Implementation of blockchain as covid-19 test and vaccine certificate storage system

Dendi Arya Raditya Prawira Putra, Yudha Purwanto, Marisa W. Paryasto
Department of Computer Engineering, School of Electrical Engineering, Telkom University, Indonesia

Article Info

Article history:

Received July 26, 2022
Revised August 18, 2022
Accepted August 19, 2022

Keywords:

Blockchain
Digital Certificate
Smart Contract

ABSTRACT

The existence of the Covid-19 virus, which was first announced at the end of 2019, in a short time was able to cause a pandemic. To overcome this, the government implemented a protocol that integrates Covid-19 test results and vaccination certificates into an application, with the aim that individuals can prove that they are free from Covid-19 infection and can return to normal activities. However, a centralized system is prone to single point of failure and data manipulation from the intervention of certain parties due to a lack of transparency. This paper proposed the use of Ethereum blockchain and smart contracts to solve this problem. By using blockchain technology and smart contracts, the data management process will be more transparent since every transaction on the blockchain is recorded by each node. Blockchain also prevents a single point of failure because there are more than one data provider. The system that has been developed has fulfilled the security and privacy aspects of patient data by implementing password-based encryption on patient data. The system's response time is strongly influenced by the computational capabilities of the Rinkeby network. On average, the system took 47,9 seconds to register a new certificate.

This is an open access article under the CC BY-SA license.

Corresponding Author:

Dendi Arya Raditya Prawira Putra
Department of Computer Engineering
School of Electrical Engineering, Telkom University
Bandung, Indonesia
Email: dendiaryar@telkomuniversity.ac.id

1. INTRODUCTION

The existence of the Covid-19 virus which was first announced at the end of the year 2019, had a huge impact on society, especially the economy and the health sector. The development of vaccines and immunity tests against Covid-19 is a priority for the global community to reduce the impact of the pandemic with vaccines and tests for Covid-19, the risk of spreading the Covid-19 virus can be reduced so that people can return to their normal activities [1].

For that reason, the government has issued a protocol that integrates Covid-19 test results and large-scale vaccinations into a system that makes it easy for users to prove that they have received the vaccine or carried out a Covid-19 test [2]. But there is always controversy regarding the security and privacy of users in a centralized system [3]. Single point of failure is also a problem in a centralized system, in which the server experience downtime so the server cannot be accessed by the client. This can occur due to an external attack or an error on the service provider's server. In addition, in a centralized system, there will be a party that can make changes to the data. Because there is only one data source, it will be difficult for other parties to prove the source and authenticity of the data. Therefore, we need a system that can solve those problems.

Blockchain can be a solution to this problem. Blockchain is a distributed system and a decentralized database in a peer-to-peer network that uses secure consensus mechanisms to allow transactions without a trusted third party [4]. Blockchain is immutable so that it prevents data changes and can maintain data integrity, and maintains data with a secure consensus model and a trustless network [5][6]. Blockchains like Ethereum also allow for a mechanism that gives users the authority to set any public identity. In addition, blockchain also benefits from decentralization so there is no single point of failure.

This paper will discuss a proposed solution to solve the problem above by implementing blockchain and smart contracts on Ethereum. This paper highlights two contributions that are as follows:

- The architecture of the system
- Ethereum Test Network is used to implement the system. An analysis of its response time is presented.

2. RELATED WORK

The recent development of blockchain technology has allowed the rapid development of decentralized applications with diverse purposes. For instance, blockchain can be used to record electronic documents so their authenticity can be easily verified. According to [7] blockchain is immutable and thus offers transparency by recording every transaction permanently. Ghanghoria et al [8] discussed the use of blockchain to securely store electronic documents through private blockchain. The result shows 100 percent availability and through verification, the system can preserve the genuity of the documents. Chaniago et al [9] proposed a solution using the Ethereum public blockchain to preserve the authenticity of diplomas and academic transcripts.

