elviraselvimagdalena@gmail.com elviraselvimagda...

Draft Jurnal Sahri Ramadan_English

class umk

Document Details

Submission ID
trn:oid:::31238:126433997

Submission Date
Jan 18, 2026, 7:37 PM GMT+7

Download Date
Jan 18, 2026, 7:42 PM GMT+7

File Name
Draft Jurnal Sahri Ramadan_ENglish - Copy.docx

File Size
638.3 KB

9 Pages

5,348 Words

32,990 Characters

16% Overall Similarity

The combined total of all matches, including overlapping sources, for each database.

Match Groups

57 Not Cited or Quoted 14%
Matches with neither in-text citation nor quotation marks

3 Missing Quotations 1%
Matches that are still very similar to source material

5 Missing Citation 1%
Matches that have quotation marks, but no in-text citation

1 Cited and Quoted 0%
Matches with in-text citation present, but no quotation marks

Top Sources

11% Internet sources
5% Publications
13% Submitted works (Student Papers)

Match Groups

- **57** Not Cited or Quoted 14%
  Matches with neither in-text citation nor quotation marks
- **3** Missing Quotations 1%
  Matches that are still very similar to source material
- **5** Missing Citation 1%
  Matches that have quotation marks, but no in-text citation
- **1** Cited and Quoted 0%
  Matches with in-text citation present, but no quotation marks

Top Sources

- 11% Internet sources
- 5% Publications
- 13% Submitted works (Student Papers)

Top Sources

The sources with the highest number of matches within the submission. Overlapping sources will not be displayed.

1	Student papers	
Universitas Khairun on 2024-04-18		1%
2	Internet	
shift.sin.fst.uin-alauddin.ac.id		1%
3	Student papers	
IUBH - Internationale Hochschule Bad Honnef-Bonn on 2025-07-28		<1%
4	Student papers	
Universitas Prima Indonesia on 2025-06-14		<1%
5	Student papers	
Asia Pacific Instutute of Information Technology on 2022-10-16		<1%
6	Internet	
ejournal.raharja.ac.id		<1%
7	Student papers	
The Scientific & Technological Research Council of Turkey (TUBITAK) on 2025-12-05		<1%
8	Internet	
www.ijiet.org		<1%
9	Internet	
www.ijraset.com		<1%
10	Internet	
iieta.org		<1%

11	Student papers	
CSU, San Jose State University on 2022-12-03		<1%
12	Internet	
jurnal.radenfatah.ac.id		<1%
13	Internet	
journal.poltekad.ac.id		<1%
14	Internet	
ejournal.unuja.ac.id		<1%
15	Internet	
ojs.unpkediri.ac.id		<1%
16	Student papers	
University of Adelaide on 2025-09-15		<1%
17	Internet	
ejournal.unkhair.ac.id		<1%
18	Publication	
Andreanata Pradifta Muksin, Budi Tjahjono. "IoT-Based Remote Electricity Contro...		<1%
19	Student papers	
Universitas Sultan Ageng Tirtayasa on 2025-07-13		<1%
20	Internet	
rsisinternational.org		<1%
21	Internet	
scholar.archive.org		<1%
22	Internet	
udinharun.lecturer.pens.ac.id		<1%
23	Student papers	
Asia Pacific University College of Technology and Innovation (UCTI) on 2023-05-12		<1%
24	Publication	
Bharat Bhushan, Nitin Rakesh, Yousef Farhaoui, Parma Nand Astya, Bhuvan Unh...		<1%

