead of keeping the health record in the block, [17] have added addresses pertaining to mobile devices and sensors to the healthcare blockchain with regards to pervasive social network (PSN) nodes. Similar to the Bitcoin approach, the block employed in [18] consists of a structure based on a Merkle tree. The tree's leaf nodes characterize patient data communications; resources adding to the official patient biomedical data record are also described. However, the actual record document is not included in these transactions, and in its place fast healthcare interoperability resources (FHIR) are referenced via uniform resource locators (URLs). Separate from the above-mentioned works that concentrate on health biomedical data sharing, [19] and [20] have concentrated on various other issues. In [19], a blockchain stage architecture is proposed pertaining to clinical trials and precision medical treatment. This work evaluates a design related to the blockchain podium that is focused on the health field, especially precision medicine and clinical trials. There have been few studies that focus on key management schemes pertaining to the blockchain technique, and [20] made an effort to develop a key discussion with regards to this area. To design a lightweight backup, it employs body sensor networks, which also help to establish an efficient recovery scheme pertaining to keys of the health blockchain. In 2016, a cloud-based electronic health record sharing system was put forward by Liu et al. [21], which supports a fuzzy keyword search. In their search scheme, a medical practitioner (or other user) is allowed to quickly retrieve electronic health records (EHRs) based on the symptoms mentioned in the queried keywords. Implementing the attribute-based encryption (ABE) algorithm also helps to authenticate users with regards to their attributes. Guo et al. [22] proposed an attribute-based encryption for the fine-grained authorization scheme pertaining to a relational database. Recently in 2017, C. Hu and P. Liu [23] put forward a searchable symmetric encryption scheme that was based on blockchain technology, in which blockchain is employed as a peer-to-peer network for storing user data based on a pay-per-use approach. In the decentralized system, each of the users possesses equal status and he/she can request other users to store his/her data through the submission of a transaction. Table 1 shows the summery of the literature review. From this, we found the following observations of interest:

- The value of the various data combinations and data integrity are poorly considered; where most of the previous studies focused on using simulated or even simple individual data in the proposed schemes;
- However, it is vital to replace lost or compromised keys; key management and access control are not strongly focused on or sometimes not even mentioned;
- Most studies focused on the proof of the main concept without using real-world data, i.e., a simulated data type; however, it is essential to use the real-world data for the evaluation of the proposed scheme.

In this study, the proposed scheme was designed to overcome the mentioned challenges and gaps found in previous studies. Therefore, two main databases were used to validate the proposed scheme. Moreover, the use of multiple databases with different data structures combined with traditional biomedical patient's record contributes to improving the effectiveness and achieving the objective of data integrity. On the other hand, the use of two blockchain structures assists the key management process and improves it.

Table 1. The summary of the literature review.

Author	Year	Data	Used Techniques	Annotations	Achievements	Drawbacks
Q. Xia et al. [12]	2017	Closed source (simulated)	N/A	Proposes a blockchain-based framework for data sharing	Permissioned-based cloud blockchain	Simulated case study without keyword search
Yue et al. [13]	2016	Individual entry (no specific database)	Blockchain-Cloud	Proposed an application for purpose-centric access model	Proposes purpose-centric access model that ensures user privacy	Uses a single data type
G. Zyskind et al. [14]	2015	Simulated	Bitcoin	The storage combination of blockchain and off-blockchain storage constructs a personal data management platform focused on privacy	Blockchain-based protocol to automate the access control manager	Uses simulated data
Kuo et al. [15]	2017	Individual entry	Bitcoin	Blockchain feature characteristics	Bitcoin blockchain -based features	Uses few case studies
Hussein et al. [16]	2018	Records from hospital	Ethereum	Modified record management that combines blockchain and a genetic algorithm	Record set managing for each patient	Uses a single data type
J. Zahang et al. [17]	2016	Simulated	Ethereum	Proposes a PSN-based healthcare secure system	Uses two protocols IEEE 802.15.6 with blockchain	Single and simulated data type
K. Peterson et al. [18]	2016	Individual entry	Bitcoin	Proposes an approach based on single centralized source of trust in favor of network consensus	A single centralized source of trust in favor of network consensus	Uses a single data type without adding keyword search
Z. Shae et al. [19]	2017	Individual entry	Bitcoin	Proposes a new blockchain podium architecture based on the general distributed and parallel computing model.	Blockchain application based on parallel processing	Only clinical trial and precision medicine data are managed
H. Zhao [20]	2017	Individual entry	N/A	Proposes a body sensor network employed to design an efficient recovery scheme for blockchain-based health keys	Employs a body sensor network to design a key recovery scheme for the health blockchain	Uses simulated data
Liu et al. [21]	2016	Individual entry	Blockchain-Cloud	Proposes a cloud-based electronic health record system supported by a binary tree utilized to save the records in encrypted form.	Uses a binary tree to save the encrypted health records	The proposed method complexity denoted by searched keyword
Guo et al. [22]	2016	Simulated	Blockchain-Cloud	Proposes the ciphertext-policy attribute-based encryption (CP-ABE) as the structure block in a saved privacy electronic health record system able to work in the attendance of semi-trusted servers	Enables different users with different privileges	Uses simulated data and performs a slower keyword search
C. Hu and P. Liu [23]	2012	Simulated	N/A	Proposes a blockchain based on a public-key encryption scheme with a designated tester (dPEKS)	Decryptable searchable public key encryption with a designated tester	Limits when applied to images (needs longer encrypting latency)

