A Study on Privacy Preservation of Medical Certificates Using Blockchain Technology

Ch. Rupa¹,* and Divya Midhun Chakkaravarthy²

¹Department of Computer Science and Engineering, Lincoln University College, Malaysia; ²Department of Computer Science and Multimedia, Lincoln University College, Malaysia

Abstract: Currently, blockchain technology has evolved into a reliable and secure platform to provide security for the data. This technology's main adoption areas are agriculture, supply chain, food sector, energy industries, Health care, Real estate, Voting system, and education sector. This paper reviewed existing related works and applications using blockchain technology. Forgery or fraud on medical documents is a significant challenge in the health care sector. Hence, this paper proposed a Blockchain-based framework using Ethereum that is a public blockchain. Users required medical documents generated and issued by officials authentically in the way of a unique blockchain-based ID. Users can submit this Blockchain-based ID anywhere instead of a physical paper. Attacks or forgery on the medical document can reduce using advanced featured technology, Blockchain. Blockchain technology has the features such as immutable, distributive, secure, reliable, and transparent. Remix Ethereum IDE, solidity programming, and Metamask Wallet were used to implement the proposed application. The main strength of this work is designing and deploying results and comparisons with the existing applications.

Keywords: Ethereum, public blockchain, medical document, remix, metamask.

1. INTRODUCTION

Blockchain technology is playing an essential role in Industry 4.0. Some renowned educational institutions, such as MIT, used blockchain technology-based Blockcert Wallet to issue students' diplomas [1, 2]. This technology consists of several advanced features like transparency, immutable, secure, and distributed [3]. Currently, the utilization of blockchain technology being increased with the association of other advanced technologies like artificial intelligence [4], the internet of things [5], Machine learning [6], and data analytics [7]. Besides, by collaborating with cloud computing and UAV (Unmanned Aerial Vehicles) technology, some researchers and academicians [8] have proposed other advanced applications. Any collaborative (hybrid) application can enhance the properties in terms of availability, reliability, security, and portability. Blockchain technology achieves security features using a cryptography mechanism [9]. The hashing algorithm uses in blockchain technology to interconnect the blocks [10].

Electronic voting system and manual voting system, both approaches faced some issues with illegal activities. To overcome these kinds of problems, Russia uses blockchain technology to conduct elections in their country. It has been designed with the Department of Information Technology (DIT) and the Moscow City election commission [11, 12]. Some other countries like the Netherlands, Sweden, the United States of America (USA), and India also would like to use blockchain technology in organizing the elections in their respective countries, although in other applications such as real estate and banking sectors [13].

Different types of cryptocurrencies are available to store, send, and receive the data in the Blockchain. Those are bitcoin (BTC), ether (ETH), bitcoin cash (BCH), USD Digital (USD –D), ripple, Monero, hyper ledger, etc. [14]. More researchers use Ethereum based public Blockchain that supports ETH cryptocurrency to compile and deploy their applications' smart contracts. The main difference between ethereum and ether (ETH) is that etherum is a blockchain network and ether (ETH) is like fuel to run the ethereum network. A chrome extension (Metamask) is available as an open-source used to compile and deploy the proposed smart contract over a blockchain network, where a smart contract is the lines of code written using solidity programming on top of the IDEs like Ganache, Remix, Visual C++, etc. [15, 16]. This work proposes a methodology to generate and preserve medical records using a public blockchain, Ethereum. This work has four components: user role, Health care sectors, Local databases, Blockchain, and the blockchain environment required to write smart contracts to perform the proposed system components functionalities. Providing privacy preservation to the medical data is a major challenging issue. As a part of
this, the health sector needs to encapsulate the blockchain technology features. They are currently facing a problem while generating the official medical documents and issuing them by the authorized persons to the users appropriately. During these stages, medical records being exposed to fraud by the users or attackers or unauthorized persons.

The rest of the paper is handled as follows. Related works are discussed in Section 2. Section 3 contains details about the proposed system architecture, and the flow of transactions in the components of the system is discussed. The results of the proposed approach are shown in Section 4. Section 5 discusses system performance and comparisons with current methods. In conclusion, the conclusion and scope of future work are described in Section 6.

