Industry 5.0: Ethereum blockchain technology based DApp smart contract

Article *in* Mathematical biosciences and engineering: MBE · August 2021

DOI: 10.3934/mbe.2021349

CITATIONS
9

READS
945

5 authors, including:

Divya Midhunchakkaravarthy
Lincoln University College, Malaysia
80 PUBLICATIONS **171** CITATIONS
SEE PROFILE

Mohammad Kamrul Hasan
Universiti Kebangsaan Malaysia
197 PUBLICATIONS **998** CITATIONS
SEE PROFILE

Rashid Saeed
Taif University
230 PUBLICATIONS **1,136** CITATIONS
SEE PROFILE

Mathematical Biosciences and Engineering

MBE, 18(5): 7010–7027.
DOI: 10.3934/mbe.2021349
Received: 03 July 2021
Accepted: 12 August 2021
Published: 23 August 2021

http://www.aimspress.com/journal/MBE

Research article

Industry 5.0: Ethereum blockchain technology based DApp smart contract

Ch. Rupa[1], Divya Midhunchakkaravarthy[2], Mohammad Kamrul Hasan[3,*], Hesham Alhumyani[4] and Rashid A. Saeed[4]

[1] Department of Computer Science and Engineering, Lincoln University College, Malaysia
[2] Department of Computer Science and Multimedia, Lincoln University College, Malaysia
[3] Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia, Bangi 43600, Selangor, Malaysia
[4] Department of Computer Engineering, College of Computers and Information Technology, Taif University, P. O. Box 11099, Taif 21944, Saudi Arabia

* **Correspondence:** Email: mkhasan@ukm.edu.my, hasankamrul@ieee.org.

Abstract: The use of advanced technologies has increased drastically to maintain any sensitive records related to education, health, or finance. It helps to protect the data from unauthorized access by attackers. However, all the existing advanced technologies face some issues because of their uncertainties. These technologies have some lapses to provide privacy, attack-free, transparency, reliability, and flexibility. These characteristics are essential while managing any sensitive data like educational certificates or medical certificates. Hence, we designed an Industry 5.0 based blockchain application to manage medical certificates using Remix Ethereum blockchain in this paper. This application also employs a distributed application (DApp) that uses a test RPC-based Ethereum blockchain and user expert system as a knowledge agent. The main strength of this work is the maintenance of existing certificates over a blockchain with the creation of new certificates that use logistic Map encryption cipher on existing medical certificates while uploading into the blockchain. This application helps to quickly analyze the birth, death, and sick rate as per certain features like location and year.

Keywords: Industry 5.0; knowledge agent; health care certificate; remix Ethereum; testRPC; metamask; Logistic Map Encryption cipher

1. Introduction

In Industry 5.0, blockchain technology, and Encryption ciphers play an essential role in designing and deploying various real-time applications. All applications are currently transferring from Industry 4.0 to Industry 5.0 because of increasing adaptability, productivity, and creating a responsive working environment. It has an impact on cost reduction [1]. This technology mainly focuses on the interaction between machines and human intelligence. It helps to design and deploy the applications to a new level of speed and performance.

Furthermore, Blockcert is an open standard used for creating, viewing, verifying, and issuing any blockchain-related certificates [2]. Number of applications such as supply chain, Internet of things (IoT) [3], agriculture [4], aquaculture [5], health care departments can be benefited from the combination of Industry 5.0 and blockchain technology. Rapid growth in blockchain utilization is because of its advanced features like immutability, transparency, distribution, accountability, security, and reliability [6]. Moreover, it enhances the integration of other disruptive technologies [7] like machine learning, artificial intelligence, and others. Therefore, the proposed system is designed by considering domain expert knowledgeable users as entities to automate the proposed proposes over a blockchain. Many countries want to conduct their elections by a fully transparent voting system using blockchain technology. Russia has launched a blockchain-based electronic-voting system pilot project with the association of the City Election Commission of Moscow and the Department of Information Technology (DIT) [8]. Similarly, some countries like the United States, Netherlands, UK, Sweden, and India announced that blockchain technology-based real estate and land registry processes would be started shortly.

This paper discusses the design and development of a distributed application for managing medical certificates. Logistic Map Encryption (LME) cipher [9] is used to encrypt the existing medical certificates before passing them over a blockchain by an expert agent, i.e., a doctor. Generally, a healthcare center's authority issued medical certificates such as birth, death, and sick (HCC). These are issued for various reasons like birth, death, and some health-related issues for employees to claim their leaves in their working environment. This application helps to avoid fraud in the generation of medical certificates from the healthcare centers.

The remaining paper is organized as follows. Section 2 presents a literature survey. The proposed architecture based on Industry 5.0 and blockchain is discussed in section 3. Section 4 depicts results and analysis. The paper is concluded in section 5.

2. Literature survey

Chuka Oham et al. [9] proposed a framework for vehicle security, B-FERL, using blockchain technology. By using blockchain, B-FERL identifies whether an intelligent vehicle’s ECU is compromised by checking the interior disposition of the vehicle. When a compromise is spotted, it is escalated to rightful officials to take necessary actions to avert the compromised automobiles from begetting harm to the vehicular complex. The proposed framework works for both identification and response operations. B-FERL, a framework, helps us to safeguard the automobile against exploitation.

Abdellatif et al. [10] proposed a system that allows the local nodes or servers to exchange medical data through a secure blockchain network. The system contains a local network and a

blockchain network where the local network processes medical data for optimization, and the vital information is shared through a blockchain network. The local data is collected through IoMT (Internet of Medical Things) and LHSP (Local Healthcare Service Provider). This entities-based network sharing helps in extensive data storing through processing and a secure approach to developing medical record exchange.

B. K. Mohanta et al. [11] discussed various real-time security, privacy issues, and solutions regarding the Ethereum blockchain technology. The main factors are mainly low processing power, unsuitable cryptography techniques, and storage capacities. The problems based on IoT are also mentioned concerning various security layers with the integration of blockchain. The layers such as network, physical, and application are categorized into multiple risk zones based on the earlier issues. This differentiation helps to choose different data collection factors, aggregation, and analysis for risk-free security techniques.

Table 1. Related works overview.

Authors	Properties					
	Admin	BCT type	Tool	Integrity check	Access control	Application
Sudeep [13]	Existed	Private	Hyper ledger caliper	Yes	Yes	Health care
Emeka Chukwu [14]	No exist	Public	Not specified	No	No	Health care
Ben Fekih R [15]	No exist	Public	Not specified	No	No	Medical records
W. Lin [16]	Exist	Consortium	DSSCB and VANET	Yes	Yes	Agriculture
Rakesh Shrestha [17]	Existed	Consortium	Not specified	Yes	Yes	Ad-hoc network
Chun Ta Li [18]	No exist	Public	Ethereum and Amazon Cloud	No	No	Medical data
M. Al Baqari[19]	No exist	Public	Not specified	No	No	EHR
M. Tabrez Quasim [20]	No exist	Public	Not specified	Yes	No	Health care App
Hasselgren A [23]	Study work	Study work	Study work	Yes	Yes	Health care
Hasselgren A [25]	Study work	Study work	Study work	Study work	Study work	Health care
Jens-Andreas H [26]	Existed	Public	Ethereum	Yes	Yes	Health care
Proposed Methodology	Existed	Public	Remix and text RPC	Yes	Yes	Medical certificate

Anushree Tandon et al. [12] discussed sharing electronic of medical records through blockchain technology. The work states that the healthcare sector has a wide range of use cases on blockchain,

such as maintaining electronic medical records, pharmaceutical supply chain, remote patient monitoring, and health insurance claims. This work helps us to understand the multiple applications available in the healthcare sector through blockchain security. Table 1 gives the information about comparison and contrast between existing works to the proposed system.

