

# Blockchain-Based E-Certificate System: Secure and Transparent Credential Management

Umi Chotijah\*, Ilham Teguh Prayudha, Achmad Rifki

## ABSTRACT

This study explores the development of a blockchain-based e-certificate system designed for secure and transparent credential management at the Muhammadiyah University of Gresik. Leveraging private blockchain technology, the system addresses the challenges of certificate forgery and unauthorized alterations by ensuring data immutability and integrity. Through the implementation of a distributed ledger, the platform facilitates seamless issuance, verification, and storage of e-certificates. The methodology encompasses system design using the waterfall model, including stages of requirement analysis, system design, implementation, integration, and testing. Smart contracts are utilized to automate certificate verification processes, enhancing efficiency and reliability. The research findings demonstrate that the blockchain-based system not only secures the certification process but also streamlines operations by eliminating intermediaries. This innovative approach holds promise for broader applications in academic institutions and beyond, offering a scalable solution for secure document management. Future studies may expand its applicability across diverse industries.

**Keyword:** Blockchain technology, credential security, e-certificate system

Received: August 22, 2024; Revised: December 09, 2024; Accepted: December 27, 2024

**Corresponding Author:** Umi Chotijah, Department of Informatics, Universitas Muhammadiyah Gresik, Indonesia; [umi.chotijah@umg.ac.id](mailto:umi.chotijah@umg.ac.id)

**Authors:** Ilham Teguh Prayudha, Department of Informatics, Universitas Muhammadiyah Gresik, Indonesia, [ihamtprayudha@gmail.com](mailto:ihamtprayudha@gmail.com); Achmad Rifki, Department of Informatics, Universitas Muhammadiyah Gresik, Indonesia, [a.rifki180603@gmail.com](mailto:a.rifki180603@gmail.com)



The Author(s) 2024

Licensee Program Studi Sistem Informasi, FST, Universitas Islam Negeri Raden Fatah Palembang, Indonesia. This article is an open access article distributed under the terms and conditions of the Creative Commons Attribution-ShareAlike (CC BY SA) license (<https://creativecommons.org/licenses/by-sa/4.0/>).

## 1. INTRODUCTION

Blockchain technology, a novel and transformative innovation, has recently garnered significant attention. Mendling et al. (2018) examine its potential in the context of Business Process Management (BPM), discussing both opportunities and challenges. They explain that companies adopt systems to facilitate the execution of inter-organizational processes, aiming to automate and expedite operations. However, the broad adoption of such processes is hindered by complex issues, notably the difficulties in joint design and establishing trust (Mendling et al., 2018). At its core, blockchain is a distributed database technology underpinning cryptocurrencies like Bitcoin. It creates a ledger of transaction records, each stamped with an immutable timestamp (Curty et al., 2023; Dzhilila et al., 2023; Kurniawan et al., 2019). This technology introduces the revolutionary capability of enabling transactions among parties without requiring mutual trust, a critical feature in trustless networks (Curty et al., 2023; Mendling et al., 2018; Rahmadika et al., 2018). This is achieved through a synergy of peer-to-peer networks, consensus algorithms, cryptography, and market mechanisms. Blockchain ensures unparalleled data integrity and transparency, allowing operations even under byzantine fault conditions—errors where observers perceive different system states (Dzhilila et al., 2023; Mendling et al., 2018; Zhu & Wang, 2019a). Each node

in the blockchain network maintains a copy of the entire ledger, and consensus is achieved using algorithms such as proof-of-work or proof-of-stake.

Blockchain technology functions as a peer-to-peer database that provides comprehensive access to the historical states of the system (Alam et al., 2022). A key feature of some blockchain networks is their ability to execute user-defined scripts, known as smart contracts (Zhu, 2019). These contracts facilitate business collaborations, particularly for implementing inter-organizational business processes (Weber et al., 2016). Ethereum serves as a prominent example of a blockchain platform utilizing smart contracts (Mendling et al., 2018; Zhu & Wang, 2019b). As a platform, Ethereum enables the creation and deployment of Decentralized Applications (DApps) that operate within its blockchain network, ensuring that the stored data remains accessible as long as the network exists (ER, 2018; Wang et al., 2019; Weber et al., 2016). Ethereum's functionality is supported by a Turing-complete programming language for smart contracts, characterized by deterministic code that assumes a closed-world model—accessing only information from blockchain transactions during runtime. Additionally, like any blockchain transaction, the implementation of smart contract code into the blockchain is immutable (Wibowo, 2019).

