Advance Sustainable Science, Engineering and Technology (ASSET)
Vol. 6, No.2, April 2024, pp. 02402010-01 ~ 02402010-08
ISSN: 2715-4211 DOI: https://doi.org/10.26877/asset.v6i2.18262

Implementing Blockchain For Publishing and Verifying Digital Certificates On EduTech

Akwan Maroso*, Dwi Shinta Angreni, Rizka Ardiansyah, Kadek Agus Dwiwijaya

Information Technology Department, Faculty of Engineering, Tadulako University, Jl. Soekarno Hatta No KM 9 Palu 94148, Central Sulawesi, Indonesia

*akwanmaroso@gmail.com

This study investigates the application of blockchain technology in enhancing the security and authenticity of digital certificates. Addressing key challenges such as fraud and the lack of a standardized verification process, the paper proposes a comprehensive framework aimed at fortifying the integrity of digital credentials. This framework is the utilization of blockchain as a distributed ledger, serving as a tamper-proof repository for recording certification transactions. Through this decentralized ledger, each certification issuance and verification action is securely recorded, enhancing trust and transparency in the certification process. The methodology includes the integration of a decentralized ledger for immutable record-keeping and implementation of smart contracts for automated authenticity checks, and the use of cryptographic measures to ensure data security. This approach promises significant implications for various sectors reliant on credential verification, advocating for a broader adoption of blockchain in digital certificates systems.

Keywords: Blockchain, Digital Certificates, Smart Contract, Decentralization, Data Security.

(Received 2024-01-25, Accepted 2024-02-20, Available Online by 2024-03-08)

1. Introduction

For almost 20 years, digital certificates have been a key aspect of Internet security [1]. The need for reliable verification of credentials has become increasingly important. Digital certificates, serving as electronic documents to certify the ownership of a public key, have emerged as a critical tool in various fields ranging from education to IT security. They are used to validate the authenticity of entities and secure communication over the internet [2].

Traditional methods of issuing and verifying digital certificates face several challenges. These include susceptibility to fraud, lack of transparency, and inefficiencies in verification processes. The centralized nature of traditional systems often leads to a single point of failure, making them vulnerable to cyber-attacks. Additionally, the process of verifying certificates can be cumbersome and time-consuming, requiring reliance on the issuing authority for validation [3].

Blockchain technology, best known for underpinning cryptocurrencies like Bitcoin, offers a decentralized and tamper-evident ledger system. Its inherent characteristics—decentralization, immutability, and transparency—make it an appealing solution to address the shortcomings of

traditional digital certificate systems [4].

Implementing blockchain technology in the issuance and verification of digital certificates introduces a paradigm shift. Blockchain's decentralized nature allows for the creation of a distributed ledger where each certificate can be securely and transparently recorded. This approach reduces the risk of fraud and unauthorized alterations [5].

Despite the potential benefits of the blockchain system, the application of blockchain in digital certificates is still in its nascent stage, with practical challenges and limitations not fully explored. This research aims to fill this gap by implementing and analyzing blockchain technology in the context of digital certificate issuance and verification. The study's findings are expected to provide valuable insights and contribute to the advancement of knowledge in this evolving field.

To guide readers through the content of this paper, the following is the structure that will be followed. The next section will delve into the Methods, discussing the research type employed and the system development undertaken. Subsequently, the paper will move on to the Results and Discussion section, covering planning, analysis, system design, prototype, implementation, and system testing. The paper will conclude with a summary and suggestive recommendations for future developments in this field.

2. Methods

The research methodology is illustrated in Figure 1, outlining the flow of the study. This process begins with problem identification, followed by data collection, system design, system implementation, system testing, and ultimately concluding with the findings.

Figure 1. Research Methodology

2.1. Identification Problem

In this section, we'll examine the existing process of publishing and verifying digital certificates, identifying potential issues along the way.