3. Proposed system: Industry 5.0 and Ethereum blockchain-based medical certificate

Blockchain technology is a disruptive technology. Currently, so many real-time applications are being designed using this advanced mechanism. This paper proposes a distributed application-based mechanism for maintaining official medical certificates under Industry 5.0 technology. It uses blockchain technology and users as knowledge agents. Initially, the Remix Etherum platform was used with Metamask wallet to deploy the proposed framework to generate medical certificates like birth, death, and sick.

Furthermore, the system is implemented with a test RPC, Web, and Metamask to design and deploy the distributed application to maintain the new medical certificates and existing certificates that are available as physical copies. Logistic Map Encryption function [21] is used to generate cipher medical certificate of existing physical copies to maintain over a blockchain. So many applications have been proposed in the health sectors using blockchain. Some of the lapses existing in the proposed work are lack of implementation results, platform details, etc.

The proposed system's main ingredients are authorized health centers as domain experts, users, blockchain as intelligent agents, and local database to maintain the Electronic Health Care Certificates (EHCC), as shown in Figure 1.

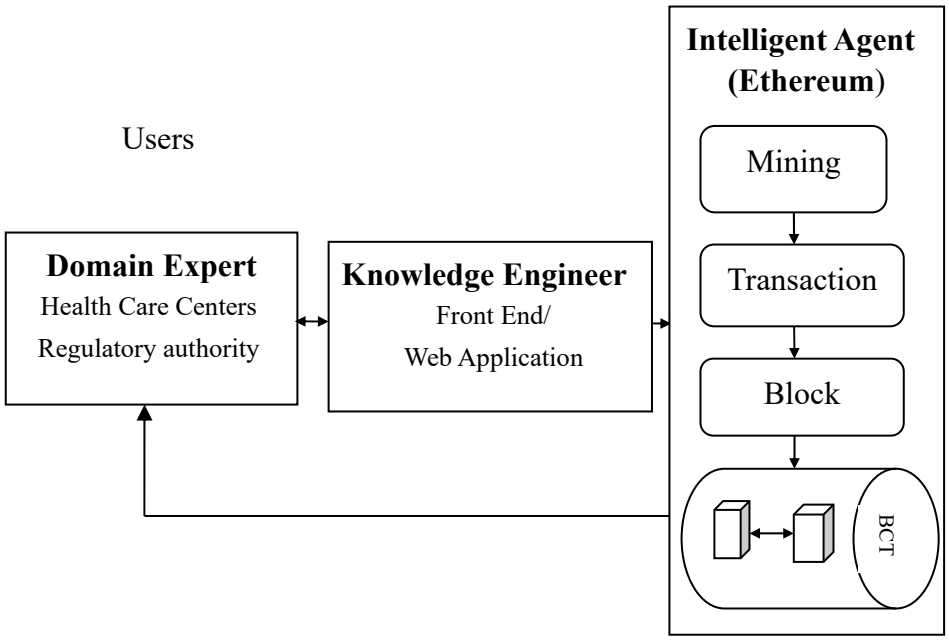

Figure 1. Industry 5.0 based proposed system.

At first, all the health care centers have to get recognition from the hospital's regulatory authority (HRA) by submitting the required documents. HRA issues a unique ID to a healthcare

center to give treatment to the patients and issue medical certificates to the users.

We have mainly focused on issuing and maintaining a blockchain-based medical certificate such as birth, death, or sick in the proposed system. Figure 2 shows the process of ethereum blockchain-based medical certificate generation and maintenance.

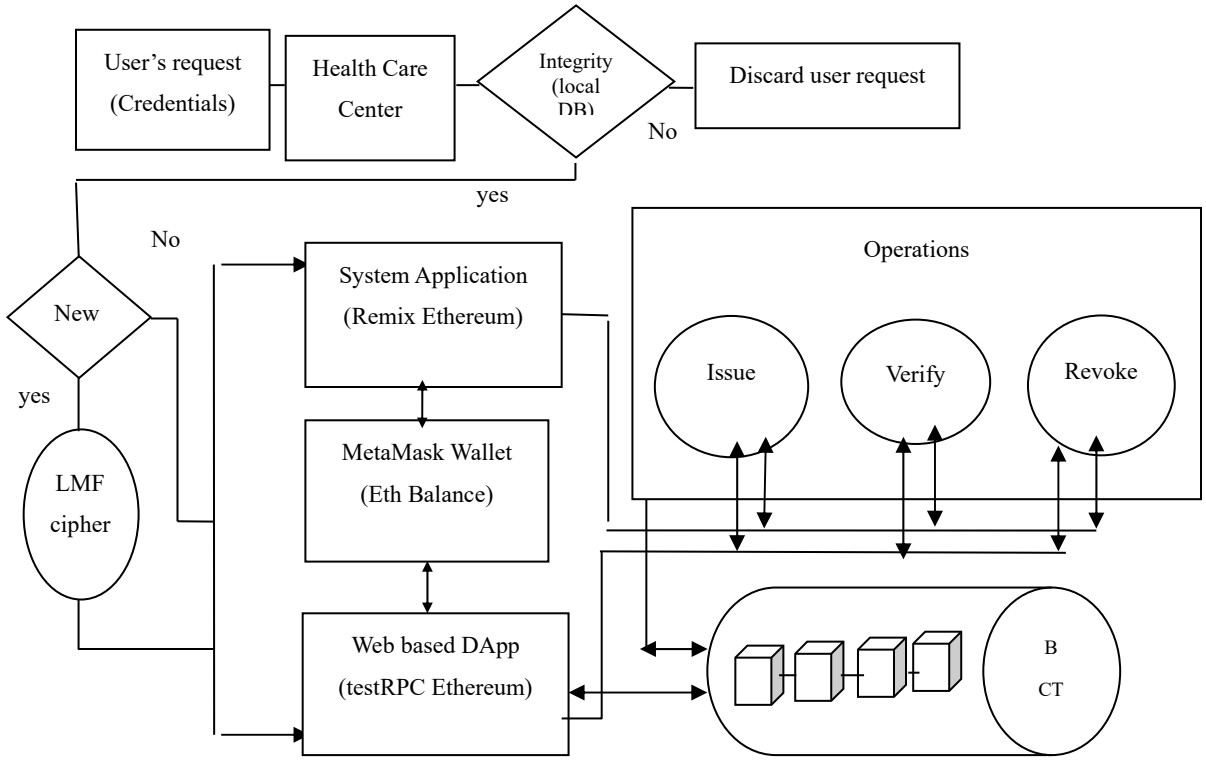

Figure 2. Proposed system methodology.

a) Smart contract

The smart contract is lines of code using solidity programming. Each operation in the proposed system is executed through smart contracts consisting of solidity programming lines [21]. This system is implemented in two ways i.e., using a Web-based distributed Application and a system-based application. Both the applications use solidity programming to write smart contacts for performing the system operations like Cert_issue ( ), Cert_revoke ( ) and Cert_verify ( ). The attributes of the certificates are Hospital Name, Hospital ID, Hospital address, Doctor Name, Certificate type, Recipient Name and address, a unique ID of the certificate in terms of a hash value. The structure of the main attributes of the medical certificate are as follows.