3. Background

3.1. The Blockchain

The blockchain can be explained as a scattered database, which also includes an ordered records list, which are linked via a continuous chain of blocks [24]. Normally, a block includes the encrypted key (hash value) of the earlier block, contributor signature, payload, and timestamp. The hash value from the earlier block imparts immutability from modification to the blockchain. The block's payload changes with the application. For original data, it can be an address pointer or some other information or the content pertaining to the transaction. The generator and generation time pertaining to the block is demonstrated by the contributor signature and timestamp. Two important entities are involved in the blockchain network: Verifiers and miners. Miners signify the nodes that can create new blocks pertaining to the blockchain. Various scenarios can define diverse node types as miners. For instance, in the Bitcoin blockchain, the nodes showing proof of work are allocated as miners to maintain records pertaining to the transactions. The acceptance of new blocks is done only when verifiers confirm the validity of the new blocks. Mining can be defined as a set of processes involving verifying, generating, and accumulating new blocks into the blockchain. In the blockchain network, the consensus mechanism is crucial for ensuring the reliability and security of the mining processes. It helps to determine who is responsible for keeping records and how the new block's validity can be checked. Since blockchain technology was originally employed for Bitcoin, transactions are broadly employed in the network to showcase new produced data. In our study, all transactions signify the secured indexes pertaining to the new emerging health records in the system. In general, blockchain technology can be divided into three groups: Private blockchain, permissionless blockchain (public blockchain), and consortium blockchain. In a permissionless blockchain, anybody from any part of the world can enter into the system, which allows access to data and the sending of transactions—for instance, the Bitcoin system. In a remote blockchain, the entry right is fully controlled by an organization. The management of a consortium blockchain is done by various organizations. With regards to our work, we have utilized the consortium blockchain and private blockchain in the e-Health system for managing and storing patient's records, which aid in enhancing the diagnosis process.

3.2. Keyword Search

Boneh et al. [25] proposed the public encryption with keyword search (PEKS) to perform searches with encrypted data maintained in asymmetric settings. Normally, from a message m, extraction of a keyword w is done. The keyword is encrypted with a public key and a trapdoor is employed for the search, which is produced by the unit that corresponds to the public key.

PEKS consists of four polynomial time randomized algorithms; KeyGen (λ), PEKS (pki, w), Trapdoor (ski, w′), and Test (pki, cw, Tw).

Afterwards, different keyword search algorithms were suggested to offer diverse searching functionality by integrating PEKS with other cryptographic primitives. PEKS schemes with a designed tester have been proposed to improve the search security [26,27]. When integrated with proxy re-encryption [28], the mechanisms of the keyword search allow a delegate to search for keywords of interest from the data of the delegator. In [26], to resolve the user privacy issue, keyword searches along with oblivious transfers were introduced. The data supplier is stopped from knowing the selected keywords as well as the corresponding cipher text due to the oblivious keyword search. Some applications need to search more than one keyword. The works of [27,28] demonstrate the public encryption key used with a conjunctive field keyword.

In this study, to achieve the needed security objectives, the cited PEKS schemes can be mixed together as explained. The use of multiple schemes enhances the keyword searching function, especially in multiple blockchain networks where the search requires longer periods.

3.3. Discrete Wavelet Transform

As is mentioned in the introduction, one of the essential objectives is to unify various patients' data (text records with images) into a single scheme; during this, it is important to efficiently use the available resources and maintain the security. Biomedical images can be very large, making it difficult to fit them inside the scheme structure. To resolve this problem, biomedical image segmentation, involving discrete wavelet transform (DWT), was done. DWT was used to reduce the image distortion that might have occurred during the segmentation process. This procedure converts bigger images into smaller, more manageable portions [29].

It is important to develop input images that function with the generated data chains. The DWT can be defined as a mathematical model to perform multi-resolution analysis [30]. A common method to perform spatial frequency analysis is the wavelet transform. Equation (1) [31] presents the 1D continuous wavelet transform (CWT).

$$CW(a,b) = \frac{1}{\sqrt{a}} \int y(t)\ \varphi\left(\frac{t-b}{a}\right), \tag{1}$$

where $y(t)$ represents the input signal and φ defines the wavelet function; a denotes the scaling parameter and b signifies the translation parameter. The base functions pertaining to a DWT were captured with the help of sampling from CWT. Equation 2 demonstrates the $\varphi_{j,\,k}(t)$ function.

$$\varphi_{j,\,k}(t) = 2^{-\frac{n}{2}}\varphi(2^{-n}t - m). \tag{2}$$

1D wavelet transform was employed to derive 2D DWT by applying filters in columns and rows. The images were segmented by 2D CWT into four diverse sub-bands i.e., LH, LL, HH, and HL. Every sub-band signifies an image, with estimated horizontal, vertical, and diagonal details, correspondingly.

4. Materials and Methods

The computer clients and hospital servers are considered as being semi-trusted. They are deemed as being trustworthy when performing the protocol but not so when it comes to accessing or deducing the health information of a patient without proper authorization. In the public channel, there is a chance that outsider attackers could eavesdrop or interfere with the transmissions, such as encrypted patients data, secure indexes, and trapdoors. The computer clients are prohibited from colluding with the server that would allow them to infer the user's real identity [32,33].

In this study, we aimed to achieve these main contributions: Access control as well as security issues. Since the record of the patient is a secrecy sensitive issue, it is crucial to maintain data refuge, including data auditing, data integrity and confidentiality, and access control. Normally, encryption and signatures ensure data integrity and confidentiality. It is crucial to maintain access control and data auditability to guarantee the monitoring of all data access activities under data generators (hospitals) and data owners (patients). These things can be achieved by employing cryptographic primitives via authentication, identification, and authorization.

Even though privacy preservation can be established partly through access control and data confidentiality, in e-Health systems, a user's identity can also leak certain privacy-sensitive information. Thus, it is crucial to keep the identity information of the user secret. In general, it is important to establish unlinkability and anonymity to achieve identity privacy. Herein, unlinkability refers to the condition in which eavesdroppers cannot judge if two or more flows of records originate from the same source. In the proposed system, a patient authorizes the doctor to access his/her history records to enhance the diagnosis. In this process, the desirable content can only be accessed by the authorized doctor. The eavesdroppers fail to deduce the keywords while the physician also looks out for pseudo-identities.

4.1. Used Datasets

In this study, two main databases were used to validate the proposed scheme. The first database contained various collections of magnetic resonance (MR) images with individual information gathered from healthy cases and patient cases. This database is available on brain-development.org/ixi-dataset/ [34]. Each case in this database was well documented and explained, and could be found as an attachment. It was used to test our proposed algorithm, which was designed to accept various data types because of this. Another common data type in hospitals and healthcare units is microscopic histological images. In this study, the images from www.microscopyu.com/galleries/pathology were employed to validate the proposed scheme [35]. Most patient's records were from these data types, consequently, using them was very helpful to improve and get high detection accuracy.