25 Student papers
Al Akhawayn University in Ifrane on 2024-10-11 <1%

26 Student papers
Universitas Negeri Medan on 2025-10-06 <1%

27 Internet
dokumen.pub <1%

28 Internet
joiv.org <1%

29 Student papers
Signal Mountain Middle High School on 2024-09-17 <1%

30 Student papers
Al Akhawayn University in Ifrane on 2024-12-05 <1%

31 Student papers
UC, Boulder on 2025-03-11 <1%

32 Internet
timur.ilearning.me <1%

33 Student papers
APJ Abdul Kalam Technological University, Thiruvananthapuram on 2025-02-19 <1%

34 Publication
Agariadne Dwinggo Samala, Soha Rawas, Zamzami Zainuddin, Natalie-Jane Howa... <1%

35 Student papers
Birla Institute of Technology and Science Pilani on 2019-04-18 <1%

36 Student papers
City University of Hong Kong on 2022-04-10 <1%

37 Student papers
IUBH - Internationale Hochschule Bad Honnef-Bonn on 2025-12-30 <1%

38 Publication
Rafah Amer Jaafar, Saad Najim Alsaad. "Enhancing Educational Certificate Verific... <1%

39 Internet

arxiv.org <1%

40 Internet

ntnuopen.ntnu.no <1%

41 Student papers

Asia Pacific University College of Technology and Innovation (UCTI) on 2020-03-02 <1%

42 Student papers

Universitas Amikom on 2023-07-21 <1%

43 Student papers

Zambia Centre for Accountancy Studies on 2024-12-13 <1%

44 Student papers

Xiamen University on 2022-07-25 <1%

JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK, No.0173/C3/DT.05.00/2025
Vol. x, No. x, April 2025, pp. x-x p-ISSN: 2614-8897
DOI: 10.33387/jiko e-ISSN: 2656-1948

IMPLEMENTATION OF BLOCKCHAIN IN A SEMINAR SYSTEM FOR ELECTRONIC CERTIFICATE VERIFICATION USING SMART CONTRACTS

Sahri Ramadan[1*], Sawali Wahyu[2]

[1, 2] Faculty of Computer Science, Universitas Esa Unggul, Bekasi
Email: [*1] sahriramadan000@student.esaunggul.ac.id, [2]sawaliwahyu@esaunggul.ac.id

(Received: dd mmm yyyy, Revised: dd mmm yyyy, Accepted: dd mmm yyyy)

Abstract

The increasing adoption of electronic certificates in academic and professional environments introduces new challenges related to document authenticity, data integrity, and the long-term feasibility of the verification process. Conventional certificate management systems generally rely on centralized databases and manual validation procedures, which are vulnerable to manipulation, duplication, and system failures due to dependence on a single authority. These conditions reduce trust in digital credentials and complicate independent verification by third parties. To address these issues, this study proposes and implements a blockchain-based electronic certificate verification mechanism using smart contracts on a private Hyperledger Fabric network. The system is designed not to store certificate files directly; instead, it records cryptographic hash values as unique representations of each document, thereby ensuring data integrity while maintaining storage efficiency. Smart contracts are employed to automate the processes of recording, validating, and retrieving certificate data in a transparent and tamper-resistant manner. The verification process is performed by recalculating the hash value of the submitted certificate and comparing it with the hash value stored on the blockchain. Matching hash values indicate that the certificate is valid, whereas discrepancies signify document alteration or invalidity. Experimental results demonstrate that this approach effectively preserves certificate integrity and is capable of detecting even the slightest modifications to the files. Therefore, the proposed blockchain-based verification system using smart contracts can serve as a secure, transparent, and reliable solution for validating electronic certificates in mobile-based academic systems.

Keywords: Blockchain, Electronic Certificates, Smart Contracts, Hyperledger Fabric, Hash-Based Verification, Data Integrity

**Corresponding Author:* *Sahri Ramadan*

1. INTRODUCTION

Digital transformation in academic services has driven the increasing use of electronic certificates in various activities, such as seminars, training programs, and competency development initiatives. Compared to physical documents, digital certificates offer greater convenience in terms of distribution, storage, and accessibility. However, these advantages also introduce new challenges, particularly regarding document authenticity, data integrity, and long-term verification mechanisms. Most current certificate management systems still rely on centralized databases and manual validation procedures, making them vulnerable to unauthorized modifications, duplication, and administrative errors. Dependence on a single authority also creates a single point of failure and reduces the transparency of the authentication process [1], [2].

In recent years, blockchain technology has been widely adopted as a solution to address these limitations. The distributed and immutable characteristics of blockchain enable data to be recorded permanently and make it difficult to manipulate, making it suitable for applications that require a high level of trust [3]. Several studies have reported that the application of blockchain in digital certification systems can enhance data integrity and information traceability [4], [5]. Furthermore, the integration of automation mechanisms through smart contracts has been shown to simplify the validation process and reduce reliance on manual inspections [6]. On the other hand, the use of QR codes also

contributes to faster access to verification services and improves user convenience [7].