For instance, the use of blockchain in the medical health sector can be seen in Dias et al [10] solution. The goal is to implement blockchain for access control to medical records. It used consortium blockchain which means nodes are predetermined. Xia et al [11] also presented a solution for how stored medical data can be shared between cloud service providers using blockchain in a limited manner. In [12] the proposed solution has included a mechanism to share data between a patient and medical professional. But it doesn’t include the result of the implementation of the proposed solution. A similar solution is also discussed by Vazini et al in [13], with an aim to leverage blockchain technology to manage medical record data. It uses a smart contract to record transactions between patient and provider. The authors note weaknesses in Blockchain that involves concepts unfamiliar to most of the population, including cryptographic signatures

Ivan in [14] proposed a solution to store patient medical records using blockchain technology, enhancing medical information transparency. Kuo et al [15] discussed the use of private blockchain to create a medical health prediction model. Another solution is Medicalchain in [16]. Medicalchain is a decentralized platform to store medical records. Built on two blockchain networks, Hyperledger fabric to control permissions to health records and Ethereum as an underlying service in its platform. Medicalchain is more focused on the patient and storing general medical records. It also allows people to buy data from patients who are willing to share their data. The solutions mentioned provide a secure system to store general medical records only by leveraging blockchain technology and not for a special case like covid-19.

Related to the covid-19 problem, Mendonça et al [17] proposed a solution to manage the history of Covid-19 vaccine temperature. The authors use blockchain to guarantee reliability, transparency, and security during the Covid-19 vaccine storing process. The authors mention that blockchain has the potential of disrupting the way monitoring and traceability are conducted in the cold chain.

Eisenstadt et al [18] proposed a solution to store vaccine and test certificates using blockchain technology. It used consortium blockchain limiting nodes participant to approved institutions or organizations. The performance benchmarking was done by measuring the time for completing the operation. The result has shown the that system is scalable, by linear growth of time in all operations. The main difference between the solution presented in [18] and this paper is the use of consortium blockchain. In this paper, the implementation of the system uses the public Ethereum blockchain

3. METHOD

The proposed system will be built on top of a blockchain network. The overview of actors and their role in the system is illustrated in figure 1. The issuer is a healthcare provider that issued Covid-19 test/vaccine certificates, the regulator is the owner of the system that could give access to the issuer for certificate creation, the patient is the owner of the certificate, and the verifier is someone who wants to verify the certificate own by a patient.

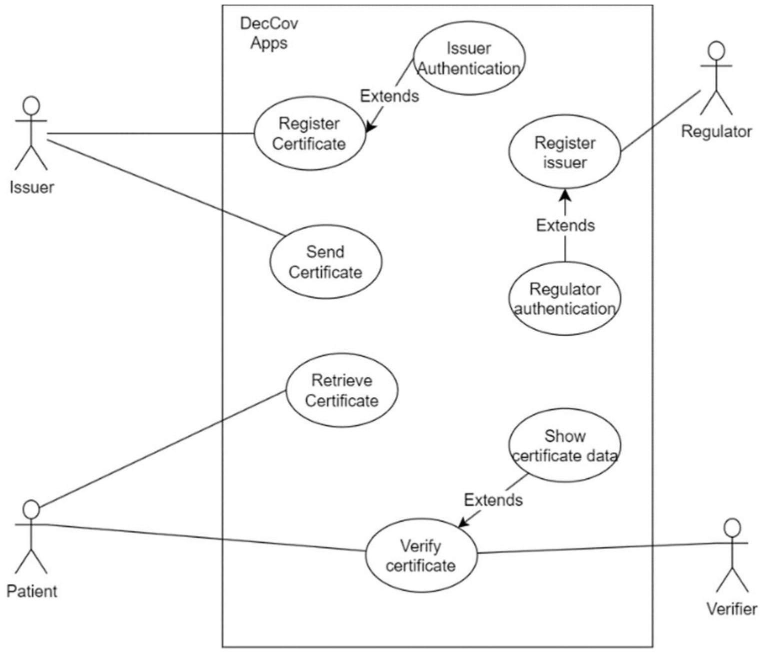


Figure 1. Use case diagram of Covid-19 certificate storage system

3.1. Requirement

This section will discuss the requirement to address the issue. Requirements are divided into two, user requirements and functional requirements each shown in Table 1 and Table 2. The user requirements were gathered from local health workers who have worked as Covid-19 vaccinators and testers. These requirements are used to help analyze the functional requirements of the system.

