Journal of Discrete Mathematical Sciences and Cryptography

ISSN: (Print) (Online) Journal homepage: https://www.tandfonline.com/loi/tdmc20

Blockchain in healthcare : Moving towards a methodological framework for protecting Biomedical Databases

G. Ramesh, Avinash Sharma, D. V. Lalitha Parameswari, Ch. Mallikarjuna Rao & J. Somasekar

To cite this article: G. Ramesh, Avinash Sharma, D. V. Lalitha Parameswari, Ch. Mallikarjuna Rao & J. Somasekar (2022) Blockchain in healthcare : Moving towards a methodological framework for protecting Biomedical Databases, Journal of Discrete Mathematical Sciences and Cryptography, 25:4, 891-901, DOI: 10.1080/09720529.2022.2068598

To link to this article: https://doi.org/10.1080/09720529.2022.2068598

Published online: 05 Jul 2022.

Journal of Discrete Mathematical Sciences & Cryptography
ISSN 0972-0529 (Print), ISSN 2169-0065 (Online)
Vol. 25 (2022), No. 4, pp. 891–901
DOI : 10.1080/09720529.2022.2068598

Taylor & Francis
Taylor & Francis Group

Blockchain in healthcare : Moving towards a methodological framework for protecting Biomedical Databases

G. Ramesh *
Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering & Technology
Hyderabad
Telangana
India

Avinash Sharma †
Department of Computer Science and Engineering
Maharishi Markandeshwar Engineering College
Haryana
India

D. V. Lalitha Parameswari §
Department of Computer Science and Engineering
G. Narayanamma Institute of Technology and Science (GNITS)
Hyderabad
India

Ch. Mallikarjuna Rao ‡
Department of Computer Science and Engineering
Gokaraju Rangaraju Institute of Engineering & Technology
Hyderabad
Telangana
India

* *E-mail:* ramesh680@gmail.com (Corresponding Author)
† *E-mail:* asharma@mmumullana.org
§ *E-mail:* lplalitap97@gmail.com
‡ *E-mail:* chmksharma@yahoo.com

J. Somasekar [@]
Department of Computer Science and Engineering
Gopalan College of Engineering and Management
Bangalore
India

Abstract

Biomedical databases or repositories have scientific information that is evidence based and protecting such documents from tampering or non-repudiation is very significant. The traditional techniques for the same have limitations in the distributed environments. Scientific contributions are to be safeguarded and it is one of the challenging problems. Blockchain is the promising technology that can support distributed ledger of transactions and thus it is found suitable for protecting biomedical repositories. As blockchain is a proven technology associated with crypto-currency known as Bitcoin in finance domain, it has plenty of opportunities in other domains. In this paper, a framework that is based on blockchain technology (BCT) for protection of biomedical databases with integrity and non-repudiation is presented. The framework will have underlying mechanisms to exploit blockchain to have a protection service and smart contracts to be more flexible and dynamic to adapt new requirements from time to time. The framework is domain specific but can pave way for motivation for adapting it to new domains as well.

Subject Classification: *68M25.*

Keywords: *Blockchain technology, Bitcoin, Smart contracts, Biomedical databases, Document protection service, Non-repudiation.*

1. Introduction

Blockchain technology is well known for its association with crypto currency like Bitcoin in financial domain. It could be used to have a distributed ledger of all transactions which is decentralized and made accessible to all users. Thus users of Bitcoin gain secure services. A Bitcoin cannot be used second time. Any integrity issue can be identified quickly due to the consensus mechanism and mining feature with incentives to users. Blockchain technology (BCT) became popular with Bitcoin. However, the concept of decentralized and distributed ledger of transactions is not tied with any domain. Therefore, as studied in [2], [6], [9] and [10], it is possible to use distributed ledger technology in different domains. Many researchers contributed towards usage of BCT in medical domain. Especially efforts were made to apply BCT to biomedical databases in the

[@] *E-mail:* `jsomasekar@gmail.com`

real world. As investigated in [10] BCT is used for secure data sharing in healthcare domain. Associated with healthcare domain is the biomedical databases such as PubMed. These databases contain evidence based peer reviewed scientific articles whose integrity is to be given highest priority. In this context, there are possibilities of misusing retrieved biomedical documents. The misuse may be in the form of reproducing the content differently and using it, making changes in the authorship and so on. Non-repudiation is another issue along with data integrity of retrieved documents. To overcome the issues aforementioned, the research presented in [16] provided a base level solution. However, it is not adequate to have a more comprehensive framework that ensures protection of biomedical documents from integrity and non-repudiation issues besides having flexible and dynamic smart contracts. The contributions in this paper are as follows.

i. A framework named Biomedical Document Protection System (BDPS) is designed to have an application based on BCT to protect biomedical documents.
ii. An algorithm known as BCT based Biomedical Document Protection (BCT-BDP) for safeguarding biomedical documents in terms of integrity and non-repudiation is proposed.

