Peer-reviewed version available at Appl. Sci. 2019, 9, 2494; doi:10.3390/app9122494

Article

An Adaptive Biomedical Data Managing Scheme Based on 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 Univeristy, Baghdad, Iraq
[2] Biomedical Engineering Division, University of Saskatchewan, Saskatchewan, Canada
[3] Department of Computer Science, Dijlah University College, Baghdad, Iraq
* Correspondence: a.f.hussein@eng.nahrainuniv.edu.iq; a.f.hussein@ieee.org

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 providers. To be specific, health records are distributed across many places and cannot be found integrated easily. In recent years, blockchain is regarded as a promising explanation that helps to achieve individual biomedical information sharing in a secured way along with privacy preservation, because of its benefit of immutability. This research work put forwards a blockchain-based managing scheme that helps to establish interpretation improvements pertaining to electronic biomedical systems. In this scheme, two blockchain were employed to construct the base of it, where the second blockchain algorithm is used to generate a secure sequence for the hash key that generated in first blockchain algorithm. The adaptively feature enable the algorithm to use multiple data types and combine between various biomedical images and text records as well. All the data, including keywords, digital records as well as the identity of patients are private key encrypted along with keyword searching capability so as to maintain data privacy preservation, access control and protected search. The obtained results which show the low latency (less than 750 ms) at 400 requests / second indicate the ability to use it within several health care units such as hospitals and clinics.

Keywords: Blockchain; Biomedical Data Managing; DWT; Keyword Search

1. Introduction

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

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

Peer-reviewed version available at Appl. Sci. 2019, 9, 2494; doi:10.3390/app9122494