Nevertheless, most existing approaches still position blockchain as a passive recording medium rather than as an active validation mechanism that is directly integrated into the system workflow. Centralized architectures continue to dominate e-certificate implementations, causing external parties who wish to verify document authenticity to directly contact the issuing institution. This procedure is often inefficient, time-consuming, and prone to human error [8], [9]. Several studies also indicate that conventional systems lack built-in mechanisms to automatically detect data modifications, making document tampering difficult to identify without extensive manual inspection [10].

Blockchain offers a different paradigm through its distributed, transparent, and tamper-resistant recording mechanism. In the context of certificate verification, blockchain can function as a single source of truth that permanently stores verification information and allows it to be audited at any time [11]. To maintain storage efficiency, the system does not need to store the entire certificate file on the ledger. Instead, cryptographic hash values can be used as unique representations of each document. Hash values are highly sensitive to data changes; therefore, even minor modifications to a certificate will result in significantly different hash values that can be automatically detected [12], [13].

The role of blockchain is further strengthened through the use of smart contracts, which enable validation rules to be executed automatically, consistently, and transparently without relying on third parties. With this mechanism, the processes of certificate recording and verification no longer depend on centralized authorities but are instead governed by predefined logic [6], [14]. Recent studies also suggest that permissioned networks such as Hyperledger Fabric are more suitable for academic environments, as they support access control, authorization policies, and more manageable audit mechanisms [11], [15].

Based on these issues, this study proposes a blockchain-based electronic certificate validation system integrated into a mobile application environment. The system utilizes a private Hyperledger Fabric network as its core infrastructure, while smart contracts are employed to manage the recording and verification processes automatically. Instead of storing the entire certificate file, the system records only cryptographic hash values on the blockchain ledger. The verification process is conducted through QR code scanning, enabling users to independently, quickly, and objectively verify certificate authenticity.

The main contribution of this study lies in the implementation of blockchain as an active validation mechanism rather than merely as a digital archive. Unlike previous approaches that are mostly conceptual or limited to web-based platforms, the proposed system integrates the verification process end-to-end into the workflow of a mobile application. With this design, the system is able to automatically detect data modifications, enhance transparency, and reduce dependence on centralized authorities. These findings are expected to serve as a reference for the development of digital certification systems that are more secure, reliable, and adaptive to the needs of modern academic environments [5], [11], [16].

2. RESEARCH METHOD

This study adopts a system engineering approach that focuses on the design, implementation, and evaluation of a blockchain-based electronic certificate validation system within a mobile application context. This approach was selected because the primary objective of the research is not only to analyze a phenomenon but also to develop a system that can be practically utilized to address digital document authentication issues. In line with several previous studies, the system engineering approach is considered appropriate for developing blockchain-based solutions that require the integration of software architecture, security mechanisms, and user interaction workflows [11], [15].

In this research, blockchain is not positioned merely as a passive storage medium but as an active component that determines certificate authenticity through data recorded on a distributed ledger. This approach aligns with the concept of a single source of truth, which is widely applied in digital credential verification systems, where validity decisions no longer rely on centralized databases [11], [12].

2.1 System Architecture

The system is developed using a private blockchain network based on Hyperledger Fabric, which belongs to the category of permissioned blockchains. This model enables identity management, access control configuration, and the enforcement of authorization policies in a controlled manner, making it more suitable for academic environments that require institutional oversight and clear audit mechanisms [11], [15]. Unlike public blockchains, this approach provides greater flexibility in defining the roles of each entity, such as administrators, organizers, and students, without compromising the principles of transparency and data integrity.

In addition, Hyperledger Fabric supports the modular implementation of smart contracts, allowing the rules for certificate recording, issuance, and verification to be explicitly defined in the form of programmed logic. This mechanism ensures that every transaction follows predefined procedures and is executed automatically, thereby reducing reliance on manual processes and minimizing the potential for human error.