Struct Medical_certificate
String Hospital_ID
String Hospital_name
String Hosipital_Address
String Recipient_ Name
String Rec_Address

1) Hospital_Name: A name of a hospital that has ready to issue the medical certificate.

2) Hospital_ID: A hospital unique identity number (ID) that is issued by the central health care centers regulatory authority.

3) Recipient_Name: A name of the receiver who has approached the hospital and requested a medical certificate.

4) Recipient_Address: Complete details of the receiver like address, phone number, purpose. etc

5) Certificate_Type: This field refers to the type of certificates such as birth, death, or a sick medical document.

6) Doctor_Name: It gives information about the physician who has approved the certificate to the user.

7) _Date: On which date the certificate was generated and issued.

8) Cert_hash: It is a unique ID of the certificate that will be generated based on the certificate's contents. And also, that will be used to refer to a specific certification that was issued by a central authority.

b) Ethereum blockchain-based system Implementation

Ethereum blockchain-based medical certificate maintenance is implemented in two ways, i.e., DApp using Web and test RPC, a system-based application using Remix. Both test PC and Remix run on the ethereum public blockchain network. Metamask wallet is a browser extension is used to get Eth. Eth is a cryptocurrency unit that is required to perform any operations over a blockchain network. Remix platform-based smart contract is deployed on Ropstern network-based ethereum blockchain. Test RPC-based DApp smart contract is deployed on localhost 8545. Algorithm 1 shows the health care centers recognition from regulatory authority assumed as a prerequisite in the proposed system.

Algorithm 1: HCC_ enroll ( )

Input: HCC_Name, HCC_address, regulatory authority name
Output: Unique ID to the HCC

Step 1: Submit the details of health care centers such as Name,
address, infrastructures, Authority Name.
Step 2: HCC_application = Name (HCC) || Addr(HCC) ||
Infra_details (HCC) || Experts (HCC) || Auth (HCC)
Step 3: Validate the details by Central regulatory authority
(CA)
If (Integrity (HCC_Application) = = True) then
issue unique ID otherwise reject the request
HCCi = IDi

The process of medical certificate issued to the user by the HCCs on both the proposed ways is shown in Algorithm 2. The user initially needs to submit the details about the required certifications such as a type of certificate (Birth, death, and sick), Name of a recipient, and address to the health

care centers. Furthermore, a physician or authorized person from the health care centers verifies the details by saving them in the healthcare centers' local database. Create a blockchain-based ID by successfully sending the certificate into ethereum based blockchain after going through the verification process. Metamask Wallet balance is required to perform any operation over a blockchain.

Algorithm 2: Cert_issue ( )

Input: Certificate type, User name, user address, Date
Output: Blockchain (BCT) based a unique ID
Step 1: Verify the details given by the user
if ((Valid (details) = = True)) && Exist_ application)
Cipher $_{Certificate}$ = E_{LMF} (Exist(certificate))
if ((Valid (details) = = True)) && New_application)
Stores in HCC_local database.
Process on blockchain network.
Step 2: Enroll the credentials using Web based DApp or
system App.
Step 3: Connect to Metamsk.
Ask confirmation to establish a connection between application to blockchain environment over a Ropestern or localhost 8545 Network.
Step 4: If confirms the metamask request
Connection established and go to Step 5
otherwise not established
Step 5: If (Eth_balance > = Operation required balance) then
Set the credentials over a blockchain
BCT based Certificate generates
Unique BCT _ID allotted to the certificate
Step 6: If Step 5 fails then shows as
Not enough Eth balance unable generate a BCT-based
certificate.

Algorithm 3 shows the process of encryption algorithm LMF that is used to encrypt the existing medical certificate document image before processing over a blockchain. LME based cipher medical certificate is uploaded through proposed Dapp from a system and is maintained over an ethereum based blockchain.

Algorithm 4 shows the validation process after authority issues an authority to the user or any authorized person. This application helps to prove their identity regarding their birth or death or sick by presenting a unique BCT_ID without showing any physical identity proofs. Anywhere and anytime, the user's claim can be proved by presenting his/her BCT_ID. An authorized person enters the user ID in the application and verifies the credentials, whether if they exist in the blockchain or not. Figure 4 shows a metamask screen with a confirmation request to connect distributed application to a blockchain environment on the Test RPC based localhost 8545 network.

Algorithm 3: Logistic Map Encryption Cipher

Input: Medical Certificate image – Existed/Older version
Output: Cipher Medical certificate

Step 1: Read a random number i.e., 'x' and plain medical certificate (MI)
Where x ϵ (0, 1) and MI_size $\leftarrow$ size (MI)
Step 2: Apply chaotic logistic map.
Step 3: For i $\leftarrow$1 to MI_size do
$\mu \leftarrow$ random number where $\mu \epsilon$ (3.5, 4)
$x_i \leftarrow \mu\, x(1-x)$
$x \leftarrow n_i$
$k1[] \leftarrow x_n$
Step 4: Generate a pseudo random sequence using a rightshift operation.
for j $\leftarrow$1 to MI_size do
$\mu \leftarrow$ random number where $\mu \epsilon$ (3.5,4)
$xj \leftarrow \mu\, x(1-x)$
$x \leftarrow xj$
$k2[] \leftarrow$ RSR (xn*255)
Step 5: Generates a key matrix
key[][] $\leftarrow$ (k1[]) $\oplus$ (k2[])
Step 6: Generates a Cipher Certificate
$Enc_{certificate} \leftarrow$ MI[][] $\oplus$ Key[][]

Algorithm 4: Cert_verify ( )

Input: BCT_ID
Output: Existed or not

Step 1: Enter BCT_ID into the Web based Distributed application (DApp) or System application
Step 2: If (BCT_ID == Existed) then go to Step 3 otherwise go to Step 4.
Step 3: Successfully verified
Step 4: Unsuccessful Entry
Revoke the user request

4. Security analysis

Blockchain technology is raised as an essential technology in Industry 5.0. Although highly well securely designed technology for resilience, some attacks are undertaking in it. The main elements of

a blockchain that can suffer from vulnerabilities are Smart Contracts, blockchain nodes, Wallets, and consensus mechanisms. Generally, blockchain attacks are categorized into four ways based on peer-to-peer network, wallet, smart contract, and consensus & ledger [27]. The lists of attacks under these categories are as follows.