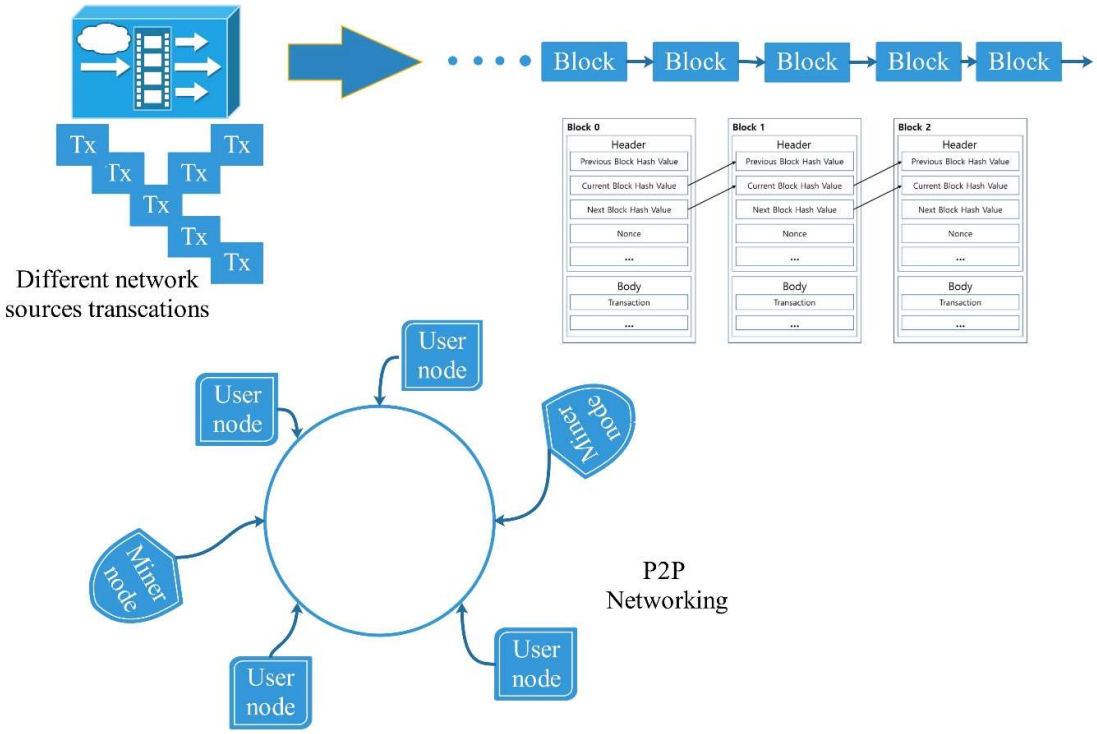

Figure 1. The blockchain structure

With regards to the access and managing authorisations, three kinds of blockchains can be considered: unrestricted, consortium and private. An unrestricted (or permissionless) blockchain is regarded to be highly distributed, wherein any person can contribute via a miner. Even though this warrants maximum immutability, the efficiency is limited due to collaborative achievement of consensus with the help of highly extended miner network. While in a private blockchain, miners process blocks for a single organisation; efficiency can be maximised and immutability 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 organisations [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 medical information of patients. In the age of Internet where cloud storage as well as the adoption of mobile health devices have facilitated sharing of data and records, the number of malicious attacks and the private information privacy getting compromised during sharing have also increased significantly. It has now become easy to obtain health information, if a patient via smart modules, and patients consult with multiple doctors, all of which has increased concerns regarding sharing and secrecy of this information. The healthcare utilities is currently facing the need for unique requirements with regards to interoperability, transfer of biomedical data, authentication, data sharing and considerations for e-health (mobile health) [6].

E-Health refers to the provision of health facilities by employing digital technology. In the e-Health area, research trend has been concentrated on employing electronic health records to perform tasks related to diagnosis and patient monitoring. Typically, a patient may be involved with various providers of healthcare service, including specialists, primary care physicians and therapists [7]. Thus, in the industry and research community, health record exchanging/sharing has been garnering attentions, as well as concerns pertaining to privacy preservation and data security.

For a particular patient, single disease could be produced by or may be linked to added pathema(s). In this case, the reliability and the interpretation accuracy is based on the patient's other health information that has been provided to the doctor. The doctor may get some information

pertaining to related sickness by asking the patient [8]. However, this process cannot always be deemed as effective for diagnosis due to two reasons: i) If some events have 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, which could impact the treatments accuracy or diagnosis he/she had got. ii) Most of the patients have limited medical knowledge and fail to describe the diagnosis or treatments they had received professionally, which could impact the current doctor's Judgment. Thus, the present physician may fail to deduce precise information when carrying out diagnosis [9].

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

2. Literature review

Recent years have seen peaked interest in blockchain to establish privacy and security in e-Health because of the associated benefits in data managing, i.e. integreted autonomy and immutability features of the blockchain.

Q. Xia et al. [10] put forwarded a framework for data sharing which based on blockchain health data sharing to address challenges pertaining to access control for sensitive data stored in the cloud. The system has been designed by considering a permissioned blockchain, which gives access to those verified users who are invited. Yue et al. [11] have also put forward a three-layer system: data usage, data storage and data managing layers. Unlike the aforementioned works in which cloud has been used as a storing infrastructure, this frame work suggests that the secluded blockchain could also act as cloud. In [12], transactions are employed so as to conduct instructions, such as querying, storing and data sharing. The authors have integrated blockchain and offblockchain storage to develop a private data administration platform with a focus on confidentiality. The latest health care/biomedical applications pertaining to blockchain technologies have been studied by Kuo et al. [13]. They have also described the potential challenges and have put forward solutions that integrate blockchain technologies in the health care/biomedical domains. A new blockchain based scheme was put forward by Hussein et al. [14] to secure and manage the medical records. The proposed algorithm employ the genetic algorithm as well as discrete wavelet transform for increasing the security and robustness.

The state-transition functions of the contract are employed to carry out policies, which allow imposing data interchange only for those transactions that are legitimate. Instead of keeping the health record in the block, [15] 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 [16] consists of a structure based on Merkle tree. The tree's leaf nodes characterise patient data communications, and resources adding to the official patient biomedical data record has also been described. However, the actual record document is not included in these transactions and, in its place; Fast Healthcare Interoperability Resources (FHIR) has been referenced via Uniform Resource Locators (URLs). Separate from the above mentioned works that concentrate on health biomedical data sharing, [17] and [18] have concentrated on various issues. [17] put forward a blockchain stage architecture pertaining to clinical trial and precision medical

treatment. This work evaluates the design pertaining to the blockchain podium that begins from the health field, especially precision medicine and the clinical trial. There have been few studies that focus on key management schemes pertaining to blockchain, and [18] made an effort to develop key negotiation 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 health blockchain. In 2016, a cloud-based electronic health record sharing system was put forward by Liu et al. [19], which backs fuzzy keyword search. In their search scheme, a medical practitioner (or other user) is allowed to quickly retrieve EHRs based on the symptoms mentioned in the queried keywords. Implementing the ABE algorithm also helps to authenticate users with regards to their attributes. Guo et al. [20] put forward an attribute-based encryption for the fine-grained authorisation scheme pertaining to a relational database. Recently in 2017, Li et al. [21] put forward a searchable symmetric encryption scheme that was based on blockchain, in which blockchain has been employed as a peer-to-peer network for storing user data based on a pay-per-use approach. In the decentralised system, each of the users possesses equal status and (s)he can request other users for storing his/her data through submission of a transaction.