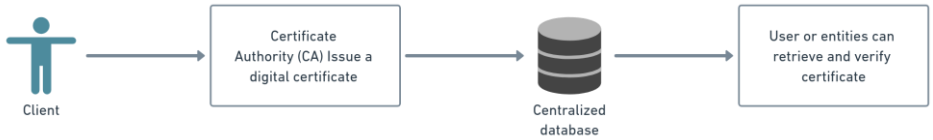

Figure 2. Current Publish Certificate System

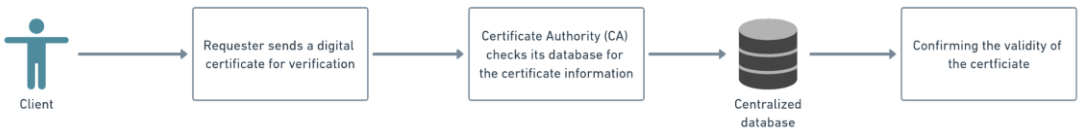

Figure 3. Current Verifying Certificate System

Figure 2 illustrates the process flow for publishing a certificate. The Certificate Authority (CA) stores data in a centralized database, such as MySQL or PostgreSQL [6], and makes the digital certificate accessible to entities. Figure 3 outlines the certificate verification process, where the client or requester sends a validation request. The CA then checks the centralized database for the provided information and confirms the validity of the certificate. The problem arises from using a centralized database to store certificate data. This creates single point failure and vulnerability to security breaches or data

manipulation [7]. Additionally, relying solely on the CA to verify certificate introduce a level of trust that may be exploited.

2.2. Data Collection

This phase focuses on gathering the necessary data to develop the system. Using quantitative techniques to generate large numbers of observations, emphasizing the necessity of large sample sizes for sophisticated quantitative analyses [8]. Data collected are associated with the process of publication and verification of digital certificates within the EduTech community Kode Karya Palu (Hammercode) are addressed. The research involved compiling recent digital certificates that have been published in the community.

2.3. System Design

In this stage, we defined how we can integrate the process of publish and verifying the certificate. The application was programmed under the Ethereum platform. Ethereum is major blockchain-based platform for smart contracts with complete programs that are executed in a decentralized network and usually manipulate digital units of value. A peer-to-peer network of mutually distrusting nodes maintains a common view of the global state and executes code upon request. The stated is stored in a blockchain secured by a proof-of-work consensus mechanism similar to that in Bitcoin [9-11]. Smart contracts will act as stateful decentralized applications that run on EVM implementations to enforce contract instructions [12]. In this system, we will use the RESTful API [13] as the protocol communication between client app and server app.

In Figure 4 we can see the process of publishing a certificate in the initial step, certificate details are input into the system and will trigger the smart contract within the EVM, utilizing the provided information. The smart contract processes the request according to the pre-defined contract, and upon successful fulfillment, stores the data as a transaction within the blockchain. Each process that creating transactions on the blockchain will be need a cost (gas) to distribute the data across each node [14][15]. Upon completion of all processes, the system generates a random hash along with a QR code to serve as an identifier for the certificate stored in the blockchain.

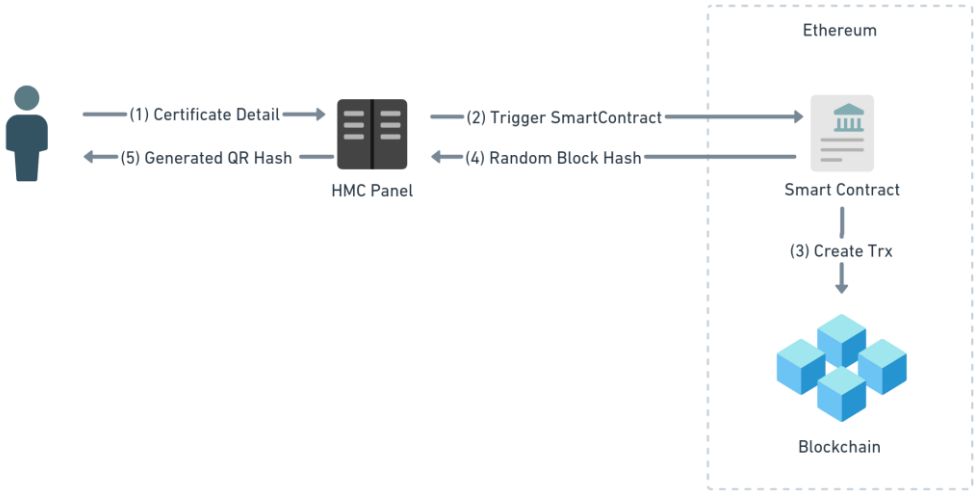

Figure 4. Publish Certificate

On Figure 5 illustrates the process of verifying a certificate. In this workflow, the client sends a hashed QR code containing the certificate identifier. The system acts as a proxy, triggering the smart contract equipped with a function to locate the certificate based on the identifier. Since the process involves only reading data from the blockchain network, there are no additional costs incurred [14]. If the data is found, it is displayed to the client.

