2021 International Conference on Advance Computing and Innovative Technologies in Engineering (ICACITE) | 978-1-7281-7741-0/20/$31.00 ©2021 IEEE | DOI: 10.1109/ICACITE51222.2021.9404654

Extended Privacy Preservation of Health Official Document using blockchain

Ch. Rupa
Dept. of CSE
Lincoln University College
rupamtech@gmail.com

Divya Midhun Chakravarthy
Dept. of CS and Multimedia
Lincoln University College
divya@lincoln.edu.my

***Abstract*—Currently, new models such as mobile clouds and data warehouses have been selected to handle records. This approach reduces costs and increases availability. However, these technologies face some problems due to uncertainties, such as data privacy, flexibility, network security, attacks, and missing transparency. In particular, sensitive applications data such as medical certificates, data distribution, and student certificate maintenance. It is essential to check the reliability of these applications. The number of scams on this issue is increasing day by day. Therefore, in this paper, we propose a blockchain-based model for the issuance and distribution of medical certificates. It reduces fraud on medical certificates such as birth, death, and sick leave due to the blockchain technical features such as immutability, transparency, security, and distribution. Furthermore, this application's vital purpose is to quickly analyze and estimate the birth and death rate due to blockchain symptoms. As part of the literature survey number of existing works were interpreted as part of the literature survey, but the maximum number of documents failed to show their implementation with the results. The main strength of the paper is the literature survey, results, and analysis. Distributed based public blockchain and metamask used to develop the proposed framework. The results show medical certificate generation and verification and the gas(cryptocurrency) consumption to store certificate credentials into a blockchain as a transaction**

***Keywords—Blockchain, Medical certificate, Transparent, Immutable, Issue, verify, Remix, Metamask*.**

I. Introduction

MIT uses blockchain technology for issuing virtual diplomas to their students using "Blockcert Wallet". Blockcert is the first open standard to create, issue, view, and verify the blockchain certificates [1]. Currently, designing Blockchain-based applications increases due to its features such as immutable, transparency, security, accountability, and distributed [2]. There is a possibility to enhance features of applications with the association of other advanced technologies such as the Internet of Things (IoT) [3], Data Analytics [4], Machine learning [5], Artificial Intelligence [6], and cloud computing [7]. This hybrid design helps to achieve specific characteristics such as portability, accessibility, and availability.

Cryptography underlying any technology helps make sure of authentication on data communication [8]. It gives assure the digital content receives from a trusted source. In a blockchain, all blocks have interconnected with a cryptographic-based one-way hash value [9]. Blockchain achieves immutable feature by this process. In blockchain, all verified transactions maintain in blocks. Later those blocks will enter into the blockchain after confirming by specific nodes. The verifying process nodes are referred to as minors [10]. All blocks in blockchain have to be affected if any block value changes due to their interconnected feature. All nodes in the blockchain know about all the transactions because of its distributed architecture [11]. Each node maintains a ledger about all the transactions. Blockchain technology has been achieving the transparency feature in this way.

Four types of blockchains are available: private, i.e., Consortium blockchain, and Hybrid Blockchain. But both have inherited the feature of accountability. In a public blockchain, all the transactions are processed by verifying cryptocurrencies in the Wallet [12]. Suppose there is no enough balance in the Wallet, then unable to do the process. In a private blockchain, only registered nodes can able to participate in the process [13]. But in the consortium blockchain, that is a semi-decentralized one managed by more than one organization. The combination of private and public blockchain is referred to as hybrid blockchain. All blockchain technologies use consensus protocols [14] such as proof of work (PoW), proof of stack (PoS), Byzantine, and other types in their process.

So many countries want to conduct their elections by a fully transparent voting system using blockchain technology. Already, Russia has launched a blockchain-based E-voting system pilot project with the association of the City Election Commission of Moscow and the Department of Information Technology (DIT) [15]. Similarly, some countries like the United States, Netherlands, UK, Sweden, and India announced that blockchain technology-based real estate and land registry process give services shortly [16]. Currently, blockchain technology is used in health care centers to store and maintain records. It helps to attack resistance on health care records [17]. It extends to that technology being applies to the design and development of various applications related to Education sectors, supply chain [18], Food processing [19], Oil and Gas Industries [20], Biomedical [21], etc.

In this paper, we proposed a system for generating and managing medical certificates using blockchain technology. The doctors issue these for various reasons like birth certificates, death certificates, and health issue certificates to claim their leaves in their working environment. This application helps to avoid fraud in the generation of medical certificates from the Health care center. It helps to maintain the sensitive data on certificates with tamper-free and transparence.

The rest of the paper was organized as follows. Related works and comparisons with the proposed system by considering specific characteristics are discussed in section 2. Proposed system architecture and its functional modules are discussed in section 3. Section 4 consists of results and analysis. Conclusion and future scope of the work depicts in section 5.