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 composed via a contieous chain on blocks [22]. Normally, a block includes encrypted key (hash value) of earlier block, contributor signature, payload and timestamp as well. The hash value from the earlier block imparts immutability to the blockchain for modification. The block's payload changes with the applications. For the original data, it could 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 contributor signature and timestamp. Two important entities are involved in the blockchain network: verifiers and miners. Miners signify the nodes that could create new blocks pertaining to the blockchain. Various scenarios could define diverse nodes types as miners. For instance, in the Bitcoin blockchain, the nodes showing proof of works are given as miners to maintain records pertaining to the transactions. Accepting of the new blocks is done only when verifiers confirm the validity pertaining to new blocks. Mining can be defined as a set of processes involving verifying, generating and accumulating new blocks toward the blockchain. In the blockchain network, consensus mechanism is crucial for ensuring 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 was originally employed for Bitcoin, transaction is 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, segmentation of blockchain could be done into three groups: private blockchain, permissionless blockchain (public blockchain) and consortium blockchain. In permissionless blockchain, anybody from any part of the world can enter into the system, which allows accessing data and sending transactions – for instance, Bitcoin system. In remote blockchain, the entree right of the scheme is fully controlled by an organisation. The management of consortium blockchain is done by various organisations. With regards to our work, we have introduced 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

Bonth et al. [21] proposed the public encryption with keyword search (PEKS) to perform search with the 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 was employed for search, which is produced by the unit that corresponds to the public key.

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

Afterwards, different keyword search algorithms have been put forward to offer diverse searching purposes by integrating PEKS with other cryptographic primitives. PEKS schemes with designed tester have been put forward to improve the search security [23, 24]. When integrated with proxy re-encryption, [25], 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 search along with oblivious transfer has been introduced. The data supplier is stopped from knowing the selected keywords as well as the corresponding cipher text due to oblivious keyword search. Some of the applications need to search more than one keyword. The works of [27, 28] demonstrate public encryption key along with conjunctive field keyword. To achieve the needed security objectives, the cited PEKS schemes could be mixed together.

3.3. Discrete Wavelet Transform

To achieve the biomedical image segmentation, in this study, we have used the discrete wavelet transform (DWT). It is important to develop input images so that they fit along with the generated data chains. The DWT can be defined as a mathematical model to perform multi-resolution analysis [29]. A common method is the wavelet transform to perform spatial frequency analysis. Eq. 1 [30] presents the 1D continuous wavelet transform (CWT).

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

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 have been captured with the help of sampling from CWT. Eq. 2 demonstrates $\varphi_{j,k}(t)$ function.

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

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

4. Materials and Methods

The computer clients and hospital servers are considered as semi-trusted. They are deemed as being truthful when performing the protocol but get curious when it comes to accessing or deducing the health information of a patient without proper authorisation. 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 allows inferring the user's real identity [31, 32].

In this study, we aim to achieve the main contributions: Access control as well as security issues. Since the record of the patient is secrecy sensitive issue, it is crucial to maintain data refuge, including data auditing, data integrity and confidentiality, and access control. Normally, encryption and

Peer-reviewed version available at Appl. Sci. 2019, 9, 2494; doi:10.3390/app9122494

signature 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 could be achieved by employing cryptographic primitives via authentication, identification and authorisation.

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

4.1. Used Datasets

In this study, two main databases are used to validate proposed scheme. The first database contains a various collections of MR images with individuals' information that gathered from healthy and patient cases as well. This database is available on brain-development.org/ixi-dataset/ [33]. Each case in this database is well documented and explained, and it can be found as an attachment, therefore it can be used to test our proposed algorithm, where it designed to accept various data types. Other common data in hospitals and healthcare units is microscopic histological images. In this study, the images from www.microscopyu.com/galleries/pathology is employed to confirm the proposed scheme concept [34]. Most patient's record will be from these data types, consequently, the using it are very helpful to improve and get high detection accuracy.