This study aims to design and implement blockchain technology for an e-certificate system within the Computer Engineering Program at Muhammadiyah University of Gresik (UMG). The program includes overseeing Himpunan Mahasiswa Teknik Informatika (HIMATIF), a student organization responsible for various undergraduate activities and programs. Certificates are awarded to participants to recognize achievements, completion of specific activities, competency tests, or learning milestones. However, maintaining the integrity and security of these certificates is crucial to prevent unauthorized alterations or forgery. To address this issue, blockchain technology provides an innovative solution by employing a distributed ledger system, which ensures data security, immutability, and cost efficiency in the secure creation and storage of certificates.

## 2. MATERIALS AND METHODS

### 2.1 Materials

Blockchain, originally recognized for its application in bitcoin, represents a novel approach to data storage and transaction recording (Noor, 2020). It comprises encrypted, interconnected blocks distributed across a network and characterized by their append-only nature. Each block contains data, a unique hash for identification, and the hash of the preceding block, forming a secure and immutable chain (Sugiharto & Musa, 2020). Any alteration to a block's hash renders it invalid within the blockchain. The hash, generated through cryptographic hashing processes such as the widely used SHA-256 algorithm, ensures the uniqueness and integrity of each block (ER, 2018; Wijaya, 2016). As the blockchain grows, the computational complexity of generating hash values increases, further enhancing its security.

Blockchain operates within a network of users, referred to as peers, who collectively participate in a decentralized system. Two primary types of blockchain exist: public blockchains and private blockchains, the latter characterized by restricted management authority (Sugiharto & Musa, 2020). This system development utilizes a private blockchain. A key feature of blockchain is the consensus process, which ensures that data additions are validated by all peers in the network. Consensus mechanisms can be implemented using various approaches, such as mining or Proof-of-Work (PoW), as illustrated in Figure 1. PoW is a method of data recording that relies on solving complex mathematical calculations to validate data additions, a task performed by users known as miners (ER, 2018; Mendling et al., 2018; Sugiharto & Musa, 2020).

Blockchain technology has diverse applications across fields such as biomedicine and healthcare (Kuo et al., 2017), supply chain (Martono, 2020), e-commerce (Dzakiy, 2019), banking industry (Guo & Liang, 2016), and education (Chen et al., 2018; Djajadi et al., 2023; Nugraha, 2022). Building on these advancements, this study focuses on developing and evaluating a blockchain-based system for certificate issuance and verification. The system is designed to securely manage e-certificates by leveraging private blockchain technology, ensuring data integrity and security. Additionally, the feasibility of practical

implementation is assessed, enabling the secure issuance and validation of e-certificates while maintaining a robust data storage mechanism.

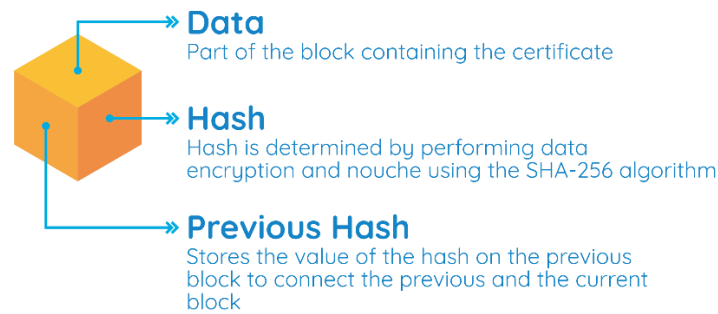


Figure 1. Proof-of-work processes in blockchain

## 2.2 Methods

The research methodology in this study, as illustrated in Figure 2, encompasses three interrelated stages: Identification, Planning and Design, and Iterative Prototype. In the identification stage, the study emphasizes the importance of detecting the potential for e-certificate forgery. Subsequently, during the planning and design stage, the system's scope and requirements are systematically formulated to ensure the project's feasibility and sustainability. Finally, the iterative prototype stage involves iterative development and testing processes, enabling continuous refinement of the e-certificate verification system until it is ready for deployment.

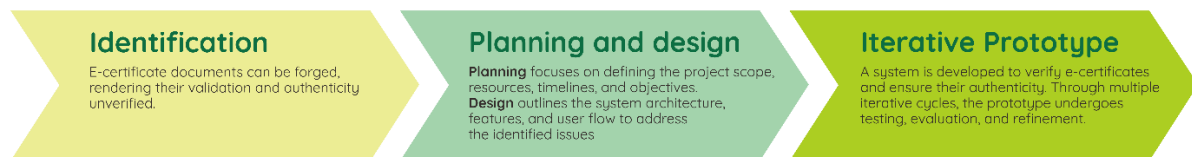


Figure 2. Research method

## 2.3 Software Development Life Cycle

This research adopts a sequential system development process using the structured workflow of the waterfall methodology, which consists of five key phases. The first phase, requirement analysis, involves identifying and analyzing the needs for a blockchain-based e-certificate system, with data sourced from the computer engineering program and Himpunan Mahasiswa Teknik Informatika (HIMATIF). In the system design phase, specific rules for system usage, module designs, interface layouts, and database structures are established, employing QSEE Superlite as the modeling tool. The subsequent implementation phase translates these designs into program modules, databases, and application interfaces. This is followed by system integration and testing, where comprehensive evaluations are conducted to ensure the system's successful implementation. While maintenance is a standard phase in the waterfall methodology, it falls outside the scope of this research.