The remainder of the paper is structured as follows. Section 2 reviews literature on BCT in current applications and issues. Section 3 presents the proposed biomedical document protection system. Section 4 provides implementation details. Section 5 concludes the paper and provides scope of future work.

2. Related Work

This section provides review of BCT security of biomedical databases. Dai *et al*. [1] used MultiChain platform for implementation of a private block chain. They integrated it with a research oriented platform. They used Python language for making an administration page using Docker with a micro service to monitor the performance of blockchain implementation. For data acquisition, they integrated another platform known as TrialChain. Zhang *et al*. [2] presented an AI platform named Genie for secure training of medical data. It used Software Guarded Extensions (SGX) and blockchain for securing source codes. Tamazirt *et al*. [3] focused on the problem of depending on third parties with a novel

approach with security and management strategy besides integration of blockchain. It offers a solution to problems in healthcare domain. It also helps professionals to share medical document securely. Choudhury *et al*. [4] investigated on a data management framework with blockchain containing private channels and smart contracts for secure and confidential communications. However, their work lacks regulatory services. Azencott [5] studied on the privacy breaches and how they occur in information systems. They considered different ethical and legal perspectives in the research associated with data protection frameworks. Siyal *et al*. [6] emphasized the importance of blockchain in the contemporary era and explored the range of applications it offers in every conceivable domain. They also opined that cyber security can be leveraged with blockchain technology. Kin and Lee [7] said that blockchain is suitable for healthcare applications as they have confidential data. Liu *et al*. [8] proposed a system known as BPDS for secure sharing of Electronic Medical Records (EMRs) with privacy preserved. When EMRs are stored, they are secured and index is used to have access. At the same time blockchain is used to have tamper-proof security to transactions. As the medical data leakage is expensive and should not occur in the first place, their method provides required privacy and security. Thus secure data sharing is accomplished with the help of privacy mechanisms and smart contracts. They also integrated it with access control mechanism which is based on CPABE. Clauson *et al*. [9] reviewed most relevant literature to understand solutions in the real world catering to different fields including healthcare and its supply chain. They found critical challenges in data integrity and suggested blockchain for data integrity. Ito *et al*. [11] threw light on challenges associated with blockchain based solutions in healthcare industry. They proposed a user-centric framework named i-Blockchain for controlled usage of healthcare data with different applications. Kleinaki *et al*. [12] explored a notarization service for protecting data in biomedical domain. Their service could verify the data retrieval as every transaction is recorded with blockchain repository. Every query for biomedical data is recorded and thus it ensures non-repudiation and confidentiality. Different advantages and challenges of using blockchain in healthcare are explored in [14], [15] and [16]. From the review of literature, it is understood that the usage of BCT for protecting biomedical databases in terms of integrity and non-repudiation is inadequate and needs further research for a comprehensive framework to safeguard such valuable databases.

3. Proposed Framework

3.1 *Problem Definition*

Biomedical databases like PubMed have millions of evidence based research documents that have been peer reviewed. The rich set of documents is being used by users across the globe. However, the data in biomedical domain is scientific in nature and sensitive to unauthorized changes. The documents retrieved by querying databases should never be modified and reproduced in the public domain. This kind of practice causes potential risk to human kind especially scientific community in one way or other. Different kinds of misuse of the medical documents are possible. Therefore, data integrity of retrieved documents and non-repudiation are very important to protect the sanctity of biomedical repositories across the globe. Therefore, the challenging problem is to have a technology driven solution to protect biomedical documents with data integrity and non-repudiation.