Table 1. User Requirement

No	User requirement
1	There are supervisors who provide access to officers to make certificates.
2	The system stores data for officers who have been granted access.
3	Officers have access to vaccination history/tests for potential vaccine recipients/Covid-19 tests.
4	The system records data on the names of patients receiving vaccines or recipients of Covid-19 test results.
5	The system records data on the population numbers of vaccine recipients or Covid-19 test results.
6	The system records data on the age of the patient receiving the vaccine or the results of the Covid-19 test.
7	The system records the gender data of patients receiving vaccines or recipients of Covid-19 test results.
8	For vaccine data received by patients, it includes the type of vaccine, dose, and time of receiving the vaccine.
9	For data on Covid-19 test results, the data that needs to be stored includes the type of test, the results, and the validity period of the test.
10	The certificate that has been created can be sent to WhatsApp to make it easier for patients.
11	The certificate that has been created must be able to be verified through the system.
12	The system displays data from certificates that have verified data from the certificate.

Table 2. Functional Requirement

No	Functional requirement
1	The system has three different portals, each of which will be used by verifier actors, issuers, and regulators.
2	Regulators can approve other users as issuers.
3	An issuer can check the vaccination history and test results of prospective vaccine recipients.
4	The system provides access to issuers who have been validated by the regulator to register vaccine certificates or Covid-19 test results into the blockchain.
5	Vaccine certificates or Covid-19 test results in the form of a QR Code can be given to WhatsApp patients (vaccine recipients).
6	The certificate also stores the user's photo data which will later be used to prove ownership of the certificate.
7	The certificate data stored in the database is encrypted with a user-generated pin for the purpose of protecting user data.
8	The verifier can verify the vaccine certificate by scanning the patient's QR code with the patient's consent as the owner of the certificate.
9	Patients can access certificate data using QR code.

3.2. System design

There are two smart contracts used in the system namely Certificate Registry Smart Contract and Issuer Registry Smart Contract. Certificate Registry Smart Contract is used to store Covid-19 certificate and issuer registry Smart contract is used to store addresses of issuers that have been registered by the regulator. In this way, the Issuer Registry Smart Contract plays a role in authorizing issuers to register certificates on to Certificate Registry Smart Contract. The authentication process uses a challenge-response mechanism figure two shows the process of the issuer authentication in the high-level view. The app that has been built first detects the issuer Ethereum address from their wallet, the app then checks whether the address has been registered into Issuer Registry Smart Contract. Then the issuer needs to sign a message to prove ownership of their account.

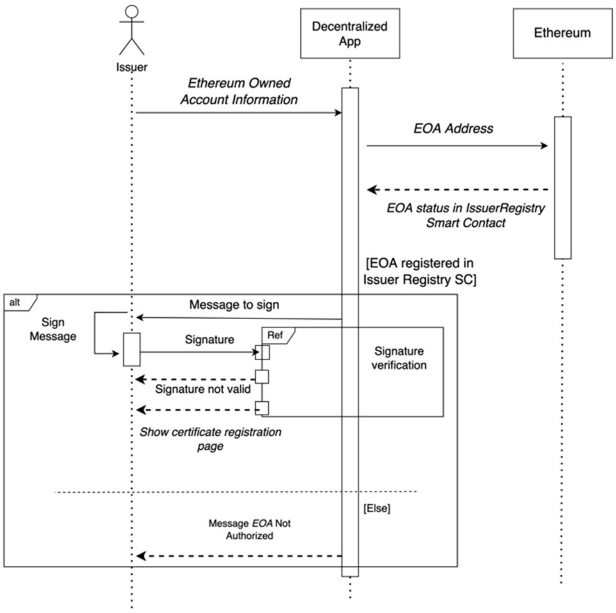

Issuer
Decentralized App
Ethereum
Ethereum Owned Account Information
EOA Address
EOA status in IssuerRegistry Smart Contact
[EOA registered in Issuer Registry SC]
alt
Message to sign
Sign Message
Signature
Ref
Signature verification
Signature not valid
Show certificate registration page
[Else]
Message EOA Not Authorized

Figure 2. Issuer authentication scheme

On the smart contract, it implemented a function modifier to validate the signer of the transaction so in this way every transaction created by the user that has not been registered by the Regulator won't be accepted**.** Next, this section also discussed the information flow in the system as shown in figure three below.