## 3. RESULTS AND DISCUSSION

### 3.1 Scope of the Developed System

The E-Certificate blockchain system, as illustrated in Figure 3, connects various stakeholders—including students, the HIMATIF organization, the head of study program, and the blockchain system itself—through a centralized platform designed to facilitate the issuance and verification of activity certificates. Students are responsible for uploading activity data and retrieving certificates, while HIMATIF contributes by providing participant information and uploading digital certificates to the blockchain. The head of study program serves as the final verifier, ensuring the certificates' validity before they are issued

to students. All related data, from activity details to e-signatures, is managed transparently and securely using blockchain-based recording processes.

Once certificates are verified, the system enables students to download their e-certificates stored on the blockchain. This ensures that every step of certificate issuance, updates, and downloads is permanently recorded and easily accessible to authorized parties. The decentralized approach enhances data integrity and minimizes the risk of document forgery. Additionally, the use of smart contracts for automated and rapid verification makes the e-certificate management process more efficient and reliable at every stage.

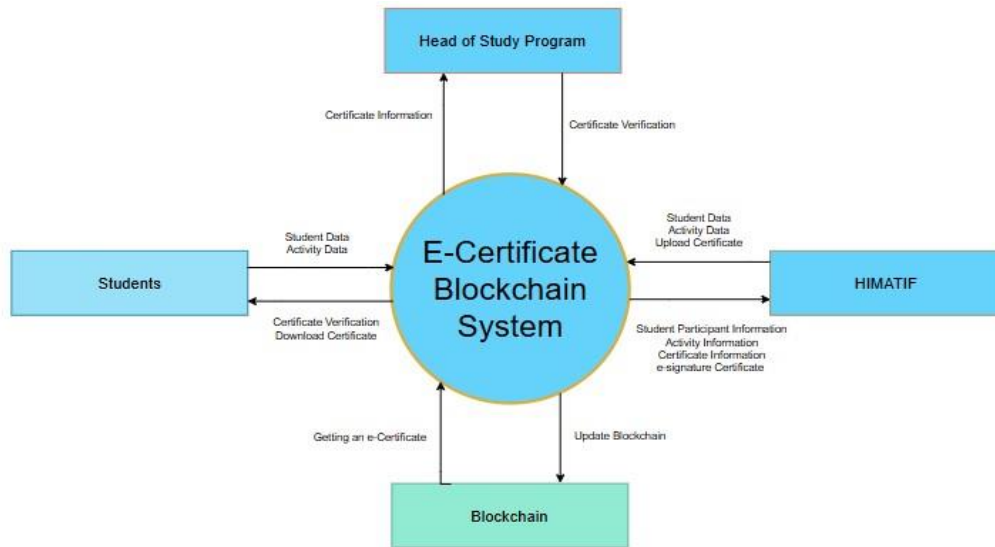


Figure 3. Scope of system

### 3.2 Document Integration Process into Blockchain

This study introduces a dynamic e-certificate generation system utilizing blockchain technology, enabling the creation of customized certificates. The process begins when a student registers on the e-certificate web portal by submitting the required documents. The portal authenticates the student's submission, and the head of the study program subsequently validates the documents. Once verification is complete, the system stores the data securely on the blockchain, generates a unique certificate identifier or QR code, and returns it to the student. The workflow for issuing certificates using blockchain technology is illustrated in Figure 4.