a. 51% attack

The fundamental assumption in the blockchain mechanism design is that only the trusted nodes with the maximum computational power control system work on the blockchain network. If the unauthorized nodes with the collective power control system are more than the trusted or authorized nodes, then the risk of 51% will have occurred. Beikverdi et al. [28] discussed 51% attacks possibilities over a blockchain, although it is decentralized. In the proposed application, all the parties participate in the network using the allotted unique ID. Hence, every user must prove them as an authorized entity like the Zero-knowledge (ZK) protocol mechanism.

b. Eclipse attack

It refers to that attack on a specific user rather than a whole network on a decentralized network. It is a known attack in which the attacker seeks to isolate the victim user by flooding with false data then exploits them. The proposed knowledge engineering-based BCT application allocated a unique ID to the user and authorized parties for making transactions and communication. Allow only the parties who are participating in the network through the allotted unique ID. Each user sends a request to the health care centers, using an assigned unique ID to get their official health documents.

c. Finney attack

It is a type of double-spending attack that creates a chain to support fraud transactions. The attacker needs to spend a lot of time and patience to perform this type of attack because mining participation is required. In response to this, the attacker creates two transactions with the same amount. An initial transaction includes a valid block, and mining will start without broadcasting it to the network by an attacker. This meanwhile, the attacker creates a second transaction with the vendor by spending the same amount.

If the vendor accepts the attacker transaction without confirmation from the network and serves the good, immediately an attacker transmits the mined block that includes the first transaction. The network takes valid blocks and rejects the vendor transaction. The vendor should wait to receive at least six confirmations before serving goods to mitigate this attack.

In a Finney attack, the time to transfer the amount by an attacker and the time for merchant acceptance is 't'. The average time to find a block is 'T.' The probability of another block to be found on the same network simultaneously is 't/T. 'Generally, the attack will fail in this case, and the attacker will lose the reward of 'B.' The average cost of attempting the attack is = (t/T) × B. As a rule of thumb, the merchant should wait at least t = V x (T/B), Where V= value of the transaction

d. Race attack

Pre-mining the block before making a transaction doesn't require here as requires in the Finney attack [29–33]. Instead, the attacker sends the same amount to more than one vendor within a short period. In addition, the vendor receives a message about transaction rejection during mining when he provides service without receiving the block confirmation. Therefore, the vendor should wait for at least one confirmation block before delivering the goods to avoid this attack.

5. Results and analysis

We have implemented the proposed system using the remix platform and also tested it using the test RPC platform. Ethereum blockchain [32, 34–39] network is used in these platforms. Moreover, this system used a browser extension, Metamask cryptocurrency wallet, to deploy the system operations over a blockchain network. An open-source, public blockchain-based application, Remix is used here to write the smart contracts using solidity programming for the functions performed by the proposed system such as issue_certificate ( ) and verify_certificate ( ). Furthermore, we have deployed the proposed system operations using a decentralized application designed using Web, Test RPC node, and solidity programming based smart contracts.

Figure 3 shows a metamask screen with a confirmation request to establish a connection between the Remix platform to the etherum blockchain running on the Ropstern network.

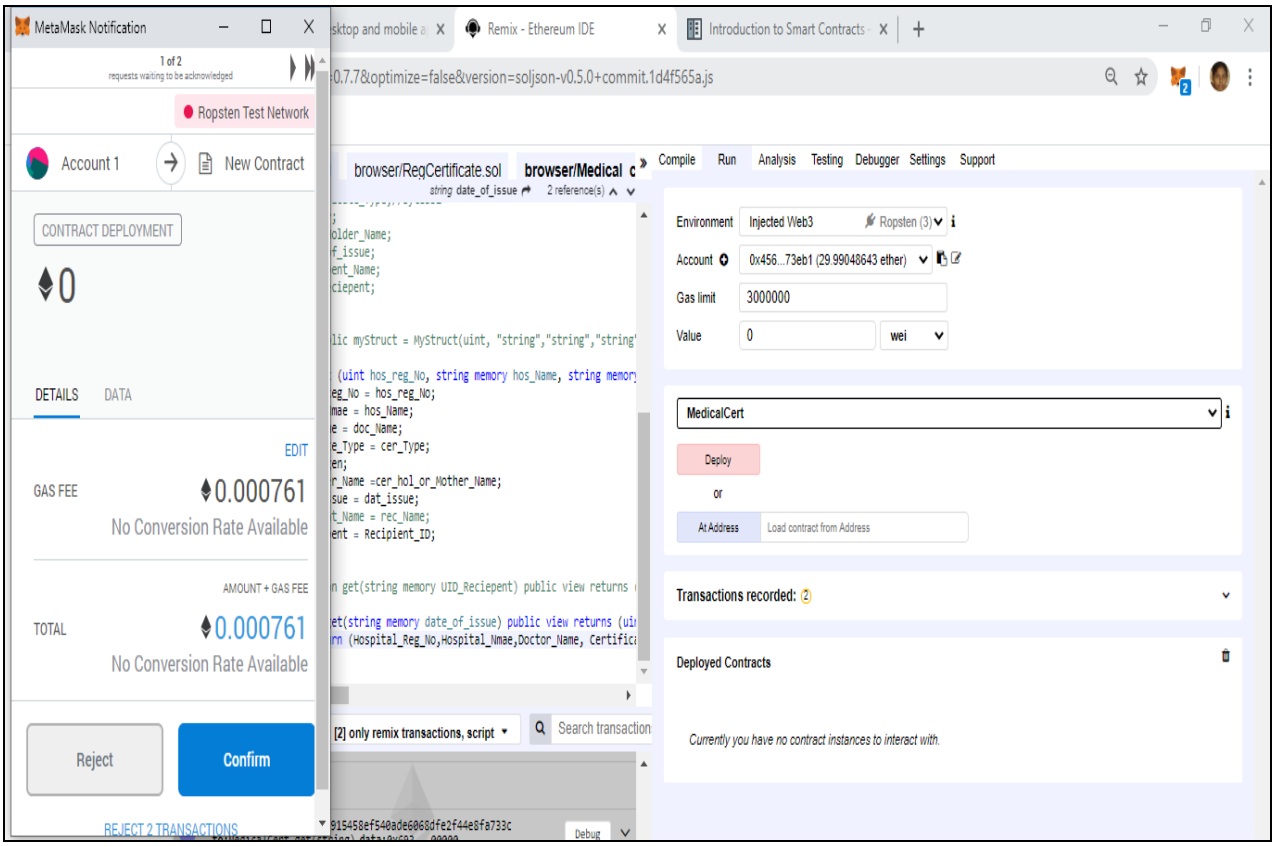

Figure 3. Metamask connection confirmation to process the smart contract over Remix platform.

We have to pay a crypto balance to operate any function over a blockchain network. Figures 3 and 4. show the confirmation request screens to establish a connection with the operating costs. The credentials enter on the webpage verified with the details in the Google Firebase at administration side. From Figure 2, we came to know that the connection establishment between a Remix-based medical certificate smart contract to the Ropstern based blockchain network cost is 0.000761 Gas. Figure 3 shows that the connection between the proposed application and the Test RPC (Localhost

8545) based blockchain cost is 0.001995 Gas.