JIKO (Jurnal Informatika dan Komputer) Accredited KEMDIKTISAINTEK, No.0173/C3/DT.05.00/2025
Vol. x, No. x, April 2025, pp. x-x p-ISSN: 2614-8897
DOI: 10.33387/jiko e-ISSN: 2656-1948

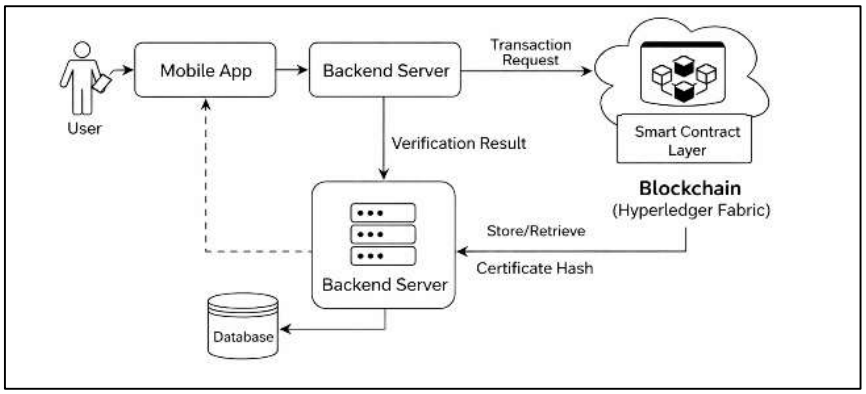

Figure 1. Blockchain-Based Certificate Validation System Architecture

As illustrated in Figure 1, the system architecture is designed into three main layers: the mobile application, the backend server, and the blockchain network. This layered approach aims to maintain system modularity, facilitate development, and enhance scalability without disrupting other existing components [4]. Furthermore, the separation of functions across layers also contributes to improved security, as each component has clearly defined responsibilities.

The mobile application serves as the user interface, enabling students and external parties to access digital certificates and initiate the verification process. At this layer, users interact only with informational data and do not have direct access to the recording mechanisms on the blockchain. The backend server is responsible for managing application logic, including processing user requests, retrieving certificate metadata, and forwarding validation requests to the blockchain network.

Meanwhile, the blockchain network acts as the primary validation layer that permanently and immutably stores certificate hash values. Through this mechanism, the system does not store the entire certificate document on the blockchain; instead, it records only its cryptographic representation, ensuring storage efficiency without compromising security.

With this separation, conventional databases are used solely to store operational data, such as user information and certificate metadata, and do not play a role in determining document authenticity. The validity status is entirely determined based on data recorded on the blockchain, thereby reducing the risk of manipulation, enhancing transparency, and avoiding dependence on a single centralized authority [3], [11]. This approach positions blockchain as the single source of truth in the digital certificate verification process.

2.2 Certificate Recording Mechanism

The certificate recording mechanism in this system is performed by generating a cryptographic hash value for each issued certificate document. The hash value serves as a unique representation of the document's content, such that even the slightest modification to the certificate will result in a significantly different hash value. With this characteristic, the hash can be used as an indicator of document authenticity without the need to store the entire file on the blockchain. This approach is commonly adopted in blockchain-based verification systems because it is more storage-efficient while still preserving data integrity [12], [13].