2. LITERATURE SURVEY

S. Chen et al. [17] have done a study work on blockchain-based supply chain management. In this regard, the authors have designed a layer-based framework called SCQI. The layers are referred to as the Internet of Things (IoT) layer, Data Layer, Business Layer, and Contract Layer. The main limitations of the work are no implementation results. As well as, there is no comparison report with the existing systems on blockchain technology. Mao.D. et al. [18] addressed a new mechanism to trace food using blockchain technology. The authors for designing the proposed application used consortium blockchain technology. It may lead to improve safety, security, and trust while food is in the transaction. Furthermore, this work has mentioned the benefits to the merchants with the proposed applications. The authors proposed a novel life cycle model called smart contract-based life cycle management to optimize food transaction costs.

Shu Yang et al. [19], using the Directed Acyclic Graph (DAG) structure, improves the traditional blockchain protocol's linear design. In this structure, the blocks are organized in levels and width, generating a compacted DAG structure (CoDAG). Some novel algorithms and protocols are designed to make this CoDAG secure and efficient. Moreover, to appropriately place the new generated blocks, CoDAG boosts the security and transaction verification time compared to the traditional blockchain protocols enjoying the stability and liveness properties of Blockchain.

Weilin Zheng [20] developed a BaaS platform called NutBaaS which provides a blockchain service over cloud computing environments, such as system monitoring and network deployment, testing, and smart contract analysis. It is usually hard and expensive for most developers or teams to build and monitor blockchain networks. Depending on the services, developers focus on the code to explore how blockchain technology can be applied appropriately without bugging to maintain and monitor it.

According to Sidra Malik et al. [21], the significant issues in increasing supply chains' complexity are integrity and traceability. Even though Blockchain technology can solve these issues, it won't solve the trust problem. In this proposed work, the authors have designed a three-layered management framework that uses consortium blockchain to observe the interactions between supply chain participants and provide trust dynamically. Based on these interactions, they provide reputation scores.

Tara Salman et al. [22] have done extension work for the probabilistic blockchain concept. This framework was designed to accommodate the requirements of a wide range of applications. Furthermore, it is used to reduce the effect on probabilistic blockchains and detect malicious nodes. The authors have assessed the framework by comparing it to the baseline by using adversarial strategies and also analyze the collaborative decisions with and without malicious node detection. These results show a sustainable performance and achieve adequate results.

According to Antonyo Douglas et al. [23], many architectures are being proposed to address security, device management, and configuration using blockchain technology. These architectures require a trusted third party to interact with the Blockchain on behalf of the edge devices. Further introduced failure in trust and security. This work proposes blockchain technology adoption to enable edge devices to communicate with Blockchain without intermediary or third parties. This architecture gives an extensible framework that enables several multi-party interactions to occur at the edge of the network.

Guozhen Zhang et al. [24] proposed a mutual trust data-sharing framework with AI technologies. The authors have worked on the distributed and tamper-proof block chain attributes to develop a data sharing framework for AI-powered network operations. This framework enables the operation of the network automatically with the help of AI technologies. In the proposed framework, the smart contract was employed to grant data permissions by the data owner. Also, a trustless environment was developed for data sharing with the help of the Behaviour Chain and Data Chain. The supervision measures and data access control are integrated for this purpose. This work's major drawback is that it still needs to be developed to work in more data sharing scenarios and be a useful data-sharing framework in real-time markets.

Hao Guo et al. [25] proposed a mechanism that can secure Electronic Health Records (EHR) by authentication of signatures, and thus the sensitive information contained in the health records is preserved. For this purpose, the authors have used the ABMS scheme and the ABE scheme. The ABE scheme is employed to encrypt the EHR data, and this encrypted data is stored on the edge node. The proposed block chain mechanism was developed to work on the Hyper Ledger platform. The blockchain module records patients' profiles of GIDs, first and last, names, signed ABMS signatures, and one-time self-destructing URL addresses for EHR data stored on the edge node. The system performance was evaluated by performing experiments on the ABMS module.

Suat Mercan et al. [26] presented a framework that could efficiently maintain data collected from various IoT devices and confirm the collected data's authenticity. The authors have developed the framework to be cost-effective and, at the same be secure. The proposed forensic framework consists of two layers and is a combination of several blockchain networks. It uses the public Blockchain, and with the help of the hash functions and the Merkle tree, the size of the data block which is to be placed onto the public Blockchain is
reduced. Since data storage on a public blockchain is expensive, the proposed framework uses multiple less expensive blockchain networks for temporary data storage before the whole data is placed in the Ethereum network. This framework thus provides affordable yet secure storage of data obtained from multiple IoT devices (Table 1).