Figure 4. Metamask connection confirmation to process the smart contract over the DApp platform.

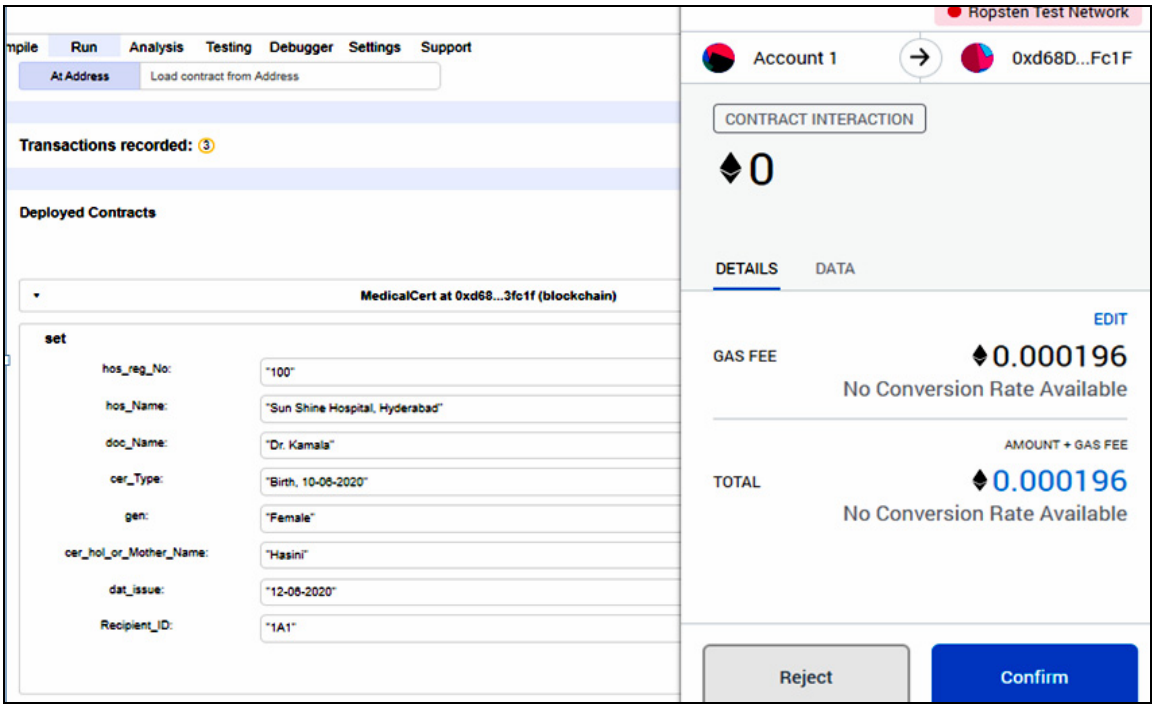

Figure 5. Set ( ) operational cost over a remix platform.

After successfully establishing the connections, medical certificates' attributes are used to issue the certificate to the user after deploying the certificates details in cipher format using LME algorithm over blockchain at administration side. Figure 5. shows the set ( ) function's operating cost to deploy the attributes of the user-required medical certificates.

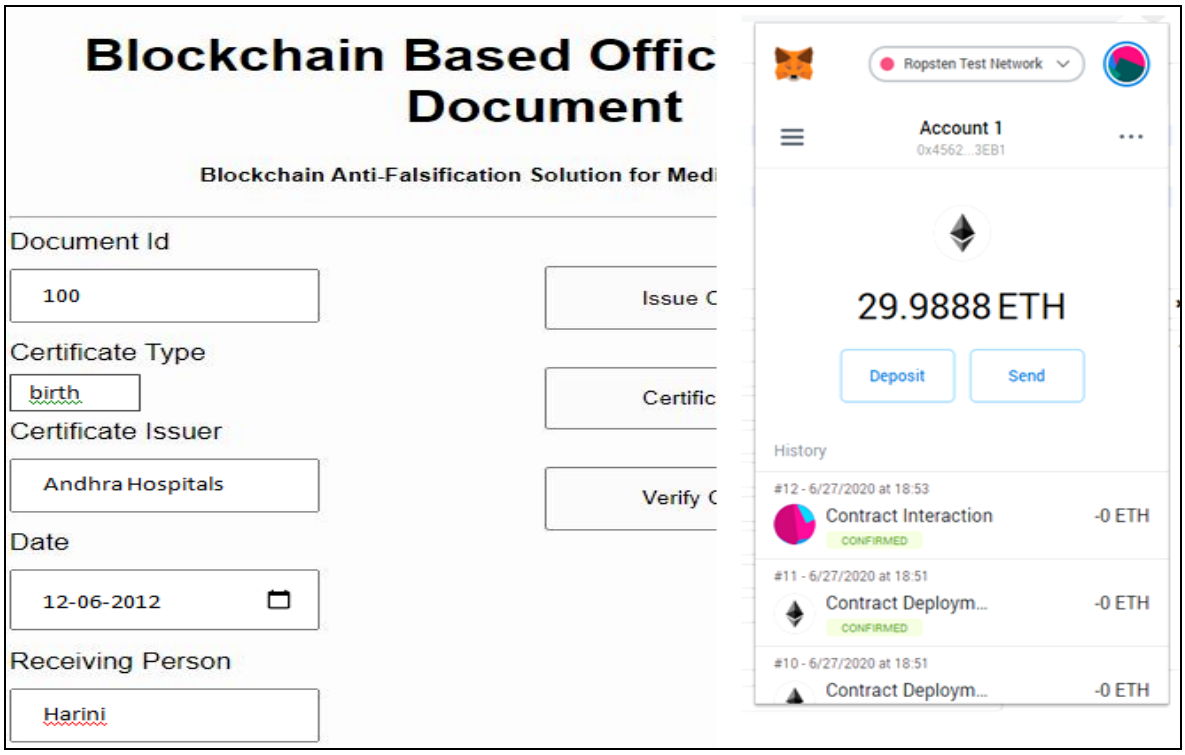

Figure 6. Set ( ) operational cost over a distributed application.

Figure 7. Verification of a medical certificate on Remix platform.