II. LITERATURE SURVEY

Jiaqi Yan et al. [18] proposed a framework called SCQI for supply chain management using blockchain technology. This architecture consists of four layers with different IoT layers, Data Layer, Contract Layer, and Business Layers. All these layers' functionalities were discussed clearly by the authors as a part of the designing system architecture. This work's main drawback is no details about implementation set up and analysis on existing approaches except referring to a system proposed by china for agri-food traceability. Dianhui Mao et al. [19] proposed a novel food tracing system using consortium blockchain that improves the security and trust in transactions. This paper addressed about profits improvement methods of merchants by using blockchain methodology. Moreover, the authors introduced a smart contract life cycle management approach that helps optimize food transactions.

HongFang Lu et al. [20] discussed the importance of blockchain technology, especially in the oil and gas industries. Here, the authors have considered five aspects as Trading, management, decision-making, and security to describe blockchain's role. This paper also consisted of information about risks, challenges, and opportunities, and development trends in the oil and gas industries. The main drawback of this work is doesn't have proper implementation and designing specification using blockchain technology. Table 1 gives a summary of the literature survey.

George Drosatos et al. [21] presented the scope of blockchain technology in the biomedical domain. This work's main strength is a literature survey that shows maximum results are still in the conceptual or designing phase only. Here, the authors have discussed information sources, required protocols, data charting, and synthesizing the results. Also, this paper doesn't mention any implementation specifications which are needed for this application. And again, Shrier [22] has discussed the infrastructure of the blockchain.

AsmaKhatoon [23] designed a blockchain technology model to manage medical data with clinical and surgery trails procedures. In this work, the author discussed how data has exchanged among the stakeholders with transparency while collecting the medical data. Zhang et al. [24] examined various Blockchain-based use cases of healthcare-related. In this paper, the authors have specified how effectively designing healthcare systems using blockchain technology and its importance in health care systems. Siyal et al. [25]discussed the importance of smart contracts and blockchain technology in healthcare systems. And also concerned about how can reduce fabrication and loss of medical data by using distributed ledger-based blockchain technology.

TABLE I. SUMMARY OF RELATEDWORKS

Authors	Characteristics						
	Blockchain Technology	**Regulatory Authority**	**Design/ Implemented**	**Access Control**	**Tool**	**Identity Management**	**Data Privacy**
[17]	Private	Yes	Both	Yes	Hyper ledger Caliper	Yes	Yes
[26]	Public	No	Only Designed No implement	No	Not specified	No	Yes
[27]	Public	No	Only Theorey proof	No	Not specified	No	Yes
[28]	Public	No	Only designed No implement	No	Not specified	No	Yes
[29]	Public	No	Both	No	Ethereum	Yes	Yes
[30]	Public	No	Only Designed	No	Not specified	No	Yes
[32]	Consortium	Yes	Implemented	Yes	DSSCB VANET	Yes	Yes
[34]	Consortium	Yes	Only Designed	Yes	Not specified	Yes	Yes
Proposed Method	Public	Yes	Implemented	Yes	Remix	Yes	Yes

III PROPOSED METHODOLOGY

In the health care sector, different applications developed using Blockchain technology. The proposed system is for medical certificates to maintain in blockchain purpose issued by the health care centers [26,27]. This framework implementation supports public blockchain, which reduces fraud in holds medical certifications like birth, death, sick, etc. Ethereum used to implement the proposed medical certificate blockchain smart contract system. Fig 1 shows that the system modules and their functional transactions. The smart contract of each module compiled into byte code using different platforms. Here, the Remix platform is used to compile a smart contract, and Metamask wallet used for Eth balance.

Initially, all hospitals required to take registration with a unique identity at the regulatory authority. Only registered hospitals will be allowed to authorize the medical certificates of users or patients. Every medical certificate needs to approve by a concerned authority from the hospital [28]. Whether it may be birth or death or sick leave purpose certificates. Moreover, that certificate needs to get approval from the central regulatory authority after verifying all the user or patient records. The proposed system consists of four modules: health care centers (hospitals), Hospital Authority, Central regulatory authority, and User/patient. Every module of the network has its functions, like issuing a certificate, authorizing, verifying, and revoking once it generates a certificate here, impossible to alter or modify or delete from this system because of blockchain's property technology i.e., immutable [29,30].