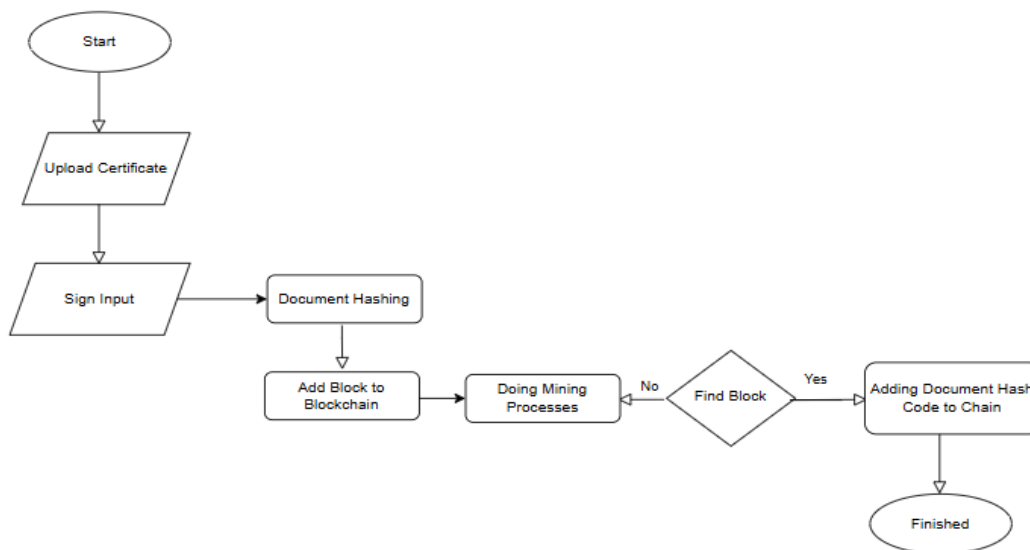


Figure 4. Flowchart of the document integration process into blockchain

### 3.3 Document Validation Process on Blockchain

The flowchart of document issuance, as shown in Figure 5, illustrates the detailed process, starting from generating digital signatures to storing the document's hash code on the blockchain. The hashing process can utilize various methods, with MD5 encryption being one of the options. Instead of storing the entire document, the system saves only the hash result within the blockchain. During the document validation process, the system compares the hash generated from the uploaded document with the hash code stored in the blockchain. If the hash codes match, the system confirms the document's validity with a message. Conversely, if the document is identified as invalid, it may indicate either that the uploaded file does not match the registered document or that the e-certificate has been modified.

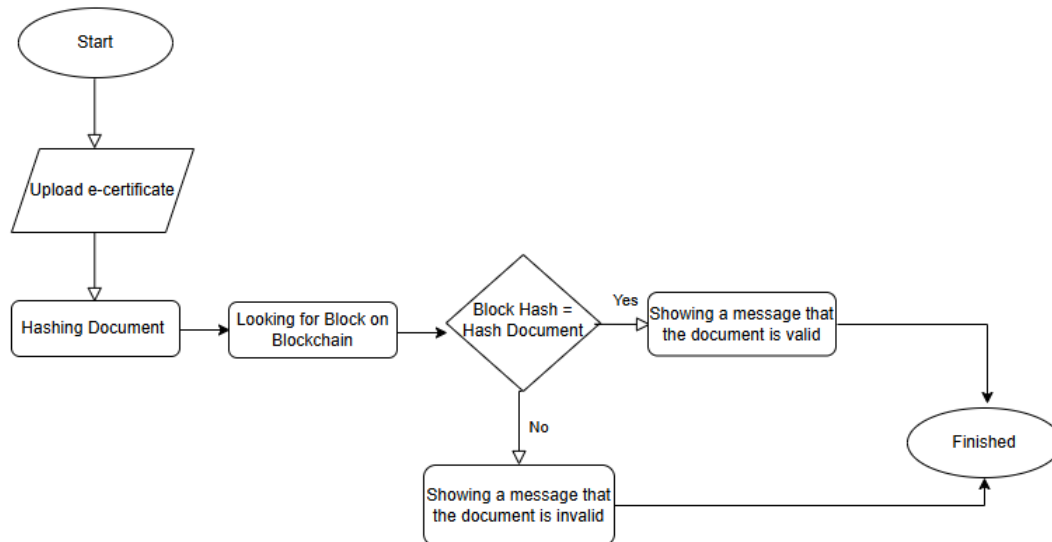


Figure 5. Flowchart of the document validation process on blockchain

### 3.4 Implementation of the Blockchain-based Certificate System

This section outlines the steps involved in transforming a system design into a fully operational program utilizing the Python programming language. The application is built on the Ethereum blockchain within a localized development environment. Key phases of the implementation are detailed below:

#### 1. Setup of local blockchain environment

- Install the Ganache CLI to simulate a private blockchain for development purposes.

```
npm install -g ganache-cli
```

- Execute the RPC server command to initialize the blockchain interface.

```
npm run ganache
```

#### 2. Deployment of smart contracts

Smart contracts, written in solidity—a language tailored for Ethereum—are deployed to the local blockchain. These contracts govern operations such as institutional registration, certificate issuance, verification, and revocation. Blockchain events are emitted to log significant transactions.

```
npm run contract-deploy
```

#### 3. Frontend development

The user interface (UI) for the certificate system is designed using HTML, CSS, and React. It provides intuitive tabs for "Certificate Issuance" and "Verification," enabling seamless navigation for users.