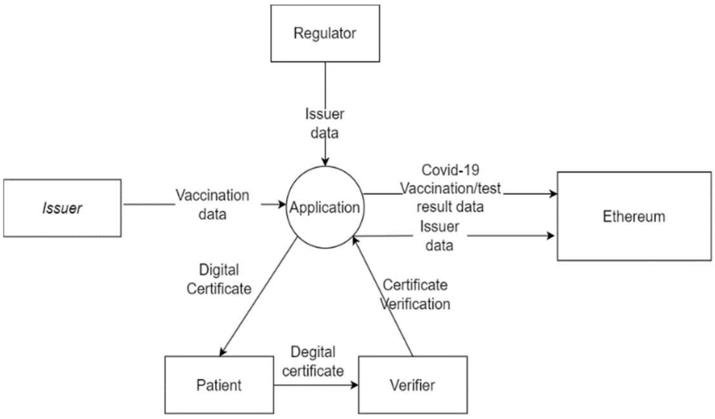
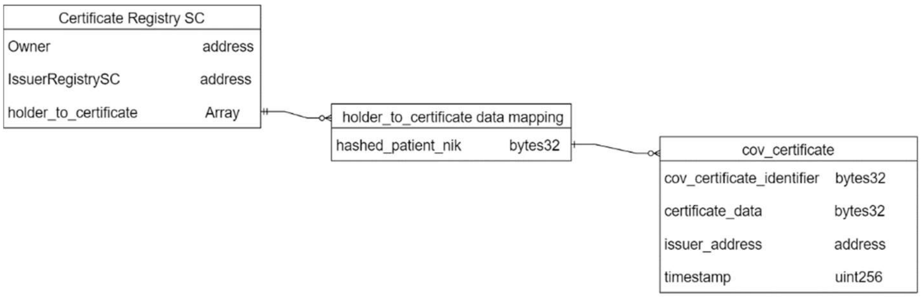


Figure 3. Data flow diagram level 0 of the system

The system that has been built uses IPFS to store the data and to make it secure the data itself first encrypted using a symmetric key owned by the patient in the form of a pin/password. The patient then can give permission to the verifier to access their certificate by giving their certificate in the form of a QR Code. A photo of the patient is also embedded in the certificate so the patient can prove ownership of the certificate. To make it clear, the data structure of the design system can be seen in figure four below.



Certificate Registry SC	
Owner	address
IssuerRegistrySC	address
holder_to_certificate	Array

holder_to_certificate data mapping	
hashed_patient_nik	bytes32

cov_certificate	
cov_certificate_identifier	bytes32
certificate_data	bytes32
issuer_address	address
timestamp	uint256

Figure 4. ER diagram inside certificate registry smart contract

Figure four shows how data is stored in the smart contract. Explanations of the data are shown below:

1. cov_certificate_identifier is an external data pointer that refers to data on IPFS. This variable is used as a unique value from the certificate data to avoid duplicate patient data. In addition, it is used by issuers to check the patient's vaccine/test history. The data stored includes the hash of the patient's NIK along with data from the patient's Covid-19 certificate.
2. certificate_data is an external data pointer that refers to the data address on IPFS. The data stored is patient encrypted certificate data.