4.2. Image Segmentation

The proposed image segmentation method shown in Figure 2 was based on a previous study [36]. Wavelet analysis was employed for the extraction of the original image as well as data fusion. Initially, various image modalities were segmented into four different channels, i.e., low horizontal and low vertical (LL1), while the detailed images included low horizontal and high vertical (LH1), high horizontal and low vertical (HL1), and high horizontal and high vertical (HH1) frequencies. In the second stage, every channel (segment) would be sub-segmented into four new channels, namely: HL2, LL2, HH1, and LH1 [37]. This procedure continued for two more levels. Finally, the original image was sub-divided into small image groups as follows:

$$R_{i,j} = \begin{bmatrix} LL4 & \cdots & HL1 \\ \vdots & \ddots & \vdots \\ LH4 & \cdots & HH1 \end{bmatrix} \tag{3}$$

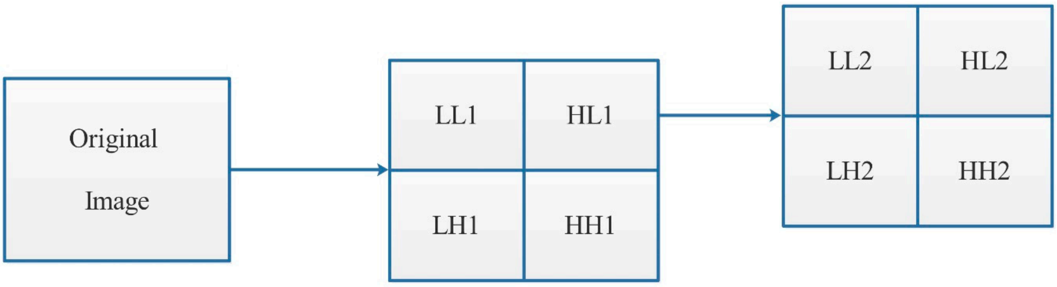


Figure 2. The image segmentation proposed method.

4.3. General Description of the Proposed Scheme Design

The blockchain architecture that forms the central part of our proposed scheme is described in Figure 3. It mainly consists of a consortium blockchain and private blockchain. The central part represents the private blockchain while the boundary represents the consortium blockchain. The centre is the core chain, composed of the scheme supervisor, these members are responsible for giving authority to any new user located inside the outer or consortium blockchain.

This chain is open for any user who needs to provide detection and evidence services to join as a member node. The link nodes have the ability to communicate over a peer-to-peer network. The network (consortium blockchain) has the features of decentration and active change, which include the ways of networking and the communication mechanisms between nodes. The central nodes are located inside the private blockchain, while the other nodes can freely join or exit the consortium network. The information is sent from each node to its neighbor node, then the neighbor node forwards the received information to its own neighbor node. Through this technique, the information increasingly spreads throughout the network. The node first directs its own block mark (like an ID) to the neighbor node. If the neighbor node's mark is less than the first node's, the block needs to obtain the missing information. If the neighbor node mark is higher, the neighbor node receives the reverse block information. As a result, all nodes continuously exchange block information with their neighbor nodes.

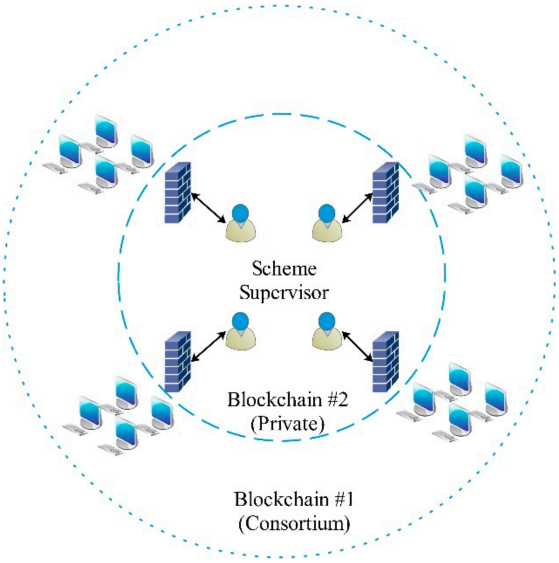


Figure 3. The proposed blockchain architecture.

The proposed scheme design is shown in Figure 4. In this design, security issues are resolved using a new technique. In this technique, we employed the blockchain twice, the second blockchain algorithm was used to generate a secure sequence for the hash key generated in first blockchain algorithm. This means that the generated hash keys were double encrypted, thus improving the security index. Moreover, modifications in block structure were prepared, and new sections were added to fulfill the scheme adaptivity for various data types.

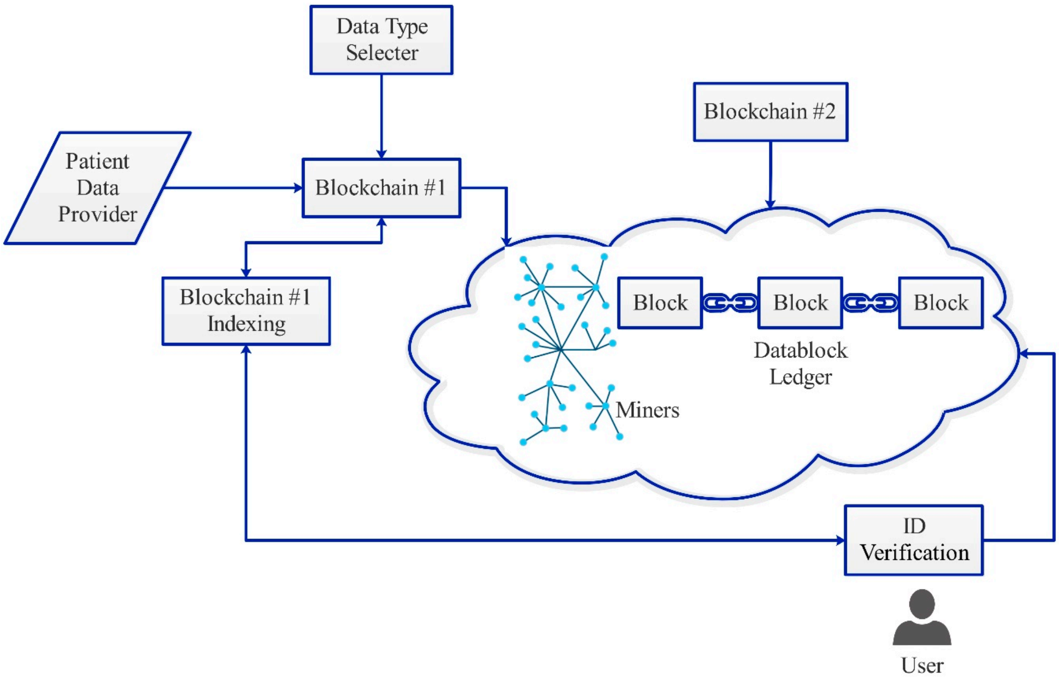


Figure 4. The proposed scheme structure.