4.2. Image Segmentation

The proposed image segmentation method shown in figure 2 where it is based on previous study [35]. Wavelet analysis is employed for extraction of the original image as well as data fusion. Initially, various image modalities are segmented into four different channels, i.e. low horizontal and low vertical (LL1), while the detailed images include 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 [36]. This procedure continues with two more levels. Finally, the original image is sub divided into small image group as follows:

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

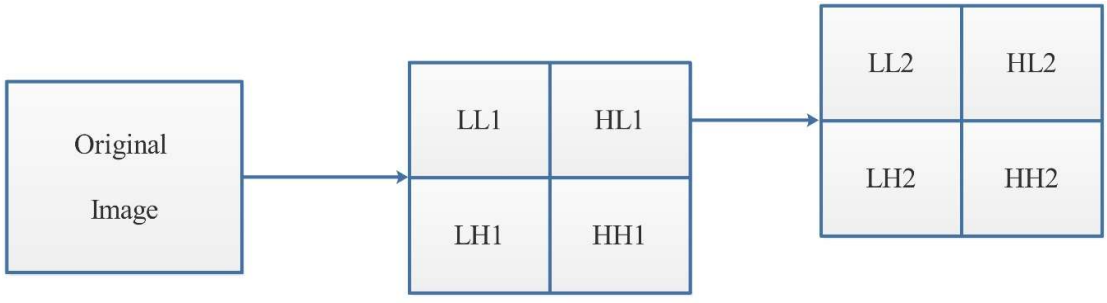

Figure 2. The image segmentation proposed method

4.3. Proposed Scheme Design General Description

The proposed scheme design depicts in figure 3. In this design, the security issue is maintained during a new technique. In this technique, we employ blockchain twice, the second blockchain algorithm is used to generate a secure sequence for the hash key that generated in first blockchain algorithm. That mean, the generated hash keys are double encrypted that contribute to improve the security index. Moreover, a modifications in block structure are prepared, where a new sections are added to fulfil the scheme adaptivity for various data types.

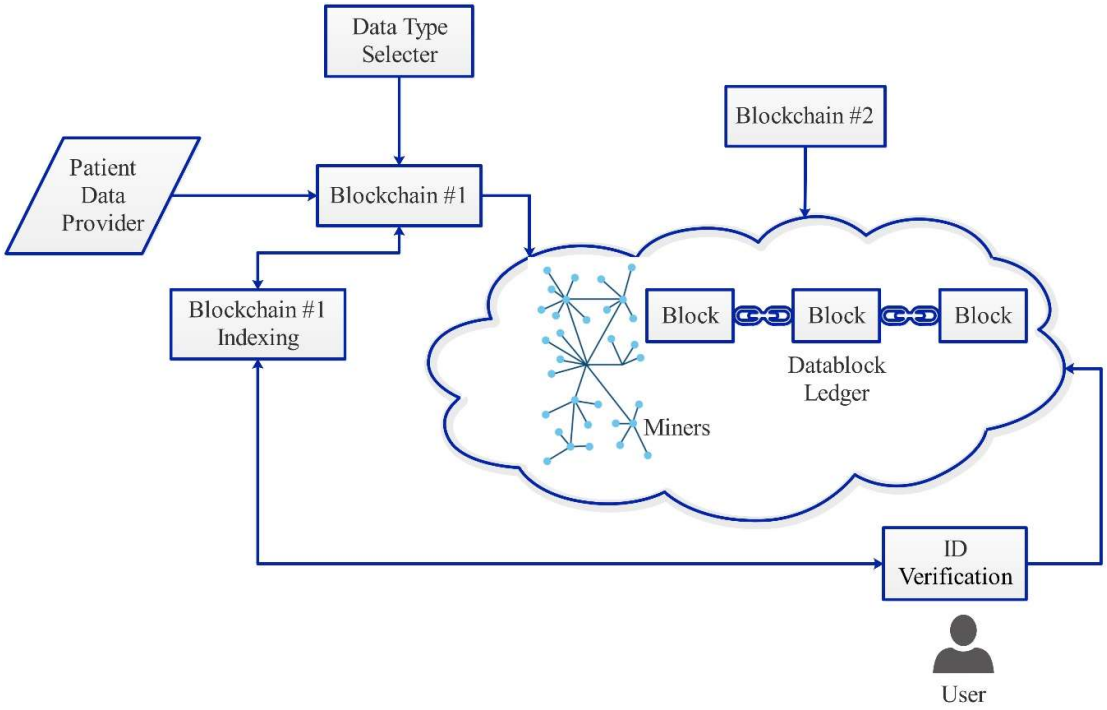

Figure 3. The proposed scheme structure

Figure 4 shows the proposed block structure that used. It contains two main parts block header and system payload. Block header consists of block index, time stamp, previous block hash, next block hash, and nonce. While system payload consists of encryption type, record type information, patient id, and system data. Note that, the information of any data type is stored inside system data section on system payload, and the other parts are used to form the security barrier that isolates the valuable patient's information. There are three entities in the system: scheme supervisor, scheme facility providers or hospitals, and operators (patients).