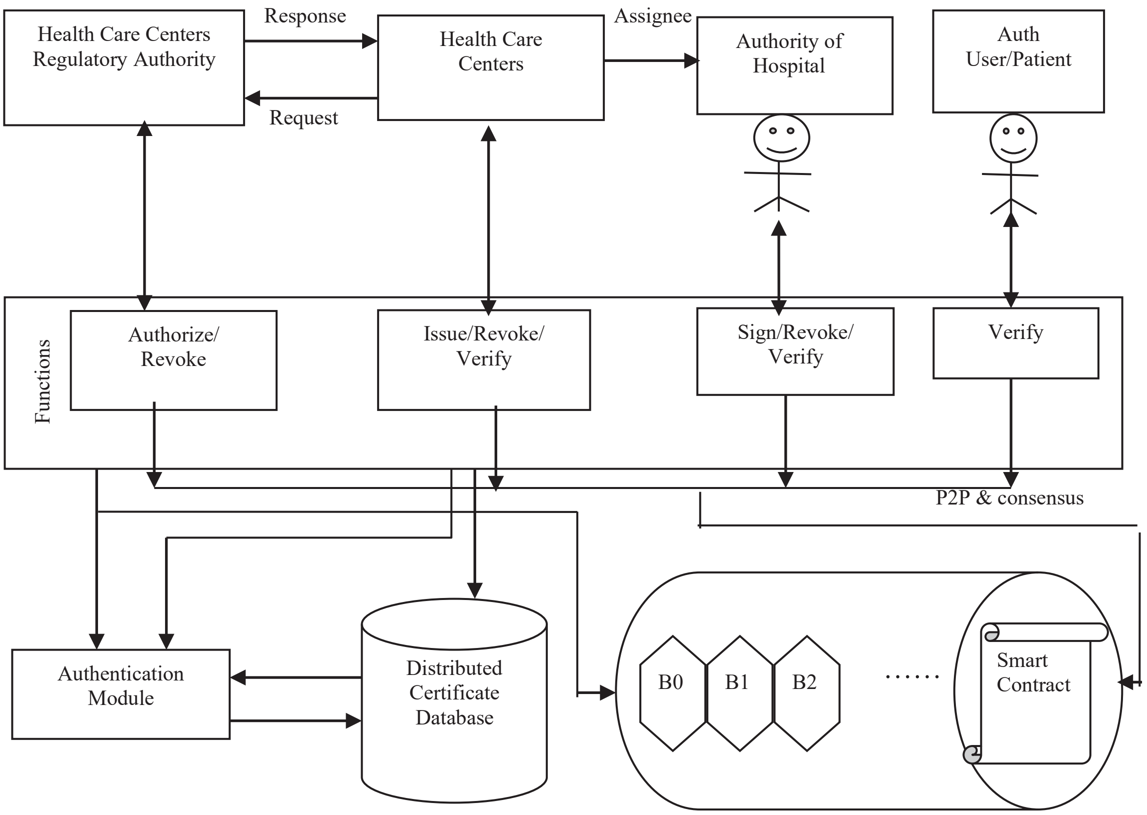


Fig 1. Proposed system Methodology

3.1 Smart contract for Medical Certificate

It is a core module of the proposed system used to provide communication between the system modules to the blockchain network. Solidity programming language [31] is used to write the smart contract. These smart contracts compiled and tested on Remix IDE [32] and Metamask [33]. The structure of the medical certificate using solidity is as follows:

```
Structissue_certificate contains
          String Hospital_Name_ID
          String recipient_ Name_Address
          String patient_Name_Address
          String certificate_type
          String doctor_Name
          String _date
          String  Remarks
          bytes32  Cert_hash
```

- Hospital_Name_ID: Full name of the hospital issuing a certificate and its unique ID issued by the central regulatory authority.
- Recipient_Name_Address: Certificate receivers' details like Name, phone number and other details
- Patient_Name_Address: This filed gives detail about the patient to whom the certificate is issuing.
- Certificate_Type: It represents for which purpose certificate is issuing such as birth or death or sick
- Doctor_Name: This field gives information about the authorized person from the health care center to issue the certificates
- _Date: On which date the certificate is issuing.
- Remarks: This filed gives information about the health condition or reason for sick leave, etc
- Cert_hash: It is a unique ID of the certificate generated based on the certificate's contents that will be used to refer to a specific certificate issued by a central authority.

3.2 Details of Implementation

Filling and issuing process of Medical Certificates by the healthcare centers and central regulatory authority discussed here. Moreover, the hospitals registration process also discussed here. Remix ethereum public blockchain and metamask wallet have been used to implement and achieve the proposed system's main objectives [34,35]. Algorithm 1 shows the healthcare center registration at the central regulatory authority. Initially, health care centers or hospital Send their details like address, hospital name, and hospital authority details to the central regulatory authority to register. Regulatory authority verifies the elements, whether it is registered or not. Reject the application if it is already registered; otherwise, assigned a unique ID based on the hospital address, hospital name, and authorized person of the hospital details. One way hash function has to be used to generate a unique ID for the health care center

```
Algorithm 1: Hospital_register ( )

Input: Address of the hospital (health care centers), Authority
person details
Output: An unique ID assigned in terms of address or Hash
based on the input

Step 1: Health care centers ready to take registration
        Reg_health_ID=Addr(health_centers)||
Auth(Health_centers)
Step 2: Verify the cetral regulatory system
        If (Reg_health_ID or uh_ID = existed)
        Revoke the registration otherwise goto step 3
Step 3: Generates a hash value for Reg_health_ID and it is
considered as unique ID of the health care centers.
uh_ID = Hash(Reg_health_ID)
Step 4: Repeat the process
```

Algorithm 2 shows issuing a certificate to the patients or users by the health care centers or hospitals. This certificate generates based on the details of the certificate requested person, patient, and hospital details. This BCT based unique ID certificate has to be developed with immutable, attack free, transparent, and distributed features. All the participant's details consider as attributes to write a smart contract for this process.

```
Algorithm 2: Issue_Certificate ( )

Input: patient details, Hospital details
Output: Blockchain-based Unique ID generation, which is an
immutable document with transparent z     and distributed
natures
Step 1: Set the details of patient, requested user, and hospital
in a smart contract
Step 2: Connect to the metamask Wallet
Step 3: Deploy smart contract on Ethereum (Remix)
Step 4: Confirm smart contract interaction over Metamask
        If( contract interaction = = completed)
        ut_IDk=Transaction [Block i] = contract details
otherwise go to step 5
Step 5: Exist from the process.
```