#### 4. Institution registration

Institutions register by submitting details such as their name, website, and offered courses. A smart contract is launched on the blockchain for each registered institution. The MetaMask wallet facilitates this process by managing Ether for transaction fees.

#### 5. Certificate issuance

Institutions generate certificates by inputting student information and course details. Each certificate is linked to a unique cryptographic hash stored on the blockchain, ensuring its security and authenticity.

#### 6. Certificate verification

Users verify certificates by navigating to the "verification" tab and entering the certificate's hash key. The system retrieves the certificate details from the blockchain for validation.

#### 7. Revocation mechanism

Users can revoke certificates by providing their hash key and activating the revocation function. This action updates the blockchain to reflect the certificate's new status.

#### 8. Testing and deployment

Comprehensive testing—including unit tests for smart contracts, integration tests for the UI and backend, and user acceptance tests—is conducted to ensure functionality, security, and user-friendliness. The final system is deployed on the Ethereum Mainnet for live use.

#### 9. User training and support

Detailed documentation and training sessions are provided to familiarize users and institutions with the system's features. Ongoing support addresses queries and technical issues.

#### 10. Security measures

Robust encryption and secure communication protocols protect sensitive data and prevent unauthorized access. Regular security audits and vulnerability assessments ensure system integrity.

The implementation of the electronic certificate issuance and verification system incorporates several key user interfaces designed to enhance usability. The following descriptions detail the available system interfaces (Figure 6, Figure 7, Figure 8, and Figure 9).

The screenshot shows a web interface for the HIMATIF system. At the top, there is a navigation bar with the HIMATIF logo on the left and links for 'Home', 'TTD', 'Validasi', 'List Data', and a user profile icon on the right. Below the navigation bar, the main heading is 'Input TTD'. The form area is titled 'Pilih Tanda Tangan' and includes a 'Choose file' button next to a text input field. Below this, there are two input fields: 'Nama' with the placeholder 'Masukkan Nama' and 'NIP' with the placeholder 'Masukkan NIP'. A 'Submit' button is located at the bottom right of the form area.