Scheme supervisor: The entire system is charged by the system manager. It is necessary that all the doctors and patients get themselves registered 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 operates 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 registrations of the users by maintaining a register table for the doctors and users. It also assumes the responsibility in terms of collecting new blocks within the private blockchain at specific intervals and 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 get registered in the hospital server prior to visiting the doctor. After registration, each patient will receive a token from the server. The patient should not disclose anything about the token and show the same only to the doctor when visiting. The beacon serves as evidence pertaining to the interaction between the patient and the doctor, which provides authorisation for the doctor willing to generate the needed 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, development of consortium blockchain and private blockchain could be done by considering the existing infrastructures pertaining to the hospitals without adding more instruments. Notably, installation of different software in the servers and computers allow establishing consortium blockchain and private blockchain.

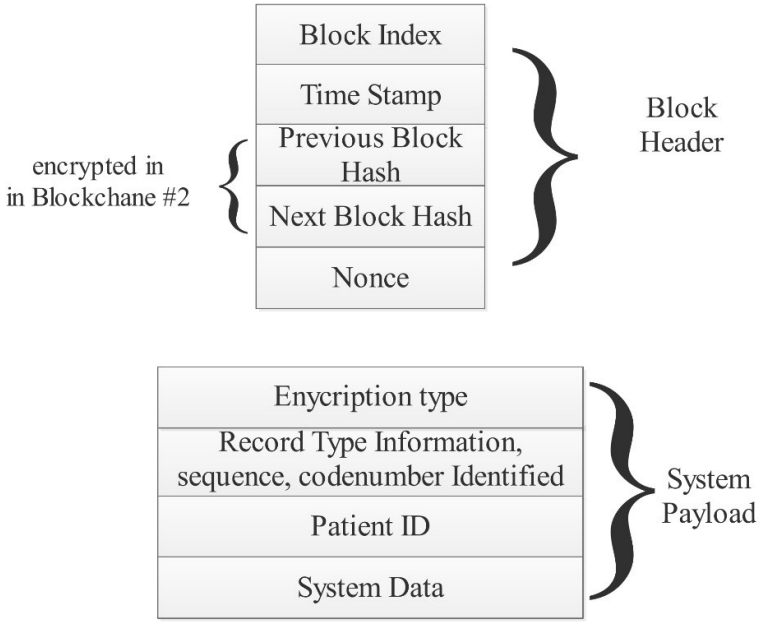

Figure **4.** The used block structure

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

$$k_i = \langle K_1(p_i), (K_1(p_i))^2, \dots, (K_1(p_i))^{n-1}, (K_1(p_i))^n \rangle \quad (3)$$

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 are used to verify scheme algorithm activity. An eight computers combination are set to act as a hospital network, three of them are core I5 CPU, 8 Gbyte RAM, while the others are core I3 CPU, 8 Gbyte RAM. The PCs are located in different places within same building and connected within same backbone. The blockchain environment is achieved by using Octave software under Ubuntu 16.04 operating system. Figure 5 depicts the original data where the most and frequent used data in hospitals are engaged (microscopic histological images, MRI image, and patient descriptive record). The operation process is worked for 210 hours continuously at different requests from different users. Figure 6 shows the generated blocks with data content, where it shows 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 7, the selection of requested number is start from 50 request/second and increase gradually to 400 request/second where it limited according to our environment (the number of Pcs). Based on the obtained results, it was established that the put forward algorithm solution confirms very good paring regarding the distribution of 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 few of the nodes. Due to this, our solution's overall operation was not hindered. Table 1 shows the average resource usage of entire designed network. It is noticed from table 1 that, the needs for bigger memory is recommended, where the physical memory modules are fully loaded. This result could be expected in cases where the biomedical images like DICOM images could occupy large spaces due to their size in terms of megabytes. Even though the location address has been provided, replications pertaining to these files in the blockchain were not anticipated.