Figure 5 shows the proposed block structure. It contains two main parts: The block header and system payload. The block header consists of the block index, time stamp, previous block hash, next block hash, and nonce. The system payload consists of the encryption type, record type information, patient ID, and system data. Note that the information (of any data type) is stored inside the system data section on the system payload, and the other parts are used to form the security barrier that isolates the patient's information. There are three entities in the system: Scheme supervisor, scheme facility providers or hospitals, and operators (patients).

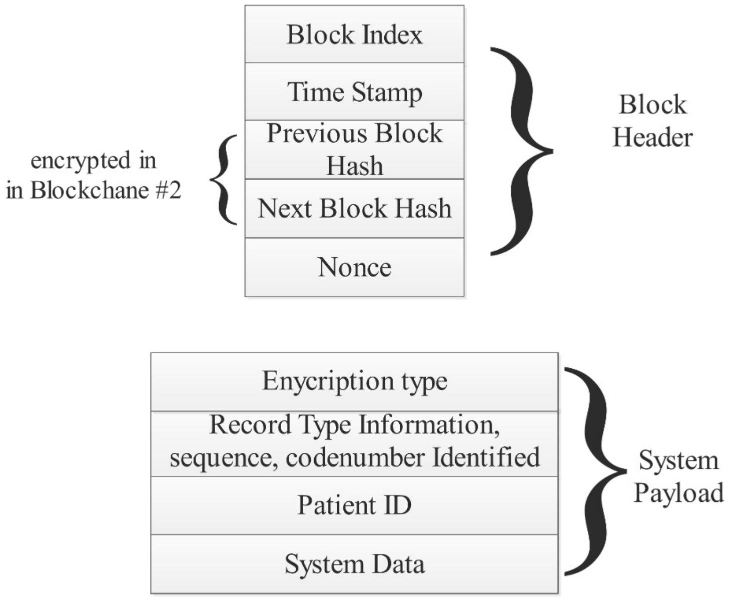


Figure 5. The used block structure.

Scheme supervisor: The entire system is supervised by the system manager. It is necessary that all the doctors and patients register with the system manager. This produces system bounds and maintains a public key tree for patients and doctors. Scheme facility providers: Medical service providers can be defined as medical institutions that offer medical services for the users. Typically, each hospital includes a server and numerous computer clients. A doctor commands each computer client to record health information of their respective patients. Then, the clients produce blocks pertaining to the patients' health records and subsequently transmit the information to the hospital's private blockchain. Furthermore, the nominated computer client also verifies the new incoming blocks. The server is also involved in the registration of the users by maintaining a register table for the doctors and users. It also assumes the responsibility of collecting new blocks within the private blockchain at specific intervals and the formulation of new blocks pertaining to the consortium blockchain. In addition, the chosen server is responsible for confirming new blocks within the consortium blockchain. Notably, the doctors who are outside the private blockchain are authenticated by the server so as to allow them to access users in the private blockchain. Operators: Users can refer to those beneficiaries (doctors and patients) who visit the hospitals to avail or offer services. They should register on the hospital server prior to visiting the doctor. After registration, each patient receives a token from the server. The patient should not disclose anything about the token and only show it to the doctor when visiting. The beacon serves as evidence related to the interaction between the patient and the doctor, providing authorization for the doctor who is generating the record for the patient. The obtained record is then stored within the hospital's private blockchains. For the doctors, they could also offer computer clients. Consequently, the development of the consortium blockchain and private blockchain can be achieved with the existing infrastructures in the hospitals without the need to add more instruments. Notably, the installation of software on the hospital servers and computers is enough to establish a consortium blockchain and private blockchain.

The system was constructed from a polynomial based sequence. Assume $P = \{p_1, p_2, \ldots, p_n\}$ with size n. It is expressed by computing $K_1(p_1), K_1(p_2), \ldots, K_1(p_n)$ and a polynomial is constructed as follows:

$$k_i = K_1(p_i),\ (K_1(p_i))^2,\ \ldots,\ (K_1(p_i))^{n-1},\ (K_1(p_i))^n. \tag{4}$$