3. MATERIALS AND METHOD

This work proposed a methodology to generate and preserve the medical records using a public blockchain, Ethereum. This work has four components such as user, Health care sectors, Local databases, and Blockchain. Blockchain environment required to write smart contracts to perform the system components functionalities.

At first, Health care systems receive a unique ID after taking the registration at the hospital authority. Health care systems or hospitals register their centers by giving information about the name of the hospital, address, physician name. The second major component of the proposed method is users who want the official medical certificates to mean birth or death or some other certificate like sick.

Users submit the requests to the health care centers by giving details for the required document means birth, death, or sick certificates. Inscribe a smart contract on a blockchain platform regards the user's requirements to generate a blockchain-based certificate using solidity programming. Furthermore, the user's details have been stored in the local database as shown in fig land verified by the physician about its integrity. Later, recommended for generating the certificate that has generated using blockchain technology.

3.1. Smart Contract

A smart contract is self-executing lines of code over a blockchain platform. Moreover, it creates a contract between hospitals or health care centers to the users [33]. Whenever predetermined conditions have been satisfied, then automatically, that smart contract will execute. The proposed approach uses a solidity program to write a smart contract on the ethereum based public Blockchain. The attributes that have used in the proposed system smart contract are as follows:

```solidity
Contract Medical_certificate

    uint public Hospital_Reg_No;
    string public Hospital_Nmae; //bytes16
    string public Doctor_Name; //bytes16
    string public Certificate_Type;//bytes32
    string public Gender;
    string public cert_Holder_Name;
    string public date_of_issue;
    string public date_of_receipt;
    string public Recipient_Name;

    uint public UID_Reciepent;
```

The health care center's name, address, and doctor's name are the attributes that have been considered in the smart contract preparation. The mentioned characteristic data was performed as logical agents in the proposed system to create the blockchain environment's official health care documents. In addition, some other attributes such as username, the purpose of the document, gender of the patient also considered while writing a smart contract. They belong to the user or patient details. The smart contract has some other elements such as certificate issue date and unique ID of the document that have related to the official medical certificate over a blockchain platform.

3.2. Implementation

To implement the proposed system uses remix IDE [34] that is an ethereum public blockchain environment. The system required smart contracts written on the web-based remix IDE. It uses the metamask wallet interface to establish an agreement between blockchain environments to the solidity code. The system executes the proposed smart contracts of the identified tasks on ropstern network-based ethereum Blockchain [35]. Health care centers registration at admin is an initial task of the proposed system. Algorithm 1 shows its process stepwise.
Algorithm 1: Health care centers registration ( )

Input: Health care center name, address, physician name
Output: Assigned a unique Number to the health care center

Process:
Take registration by assigning the health care centers details.

Health care_details = Center_Name || address || Physician name

Regulatory authority or Central Authority of the hospitals verify the Health care centers details.

If (integrity (Health care_details ) = true)
If predetermined rules satisfied, then issue a unique ID to the center; otherwise, discard the request.

else

discard (request)

Fig. 2 shows the process of transactions among the proposed system objectives. As discussed earlier, healthcare centers, after taking the registrations from the regulatory authority, the details of the user's who have required medical documents need to submit at the health care centers. Physicians of the hospitals or the health care centers verified the details submitted by the users and stored them in their local databases. Also, healthcare centers process the verified data on the blockchain environment using the proposed application system.

Algorithm 2: Medical documents generation ( )

Input: User's medical record details
Output: A blockchain-based unique ID to the record

Process:
Set the values of medical documents using the following statement on etherum platform

function set (uint reg_No, string memory hos_Name , string memory doc_Name, string memory cer_Type, string memory gen, string memory cer_hol_Name, string memory dat_issue, string memory dat_rec, string memory rec_Name, uint ID)

Metamask creates an interface between proposed application to the etherum Blockchain using Ropsten network.

Initially, Metamask consists of some ETH balance to process the function set ( )
For (i = 1; i <= total users ; i++)

If ((Eth_bal == Null) or (Eth_Bal < mini_bal))
Not processed the set ( )

Else
Fig. (2). Flow Transactions among the system objects.
Fig. (3). Smart contract deployed results over an Ethereum blockchain.