Figure 6. Input signature of head of study program page

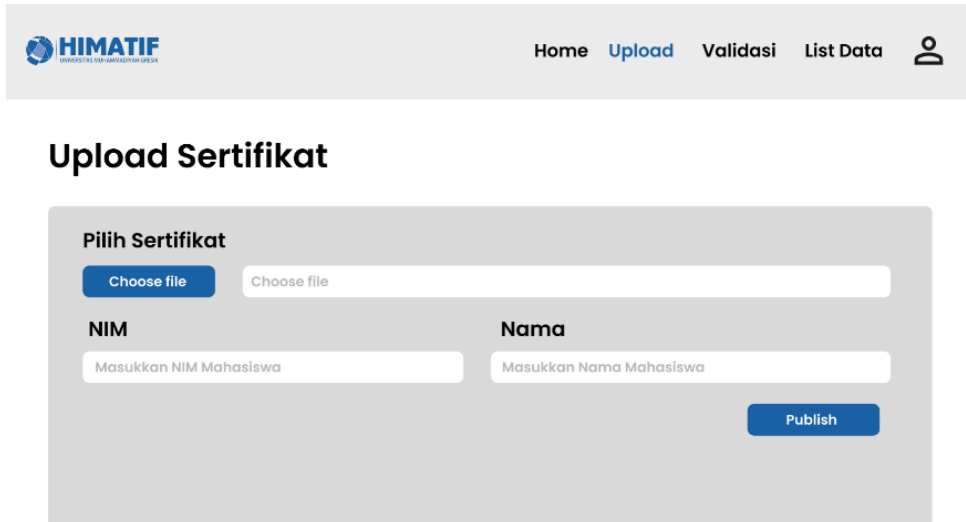


Figure 7. Certificate upload page

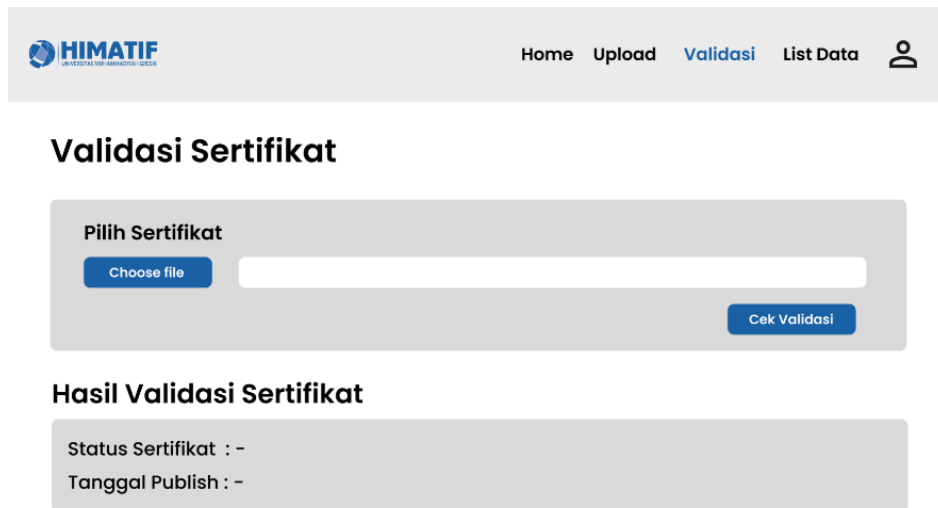
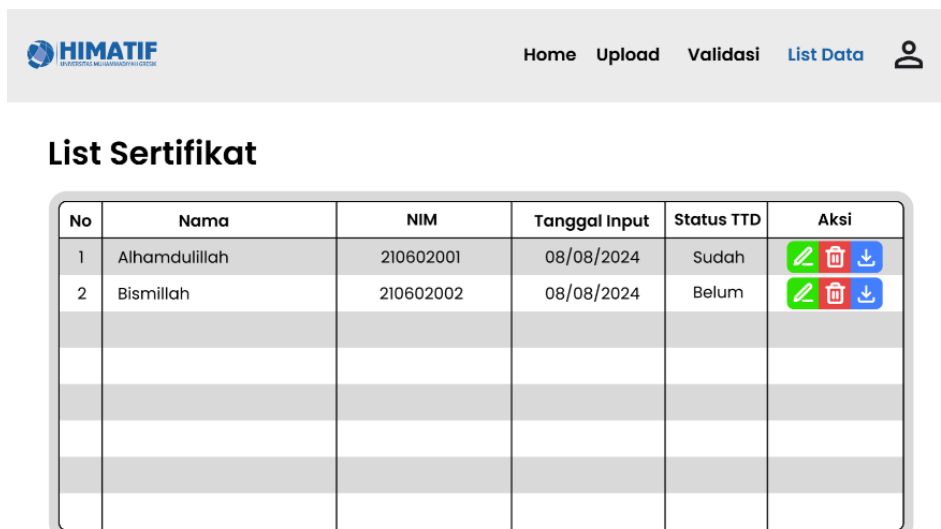


Figure 8. Certificate validation page









| No | Nama          | NIM       | Tanggal Input | Status TTD | Aksi  |
|----|---------------|-----------|---------------|------------|---|
| 1  | Alhamdulillah | 210602001 | 08/08/2024    | Sudah      |    |
| 2  | Bismillah     | 210602002 | 08/08/2024    | Belum      |    |
|    |               |           |               |            |   |
|    |               |           |               |            |   |
|    |               |           |               |            |   |
|    |               |           |               |            |   |

Figure 9. List of certificates managed by the program head

### 3.5 System Testing

System testing is conducted to evaluate whether the implemented system functions as intended and meets user requirements. The testing process provides valuable insights into the system's functionality and identifies areas for improvement. Essential criteria for the testing phase include the use of specific browsers, active user accounts, and accurate student data.

The Black Box testing method was employed during this phase, focusing on the system's output rather than its internal processes. The results of the tests performed on various system modules are summarized as follows:

#### 1. Testing the certificate issuance module

This test evaluates the document issuance module, ensuring that the admin can execute the certificate issuance process smoothly. The results of the test are summarized in Table 1.

Table 1. Testing the certificate issuance module

| Tested module             | Procedure  | Input testing                       | Expected output    |
|---------------------------|--|-------------------------------------|--------------------|
| Issuance of e-certificate | <ul style="list-style-type: none"> <li>✓ Upload certificate,</li> <li>✓ Set up signature,</li> <li>✓ Submit</li> </ul> | Certificate and signature documents | E-Certificate file |

#### 2. Testing the certificate validation module

This test focuses on the certificate validation module, allowing users to verify the authenticity of certificates efficiently. The outcomes of this testing are presented in Table 2.