Table 1. Network Resource Monitoring

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

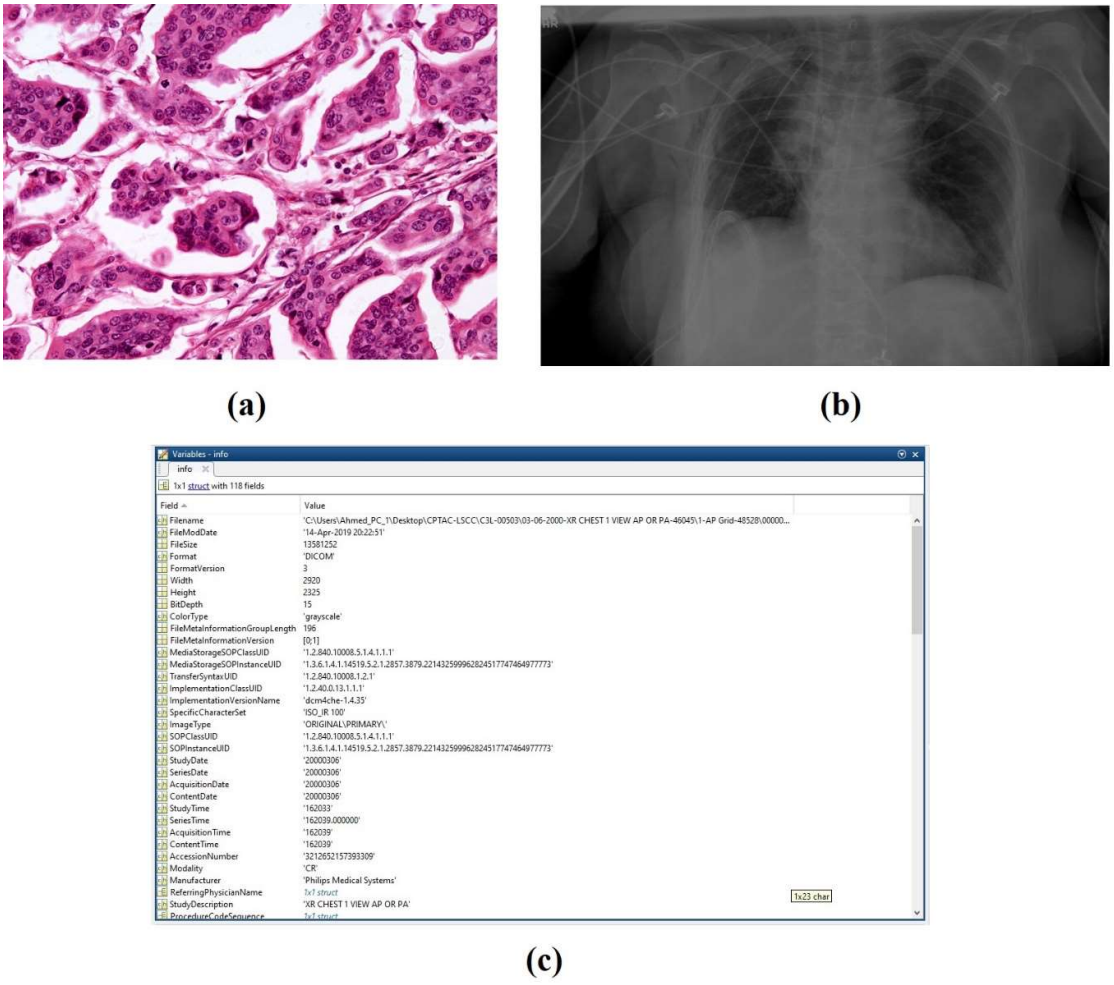

Figure 5. The original data that used where: (**a**) refer to the pathological microscope images; (b) refer to MRI image; (c) refer to digital patient record