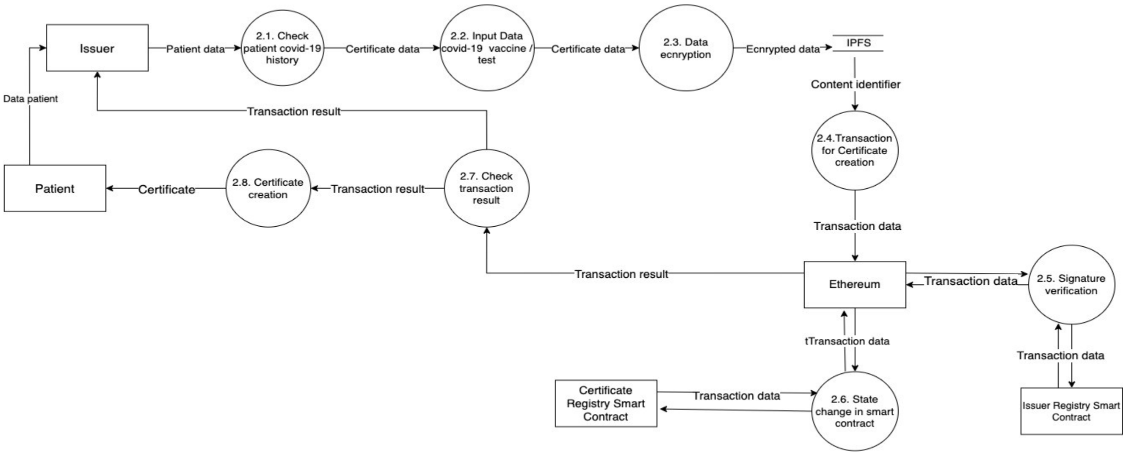

Issuer
Patient data
2.1. Check patient covid-19 history
Certificate data
2.2. Input Data covid-19 vaccine / test
Certificate data
2.3. Data ecnryption
Ecnrypted data
IPFS
Content identifier
2.4.Transaction for Certificate creation
Transaction data
Data patient
Transaction result
Patient
Certificate
2.8. Certificate creation
Transaction result
2.7. Check transaction result
Transaction result
Ethereum
Transaction data
2.5. Signature verification
tTransaction data
Transaction data
Certificate Registry Smart Contract
Transaction data
2.6. State change in smart contract
Issuer Registry Smart Contract

Figure 5. Data flow diagram of certificate

Figure 5 shows the information flow of covid-19 certificate creation. The patient first gives their data to the issuer. The issuer then inputs all the data necessary for the Covid-19 certificate through the designed decentralized application. After that, encryption took place before covid-19 certificate data is uploaded to the IPFS. Then certificate creation transaction is created to store the data into the certificate registry smart contract. The smart contract then handles the transaction to be verified by nodes in the Ethereum network. After the transaction is verified, the decentralized application then creates a certificate for the patient in the form of a QR code. Later the verification process will be done by scanning the QR code.

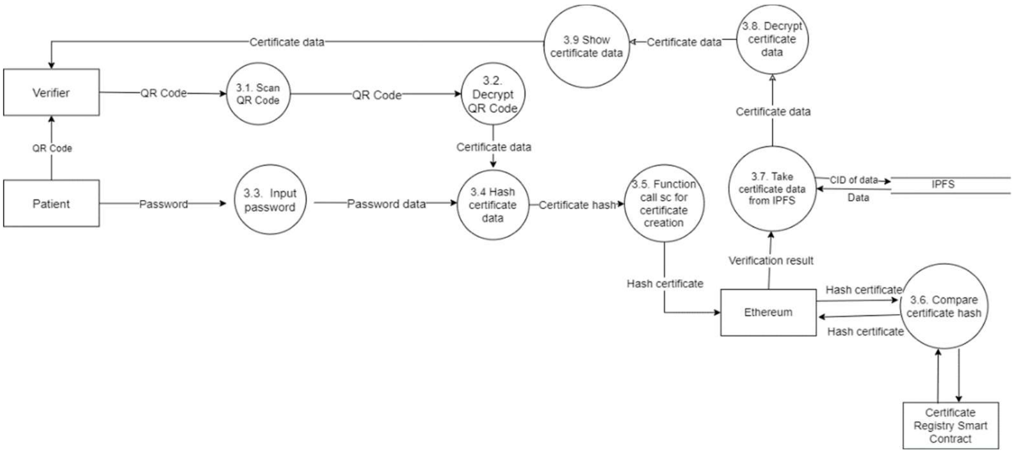


Figure 6. Data flow diagram of certificate verification

The process of certificate verification can be seen in figure 6. The verification process starts with the patient giving their QR code to the verifier. Then the verifier scans the QR code, and data from the QR code then compared to data in the Certificate registry smart contract. The result then will be shown in the application which includes a photo of the owner.

4. RESULT AND ANALYSIS

4.1. Result

The system built includes a web-based application and smart contracts that have been deployed into the Rinkeby Test network. Rinkeby test network is a network that was specifically developed to test the decentralized app before deployment to the main Ethereum network. For the app development, it used the ReactJs framework, and it doesn’t have any backend server which means interaction happened directly from client to blockchain network. The app has three features to meet every actor's needs.