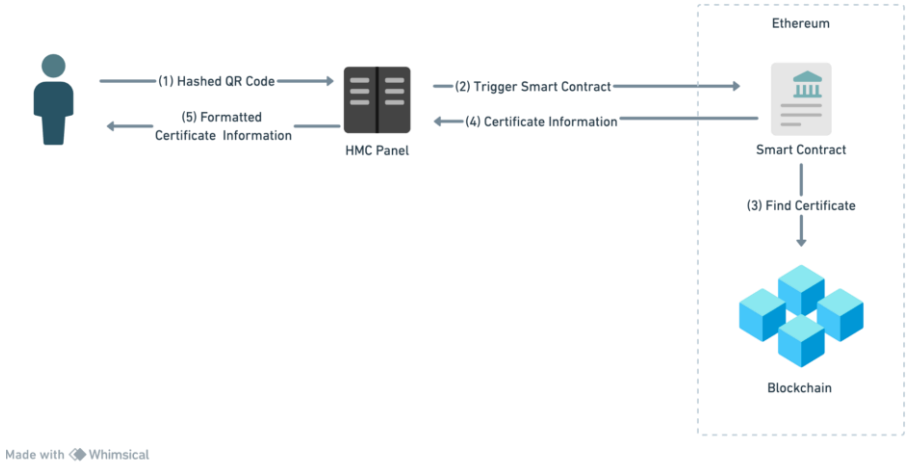

Figure 5. Verify Certificate

2.4. Implementation

The system has separate backend and frontend components. The backend is built using the Go programming language. Go is expressive, concise, clean, and efficient. Its concurrency mechanisms make it easy to write programs that get the most out of multicore and networked machines, while its novel type system enables flexible and modular program construction [16], while the frontend development incorporates JavaScript, utilizing NextJS as the framework. Additionally, the system's interaction with the Ethereum network is facilitated through smart contracts written in Solidity[17].

The client-side interface allows for two methods of inputting the certificate ID. Firstly, users can manually enter the certificate ID and initiate verification; the system will then validate the certificate. Alternatively, users can scan the QR code on the certificate, which automatically extracts the ID. This implementation is illustrated in Figure 6.

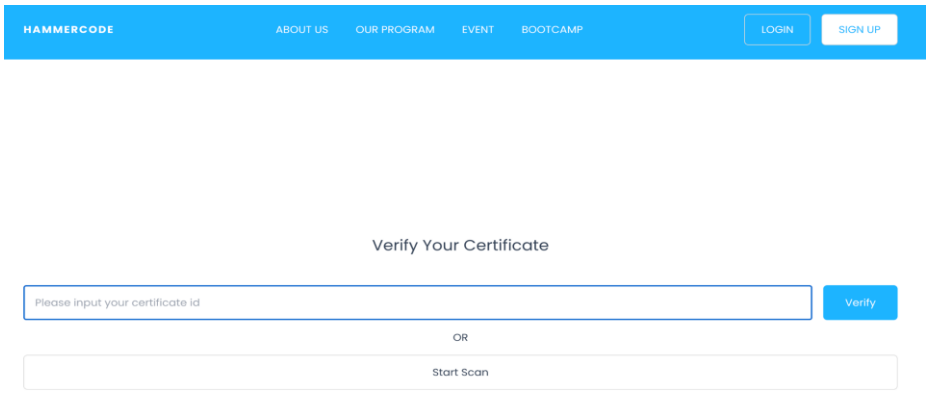

Figure 6. Validation Page

When a value is inputted as shown in Figure 6, it undergoes verification within the blockchain network. Should the data be found on the network, the details of the certificate will be presented on the system. The outcomes of this verification process are illustrated in Figure 7.