Figure 6. The generated blockckain

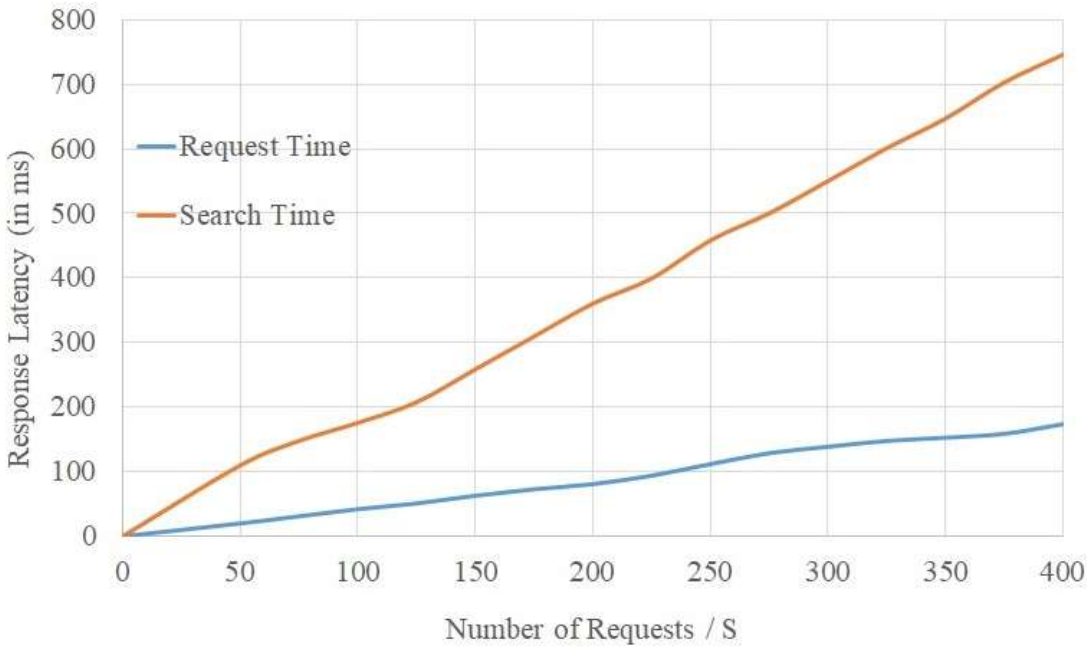

Figure 7. The proposed scheme latency test

6. Conclusion

In this study, a new scheme for managing a biomedical data is presented. Two blockchains are employed to improve the system security and increase the overall stability. Besides, the combining between various data types contributes to reduce the overall system costs and improve searching and processing time as well. Moreover, for the blockchains, the conformance proof can be well-defined and planned as an accord mechanism wherein authenticated blocks are constructed. With regards to the blockchains, public key encryption with keyword search is employed to put forward the records sharing protocol. After receiving hatches from the patient, authorisation of the physician is done to explore and access the desirable history biomedical records to enhance diagnosis. The acceptable obtained results indicate that the scheme is fast and good enough to use it within large hospitals where it has the ability to fit and work under dense payload environments.

References

1. Sikorski, J.J., J. Haughton, and M. Kraft, *Blockchain technology in the chemical industry: Machine-to-machine electricity market.* Applied Energy, 2017. **195**: p. 234-246.
2. Hölbl, M., et al., *A systematic review of the use of blockchain in healthcare.* Symmetry, 2018. **10**(10): p. 470.
3. Zhang, A. and X. Lin, *Towards secure and privacy-preserving data sharing in e-health systems via consortium blockchain.* Journal of medical systems, 2018. **42**(8): p. 140.
4. Bozic, N., G. Pujolle, and S. Secci. *A tutorial on blockchain and applications to secure network control-planes*. in *2016 3rd Smart Cloud Networks & Systems (SCNS)*. 2016. IEEE.
5. Truby, J., *Decarbonizing Bitcoin: Law and policy choices for reducing the energy consumption of Blockchain technologies and digital currencies.* Energy research & social science, 2018.
6. Uddin, M.A., et al., *Continuous patient monitoring with a patient centric agent: a block architecture.* IEEE Access, 2018. **6**: p. 32700-32726.
7. Ali, M., S.U. Khan, and A.V. Vasilakos, *Security in cloud computing: Opportunities and challenges.* Information sciences, 2015. **305**: p. 357-383.
8. Calabrese, B. and M. Cannataro, *Cloud computing in healthcare and biomedicine.* Scalable Computing: Practice and Experience, 2015. **16**(1): p. 1-18.
9. Jiang, Q., et al., *A privacy preserving three-factor authentication protocol for e-Health clouds.* The Journal of Supercomputing, 2016. **72**(10): p. 3826-3849.
10. Xia, Q., et al., *BBDS: Blockchain-based data sharing for electronic medical records in cloud environments.* Information, 2017. **8**(2): p. 44.
11. Yue, X., et al., *Healthcare data gateways: found healthcare intelligence on blockchain with novel privacy risk control.* Journal of medical systems, 2016. **40**(10): p. 218.
12. Zyskind, G. and O. Nathan. *Decentralizing privacy: Using blockchain to protect personal data*. in *2015 IEEE Security and Privacy Workshops*. 2015. IEEE.
13. Kuo, T.-T., H.-E. Kim, and L. Ohno-Machado, *Blockchain distributed ledger technologies for biomedical and health care applications.* Journal of the American Medical Informatics Association, 2017. **24**(6): p. 1211-1220.
14. Hussein, A.F., et al., *A medical records managing and securing blockchain based system supported by a genetic algorithm and discrete wavelet transform.* Cognitive Systems Research, 2018. **52**: p. 1-11.