Table 2. Testing the certificate validation module

| Tested module                                 | Procedure  | Input testing                      | Expected output   |
|---|--|------------------------------------|---|
| Certificate validation – Iteration 2          | <ul style="list-style-type: none"> <li>✓ Open page,</li> <li>✓ Validate document,</li> <li>✓ Upload document,</li> <li>✓ Enter hash code,</li> <li>✓ Submit</li> </ul> | Certificate and hash code document | A statement appears: "The document has been validated with the last block in the blockchain." |
| Certificate validation (Failed) – Iteration 1 | <ul style="list-style-type: none"> <li>✓ Open page,</li> <li>✓ Validate document,</li> <li>✓ Upload document,</li> <li>✓ Enter hash code,</li> <li>✓ Submit</li> </ul> | Certificate and hash code document | A note appears: "The document cannot be validated with the last block on the blockchain."     |

### 3.6 Discussion

The implementation of a blockchain-based certificate verification system has demonstrated promising results, proving the proposed approach to be both feasible and effective. Student registration details, including the institution's website and offered courses, are securely stored on the blockchain ledger to confirm institutional registration within the system. The MetaMask wallet plays a crucial role in facilitating the seamless execution of smart contracts on the Ethereum blockchain during the registration process. Each certificate issued by HIMATIF includes the student's name and course details, with a unique MetaMask wallet account created for every certificate to ensure robust security. Each certificate is linked to a one-of-a-kind hash key, serving as a reliable verification mechanism. Users verify certificates by accessing the "verification" page, entering the hash key, and allowing the system to query the Ethereum blockchain for associated certificate information. This process ensures quick and accurate validation, enabling users to confirm the legitimacy of certificates with ease.



In addition to verification, the system incorporates a revocation mechanism to address invalid certificates or fraudulent activities. Users can revoke a certificate by entering its hash key and activating the revocation function, which immediately updates the certificate's status on the blockchain to indicate its invalidity. To uphold data security and transaction integrity, the system employs stringent encryption methods and secure communication protocols, complemented by regular security assessments and vulnerability evaluations. User feedback highlights a positive experience with the system, bolstered by user-friendly interfaces, comprehensive training materials, and continuous support. Overall, the implementation showcases blockchain technology's potential to revolutionize certificate verification by offering a secure, transparent, and efficient solution that resolves issues inherent in traditional methods. Future refinements aim to enhance the system's scalability and usability for broader adoption.

#### 4. CONCLUSION

This study developed a blockchain-based certificate system to ensure security, integrity, and transparency in the management of electronic certificates. The results demonstrate that the system successfully achieves its primary objectives by leveraging blockchain technology to securely store registration data, issue certificates, and verify documents. Utilizing smart contracts on the Ethereum blockchain, the system ensures that every step of the process is immutably recorded. The implementation results indicate that this approach is both feasible and effective in addressing issues associated with traditional methods, such as document forgery and data manipulation.

These findings have significant implications for enhancing the reliability and efficiency of certificate management across various domains. However, the study has certain limitations, including its implementation scale being confined to a university environment and its reliance on blockchain infrastructure, which incurs high operational costs. Moving forward, further optimization is necessary to improve the scalability and usability of this system for broader applications. Overall, this research highlights the potential of blockchain technology as a transformative solution for electronic certificate management, making a valuable contribution to both the literature and practical applications in this field.

#### CONFLICT OF INTEREST

The authors declare no conflict of interest.

#### REFERENCES

- Alam, S., Zardari, S., & Shamsi, J. A. (2022). Blockchain-based trust and reputation management in sIoT. *Electronics* 2022, Vol. 11, Page 3871, 11(23), 3871. <https://doi.org/10.3390/ELECTRONICS11233871>
- Chen, G., Xu, B., Lu, M., & Chen, N.-S. (2018). Exploring blockchain technology and its potential applications for education. *Smart Learning Environments* 2018 5:1, 5(1), 1–10. <https://doi.org/10.1186/S40561-017-0050-X>
- Curty, S., Härer, F., & Fill, H. G. (2023). Design of blockchain-based applications using model-driven engineering and low-code/no-code platforms: a structured literature review. *Software and Systems Modeling* 2023 22:6, 22(6), 1857–1895. <https://doi.org/10.1007/S10270-023-01109-1>
- Djajadi, A., Lestari, K. S., Englista, L. E., & Destaryana, A. (2023). Blockchain-based e-certificate verification and validation automation architecture to avoid counterfeiting of digital assets in order to accelerate digital transformation. *CCIT (Creative Communication and Innovative Technology) Journal*, 16(1), 68–85. <https://doi.org/10.33050/CCIT.V16I1.2367>
- Dzakiy, M. I. (2019). *Pemanfaatan smart contract dalam blockchain untuk mengoptimasi e-commerce*.
- Dzhalila, D., Siahaan, D., Fauzan, R., Asyrofi, R., & Karimi, M. I. (2023). A Systematic literature review on blockchain technology in software engineering. *Jurnal ELTIKOM: Jurnal Teknik Elektro, Teknologi Informasi Dan Komputer*, 7(1), 38–49. <https://doi.org/10.31961/ELTIKOM.V7I1.725>
- ER, M. (2018). *Business process management: konsep dan implementasi*. Andi Publisher.
- Guo, Y., & Liang, C. (2016). Blockchain application and outlook in the banking industry. *Financial Innovation*, 2(1), 1–12. <https://doi.org/10.1186/S40854-016-0034-9/TABLES/3>