3.2 *The Framework*

A framework is proposed to have a BCT based solution to achieve data integrity of retrieved biomedical documents and non-repudiation. Besides, it will have smart contracts to be flexible and dynamic to the needs of the system. It is named as Biomedical Document Protection System (BDPS). Biomedical databases are queries by either user directly

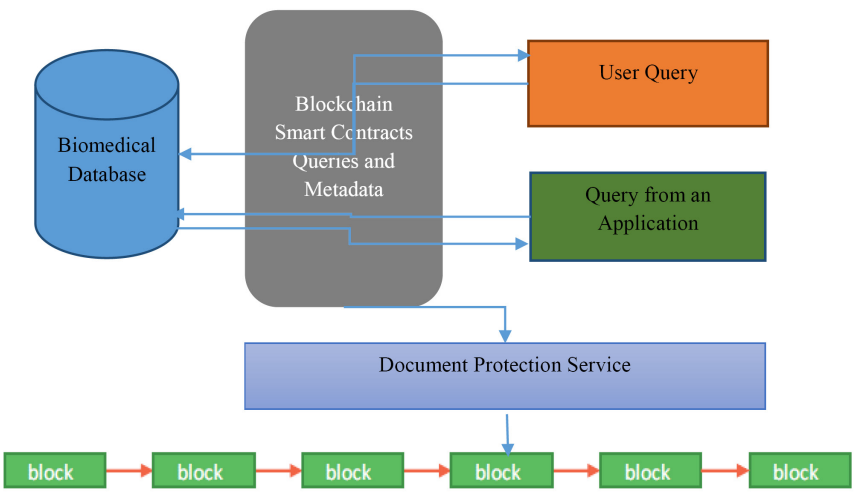

Fig. 1

Overview of the proposed framework (BDPS)

or programs in Machine-to-Machine (M2M) distributed environments. It is most likely that both kinds of interface are provided by biomedical databases like PubMed.

In the existing approach, the users can access biomedical documents. Afterwards, there is no mechanism to track and find whether those documents are subjected to changes causing data integrity issues and also non-repudiation. These problems are overcome with the proposed framework. The overview of the same is provided in Fig. 1. When a query is made to biomedical database for which this framework is integrated, the queries and the responses to queries are securely maintained with document protection mechanism. Smart contracts can help in this regard to meet the security requirements. The smart contracts, user queries and metadata are maintained in a repository. This repository is exploited by the proposed query notary service. Every transaction is subjected to security primitives and they are maintained using BCT. Thus a distributed ledger of query based transactions is maintained in decentralized fashion. This ledger is accessible to all users of the biomedical databases. Then all users will be able to mine and gain consensus related to integrity and non-repudiation. Therefore, it will create very reliable and dependable environment where all stakeholders of biomedical databases can have their role to play in a secure fashion. With this framework it is possible to achieve the aim of this research for protection of biomedical databases with data integrity of retrieved articles and non-repudiation. This framework has good prospects which has impact on academia and scientific community in successful usage of BCT for different domains other than finance. It will have impact on enterprises of different domains to safeguard their data and transactions if this framework is employed to their domains. It will have huge impact on the users of biomedical databases and providers of the same as there will be data integrity and non-repudiation. It helps healthcare domains to adapt and safeguard sensitive data from being misused. It also provides ideas to have security solutions to banking and insurance domains. This kind of service may also help government sector in future.

4. Implementation Details

In Implementation of the proposed framework has many important components. They include BCT, query service and document protection service (in terms of non-repudiation and integrity with respect to evidence retrieval).