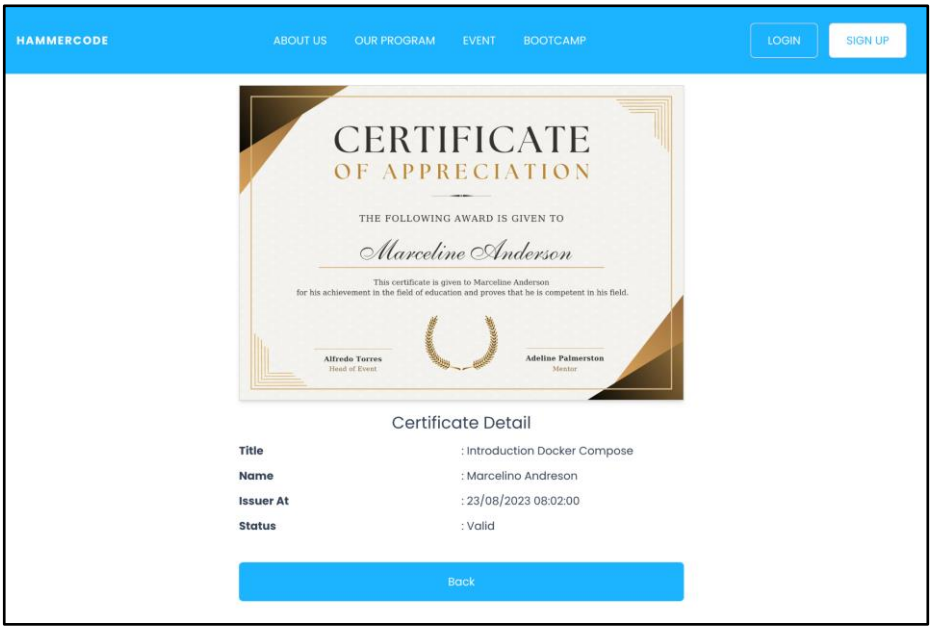

Figure 7. Certificate Validation Result

2.5. Testing Phase

In this study, the performance evaluation of the application hinges on analyzing key metrics. These metrics encompass the calculation of transaction throughput (TTP) and verification latency (VL). By focusing on these parameters, we aim to gain insights into the efficiency and responsiveness of the application.

1. Transaction Throughput (TPP)
   This metric reflects of the number of certificate verification transactions the system can handle per unit of time[18], indicating scalability and performance efficiency.

$$TTP = \frac{Total\ Number\ of\ Transaction\ Processed}{Total\ Time\ Taken}$$

2. Verification Latency
   Average time taken to verify a single certificate, this indicate the responsiveness the system [18].

$$VL = \frac{Total\ Time\ Taken\ to\ Verify\ N\ Certificate}{N}$$

3. Results and Discussion

3.1. Result

In our assessment of the blockchain application developed for issuing and verifying digital certificates, we noted significant achievements in several metrics, along with areas that require enhancement, particularly addressing the issue of a single point of failure in the database. The outcomes of our performance analysis, focusing on Transaction Throughput(TTP) and Verification Latency(VL), are presented below.