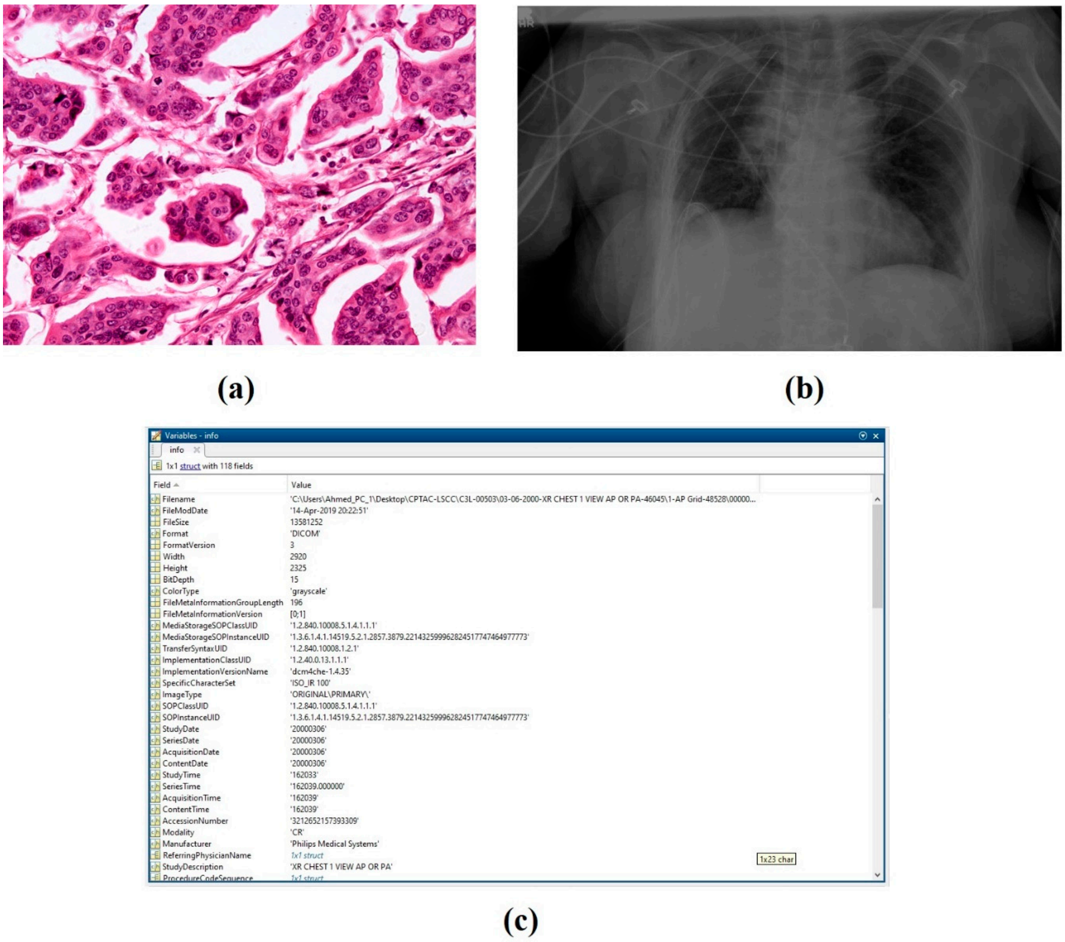
The scheme algorithm is expressed as follows:

```
Scheme algorithm
Input: Various data types
Output: Blockchain series

1.  The data type selection is made by doctor (physician)
2.  If data type is text → step 7
3.  Do
4.  Image segmentation process
5.  Wavelet coefficients computation $CW(a, b)$, $\varphi_{j,\,k}(t)$
6.  Initiate image matrix vector $R_{i,j}$
7.  Initiate the data vector $k_i$
8.  Generate the hash keys for Blockchain#1
9.  Indexing the Blockchain#1 requests
10. Generate the Blockchain#2 hash keys
11. While $i$
12. Output: Blockchain series based on data input
```

5. Results

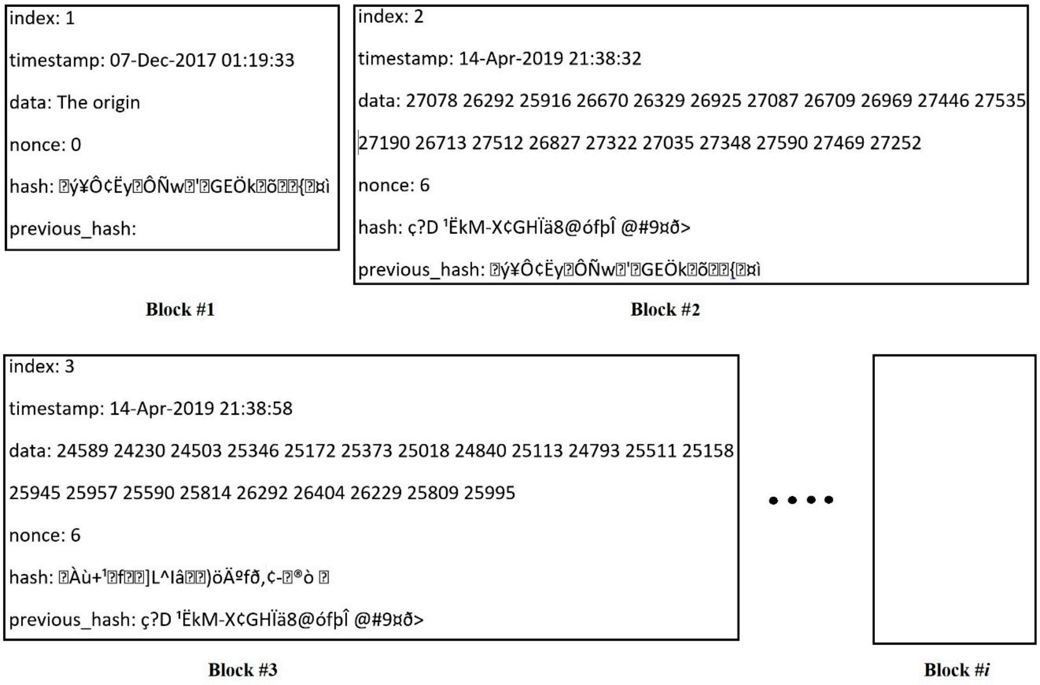
In this study, 1749 images and 859 patients' records were used to verify the scheme algorithm activity. An eight computer combination was set up to act as a hospital network; three of them were core I5 CPU, 8 Gbyte RAM, while the others were core I3 CPU, 8 Gbyte RAM. The PCs were located in different places within the same building and connected within the same backbone. The blockchain environment was achieved using Octave software under the Ubuntu 16.04 operating system. Figure 6 shows the types of data that are most frequently used in hospitals (microscopic histological images, magnetic resonance imaging (MRI) images, and patient descriptive records). The operation process ran for 210 hours continuously receiving different requests from different users. Figure 7 shows the generated blocks with data content, showing the image data after segmenting and inserting into generated blocks. The acquiring time for requesting and searching a certain patient record is depicted in Figure 8, the selection of the requested number started at 50 request/second and increased gradually to 400 request/second where it was limited by the number of PCs. The response latency increased gradually with the increase in the request number. This is normal because of the extra functions needed in each transaction. It can be seen that when the requests were about 200, the total latency was below 100 ms. However, it became 750 ms when the number of requests reached 400. The increment ratio is acceptable when compared with the complexity of the implemented system (linking between two blockchains). The system scalability was maintained and depended upon the number of private miner nodes. On the basis of the obtained results, it was established that the suggested algorithm solution performs a very good paring regarding the distribution of the other nodes that were linked to them. As the Chord algorithm offers access to nodes pertaining to replicated content, it also enables peers to access other nodes with replicated data regardless of persisting communication issues in a few of the nodes. As a result of this, our solution's overall operation was not hindered. Table 2 shows the average resource usage of the entire designed network. It can be seen from Table 2 that more memory would be recommended for when the physical memory modules are fully loaded. This can be expected in cases where biomedical images (such as DICOM images) occupy a large amount of space. Even though the location address was provided, replications pertaining to these files in the blockchain were not anticipated.