Algorithm 3 depicts the step by step process of integrity checking of a medical certificate using blockchain technology. Through this application, the user can prove, submit, and show his medical certificate without carrying any documents along with him. Anytime and anywhere easily can show and verify the user medical certificate with his blockchain-based unique ID i.eut_IDk, without taking any physical records [36]. The user medical certificate has maintained as a transaction in a blockchain block with a unique ID (ut_IDk). No one was able to modify or delete these ledgers' details. Moreover, it is transparent and distributed to all registered nodes in the blockchain network

```
Algorithm 3: Verify_Certificate ( )

Input: Identity of medical certificate
Output: Existed or not

Step 1: Enter a Unique ID (Ut_IDk) of the medical certificate
Step 2: Verify whether it existed or not
        If(Ut_IDk == Existed)
        Accepted otherwise go to step 3
Step 3: Requested Revoked and considered it as not existed.
```

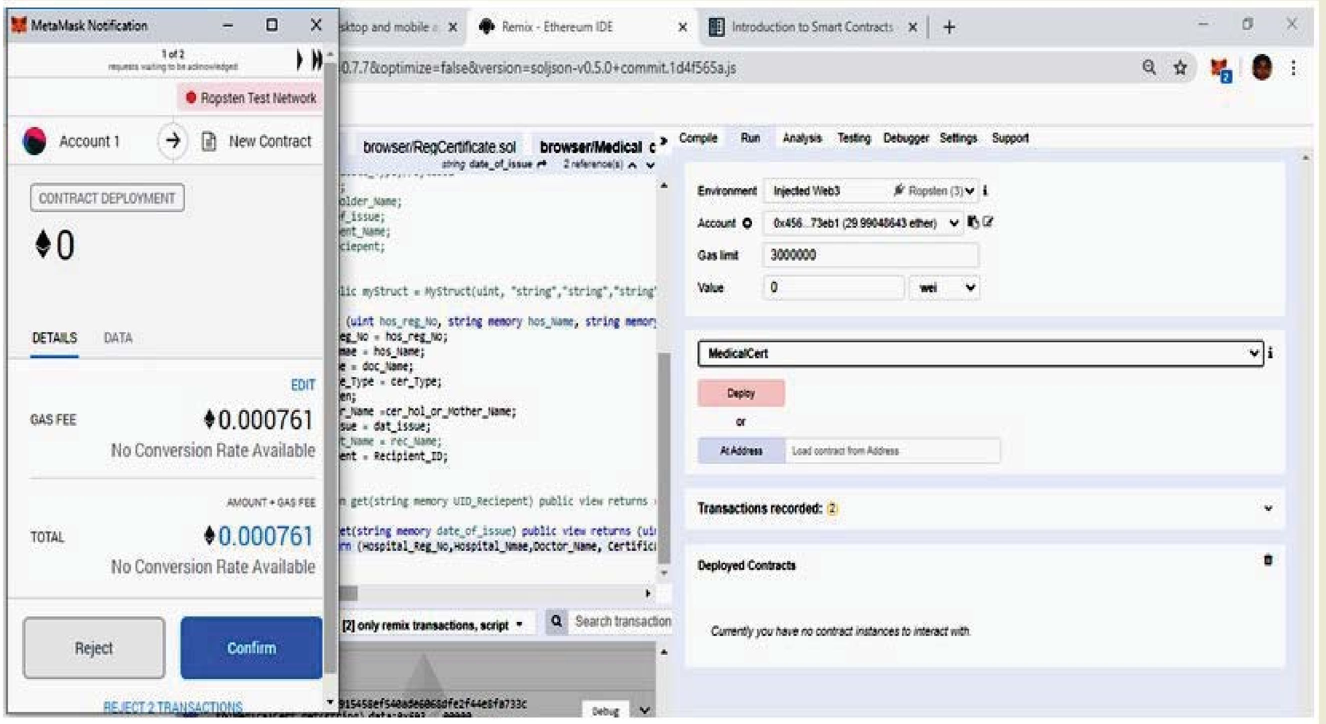
IV. RESULTS & ANALYSIS

We selected Remix Etherumblockchain and Metamsk as the underlying technology for our application. The remix is an open source-based ecosystem that adopts a blockchain environment. Metamsk wallet consists of temporary cryptocurrencies in terms of Eths [35].

This Eth value consumes from a wallet for every transaction when a contract has deployed on the blockchain. Here Eth consumption happens in terms of Gas [35]. Fig 2 shows that Metamask connection request to establish a connection with the smart contracts. The link has to be established after confirming the claim. Here we used the Ropsten Test network to trace the transactions over a blockchain.

We are required to pay the crypto balance to deploy the smart contract on a network. This application helps like no need to carry any physical records of a medical certificate to submit or for verification. Once a medical certificate generates on a blockchain, authorized persons can access it with its unique ID. Fig 3 shows the confirmation of the generated medical certificate at the hospital level based on a specific date.