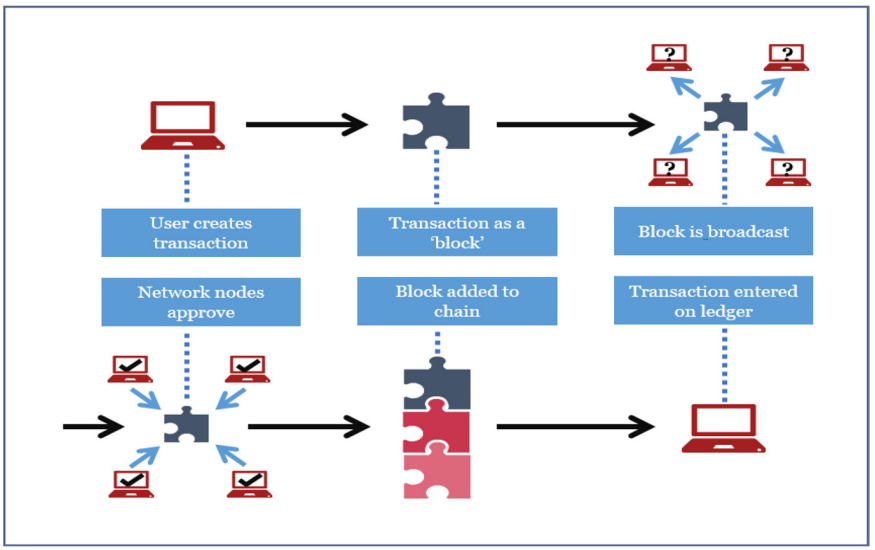

Fig. 2

Blockchain technology usage

4.1 *Blockchain Technology Usage*

Blockchain technology when employed for protecting biomedical documents, the typical technological solution appears as shown in Figure 2. It is adapted from [13] which is the underlying mechanism in the proposed framework as far as BCT usage is concerned. There are different blockchain platforms for application development. They include IOTA, Chain, IBM Bluemix Blockchain, Open Chain, HydraChain, Multichain, Hyperledger and Ethereum. All of them can be used to develop an application with typical scenarios. For protecting biomedical databases, the proposed system is realized with the Ethereum platform and solidarity language.

4.2 *Document Protection Service*

This service is crucial in the proposed framework. Its purpose is to ensure integrity and non-repudiation pertaining to biomedical database evidence retrieval. A wrapper is built to a conventional database to exploit BCT. This service is meant for recording all transactions in such a way that they follow the procedure illustrated in Figure 2. It tracks data consumers and their activities to have evidence retrieval which leads to

biomedical document integrity and non-repudiation. It provides proof of data retrieval which is irrevocable in nature. This will prevent users from intentionally repudiating a past transaction. This service is part of the framework shown in Figure 1. The contract service of the BCT enables realization of this service. The database model is supported with NoSQL, Resource Description Framework (RDF) and also conventional structured databases like MY SQL.

4.3 *Layers of the Prototype*

The service aforementioned is realized with a prototype containing three layers. They are known as front end layer, interface (to communicate with biomedical databases) layer and contract layer. The front end layer provides interaction between user and application or application to application in M2M scenarios. The interface layer helps the front end to interact with the biomedical databases. The contract layer plays crucial role in realizing document protection service. It is the layer with provision to collate a query transaction and its results tied to the consumer. Thus contracts are managed with data meta data which helps in proving evidence of retrieval and repudiation attempts if any.

4.4 *Realization of Service with Solidity Language in Ethereum Platform*

Solidity is a high level language which is contract-oriented and suitable for realizing BCT. It can be used to adapt BCT for any domain specific needs. The document protection service written in Solidity language is shown in Listing-1.

```
pragma solidity ^0.4.18
contract Document_Protection_Service {
  //initialization of values needed for creation of contract
  function getHashValue() view public returns(byte32) {
    //code
  }
  function getTimeStamp() view public returns(byte32) {
    //code
  }
}
```

Listing 1: Shows outline of the service contract (part of BCT-BDP algorithm)

The document protection service is realized with the solidity script in Listing 1 and along with other scripts. Ethereum BCT infrastructure is used to realize the complete framework. The details of prototype execution and results evaluation are deferred to next research paper. Therefore, the results and evaluation are not in the scope of this paper. Smart contracts are defined using Solidity language. NoSQL database such as MongoDB is used for storing contracts and the metadata. Front end is a web based tool that provides required interface to users. It is made up of Hypertext Mark-up Language (HTML), Cascading Style Sheets (CSS), JavaScript and Asynchronous JavaScript and XML (AJAX) to be rich in user experience. The frontend interacts with PubMed MEDLINE (biomedical database). When a new query is made by user, the document protection service with exploit the smart contract to ensure that the transaction is associated with BCT and a distributed ledger of the transactions is maintained for evidence retrieval leveraging integrity and non-repudiation.