Peer-reviewed version available at Appl. Sci. 2019, 9, 2494; doi:10.3390/app9122494

15. Zhang, J., N. Xue, and X. Huang, *A secure system for pervasive social network-based healthcare.* IEEE Access, 2016. **4**: p. 9239-9250.
16. Peterson, K., et al. *A blockchain-based approach to health information exchange networks*. in *Proc. NIST Workshop Blockchain Healthcare*. 2016.
17. Shae, Z. and J.J. Tsai. *On the design of a blockchain platform for clinical trial and precision medicine*. in *2017 IEEE 37th International Conference on Distributed Computing Systems (ICDCS)*. 2017. IEEE.
18. Zhao, H., et al. *Lightweight backup and efficient recovery scheme for health blockchain keys*. in *2017 IEEE 13th International Symposium on Autonomous Decentralized System (ISADS)*. 2017. IEEE.
19. Liu, Z., et al., *Cloud-based electronic health record system supporting fuzzy keyword search.* Soft Computing, 2016. **20**(8): p. 3243-3255.
20. Guo, C., et al., *Fine-grained database field search using attribute-based encryption for e-healthcare clouds.* Journal of medical systems, 2016. **40**(11): p. 235.
21. Hu, C. and P. Liu, *An enhanced searchable public key encryption scheme with a designated tester and its extensions.* J. Comput, 2012. **7**(3): p. 716-723.
22. Esposito, C., et al., *Blockchain: A panacea for healthcare cloud-based data security and privacy?* IEEE Cloud Computing, 2018. **5**(1): p. 31-37.
23. Zhu, L., et al., *Controllable and trustworthy blockchain-based cloud data management.* Future Generation Computer Systems, 2019. **91**: p. 527-535.
24. Yang, Y. and M. Ma, *Conjunctive keyword search with designated tester and timing enabled proxy re-encryption function for e-health clouds.* IEEE Transactions on Information Forensics and Security, 2016. **11**(4): p. 746-759.
25. Shao, J., et al., *Proxy re-encryption with keyword search.* Information Sciences, 2010. **180**(13): p. 2576-2587.
26. Ogata, W. and K. Kurosawa, *Oblivious keyword search.* Journal of complexity, 2004. **20**(2-3): p. 356-371.
27. Ryu, E.-K. and T. Takagi. *Efficient conjunctive keyword-searchable encryption*. in *21st International Conference on Advanced Information Networking and Applications Workshops (AINAW'07)*. 2007. IEEE.
28. Bethencourt, J., D. Song, and B. Waters. *New constructions and practical applications for private stream searching*. in *2006 IEEE Symposium on Security and Privacy (S&P'06)*. 2006. IEEE.
29. Addison, P.S., *The illustrated wavelet transform handbook: introductory theory and applications in science, engineering, medicine and finance*. 2017: CRC press.
30. Hussein, A.F., et al., *Performance evaluation of time-frequency distributions for ECG signal analysis.* Journal of medical systems, 2018. **42**(1): p. 15.
31. Azaria, A., et al. *Medrec: Using blockchain for medical data access and permission management*. in *2016 2nd International Conference on Open and Big Data (OBD)*. 2016. IEEE.
32. Back, A., et al., *Enabling blockchain innovations with pegged sidechains.* URL: http://www. opensciencereview. com/papers/123/enablingblockchain-innovations-with-pegged-sidechains, 2014: p. 72.

33. Gousias, I.S., et al., *Magnetic resonance imaging of the newborn brain: automatic segmentation of brain images into 50 anatomical regions.* PloS one, 2013. **8**(4): p. e59990.
34. Oheim, M., et al., *Principles of two-photon excitation fluorescence microscopy and other nonlinear imaging approaches.* Advanced drug delivery reviews, 2006. **58**(7): p. 788-808.
35. Daneshvar, S. and H. Ghassemian, *MRI and PET image fusion by combining IHS and retina-inspired models.* Information Fusion, 2010. **11**(2): p. 114-123.
36. Pajares, G. and J.M. De La Cruz, *A wavelet-based image fusion tutorial.* Pattern recognition, 2004. **37**(9): p. 1855-1872.