1x1 struct with 118 fields

Field	Value
Filename	'C:\Users\Ahmed_PC_1\Desktop\CPTAC-LSCC\C3L-00503\03-06-2000-XR CHEST 1 VIEW AP OR PA-46045\1-AP Grid-48528\00000...
FileModDate	'14-Apr-2019 20:22:51'
FileSize	13581252
Format	'DICOM'
FormatVersion	3
Width	2920
Height	2325
BitDepth	15
ColorType	'grayscale'
FileMetaInformationGroupLength	196
FileMetaInformationVersion	[0;1]
MediaStorageSOPClassUID	'1.2.840.10008.5.1.4.1.1.1'
MediaStorageSOPInstanceUID	'1.3.6.1.4.1.14519.5.2.1.2857.3879.221432599962824517747464977773'
TransferSyntaxUID	'1.2.840.10008.1.2.1'
ImplementationClassUID	'1.2.40.0.13.1.1.1'
ImplementationVersionName	'dcm4che-1.4.35'
SpecificCharacterSet	'ISO_IR 100'
ImageType	'ORIGINAL\PRIMARY\'
SOPClassUID	'1.2.840.10008.5.1.4.1.1.1'
SOPInstanceUID	'1.3.6.1.4.1.14519.5.2.1.2857.3879.221432599962824517747464977773'
StudyDate	'20000306'
SeriesDate	'20000306'
AcquisitionDate	'20000306'
ContentDate	'20000306'
StudyTime	'162033'
SeriesTime	'162039.000000'
AcquisitionTime	'162039'
ContentTime	'162039'
AccessionNumber	'3212652157393309'
Modality	'CR'
Manufacturer	'Philips Medical Systems'
ReferringPhysicianName	*1x1 struct*
StudyDescription	'XR CHEST 1 VIEW AP OR PA'
ProcedureCodeSequence	*1x1 struct*

Figure 6. The original data used. (**a**) Pathological microscope images; (**b**) MRI images; (**c**) digital patient records.



index: 1

timestamp: 07-Dec-2017 01:19:33

data: The origin

nonce: 0

hash: ⍰ý¥Ô¢Ëy⍰ÔÑw⍰'⍰GEÖk⍰õ⍰⍰{⍰¤ì

previous_hash:

Block #1

index: 2

timestamp: 14-Apr-2019 21:38:32

data: 27078 26292 25916 26670 26329 26925 27087 26709 26969 27446 27535 27190 26713 27512 26827 27322 27035 27348 27590 27469 27252

nonce: 6

hash: ç?D ¹ËkM-X¢GHÏä8@ófþÎ @#9¤ð>

previous_hash: ⍰ý¥Ô¢Ëy⍰ÔÑw⍰'⍰GEÖk⍰õ⍰⍰{⍰¤ì

Block #2

index: 3

timestamp: 14-Apr-2019 21:38:58

data: 24589 24230 24503 25346 25172 25373 25018 24840 25113 24793 25511 25158 25945 25957 25590 25814 26292 26404 26229 25809 25995

nonce: 6

hash: ⍰Àù+¹⍰f⍰⍰]L^Iâ⍰⍰)öÄºfð,¢-⍰®ò ⍰

previous_hash: ç?D ¹ËkM-X¢GHÏä8@ófþÎ @#9¤ð>

Block #3

Block #*i*

Figure 7. The generated blockchain.

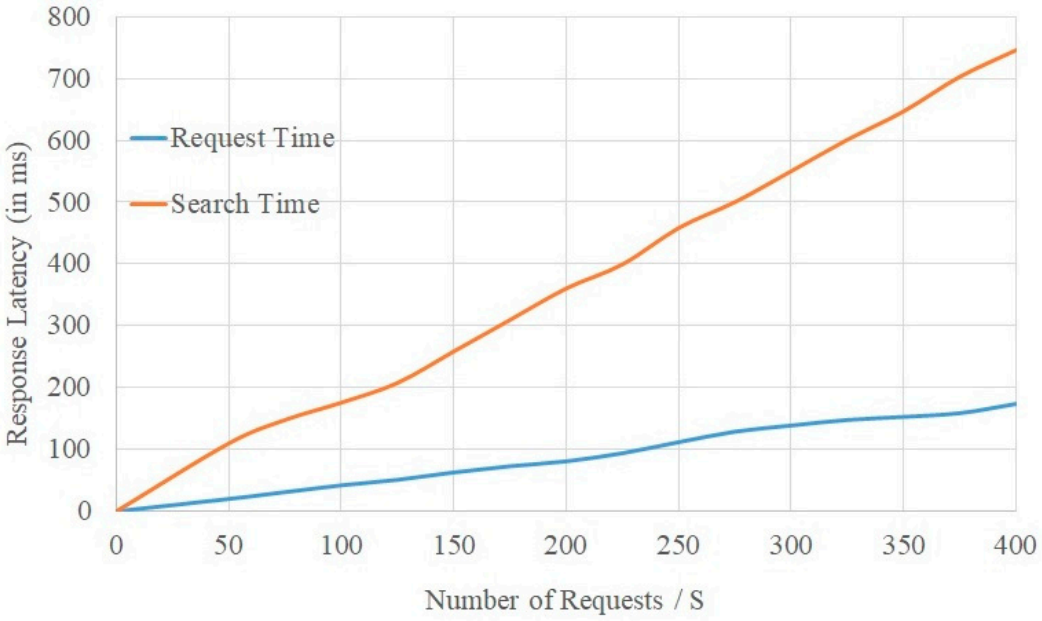


Figure 8. The proposed scheme latency test.