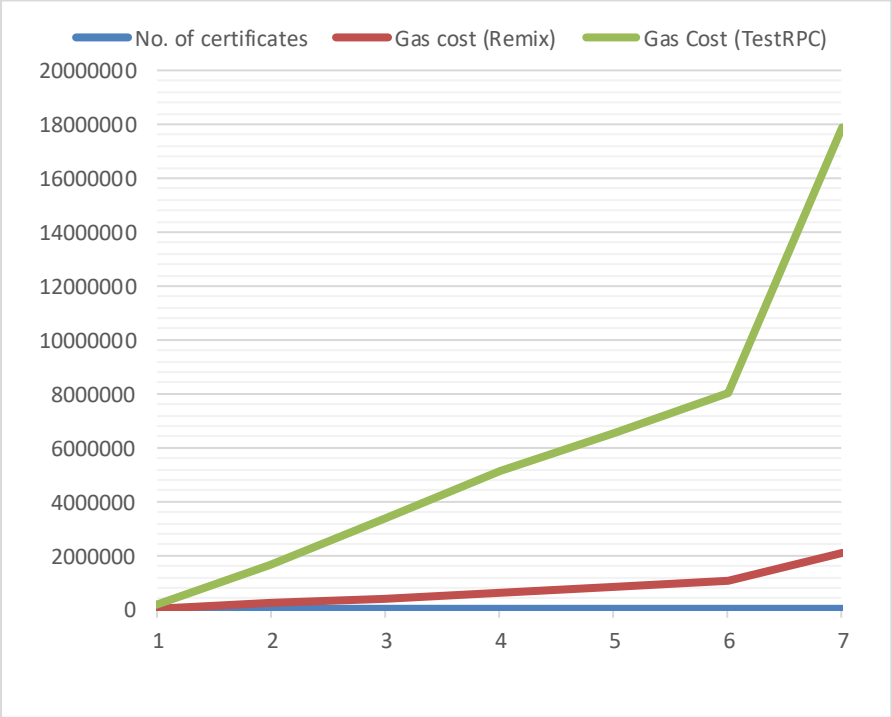

Figure 8. Gas cost to set the medical certificates credentials on various platforms.

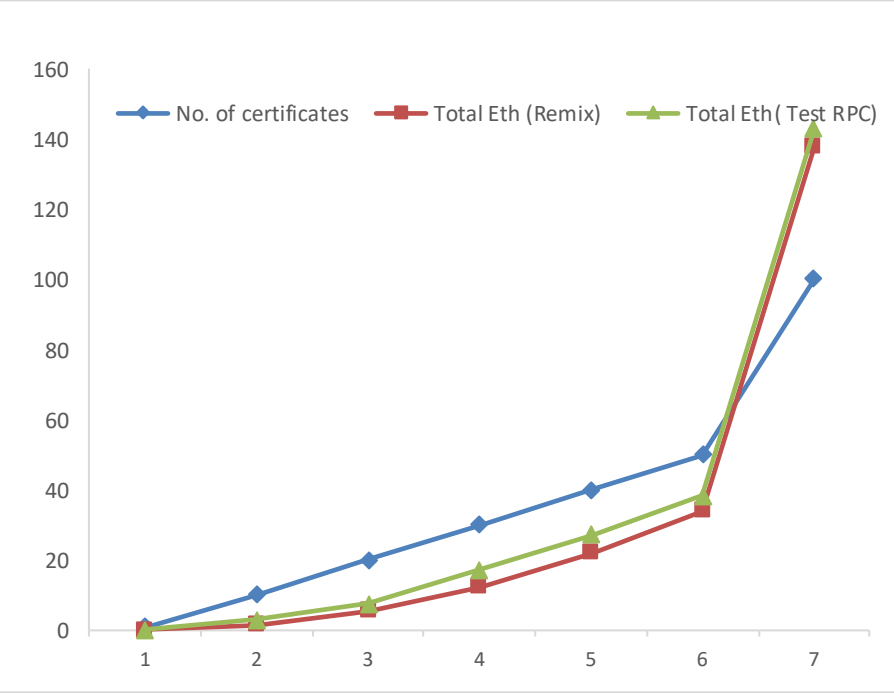

Figure 9. Consumption of total Eth for certificates generation.

Figure 6 shows the cost of operation on an etherum blockchain-based distributed application. This certificate consists of a hospital registered ID, doctor name, hospital name, a required certificate

type, i.e., death, birth or sick, date of issue, etc. The results regarding the verification of the generated medical certificate is shown in Figure 7. The proposed method's operational cost over an etherum based blockchain network is shown in Table II. This table shows the cost of deployed functions of the system such as set_credentials ( ), issue_certificate ( ) and verify_certificate ( ).

Figure 8 shows Gas's consumption to generate medical certificates on both the platforms such as Remix Ethereum blockchain and test RPC etherum blockchain using Metamask Wallet. Gas consumption is measured in the units of Eths and GWei. Here we tested the application by generating up to 100 certificates.

Figure 9 shows the details of the proposed system's operational cost on the Ropstern network and the localhost 8545 network by Web-based distributed application and remix-based system application.

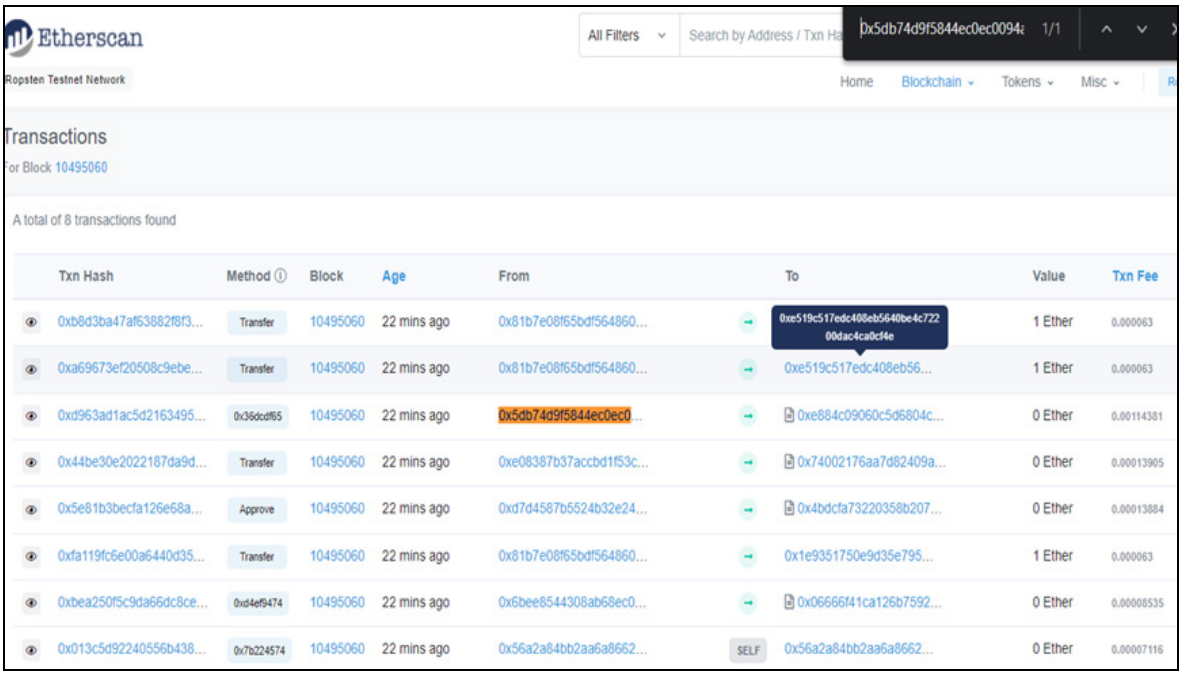

Figure 10. Proof of Etherscan to the certificate maintains over a blockchain.