1. Register issuer
   This feature is used to register a user as an issuer. This feature can only be accessed by regulators.
2. Verify certificate
   This feature is used to verify certificates and can be accessed by every user.
3. Register certificate
   This feature is used to register a new covid-19 certificate. This feature can only be accessed by an issuer.

4.2. **Analysis**

The system that has been built has been tested through some testing scenarios. For functional validation, the system is tested by running 52 test cases linked to table 2. The test cases focus on covering these four points:

1.Smart Contract Deployment
2.Register new issuer
3.Register new Covid-19 certificate
4.Verify certificate

The result has shown that the system has met behavior as expected and from that result, the system has been declared to meet all functional requirements. The summary of the results of the test can be seen in the following table.

Table 4 Functional test summary

Functional Test	Functional Requirement	Test conclusion	Status
Smart contract deployment	FR02, FR03, FR04, FR06, FR08	Contract deployed into test network.	Fulfilled
Register new issuer	FR01, FR02	The system can grant access to the regulator to register a new issuer.	Fulfilled
Register Covid-19 certificate	FR01, FR03, FR04, FR05, FR06, FR07	System is able to grant access to an issuer to register a new covid-19 certificate in form of a QR Code.	Fulfilled
Verify certificate	FR07, FR08, FR09	The system is able to verify the integrity of the certificate.	Fulfilled

After functional validation, the system also has been tested by six health workers to validate user requirements shown in table 1. The result has shown that the system has met the requirements of the user since it showed high satisfaction results from the respondent. The following is a summary of the user acceptance test that has been done.

Table 5 User acceptance test summary

Testing method	Testing detail		Result		
	Number of surveyors	Number of questions	Good	Enough	Bad
UAT	6	25	149	1	-

For security measures, the system that has been built is able to limit access to certain features so only authorized users can access the designated feature. The system also has been able to limit access of transactions on smart contracts, only the user that has been authorized before can make transactions. The system also uses password-based encryption to keep user data secure.

As for the performance, the test was done to measure the response time of the system to complete a task. Figure seven shows response times of the application are dependent on how much time is needed for a single transaction to be validated by the Rinkeby Ethereum network due to the Ethereum blockchain use of consensus mechanism which makes every transaction need to be validated. On average certificate, registration takes 47,9 seconds and the Ethereum transaction for certificate registration takes on average 33,421 seconds. This is expected since transactions are dependent on the computational capabilities of the network and the number of transactions taking place at the same time.

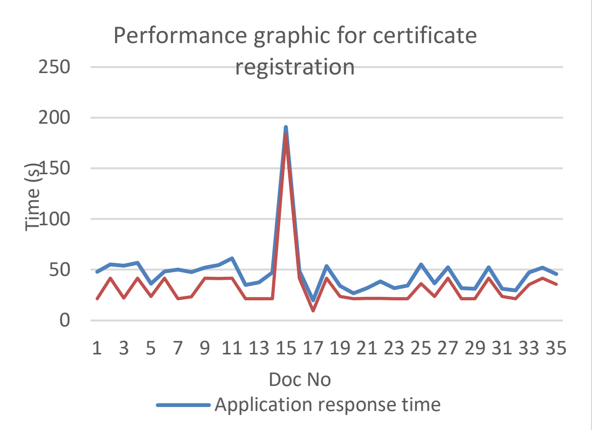


Figure 7. Response time for certificate

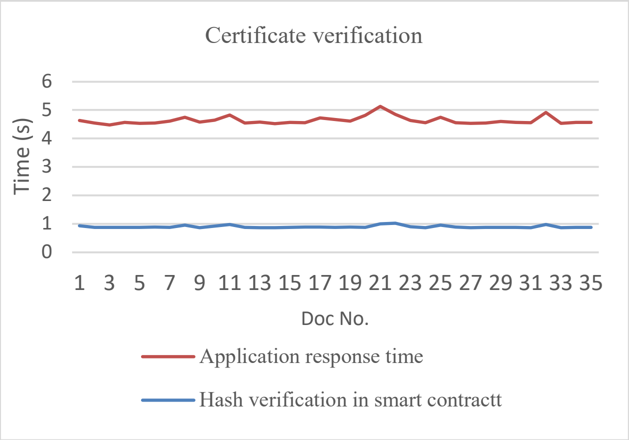


Figure 8. Response time for certificate verification

Figure eight shows the graphics performance of certificate verification. On average it took 3,73 seconds for the application to complete the verification process. The hash verification in the blockchain on average took 0,89 seconds to complete. Contrary to certificate registration, certificate verification took less time, as shown in figure 10. This is because verification nodes on the blockchain network do not need to verify as is done in the transaction process. Therefore it does not require a lot of computing resources.