Processed and generates a blockchain based ID to the medical document.

\[
\text{Medi}_{-}\text{Cert}(\text{Transaction}) = \text{BCT}_{-}\text{TID} \ [i]
\]

\[
\text{Medi}_{-}\text{Cert}(\text{Block}) = \text{BCT}_{-}\text{BID} \ [i]
\]

This process repeats for all the users.

4. RESULTS

The proposed system implemented using solidity programming language and Remix IDE. Metamask, a web-based Wallet used for crypto-balance (E³⁰) to run the system operations. Temporary cryptocurrency, referred to as eth [36], is available in the wallet to execute the functions on IDE. While deploying a contract of a medical document on Remix IDE, initially receives a notification from the metamask as shown in Fig. (3). After confirmed the notification, only an available block has assigned for the corresponding smart contract. The Gas used to deploy the smart contract, total transactions in the block, and the miner address who have organized the smart contract transaction into block detail are shown in Fig (1).

Fig. 4 shows information about the block's status as 'Success' and contract created addresses in terms of 'from' and 'To'. It shows the required transaction fee and gas price to deploy the connection establishment between the proposed application to the blockchain smart contract over Ropsten network-based blockchain [37]. Each transaction maintains in the block with its hash value. A hash value of the current smart contract is shown in Fig 4.

Fig. 5 shows details of the user medical document set in the proposed system application. Metamask notification received while compiling the set ( ) operation on the remix ethereum blockchain. A transaction has been generated in the Blockchain after confirming the metamask interface. Fig. 5 shows the details about the consumed gas fee to perform the 'set ( )' operation.
Fig. (4). Metamask connection confirmation to process the smart contract over the blockchain network.

```
| Transaction Hash: | 0x0c349074a86c5d0ce23d366451cf55e8d904680f7d8cfe8d852b3a75cd1fe9 |
| Status:           | Success                                                               |
| Block:            | 9667023                                                               |
| Timestamp:        | 1 min ago (Feb-15-2021 09:06:19 AM +UTC)                              |
| From:             | 0x2f6a1a333a823c566bdc45ee3966f9411c41a127                            |
| To:               | [Contract 0xa93c61b54e43236b405056cb39a0e9678deaf024 Created]         |
| Value:            | 0 Ether ($0.00)                                                       |
| Transaction Fee:  | 0.00199488571131 Ether ($0.000000)                                    |
| Gas Price:        | 0.0000000001658812049 Ether (1.688812049 Gwei)                        |
```

Fig. (5). Verification of a medical certificate after confirmed the contract on metamask.

```
<table>
<thead>
<tr>
<th>set</th>
</tr>
</thead>
<tbody>
<tr>
<td>reg_No:</td>
</tr>
<tr>
<td>hos_Name:</td>
</tr>
<tr>
<td>doc_Name:</td>
</tr>
<tr>
<td>cer_Type:</td>
</tr>
<tr>
<td>gen:</td>
</tr>
<tr>
<td>cer_hot_Name:</td>
</tr>
<tr>
<td>dat_issue:</td>
</tr>
<tr>
<td>ID:</td>
</tr>
</tbody>
</table>
```
Fig. (6). Birth Certificate block details over Ropsten blockchain Network.

Fig. (7). Birth Certificate block details over a Ropsten Testnet (Ethereum Blockchain).
A Study on Privacy Preservation of Medical Certificates

Recent Patents on Engineering, 2021, Vol. 15, No. 1

Table 2. Proposed system operations costs on Ropsten Ethereum blockchain

<table>
<thead>
<tr>
<th>Operations/Properties</th>
<th>Smart Contract ()</th>
<th>Medical Document setup ()</th>
</tr>
</thead>
<tbody>
<tr>
<td>Block Number</td>
<td>9667023</td>
<td>9667832</td>
</tr>
<tr>
<td>Gas used</td>
<td>4,089,269 (51.12%)</td>
<td>2,945,452 (36.82%)</td>
</tr>
<tr>
<td>Gas Limit</td>
<td>8,000,000</td>
<td>8,000,000</td>
</tr>
<tr>
<td>TxDN size (in bytes)</td>
<td>19,496</td>
<td>13,494</td>
</tr>
<tr>
<td>Mined by</td>
<td>0x56a8e9614f19e46c7e2f60cfcda217ca65e960a60</td>
<td>0x2830b5a3b5242bc64ce390594ed971e7d4d7d2</td>
</tr>
<tr>
<td>Hash</td>
<td>0xbafae4f4168f02c24cad209c7062d5ca026b68d32d1521324021def8c9b972</td>
<td>0xbe6d197351d298fb0e19e6220e4021359ede41a03c3e671fcb734a871c76ec4d</td>
</tr>
</tbody>
</table>

Table 3. Comparison with the existing systems.