Fig 4 shows the deployment of a smart contract written to issue a medical certificate by the hospitals. To process this, required to pay cryptocurrency from the Wallet that to be collected as gas.Later, after getting the confirmation, 0.000196 eth collects as a Gas fee for placing these records as a transaction in a block. Fig 5 shows the consumption of Gas to generate the medical certificates. Here we tested by generating the 100 certificates. To generate a single certificate, consumed 137622, for generating 10 certificates, it took 1376220, like this 6881100 consumed for generating 50 certificates. As well as 13762200 finished for 100 certificates



0

GAS FEE 0.000761
No Conversion Rate Available

AMOUNT + GAS FEE
TOTAL 0.000761
No Conversion Rate Available

0.7.7&optimize=false&version=soljson-v0.5.0+commit.1d4f565a.js

string date_of_issue 2 reference(s)

```
;
older_Name;
f_issue;
ent_Name;
ciepent;

lic myStruct = MyStruct(uint, "string","string","string'

(uint hos_reg_No, string memory hos_Name, string memory
eg_No = hos_reg_No;
ame = hos_Name;
e = doc_Name;
e_Type = cer_Type;
en;
r_Name =cer_hol_or_Mother_Name;
sue = dat_issue;
t_Name = rec_Name;
ent = Recipient_ID;

n get(string memory UID_Reciepent) public view returns

et(string memory date_of_issue) public view returns (ui
rn (Hospital_Reg_No,Hospital_Nmae,Doctor_Name, Certifica
```

[2] only remix transactions, script

```
915458ef540ade6068dfe2f44e8fa733c
```

Environment: Injected Web3 Ropsten (3)
Account: 0x456...73eb1 (29.99048643 ether)
Gas limit: 3000000
Value: 0 wei

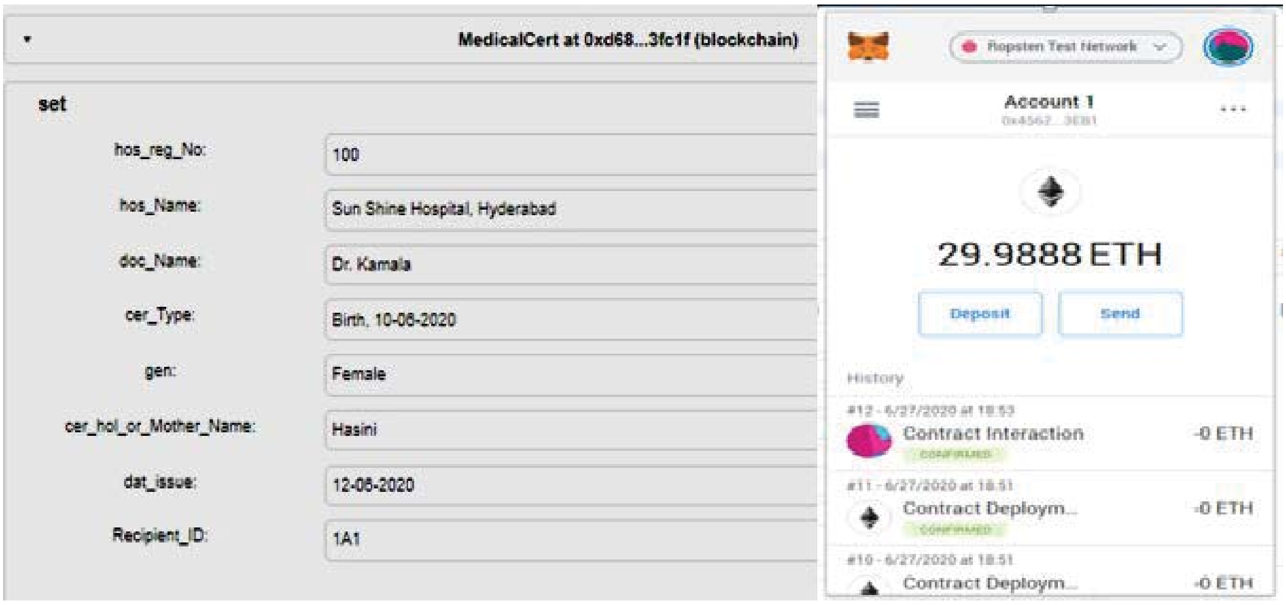
MedicalCert

Transactions recorded: 2

Deployed Contracts

Currently you have no contract instances to interact with.