- Kuo, T.-T., Kim, H.-E., & Ohno-Machado, L. (2017). Blockchain distributed ledger technologies for biomedical and health care applications. *Journal of the American Medical Informatics Association*, 24(6), 1211–1220. <https://doi.org/10.1093/JAMIA/OCX068>
- Kurniawan, A., Wulandari, W. A., Saragih, R. E., & Verdian, I. (2019). A Review of blockchain: how does it work, applications, and challenges. *Journal of Telematics and Informatics*, 7(2), 69–79. <https://doi.org/10.12928/JTI.V7I2>
- Martono, R. V. (2020). *Supply chain 4.0 berbasis blockchain dan platform*. PT Gramedia Pustaka Utama.
- Mendling, J., Weber, I., Van Der Aalst, W., Brocke, J. Vom, Cabanillas, C., Daniel, F., Debois, S., Di Ciccio, C., Dumas, M., Dustdar, S., Gal, A., García-Bañuelos, L., Governatori, G., Hull, R., La Rosa, M., Leopold, H., Leymann, F., Recker, J., Reichert, M., ... Zhu, L. (2018). Blockchains for business process management - challenges and opportunities. *ACM Transactions on Management Information Systems (TMIS)*, 9(1). <https://doi.org/10.1145/3183367>
- Noor, M. U. (2020). Implementasi blockchain di dunia kearsipan: peluang, tantangan, solusi atau masalah baru? *Khazanah Al-Hikmah: Jurnal Ilmu Perpustakaan, Informasi, Dan Kearsipan*, 8(1), 81. <https://doi.org/10.24252/kah.v8i1a9>
- Nugraha, A. C. (2022). Penerapan teknologi blockchain dalam lingkungan pendidikan. *Produktif: Jurnal Ilmiah Pendidikan Teknologi Informasi*, 4(1), 302–307. <https://doi.org/10.35568/produktif.v4i1.386>
- Rahmadika, S., Ramdania, D. R., & Harika, M. (2018). Security analysis on the decentralized energy trading system using blockchain technology. *Jurnal Online Informatika*, 3(1), 44–47. <https://doi.org/10.15575/JOIN.V3I1.207>
- Sugiharto, A., & Musa, M. Y. (2020). *Blockchain and cryptocurrency dalam perspektif hukum di indonesia dan dunia* (1st ed.). Perkumpulan Kajian Hukum Terdesentralisasi.
- Wang, Y., Han, J. H., & Beynon-Davies, P. (2019). Understanding blockchain technology for future supply chains: a systematic literature review and research agenda. *Supply Chain Management*, 24(1), 62–84. <https://doi.org/10.1108/SCM-03-2018-0148/FULL/XML>
- Weber, I., Xu, X., Riveret, R., Governatori, G., Ponomarev, A., & Mendling, J. (2016). Untrusted business process monitoring and execution using blockchain. *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, 9850 LNCS, 329–347. [https://doi.org/10.1007/978-3-319-45348-4\\_19](https://doi.org/10.1007/978-3-319-45348-4_19)
- Wibowo, D. F. H. S. (2019). *Perancangan dan implementasi teknologi blockchain pada sistem pencatatan hasil rekapitulasi pemilu berdasarkan formulir c1 pindaian kpu* [Thesis]. Institut Teknologi Bandung.
- Wijaya, D. A. (2016). *Mengenal bitcoin dan cryptocurrency* (1st ed.). Puspantara.
- Zhu, X. (2019). Application of blockchain technology in energy internet market and transaction. *IOP Conference Series: Materials Science and Engineering*, 592(1), 012159. <https://doi.org/10.1088/1757-899X/592/1/012159>
- Zhu, X., & Wang, D. (2019a). Application of blockchain in document certification, asset trading and payment reconciliation. *Journal of Physics: Conference Series*, 1187(5), 052080. <https://doi.org/10.1088/1742-6596/1187/5/052080>
- Zhu, X., & Wang, D. (2019b). Research on blockchain application for e-commerce, finance and energy. *IOP Conference Series: Earth and Environmental Science*, 252(4), 042126. <https://doi.org/10.1088/1755-1315/252/4/042126>