Table 2. Network resource monitoring.

Pc Item	Resource Usage %
CPUs	27–39%
Memory (physical)	90–98%
Memory (virtual / page file)	50–78%
Network throughput	7 MB/s
HDD throughput	9 MB/s

To validate the scheme robustness, the publishing time cost of a transaction (blockchain publishing transactions) was calculated. We initially calculated the size of the transactions in the blockchain, which were by 128 bytes for the private blockchain and 512 bytes for the consortium blockchain. We then set the number of transaction for different cases as n = 500, 1000, 1500, and 2000 to study the scheme under various payloads.

Table 3 depicts the statistical analysis for publishing time cost (transactions). In the table, the average time cost changed slightly with the transaction numbers for both the private and consortium blockchain. However, this difference increased at higher transaction numbers. The reasons for this can be explained by studying the transaction publishing procedure. It includes stuffing the transaction into a package, signing the package, and distributing it. After being confirmed by the other nodes, the transaction is accepted and added to the chain. For each transaction, these steps yield a basic time cost, which is varying for each case. The time cost rises gradually with the progress of the package where the signature time cost, transmission, and confirmation procedures rise with the package length. This result confirms that the setting of keyword size should not be too large to control the transaction efficiency and achieve the availability of the system.

Table 3. The publishing time cost.

Blockchain	Private				Consortium			
	n = 500	n = 1000	n = 1500	n = 2000	n = 500	n = 1000	n = 1500	n = 2000
Max. time (ms)	2589	5124	7751	9985	2848	5636	9604	12183
Min. time (ms)	1987	2104	2360	3047	2186	2314	4620	4413
Average time (ms)	2154	4851	6980	8742	2369	5336	8748	10791

6. Conclusions

The main aim of this study was to provide a state-of-the-art solution for managing different biomedical data types in a scheme that improves data integrity and makes the working system more reliable and adaptable. Such a scheme must be evaluated and tested under real-environment conditions, as biomedical data is an extremely sensitive issue.

In this study, a new scheme for managing biomedical data was presented. Two blockchains were employed to improve the system security and increase the overall stability. Furthermore, the combination of various data types contributed to an overall reduction in system costs whilst also improving the searching and processing time. To validate the data integrity, two real databases with a traditional hospital patients' record were employed. Moreover, for the blockchains, the conformance proof could be well defined and planned as an accord mechanism wherein authenticated blocks were constructed. With regards to the blockchains, public key encryption with a keyword search was proposed for the records sharing protocol. After receiving hatches from the patient, the authorization of the physician was completed allowing access to the desirable biomedical records, thus enhancing their diagnosis ability. The obtained results indicated that the scheme was fast, had the ability to work under dense payloads, and thus performed well enough to be used within a large hospital environment.

For potential future work, the proposed technique is promising in respect to improving the security of the Internet of Things' (IoT) connections. It has the ability to work with a fast response rate and a low latency. The specialized blockchain features (decentralized, integrity, and anonymity) can further be used as an optimum security solution.

Author Contributions: Conceptualization, A.F.H.; Formal analysis, A.K.A.; Investigation, A.K.A. and Q.A.H.; Methodology, A.F.H.; Resources, M.M.J.; Software, Q.A.H. and M.M.J.; Writing—review & editing, A.F.H. and A.K.A.

Funding: This research received no external funding.

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

References

1. Sikorski, J.J.; Haughton, J.; Kraft, M. Blockchain technology in the chemical industry: Machine-to-machine electricity market. *Appl. Energy* **2017**, *195*, 234–246. [CrossRef]
2. Hölbl, M.; Kompara, M.; Kamišalić, A.; Nemec Zlatolas, L. A systematic review of the use of blockchain in healthcare. *Symmetry* **2018**, *10*, 470. [CrossRef]
3. Zhang, A.; Lin, X. Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain. *J. Med. Syst.* **2018**, *42*, 140. [CrossRef] [PubMed]
4. Bozic, N.; Pujolle, G.; Secci, S. A tutorial on blockchain and applications to secure network control-planes. In Proceedings of the 2016 3rd Smart Cloud Networks & Systems (SCNS), Dubai, UAE, 19–21 December 2016; pp. 1–8.
5. Truby, J. Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies. *Energy Res. Soc. Sci.* **2018**, *44*, 399–410. [CrossRef]
6. Zhang, P.; Schmidt, D.C.; White, J.; Lenz, G. Blockchain technology use cases in healthcare. In *Advances in Computers*; Elsevier: Amsterdam, The Netherlands, 2018; Volume 111, pp. 1–41.
7. Uddin, M.A.; Stranieri, A.; Gondal, I.; Balasubramanian, V. Continuous patient monitoring with a patient centric agent: A block architecture. *IEEE Access* **2018**, *6*, 32700–32726. [CrossRef]
8. Ali, M.; Khan, S.U.; Vasilakos, A.V. Security in cloud computing: Opportunities and challenges. *Inf. Sci.* **2015**, *305*, 357–383. [CrossRef]
9. Khezr, S.; Moniruzzaman, M.; Yassine, A.; Benlamri, R.J.A.S. Blockchain Technology in Healthcare: A Comprehensive Review and Directions for Future Research. *Appl. Sci.* **2019**, *9*, 1736. [CrossRef]
10. Calabrese, B.; Cannataro, M. Cloud computing in healthcare and biomedicine. *Scalable Comput. Pract. Exp.* **2015**, *16*, 1–18. [CrossRef]