Fig 2. Metamask connection confirmation to process the smart contract over the blockchain network



MedicalCert at 0xd68...3fc1f (blockchain)

set

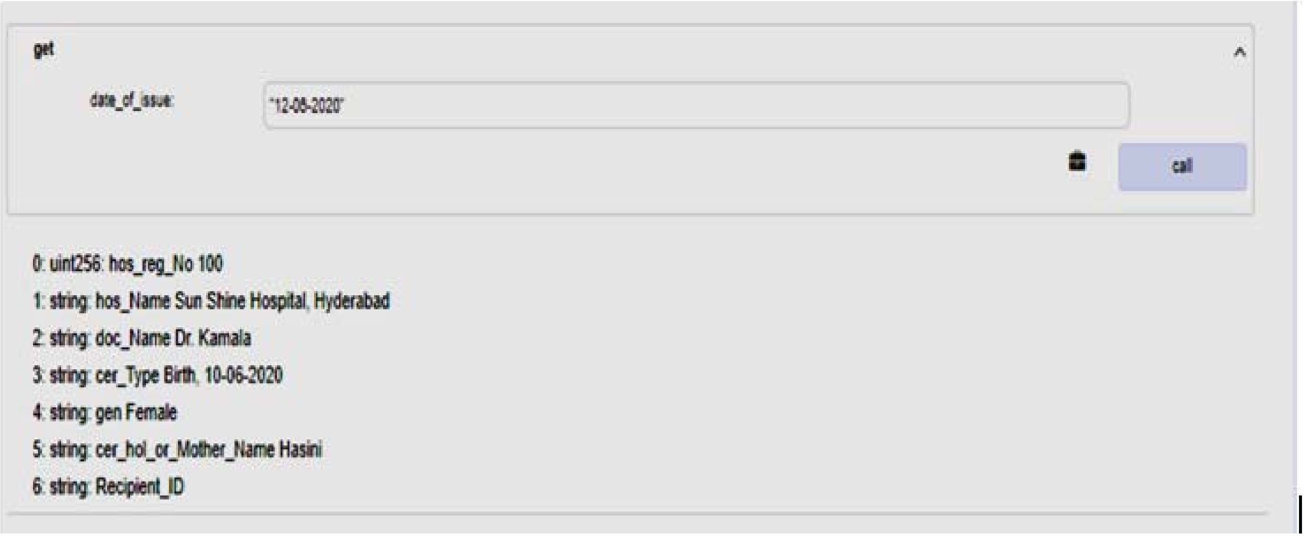
hos_reg_No: 100
hos_Name: Sun Shine Hospital, Hyderabad
doc_Name: Dr. Kamala
cer_Type: Birth, 10-06-2020
gen: Female
cer_hol_or_Mother_Name: Hasini
dat_issue: 12-06-2020
Recipient_ID: 1A1

Account 1
0x4562...3EB1

29.9888 ETH

#12 - 6/27/2020 at 18:53 Contract Interaction CONFIRMED -0 ETH
#11 - 6/27/2020 at 18:51 Contract Deploym... CONFIRMED -0 ETH
#10 - 6/27/2020 at 18:51 Contract Deploym... -0 ETH

Fig 3. Verification of a medical certificate after confirmed the contract on metmask



date_of_issue: "12-06-2020"

0: uint256: hos_reg_No 100
1: string: hos_Name Sun Shine Hospital, Hyderabad
2: string: doc_Name Dr. Kamala
3: string: cer_Type Birth, 10-06-2020
4: string: gen Female
5: string: cer_hol_or_Mother_Name Hasini
6: string: Recipient_ID

Fig 4. Smart contract deployment process to issue a medical certificate

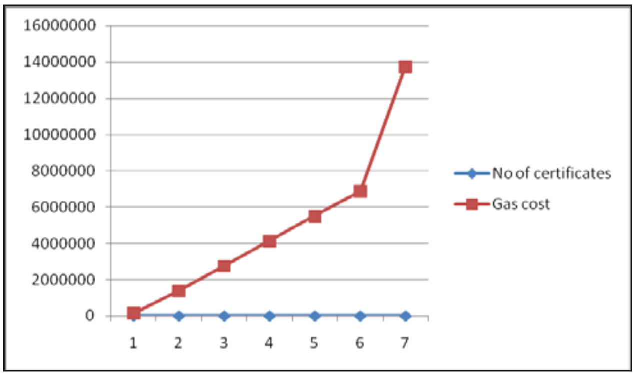


Fig 5. Gas consumption for medical certificates

Table 2 shows the Gas costs of the smart contracts for issue_certificate () function and verify_certificate ( ) the proposed system's operation. These smart contract functions execute by the communication parties of the proposed method. Verification cost is lease because it does not perform any modifications in the blockchain. Issue_vertificate cost is more because some changes occurred on blockchain in terms of storing variables states.

Table 2. Cost of smart contract functions

Caller	**Function Name**	**Gas cost**	**TxN size (bytes)**
Healthcare Center	Issue_Certificate( )	152010	337
Healthcare Center, Auth user/patient	Verify_Certificate()	76412	233

Gas price denoted in gwei. Ether unit represents with GWEI i.e., Giga wei. Where wei is the smallest unit of ether, it is worth 0.000000001 ether. Fig 6 shows the gas price for generating the medical certificates. In the same way, fig 7 represents eth consumption for generating the certificates range from 1 to 100. These analyses performed based on the results generated on the ropsten network-based blockchain.