Figure 10 shows the details of transaction hash, block number, from address, to address, the value of the transaction interms of Ether, Txn Fee, Nonce, etc. The proposed system performance analyzed by considering the existing systems by considering the non functional operations such as latency and processing time. Here considered 100 certificates to process over a blockchain to investigate the system's latency and processing time. The processing time increases as the number of users increase to process their request over a system. Figures 11 and 12 show the comparison results with the existed systems which have implementation results.

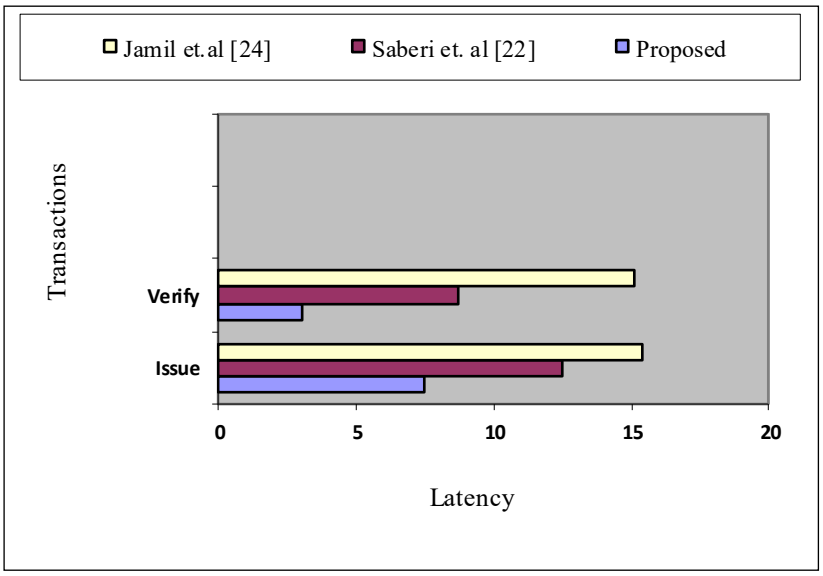

Figure 11. Latency time for different transactions.

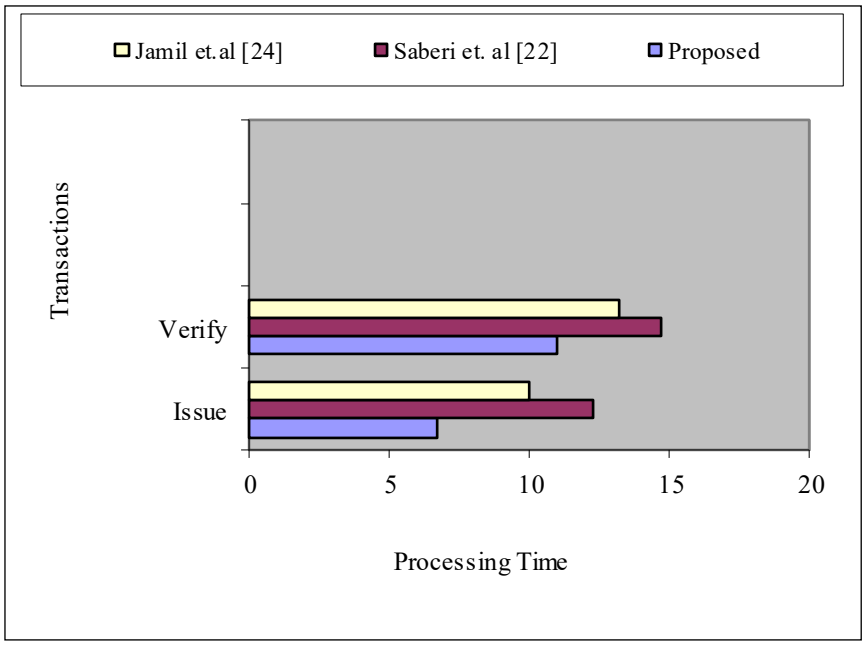

Figure 12. Processing time for different transactions.

6. Conclusions

Blockchain technology can help reduce fraud in the distribution and management of medical certificates. The proposed system will automate the certificate generation and certification process and maintenance and make it an attack resistance system using Ethereum based public blockchain technology. A single point and Central Authority failure affect the reliability of the system. The proposed approach reduces these kinds of problems with the immutable feature of the blockchain.

Due to its transparent feature, every node in the system gets information about creating a new medical certificate in a block as a transaction. Here Mata mask wallet is used for cryptocurrency balance in terms of Eths to operate system functionalities over a blockchain. The proposed system is a user-friendly application to issue or verify medical certificates from anywhere at any time.

Acknowledgments

Authors would like to acknowledge to the Center for Cyber Security, Faculty of Information Science and Technology, Universiti Kebangsaan Malaysia (UKM), Lincoln University College, Malaysia, and Taif University Saudi Arabia for supporting this work.

Funding

This research was supported by Taif University Researchers Supporting Project number (TURSP-2020/216), Taif University, Taif, Saudi Arabia.

Conflict of interest

Authors declare that they have no conflict of interest.

References

1. R Kumar, P Gupta, S Singh, D Jain, Human Empowerment by Industry 5.0 in Digital Era: Analysis of Enablers, in *Advances in Industrial and Production Engineering: Select Proceedings of FLAME*, Springer, (2020), 401.
2. Blockcerts, *Blockchain Credentials*, 2019. Available from: https://www.blockcerts.org.
3. S. Sun, R. Du, S. Chen, W. Li, Blockchain-based IoT access control system: towards security, lightweight, and cross-domain, *IEEE Access*, **9** (2021), 36868–36878.
4. W. Lin, X. Huang, H. Fang, V. Wang, Y. Hua, J. Wang, et al., Blockchain technology in current agricultural systems: from techniques to applications, *IEEE Access*, **8** (2020), 143920–143937.
5. R. Garrard, S. Fielke, Blockchain for trustworthy provenances: A case study in the Australian aquaculture industry, *Technol. Soc.*, **62** (2020), 101298.
6. M. K. Lim, Y. Li, C. Wang, M. L. Tseng, A literature review of blockchain technology applications in supply chains: a comprehensive analysis of themes, methodologies and industries, *Comput. Ind. Eng.*, **154** (2021), 107133.
7. A. J. Sherule, R. Dudhe, Disruptive technologies in energy and environment,*2021 International Conference on Computational Intelligence and Knowledge Economy (ICCIKE)*, 2021, 37–41.
8. M. Turkanović, M. Hölbl, K. Košič, M. Heričko, A. Kamišalić, EduCTX: A blockchain-based higher education credit platform, *IEEE Access*, **6** (2018), 5112–5127.
9. C. Oham, R. A. Michelin, R. Jurdak, S. S. Kanhere, S. Jha, B-FERL: Blockchain based framework for securing smart vehicles, *Inf. Proc. Manage.*, **58** (2021), 102426.
10. A. A. Abdellatif, A. Z. Al-Marridi, A. Mohamed, A. Erbad, C. F. Chiasserini, A. Refaey, ssHealth: toward secure, blockchain-enabled healthcare systems, *IEEE Network*, **34** (2020), 312–319.