$$TTP = \frac{135}{4}$$
$$TTP = 33\ transaction\ per\ second$$

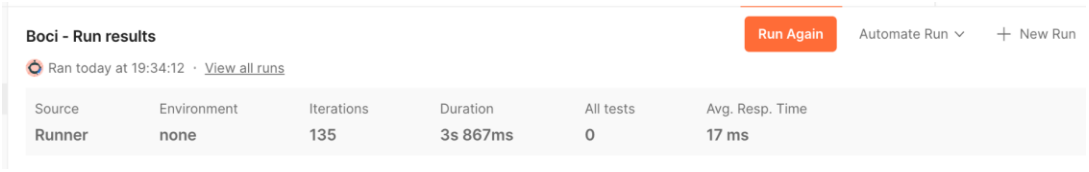

Figure 8. Load Test Publish Certificate

$$_{V}L = \frac{9}{135}$$

$$VL = 60ms\ per\ certificate$$

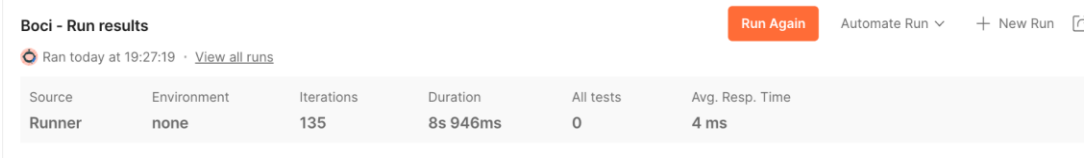

Figure 9. Load Test Verify Certificate

The detailed examination of our load testing, conducted using Postman as the load testing client [19] on Figure 8 and Figure 9, involved a scenario with 135 certificates undergoing the process of publication and verification. This thorough evaluation demonstrated a Transaction Throughput (TTP) of 33 transactions per second. Concurrently, the Verification Latency (VL) for each transaction was recorded at 60 milliseconds. These results underscore a significant opportunity for enhancing the system's speed, particularly in optimizing the verification process to achieve a more efficient transaction handling rate.

3.2. Blackbox Testing

This stage will test all process that are already develop. The testing process gonna use Black Box testing method also know a functional testing or input output driven testing, it means on the process testing will be focus on the input and output of the system [20]. The following are the results of system testing using the Blackbox method can be seen in Table 1.

Table 1. System Testing Results

Test Case	Description	Results
Deploy smart contract	Test the deployment of the smart contract on the Ethereum network.	Success
Verify Certificate	Validate if the inputted certificate ID is valid or not.	Success
Publish Certificate	Store certificate details on the blockchain network.	Success
Invalid Certificate Check	Verify system's response to an invalid certificate ID.	Success
Certificate Data Retrieval	Retrieve the details of a stored certificate.	Success
Smart Contract Update	Test updating the smart contract code on the Ethereum network.	Success

4. Conclusion

Based on the system testing result and observation this research about adopting blockchain to process publishing and verifying certificate digital with blockchain has been successfully implemented. This adoption make the each process publish and verify certificate more transparent and more secure. This approach not only enhances on factor integrity and security but also expand solution to the limitations associated with traditional systems. The results of the system testing provided us visual evidence of the system accelerated speed. These result offer significantly improved processing times, showcasing the efficiency gains achieved through the adoption of this technology

One of the critical advantages addressed in this study is blockchain's ability to mitigate the risks associated with single points of failure in centralized database systems. In traditional systems, the centralization of data storage and management creates vulnerabilities, making the entire system susceptible to data breaches, tampering, and downtime. Future research could focus on further exploring the scalability of blockchain solutions on the digital certificates, examining the integration with existing educational and professional credentialing systems, and developing more advanced cryptographic methods to enhance privacy and security even further. Additionally, investigating mechanisms to address potential scalability challenges and ensuring the interoperability of blockchain-based certification systems across various sectors and platforms would be invaluable.

References

[1] N. Leavitt, "Internet Security under Attack: The Undermining of Digital Certificates," in Computer, vol. 44, no. 12, pp. 17-20, Dec. 2011, doi: 10.1109/MC.2011.367.

[2] Maulani, G., Gunawan, G., Leli, L., Ayu Nabila, E., & Yestina Sari, W. (2021). Digital Certificate Authority with Blockchain Cybersecurity in Education. *International Journal of Cyber and IT Service Management*, *1*(1), 136–150. https://doi.org/10.34306/ijcitsm.v1i1.40

[3] Jirgensons, M., & Kapenieks, J. (2018). Blockchain and the Future of Digital Learning Credential Assessment and Management. *Journal of Teacher Education for Sustainability*, *20*(1), 145–156. https://doi.org/10.2478/jtes-2018-0009

[4] S. Nakamoto, “Bitcoin: A Peer-to-Peer Electronic Cash System,” Www.Bitcoin.Org, p. 9, 2008.

[5] T. T. Huynh, T. Tru Huynh, D. K. Pham and A. Khoa Ngo, "Issuing and Verifying Digital Certificates with Blockchain," 2018 International Conference on Advanced Technologies for Communications (ATC), Ho Chi Minh City, Vietnam, 2018, pp. 332-336, doi: 10.1109/ATC.2018.8587428.

[6] Poljak, R., Poščić, P., & Jakšić, D. (2017). Comparative analysis of the selected relational database management systems. 2017 40th International Convention on Information and Communication Technology, Electronics and Microelectronics (MIPRO), 1496-1500. https://doi.org/10.23919/MIPRO.2017.7973658.