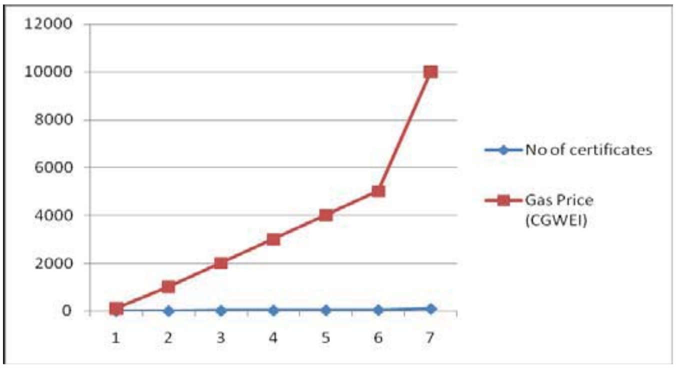


Fig 6. Gas price for Medical certificates

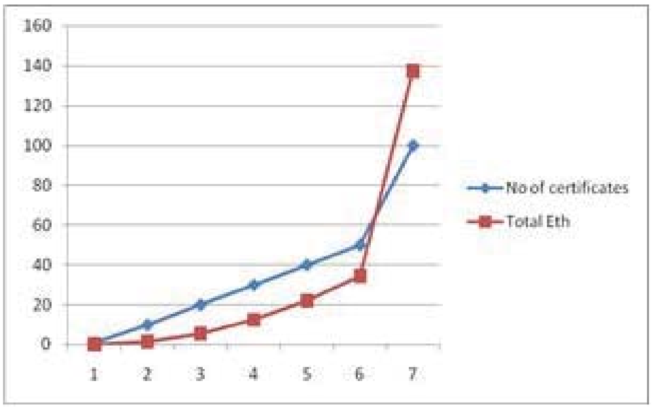


Fig 7. Total Eth consumption for certificates generation

CONCLUSION

Blockchain technology helps to reduce fraud in the distribution and maintenance of medical certificates. The proposed system helps to automate the certificate generation and verification process using public blockchain technology. This application supports distributed data with attack resistance and avoids a single point of failure and a central authority system. It is a tamper-free application due to its immutable feature. Moreover, every node in blockchain's communication network will notify about new entries in every node's ledger. It means that every node gets information about an original medical certificate generated in a block as a transaction due to its transparent feature. Cryptocurrency balance is required to perform any action on public blockchain. Here matamask Wallet was used to get cryptocurrency in terms of Eths. 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.

REFERENCES

1. "Blockchain Credentials," Blockcerts, 2019. [Online]. Available: https://www.blockcerts.org.
2. A. A. Monrat, O. Schelén, and K. Andersson, "A Survey of Blockchain From the Perspectives of Applications, Challenges, and Opportunities," IEEE Access, vol. 7, pp. 117134-117151, 2019.
3. Sk.Irfan, K. Ch. Rupa, K. Vinay, M. Krishna Veni, R. Rachana, "Smart Virtual Circuit based Secure Vehicle Operating System," IEEE International conference on innovative mechanisms for industry applications, Bangalore, India, 2020
4. C. Komalavalli and C. Laroiya, "Challenges in Big Data Analytics Techniques: A Survey," 2019 9th International Conference on Cloud Computing, Data Science & Engineering (Confluence), Noida, India, pp. 223-228, 2019.
5. T. SatyaSudha, Ch. Rupa, " Analysis and Evaluation of Integrated Cyber Crime Offences using Machine Learning Techniques, "IEEE International conference i-pact 2019, VIT- Vellore, March 23, 2019
6. Khaled Salah, M. Habib Ur Rehman, NisharaNizamuddin, Ala Al-Fuqaha, "Blockchain for AI: Review and Open Research Challenges," IEEE Access, Vol . 7, pp. 10127-10149, 2019
7. BahramRashidi, "Authentication issues for cloud applications," IET Authentication Technologies for cloud computing, IoT and Big Data, pp. 209-240, 2019.
8. Ch. Rupa, Devi, "Privacy and Protection of Medical Images ROI Using SPLSB and Bit-plane based Watermarking, "ACM International Conference on Cryptography, Security and Privacy 2019, University of Malaya, Malaysia, 19th – 21st January 2019
9. H. Liu, A. Kadir, and J. Liu, "Keyed Hash Function Using Hyper Chaotic System With Time-Varying Parameters Perturbation," in IEEE Access, Vol. 7, pp. 37211-37219, 2019.
10. Md. Turkanovic, M. Holbl, K. Kosic, M. Hericko, and A. Kamisalic, "EduCTX: A blockchain-based higher education credit platform," IEEE Access, pp. 1–20, 2018.
11. H. Paik, X. Xu, H. M. N. D. Bandara, S. U. Lee and S. K. Lo, "Analysis of Data Management in Blockchain-Based Systems: From Architecture to Governance," in IEEE Access, vol. 7, pp. 186091-186107, 2019.
12. Ch. Rupa, D. Jaya Kumari," Network-Based Adaptation of Blockchain Technology," International Journal of Innovative Technology and Exploring Engineering, Vol.8, No.9, 2019.
13. S. Pongnumkul, C. Siripanpornchana and S. Thajchayapong, "Performance Analysis of Private Blockchain Platforms in Varying Workloads," 2017 26th International Conference on Computer Communication and Networks (ICCCN), Vancouver, BC, pp. 1-6, 2017
14. K. Sharma and D. Jain, "Consensus Algorithms in Blockchain Technology: A Survey," 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, pp. 1-7, 2019.
15. Anna Bayadakova," Moscow said to hire Kaspersky to build voting blockchain with bitfury software," Article from Coindesk, 2020
16. Hugo Pieter Wouda, Raymond Opdenakker," Blockchain technology in commercial real estate transactions," Journal of property investment & Finance, Vol. 37, No.6, 2019.
17. SudeepTanwar, Karan Paresh, Richard Evans, "Blockchain-based electronic healthcare record system for healthcare 4.0 applications", Journal of Information security and Applications, Vol. 50, 2020,
18. S. Chen, R. Shi, Z. Ren, J. Yan, Y. Shi, and J. Zhang, "A Blockchain-Based Supply Chain Quality Management Framework," 2017 IEEE 14th International Conference on e-Business Engineering (ICEBE), Shanghai, pp. 172-176, 2017.
19. Mao, D., Hao, Z., Wang, F. et al. Novel Automatic Food Trading System Using Consortium Blockchain. Arab J SciEng, Vol. 44, pp. 3439–3455 2019.
20. H. Lu, K. Huang, M. Azimi, and L. Guo, "Blockchain Technology in the Oil and Gas Industry: A Review of Applications, Opportunities, Challenges, and Risks," in IEEE Access, vol. 7, pp. 41426-41444, 2019.
21. George Drosatos, EleniKaldoudi, "Blockchain Applications in the Biomedical Domain: A Scoping Review," Computational and Biotechnology Journal, Vol. 17, pp. 229-240, 2019.
22. Shrier, D.; Wu, W.; Pentland, A. Blockchain& infrastructure (identity, data security). Mass. Inst. Technol. Connect. Sci. pp.1–19, 2016.
23. AsmaKhatoon, "A Blockchain-Based Smart Contract System for Healthcare Management," Journal of Electronics, Vol. 94, No.9, 2020
24. Zhang, P. Schmidt, D.C. White, J. Lenz, G. "Blockchain Technology Use Cases in Healthcare. In Advances in Computers; Elsevier: Amsterdam, The Netherlands", Vol. 111, pp. 1–41, 2018
25. Siyal, A. Junejo, A. Zawish, M. Ahmed, K. Khalil, A. Soursou, G. "Applications of Blockchain Technology in Medicine and Healthcare: Challenges and Future Perspectives," Cryptography, Vol. 3, No. 3, 2019
26. 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. Vol. 40, No.10, 2016
27. X. Zhang and S. Poslad, "Blockchain Support for Flexible Queries with Granular Access Control to Electronic Medical Records (EMR)," 2018 IEEE International