11. B. K. Mohanta, D. Jena, S. Ramasubbareddy, M. Daneshmand, A. H. Gandomi, Addressing security and privacy issues of IoT using blockchain technology, *IEEE Internet Things J.*, **8** (2021), 881–888.
12. A. Tandon, A. Dhir, N. Islam, M. Mäntymäki, Blockchain in healthcare: A systematic literature review, synthesizing framework and future research agenda, *Comput. Ind.*, **122** (2020), 103290.
13. S. Tanwar, K. Parekh, R. Evans, Blockchain-based electronic healthcare record system for healthcare 4.0 applications, *J. Inf. Secur. Appl.*, **50** (2020), 102407.
14. E. Chukwu, L. Garg, A Systematic review of blockchain in healthcare: rrameworks, prototypes, and implementations, *IEEE Access*, **8** (2020), 21196–21214.
15. R. B. Fekih, M. Lahami, Application of Blockchain Technology in Healthcare: A Comprehensive Study, *International Conference on Smart Homes and Health Telematics*, 2020, 268–276.
16. W. Lin, X. Huang, H. Fang, V. Wang, Y. Hua, J. Wang, Blockchain technology in current agricultural systems: from techniques to applications, *IEEE Access*, **8** (2020), 143920–143937.
17. R. Shrestha,R. Bajracharya,A. P. Shrestha,S. Y. Nam, A new type of blockchain for secure message exchange in VANET, *Digital Commun. Networks*, **6** (2020), 177–186.
18. C. T. Li, D. H. Shih, C. C. Wang, C. L. Chen, C. C. Lee, A blockchain based data aggregation and group authentication scheme for electronic medical system, *IEEE Access*, **8**(2020),173904–173917.
19. M. Al Baqari, E. Barka, Biometric-based blockchain ehr system (bbehr),*2020 International Wireless Communications and Mobile Computing (IWCMC)*, 2020, 2228–2234.
20. M. T. Quasim, F. Algarni, A. A. E. Radwan, G. M. M. Alshmrani, A Blockchain based Secured Healthcare Framework, *2020 International Conference on Computational Performance Evaluation (ComPE)*, 2020, 386–391.
21. N. Tsafack, S. Sankar, B. Abd-El-Atty, J. Kengne, K. C. Jithin, A. Belazi, et al., A new chaotic map with dynamic analysis and encryption application in internet of health things, *IEEE Access*, **8** (2020), 137731–137744.
22. S. Saberi, M. Kouhizadeh, J. Sarkis, L. Shen, Blockchain technology and its relationships to sustainable supply chain management, *Int. J. Prod. Res.*,**57** (2019), 2117–213.
23. A. Hasselgren, J. A. H. Rensaa, K. Kralevska, D. Gligoroski, A. Faxvaag, Blockchain for Increased Trust in Virtual Health Care: Proof-of-Concept Study, *J. Med. Internet Res.*, **23** (2021), e28496.
24. F. Jamil, L. Hang, K. H. Kim, D. H. Kim, A novel medical blockchain model for drug supply chain integrity management in a smart hospital, *Electronics*, **8** (2018), 505.
25. A. Hasselgren, K. Kralevska, D. Gligoroski, S. A. Pedersen, A. Faxvaag, Blockchain in healthcare and health sciences-A scoping review, *Int. J. Med. Inf.*, **134** (2020), 104040.
26. J. A. H. Rensaa, D. Gligoroski, K. Kralevska, A. Hasselgren, A. Faxvaag, VerifyMed-A blockchain platform for transparent trust in virtualized healthcare: Proof-of-concept, *Proceedings of the 2020 2nd International Electronics Communication Conference (IECC 2020)*, 2020, 73–80.
27. N. Faour, Transparent E-Voting dApp Based on Waves Blockchain and RIDE Language, *2019 XVI International Symposium "Problems of Redundancy in Information and Control Systems" (REDUNDANCY)*, 2019, 219–223.

28. A. Beikverdi, J. S. Song, Trend of centralization in Bitcoin's distributed network, *2015 IEEE/ACIS 16th international conference on software engineering, artificial intelligence, networking and parallel/distributed computing (SNPD)*, 2015, 1–3.
29. C. Rupa, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, S. Bhattacharya, A Blockchain Based Cloud Integrated IoT Architecture Using a Hybrid Design, *International Conference on Collaborative Computing: Networking, Applications and Worksharing*, 2020, 550–559.
30. S. S. R. Krishnan, M. K. Manoj, T. R. Gadekallu, N. Kumar, P. K. R. Maddikunta, S. Bhattacharya, et al., A Blockchain-Based Credibility Scoring Framework for Electronic Medical Records, *2020 IEEE Globecom Workshops (GC Wkshps)*, 2020, 1–6.
31. T. R. Gadekallu, N. Kumar, S. Hakak, N. Kumar, S. Hakak, S. Bhattacharya, Blockchain based Attack Detection on Machine Learning Algorithms for IoT based E-Health Applications, preprint, arXiv: 2011.01457.
32. W. Wang, H. Xu, M. Alazab, T. R. Gadekallu, Z. Han, C .Su, Blockchain-Based Reliable and Efficient Certificateless Signature for IoT Devices, *IEEE Trans. Ind. Inf.*, **2021** (2021).
33. R. Ch, G. Srivastava, T. R. Gadekallu, P. K. R. Maddikunta, S. Bhattacharya, Security and privacy of UAV data using blockchain technology, *J. Inf. Secur. Appl.*, **55** (2020), 102670.
34. M. M. Saeed, R. A. Saeed, E. Saeid, Preserving privacy of paging procedure in 5thG using identity-division multiplexing, *2019 First International Conference of Intelligent Computing and Engineering (ICOICE)*, 2019, 1–6.
35. R. A. Saeed, M. M. Saeed, R. A. Mokhtar, H. Alhumyani, S. Abdel-Khalek, Pseudonym mutable based privacy for 5G user identity, *J. Comput. Syst. Sci. Eng.*, **29** (2021), 1–14.
36. N. Nurelmadina, M. K. Hasan, I. Memon, R. A. Saeed, K. A. Z. Ariffin, E. S. Ali, et al., A systematic review on cognitive radio in low power wide area network for industrial IoT applications, *Sustainability*, **13** (2021), 338.
37. P. K. R. Maddikunta, P. Quoc-Viet, B. Prabadevi, N. Deepa, D. Kapal, et al., Industry 5.0: a survey on enabling technologies and potential applications, *J. Ind. Inf. Integr.*, **2021** (2021), 100257.
38. M. K. Hasan, S. Islam, S. Sulaiman, S. Khan, A. H. Hashim, S. Habib, et al., Lightweight encryption technique to enhance medical image security on internet of medical things applications, *IEEE Access*, **9** (2021), 47731–47742.
39. M. Akhtaruzzaman, M. K. Hasan, S. R. Kabir, S. N. Abdullah, M. J. Sadeq, E. Hossain, HSIC bottleneck based distributed deep learning model for load forecasting in smart grid with a comprehensive survey, *IEEE Access*, **2020** (2020).

AIMS Press