[7] Jung, M. Y., & Jang, J. W. (2017). Data management and searching system and method to provide increased security for IoT platform. Information and Communication Technology Convergence, 2017-December, 873–878. https://doi.org/10.1109/ICTC.2017.8190803.

[8] Ragin, C.C. (1999). The distinctiveness of case-oriented research. Health services research, 34 5 Pt 2, 1137-51.

[9] Tikhomirov, S. (2018). Ethereum: State of Knowledge and Research Perspectives. In: Imine, A., Fernandez, J., Marion, JY., Logrippo, L., Garcia-Alfaro, J. (eds) Foundations and Practice of Security. FPS 2017. Lecture Notes in Computer Science(), vol 10723. Springer, Cham. https://doi.org/10.1007/978-3-319-75650-9_14

[10] D. Vujičić, D. Jagodić and S. Ranđić, "Blockchain technology, bitcoin, and Ethereum: A brief overview," 2018 17th International Symposium INFOTEH-JAHORINA (INFOTEH), East Sarajevo, Bosnia and Herzegovina, 2018, pp. 1-6, doi: 10.1109/INFOTEH.2018.8345547.

[11] Oliva, G.A., Hassan, A.E. & Jiang, Z.M.(. An exploratory study of smart contracts in the Ethereum blockchain platform. Empir Software Eng 25, 1864–1904 (2020). https://doi.org/10.1007/s10664-019-09796-5

[12] Chan, W., & Olmsted, A. (2017). Ethereum transaction graph analysis. 2017 12th International Conference for Internet Technology and Secured Transactions (ICITST), 498–500. https://doi.org/10.23919/ICITST.2017.8356459
[13] Ehsan, A., Abuhaliqa, M. A. M. E., Catal, C., & Mishra, D. (2022). RESTful API Testing Methodologies: Rationale, Challenges, and Solution Directions. In Applied Sciences (Switzerland) (Vol. 12, Issue 9). MDPI. https://doi.org/10.3390/app12094369
[14] L. Marchesi, M. Marchesi, G. Destefanis, G. Barabino and D. Tigano, "Design Patterns for Gas Optimization in Ethereum," 2020 IEEE International Workshop on Blockchain Oriented Software Engineering (IWBOSE), London, ON, Canada, 2020, pp. 9-15, doi: 10.1109/IWBOSE50093.2020.9050163.
[15] B. Severin, M. Hesenius, F. Blum, M. Hettmer and V. Gruhn, "Smart Money Wasting: Analyzing Gas Cost Drivers of Ethereum Smart Contracts," 2022 IEEE International Conference on Software Maintenance and Evolution (ICSME), Limassol, Cyprus, 2022, pp. 293-304, doi: 10.1109/ICSME55016.2022.00034.
[16] Russ Cox, Robert Griesemer, Rob Pike, Ian Lance Taylor, and Ken Thompson. 2022. The Go programming language and environment. Commun. ACM 65, 5 (May 2022), 70–78. https://doi.org/10.1145/3488716.
[17] Analyzing the Impact of Next.JS on Site Performance and SEO. (2023). International Journal of Computer Applications Technology and Research. https://doi.org/10.7753/ijcatr1210.1004.
[18] Yadav, J., & Shevkar, R. (2021). Performance-Based Analysis of Blockchain Scalability Metric. Tehnicki Glasnik, 15(1), 133–142. https://doi.org/10.31803/TG-20210205103310.
[19] Andrianto, L. D., & Suyatno, D. F. (2024). Analisis Performa Load Testing Antara Mysql Dan Nosql Mongodb Pada RestAPI Nodejs Menggunakan Postman. Journal of Emerging Information System and Business Intelligence (JEISBI), 5(1), 18–26. https://ejournal.unesa.ac.id/index.php/JEISBI/article/view/58157.
[20] Syarif, M., & Pratama, E. B. (2021). ANALISIS METODE PENGUJIAN PERANGKAT LUNAK BLACKBOX TESTING DAN PEMODELAN DIAGRAM UML PADA APLIKASI VETERINARY SERVICES YANG DIKEMBANGKAN DENGAN MODEL WATERFALL. *Jurnal Teknik Informatika Kaputama (JTIK)*, *5*(2).