11. Jiang, Q.; Khan, M.K.; Lu, X.; Ma, J.; He, D. A privacy preserving three-factor authentication protocol for e-Health clouds. *J. Supercomput.* **2016**, *72*, 3826–3849. [CrossRef]
12. Xia, Q.; Sifah, E.; Smahi, A.; Amofa, S.; Zhang, X. BBDS: Blockchain-based data sharing for electronic medical records in cloud environments. *Information* **2017**, *8*, 44. [CrossRef]
13. Yue, X.; Wang, H.; Jin, D.; Li, M.; Jiang, W. Healthcare data gateways: Found healthcare intelligence on blockchain with novel privacy risk control. *J. Med. Syst.* **2016**, *40*, 218. [CrossRef] [PubMed]
14. Zyskind, G.; Nathan, O. Decentralizing privacy: Using blockchain to protect personal data. In Proceedings of the 2015 IEEE Security and Privacy Workshops, San Jose, CA, USA, 18–20 May 2015; pp. 180–184.
15. Kuo, T.-T.; Kim, H.-E.; Ohno-Machado, L. Blockchain distributed ledger technologies for biomedical and health care applications. *J. Am. Med. Inform. Assoc.* **2017**, *24*, 1211–1220. [CrossRef] [PubMed]
16. Hussein, A.F.; ArunKumar, N.; Ramirez-Gonzalez, G.; Abdulhay, E.; Tavares, J.M.R.; de Albuquerque, V.H.C. A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform. *Cogn. Syst. Res.* **2018**, *52*, 1–11. [CrossRef]
17. Zhang, J.; Xue, N.; Huang, X. A secure system for pervasive social network-based healthcare. *IEEE Access* **2016**, *4*, 9239–9250. [CrossRef]
18. Peterson, K.; Deeduvanu, R.; Kanjamala, P.; Boles, K. A blockchain-based approach to health information exchange networks. *Proc. NIST Workshop Blockchain Healthc.* **2016**, *1*, 1–10.
19. Shae, Z.; Tsai, J.J. On the design of a blockchain platform for clinical trial and precision medicine. In Proceedings of the 2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS), Atlanta, GA, USA, 5–8 June 2017; pp. 1972–1980.
20. Zhao, H.; Zhang, Y.; Peng, Y.; Xu, R. Lightweight backup and efficient recovery scheme for health blockchain keys. In Proceedings of the 2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS), Bangkok, Thailand, 22–24 March 2017; pp. 229–234.
21. Liu, Z.; Weng, J.; Li, J.; Yang, J.; Fu, C.; Jia, C. Cloud-based electronic health record system supporting fuzzy keyword search. *Soft Comput.* **2016**, *20*, 3243–3255. [CrossRef]
22. Guo, C.; Zhuang, R.; Jie, Y.; Ren, Y.; Wu, T.; Choo, K.-K.R. Fine-grained database field search using attribute-based encryption for e-healthcare clouds. *J. Med. Syst.* **2016**, *40*, 235. [CrossRef]
23. Hu, C.; Liu, P. An enhanced searchable public key encryption scheme with a designated tester and its extensions. *J. Comput.* **2012**, *7*, 716–723. [CrossRef]
24. Esposito, C.; De Santis, A.; Tortora, G.; Chang, H.; Choo, K.-K.R. Blockchain: A panacea for healthcare cloud-based data security and privacy? *IEEE Cloud Comput.* **2018**, *5*, 31–37. [CrossRef]
25. Baek, J.; Safavi-Naini, R.; Susilo, W. Public key encryption with keyword search revisited. In Proceedings of the International conference on Computational Science and Its Applications, Perugia, Italy, 30 June–3 July 2008; pp. 1249–1259.
26. Zhu, L.; Wu, Y.; Gai, K.; Choo, K.-K.R. Controllable and trustworthy blockchain-based cloud data management. *Future Gener. Comput. Syst.* **2019**, *91*, 527–535. [CrossRef]
27. 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]
28. Shao, J.; Cao, Z.; Liang, X.; Lin, H. Proxy re-encryption with keyword search. *Inf. Sci.* **2010**, *180*, 2576–2587. [CrossRef]
29. Vijayarajan, R.; Muttan, S. Discrete wavelet transform based principal component averaging fusion for medical images. *Aeu-Int. J. Electron. Commun.* **2015**, *69*, 896–902. [CrossRef]
30. Addison, P.S. *The Illustrated Wavelet Transform Handbook: Introductory Theory and Applications in Science, Engineering, Medicine and Finance*; CRC Press: Boca Raton, FL, USA, 2017.
31. Hussein, A.F.; Hashim, S.J.; Aziz, A.F.A.; Rokhani, F.Z.; Adnan, W.A.W. Performance evaluation of time-frequency distributions for ECG signal analysis. *J. Med. Syst.* **2018**, *42*, 15. [CrossRef] [PubMed]
32. Azaria, A.; Ekblaw, A.; Vieira, T.; Lippman, A. Medrec: Using blockchain for medical data access and permission management. In Proceedings of the 2016 2nd International Conference on Open and Big Data (OBD), Vienna, Austria, 22–24 August 2016; pp. 25–30.
33. Back, A.; Corallo, M.; Dashjr, L.; Friedenbach, M.; Maxwell, G.; Miller, A.; Poelstra, A.; Timón, J.; Wuille, P. Enabling Blockchain Innovations with Pegged Sidechains. 2014, p. 72. Available online: http://www.opensciencereview.com/papers/123/enablingblockchain-innovations-with-pegged-sidechains (accessed on 5 May 2019).

34. Gousias, I.S.; Hammers, A.; Counsell, S.J.; Srinivasan, L.; Rutherford, M.A.; Heckemann, R.A.; Hajnal, J.V.; Rueckert, D.; Edwards, A.D. Magnetic resonance imaging of the newborn brain: Automatic segmentation of brain images into 50 anatomical regions. *PLoS ONE* **2013**, *8*, e59990. [CrossRef] [PubMed]
35. Oheim, M.; Michael, D.J.; Geisbauer, M.; Madsen, D.; Chow, R.H. Principles of two-photon excitation fluorescence microscopy and other nonlinear imaging approaches. *Adv. Drug Deliv. Rev.* **2006**, *58*, 788–808. [CrossRef] [PubMed]
36. Daneshvar, S.; Ghassemian, H. MRI and PET image fusion by combining IHS and retina-inspired models. *Inf. Fusion* **2010**, *11*, 114–123. [CrossRef]
37. Pajares, G.; De La Cruz, J.M. A wavelet-based image fusion tutorial. *Pattern Recognit.* **2004**, *37*, 1855–1872. [CrossRef]