5. CONCLUSION

The solution which implements smart contracts in the Ethereum blockchain has been able to store digital certificates for Covid-19 test or vaccination results. The system can detect the authenticity of the certificate by comparing the hash that has been stored in the smart contract. The designed application is also able to interact with smart contracts on the Rinkeby Test network. Based on the test and validation, the design system has also met both user requirements and functional requirements. Transactions to smart contracts are affected by the capability of the nodes on the Rinkeby network to perform computations and the number of transactions that are processed at the same time. In future work, transaction time should be more considered, so the system can have better performance.

REFERENCES

[1] *K. Proctor, I. Sample, and P. Oltermann, "'Immunity passports' could speed up return to work after Covid-19," The Guardian, 30-Mar-2020.*[Online] Available : https://www.theguardian.com/world/2020/mar/30/immunity-passports-could-speed-up-return-to-work- after-covid-19 *(accessed October 5, 2021)*

[2] *Widyawati, "Pemerintah Integrasikan Data Kesehatan dengan Aplikasi Pedulilindungi untuk Mencegah Pemalsuan Hasil Tes COVID-19 sebagai Syarat Perjalanan," Sahabat Negeriku, 04-Jul-2021.* [online] Available: https://sehatnegeriku. kemkes.go.id/baca/rilis-media/20210704/0738021/pemerintah-integrasikan-data-kesehatan-dengan-aplikasi-pedulilindungi-untuk-mencegah-pemalsuan-hasil-tes-covid-19-sebagai-syarat-perjalanan/ *(accessed October 5, 2021)*

[3] "*Pakar kritisi kebocoran data sertifikat vaksin pedulilindungi*," 5-September-2021. [Online] Available: https://www.cnnindonesia.com/teknologi/20210905085011-185-689866/pakar-kritisi-kebocoran-data-sertifikat-vaksin-pedulilindungi (accessed October 5, 2021)

[4] H. Sheth and J. Dattani, "Overview of blockchain technology," *Asian Journal For Convergence In Technology (AJCT)*, vol. 5, no. 1, 2019.

[5] S. Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash*, 2008.

[6] V. Buterin "A next-generation smart contract and decentralized application platform," 2014, report.

[7] S. Salam and K. P. Kumar, "Survey on applications of blockchain in e-governance," *Revista Gestão Inovação e Tecnologias*, vol. 11, no. 4, pp. 3807–3822, 2021, doi: 10.47059/revistageintec.v11i4.2409.

[8] A. S. Ghanghoria, S. A. Raja, V. J. Bachche, and M. N. Rathi, "Secure e-documents storage using blockchain," *Int. Res. J. Eng. Technol.(IRJET)*, vol. 7, pp. 1972-1974, 2020.

[9] N. Chaniago, P. Sukarno, and A. A. Wardana, "Electronic document authenticity verification of diploma and transcript using smart contract on ethereum blockchain," *Register: Jurnal Ilmiah Teknologi Sistem Informasi*, vol. 7, no. 2, p. 149, 2021, doi: 10.26594 /register.v7i2.1959

[10] J. P. Dias, H. Sereno Ferreira, and Â. Martins, "A blockchain-based scheme for access control in e-health scenarios," *Proceedings of the Tenth International Conference on Soft Computing and Pattern Recognition (SoCPaR 2018)*, pp. 238–247, 2018, doi: 10.1007/978-3-030-17065-3_24

[11] Q. Xia, E. B. Sifah, K. O. Asamoah, J. Gao, X. Du, and M. Guizani, "MeDShare: trust-less medical data sharing among cloud service providers via blockchain," *IEEE Access*, vol. 5, pp. 14757-14767, 2017, doi: 10.1109/ACCESS.2017.2730843.

[12] A. F. da Conceição, F. S. C. da Silva, V. Rocha, A. Locoro, and J. M. Barguil, "Eletronic Health Records using Blockchain technology," arXiv.org, 26-Apr-2018. [Online]. Available: https://arxiv.org/abs/1804.10078. [Accessed: 25-Feb-2022].