Conference on Communications (ICC), Kansas City, MO, pp. 1-6, 2018.

28. Zhng, P. White, J. Schmidt, D.C. Lenz, G. "Design of Blockchain-Based Apps Using Familiar Software Patterns to Address Interoperability Challenges in Healthcare." In Proceedings of the PLoP-24th Conference on Pattern Languages of Programs, Vancouver, BC, Canada, 2017.
29. X. Liu, Z. Wang, C. Jin, F. Li, and G. Li, "A Blockchain-Based Medical Data Sharing and Protection Scheme," in IEEE Access, Vol. 7, pp. 118943-118953, 2019.
30. Wang, H., Song, Y, "Secure Cloud-Based EHR System Using Attribute-Based Cryptosystem and Blockchain," Journal of Med System, Vol. 42, No. 152, 2018.
31. Kumar, T, Ramani, V, Ahmad, I, Braeken, A., Harjula, E.; Ylianttila, M. "Blockchain Utilization in Healthcare: Key Requirements and Challenges," In Proceedings of the 2018 IEEE 20th International Conference on e-Health Networking, Applications and Services (Healthcom), Ostrava, Czech Republic, 17–20 September 2018.
32. X. Zhang and X. Chen, "Data Security Sharing and Storage Based on a Consortium Blockchain in a Vehicular Ad-hoc Network," in IEEE Access, Vol. 7, pp. 58241-58254, 2019.
33. S. Zhu, H. Hu, Y. Li, and W. Li, "Hybrid Blockchain Design for Privacy-Preserving Crowdsourcing Platform," 2019 IEEE International Conference on Blockchain (Blockchain), Atlanta, GA, USA, pp. 26-33, 2019.
34. Priya, Ch. Rupa, "BlockChain Technology-based Electoral Franchise," IEEE International Conference on Innovative Mechanisms for Industry Applications (ICIMIA), Bangalore, 2020.
35. W. Hong, Y. Cai, Z. Yu, and X. Yu, "An Agri-product Traceability System Based on IoT and Blockchain Technology," IEEE International Conference on Hot Information-Centric Networking (HotICN), Shenzhen, pp. 254-255, 2018.
36. Rupa, Gautam, Thippareddy, Praveen Kumar, Sweta, "Security and Privacy of UAV data using blockchain technology", Journal of Information security and Applications, Vol. 55, pp. 1 – 11, 2020