<table>
<thead>
<tr>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
<th></th>
</tr>
</thead>
<tbody>
<tr>
<td>Designed/Implemented</td>
<td>Designed No results</td>
<td>Designed No results</td>
<td>Designed No results</td>
<td>Designed Theory</td>
<td>Designed</td>
<td>Designed Implemented</td>
<td>Designed Implemented</td>
<td>Designed Implemented</td>
<td>Designed Implemented</td>
<td></td>
</tr>
<tr>
<td>Application</td>
<td>EMR</td>
<td>Health care</td>
<td>Medical Data</td>
<td>HER</td>
<td>Challenges in Health care</td>
<td>Vehicular Ad-hoc Network</td>
<td>Securing Crowdsourcing</td>
<td>Voting</td>
<td>Agri products</td>
<td>Medical certificates</td>
</tr>
<tr>
<td>Used/considered Blockchain</td>
<td>Public</td>
<td>Public</td>
<td>Public</td>
<td>Public</td>
<td>Private</td>
<td>Consortium</td>
<td>Hybrid</td>
<td>Ethereum</td>
<td>Public</td>
<td>Ethereum</td>
</tr>
</tbody>
</table>

A birth certificate option is chosen in the proposed system application to get a blockchain-based ID to the user's medical document, as shown in Figs 5 and 6 gives the data about the certificate's location in the Blockchain as mentioned as block number and transaction hash. The status of the transaction represents as 'success' in Fig. 6. The consumed Gas price and the transaction fee for deploying the function 'set (' as mentioned in Fig. 6.

Fig. 7 gives the information about a block where the 'birth certificate' related transaction is stored. Moreover, showing the details about its size, consumed gas value, and minor address.

5. DISCUSSION

Blockchain technology plays an essential role in the medical field. The proposed application system implemented results on ethereum based Blockchain have shown in the earlier session. Table 2 is showing the consumed cost for operating the proposed system tasks on Ropsten based ethereum blockchain. And also showing some other details, such are the block number and the address of the transactions, and miner details. Initial smart contract () and user medical details set up in the blockchain database i.e, setup () operations of the proposed application have operated on the public Blockchain.

Table 3 shows the information about the existing works using blockchain technology. The applications have been designed by the researchers but failed to present the results in their work. The proposed work's main strength is to design the application and present the deployment results using Ethereum based public Blockchain. Moreover, the application operations' consumption costs over a ropsten network-based blockchain were also presented in the discussion session.

CONCLUSION

The medical sector is essential in society and has many sensitive data about the users: physicians, patients, and also other data maintained by this sector databases. Privacy preservation of the medical sector data is an essential factor in an insecure society. Hence, the proposed work uses to generate and preserve the medical certificates using an advanced feature technology blockchain. This application uses to create a unique ID for the user's certificate. That can either birth or death or sick medical document. Users can carry that unique ID instead of bringing their physical record to submit anywhere.
FUTURE DEVELOPMENT

In the future, we would like to design and develop a front-end-based distributed application (DAPP) for this application using TestRPC. Public blockchain-based architecture would like to design for future work. It makes it more users friendly that helps to increase the utilization rate of the application.

CONSENT FOR PUBLICATION

Not applicable.

FUNDING

None.

CONFLICT OF INTEREST

The authors declare no conflict of interest financial or otherwise.

ACKNOWLEDGEMENT

I thank Dept. of CSE of Lincoln University College for giving cooperation to complete this work.

REFERENCES


[11] Anna Bayadakova, "Moscow said to hire Kaspersky to build voting blockchain with bifurcy software", Article from CoinDesk


X. Zhang, and S. Poslad, "Blockchain support for flexible queries with granular access control to electronic medical records (EMR)", *IEEE International Conference on Communications (ICC)*, 2018pp. 1-6 Kansas City, MO

DISCLAIMER: The above article has been published, as is, ahead-of-print, to provide early visibility but is not the final version. Major publication processes like copyediting, proofing, typesetting and further review are still to be done and may lead to changes in the final published version, if it is eventually published. All legal disclaimers that apply to the final published article also apply to this ahead-of-print version.