[13] A. A. Vazirani, O. O'Donoghue, D. Brindley, and E. Meinert, "Blockchain vehicles for efficient medical record management," *npj Digital Medicine*, vol. 3, no. 1, 2020, doi: 10.1038/s41746-019-0211-0

[14] D. Ivan "Moving toward a blockchain-based method for the secure storage of patient records," *ONC/NIST Use of Blockchain for Healthcare and Research Workshop*, Gaithersburg, Maryland, United States, 2016.

[15] T.-T. Kuo and L. Ohno-Machado, "Modelchain: decentralized privacy-preserving healthcare predictive modeling framework on private blockchain networks," arXiv.org, 06-Feb-2018. [Online]. Available: https://arxiv.org/abs/1802.01746. [Accessed: 25-Jan-2022].

[16] *Medical Chain Whitepaper 2.1*, 2018.

[17] R. D. Mendonça, O. S. Gomes, L. F. Vieira, M. A. Vieira, A. B. Vieira, and J. A. Nacif, "Blockcoldchain: vaccine cold chain blockchain," arXiv preprint arXiv:2104.14357, 2021, doi: 10.48550/arXiv.2104.14357

[18] M. Eisenstadt, M. Ramachandran, N. Chowdhury, A. Third and J. Domingue, "COVID-19 antibody test/vaccination certification: there's an app for that," *IEEE Open Journal of Engineering in Medicine and Biology*, vol. 1, pp. 148-155, 2020, doi: 10.1109/OJEMB.2020.2999214

[19] U. Chelladurai and S. Pandian, "A novel blockchain based electronic health record automation system for healthcare," *Journal of Ambient Intelligence and Humanized Computing*, vol. 13, no. 1, pp. 693–703, 2021, doi: 10.1007/s12652-021-03163-3

[20] B. Arianto, "Dampak pandemi covid-19 terhadap perekonomian dunia," *Jurnal Ekonomi Perjuangan*, vol. 2, no. 2, 2021, doi: 10.36423/jumper.v2i2.665

[21] 'Landmark collaboration' to make COVID-19 testing and treatment available to all," 2020, eetrieved October 5, 2021, from United Nation: https: //news.un.org/en/story/2020/04/1062512

[22] J. Wu and N. Tran, "Application of blockchain technology in sustainable energy systems: an overview," *Sustainability*, vol. 10, no. 9, p. 3067, 2018, doi: 10.3390/su10093067

[23] A. Bansal, C. Garg, and R. P. Padappayil, "Optimizing the implementation of covid-19 'immunity certificates' using blockchain," *Journal of Medical Systems*, vol. 44, no. 9, 2020, doi: 10.1007/s10916-020-01616-4

[24] M. Xu, X. Chen, and G. Kou, "A systematic review of blockchain," *Financial Innovation*, vol. 5, no. 1, 2019, doi: 10.1186/s40854-019-0147-z

[25] H. Zodpe and A. Shaikh, "A survey on various cryptanalytic attacks on the aes algorithm," *International Journal of Next-Generation Computing*, vol. 12, pp. 115-123, 2021.

[26] "what is ipfs?," IPFS Docs. [Online]. Available: https://docs.ipfs.io/concepts/what-is-ipfs/. [Accessed: 06-Jul-2022].

[27] S. S. Kushwaha, S. Joshi, D. Singh, M. Kaur and H. -N. Lee, "Systematic review of security vulnerabilities in ethereum blockchain smart contract," *IEEE Access*, vol. 10, pp. 6605-6621, 2022, doi: 10.1109/ ACCESS. 2021.3140091..

[28] A. Verma, P. Bhattacharya, N. Madhani, C. Trivedi, B. Bhushan, S. Tanwar, G. Sharma, P. N. Bokoro, and R. Sharma, "Blockchain for industry 5.0: vision, opportunities, key enablers, and future directions," *IEEE Access*, vol. 10, pp. 69160-69199, 2022, doi: 10.1109/ACCESS.2022.3186892.

[29] "Ethereum Development Documentation," ethereum.org. [Online]. Available: https://ethereum.org/en/develo pers/docs/. [Accessed: 25-Jan-2022].