5. Conclusion and Future Work

In this paper, a framework named BDPS is proposed based on BCT. It has an underlying service that protects biomedical documents from integrity issues and ensures non-repudiation. The service is meant for evidence retrieval which is essential in the healthcare industry. The proposed framework is realized with Ethereum BCT platform with Solidity language. Every transaction of the users is associated with blockchain which provides distributed ledger and every transaction can be verified by public. Thus it does not allow repudiation and denial of any past transactions by users or data consumers. The framework is realized with three layers known as front end layer, interface layer and contract layer. The first layer provides user to application interface or application to application interface. The second layer provides interacting with PubMed MEDLINE (biomedical database). The third layer is related to smart contracts that are actually used to realize the proposed service. Details of experiments and the results evaluation are not in the scope of this paper. They are deferred for future work that focuses on the evaluation of the framework with the prototype implemented.

References

[1] Hao Dai, H Patrick Young PhD, Thomas JS Durant MD, Guannan Gong MS, Mingming Kang, Harlan M Krumholz MD SM, Wade L

Schulz, Lixin Jiang. TrialChain: A Blockchain-Based Platform to Validate Data Integrity in Large, Biomedical Research Studies, p1-7, (2014).

[2] Shifa Zhang, Anne Kim, Dianbo Liu, Sandeep C. Nuckchady, Lauren Huang, Aditya Masurkar, Jingwei Zhang, Lawrence Tseng, Pratheek Karnati, Laura Martinez, Thomas Hardjono, Manolis. Genie: A Secure, Transparent Sharing and Services Platform for Genetic and Health Data, p1-10, (2018).

[3] Lotfi Tamazirt, Farid Alilat, Nazim Agoulmine. Blockchain Technology: A new secured Electronic Health Record System, p1-9, (2018).

[4] Olivia Choudhury, Noor Fairoza, Issa Sylla, Amar Das. A Blockchain Framework for Managing and Monitoring Data in Multi-Site Clinical Trials, p1-13, (2019).

[5] Chloe-Agathe Azencott. Machine learning and genomics: precision medicine vs. patient privacy, p1-14, (2018).

[6] Asad Ali Siyal, Aisha Zahid Junejo, Muhammad Zawish, Kainat Ahmed, Aiman Khalil and Georgia Soursou. Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives, p1-16, (2018).

[7] Chi Kin, Lee. Blockchain Application with Health Token in Medical & Health Industrials. *International Conference on Social Science, Public Health and Education*. 196, p1-4, (2018).

[8] Jingwei Liu, Xiaolu Li, Lin Ye, Hongli Zhang, Xiaojiang Du, and Mohsen Guizani. BPDS: A Blockchain based Privacy-Preserving Data Sharing for Electronic Medical Records p1-6, (2018).

[9] Kevin A. Clauson, Elizabeth A. Breeden,2 Cameron Davidson, Timothy K. Mackey. Leveraging Blockchain Technology to Enhance Supply Chain Management in Healthcare: An Exploration of Challenges and Opportunities in the Health Supply Chain, p1-12, (2015).

[10] Jieying Chen, Xiaofeng Ma, Mingxiao Du, Zhuping Wang. (2018). A Blockchain Application for Medical Information Sharing, p1-7.

[11] Kenichi Ito, Kiichi Tago, Qun Jin. i-Blockchain: A Blockchain-Empowered Individual-Centric Framework for Privacy-Preserved Use of Personal Health Data. *2018 9th International Conference on Information Technology in Medicine and Education*, p1-5, (2018).

[12] Athina-Styliani Kleinaki, Petros Mytis-Gkometh, George Drosatos, Pavlos S. Efraimidis, Eleni Kaldoudi. A Blockchain-Based Notarization Service for Biomedical Knowledge Retrieval. *Computational Industrial Biotechnology Journal,* Elsevier, 16, 288-297, (2018).

[13] Blockchain Usage. Retrieved from

https://www.europeanpaymentscouncil.eu/sites/default/files/inline-images/ Blockchain %20 diagram Pwc-Def.png.

[14] Hasselgren, A., Kralevska, K., Gligoroski, D., Pedersen, S. A., & Faxvaag, A., Blockchain in healthcare and health sciences—A scoping review. *International Journal of Medical Informatics*, 134, 104040, (2020).

[15] Yaqoob, I., Salah, K., Jayaraman, R., & Al-Hammadi, Y., Blockchain for healthcare data management: opportunities, challenges, and future recommendations. *Neural Computing and Applications* (2021).

[16] Tandon, A., Dhir, A., Islam, N., & Mäntymäki, M., Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda. Computers in Industry, 122, 103290, (2020). doi:10.1016/j.compind.2020.103290 .