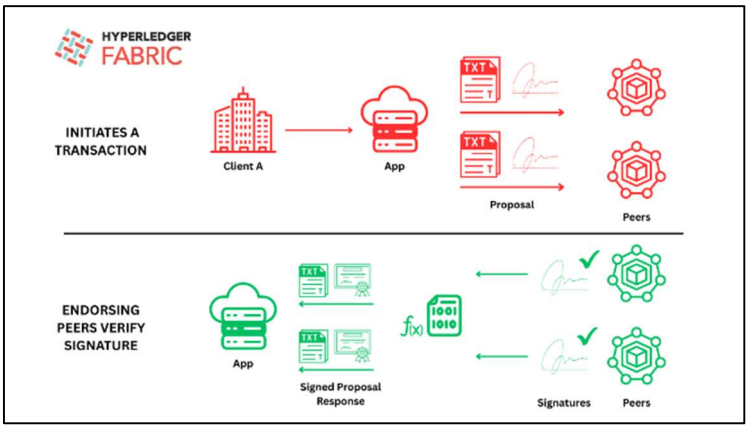

Figure 2. Proposal Submission and Endorsement Process in Hyperledger Fabric

As illustrated in Figure 2, once the hash value is generated, the data is submitted as a transaction proposal to the Hyperledger Fabric network. This proposal is then verified by multiple endorsing peers according to the rules defined in the smart contract. Each peer examines whether the transaction complies with the applicable policies, ensuring that only transactions that meet the validation criteria can proceed further. This mechanism enables a distributed verification process without relying on a single entity [15] .

If the endorsement policy is satisfied, the transaction is forwarded to the ordering service to be assembled into a block before being permanently recorded on the ledger. This stage ensures that the transaction order remains consistent across all network nodes and prevents data conflicts. Through this process, the recorded data cannot be modified or deleted, thereby fulfilling the immutability property that characterizes blockchain technology [11], [4].

Furthermore, each successfully recorded transaction generates a unique transaction ID that can be used as an audit trail. This identifier enables transparent and verifiable tracking of certificate history by both institutions and external parties, thereby enhancing the overall accountability of the system [11].

2.3 Certificate Verification Process

The certificate verification process is designed to be independently performed by users through scanning the QR code embedded in the digital document. The QR code serves as an initial identifier that directs the system to retrieve the corresponding certificate hash data stored on the blockchain network. This approach enables the authentication process to be conducted quickly without requiring direct interaction with the issuing institution. In addition to improving efficiency, this mechanism also enhances user convenience by allowing access to verification services whenever needed [7].

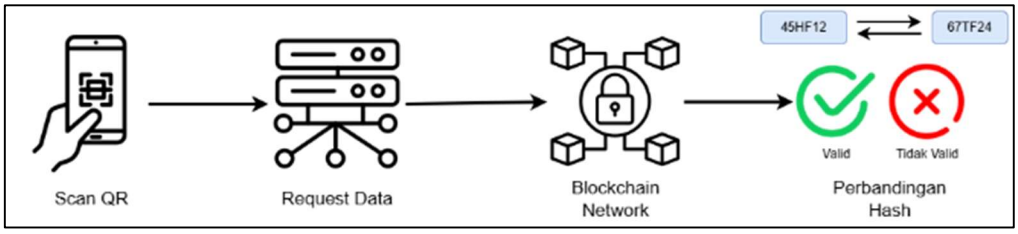

Figure 3. Blockchain-Based Certificate Verification Workflow

As illustrated in Figure 3, once the hash data is retrieved from the blockchain, the system recalculates the hash value of the certificate document submitted by the user. This newly generated hash value is then compared with the hash value stored on the ledger. This comparison serves as the primary basis for determining the authenticity of the document. If both hash values are identical, the certificate is declared valid. Conversely, any discrepancy indicates that the document has been altered or does not match the recorded data, and is therefore considered invalid.

This mechanism positions the blockchain as the single source of truth in the validation process, rather than a centralized database [3], [11]. Consequently, the verification process does not rely on claims from specific parties but on data that has been permanently and distributively recorded. This enhances the objectivity of the validation process and reduces the potential for data manipulation.

The use of hash values as document representations ensures data integrity, as the highly sensitive nature of cryptographic hashes enables

automatic detection of any modifications [12], [13]. With this approach, the system not only verifies certificate authenticity but also provides early warnings of even the slightest changes to the document content, without requiring subjective manual inspection.

2.4 Scope of System Testing

System testing is focused on the reliability of the blockchain-based validation mechanism rather than on interface aesthetics or user experience aspects. This focus was chosen because the primary objective of this research is to evaluate the system's capability to preserve data integrity and to determine certificate authenticity objectively. Accordingly, the testing is directed toward the core functionalities of the system, namely the processes of data recording, storage, and verification within the blockchain network. A similar approach has been adopted in several previous studies that emphasize evaluation on security, data consistency, and the reliability of verification mechanisms [5], [11].

All testing scenarios are used to assess the extent to which the system can maintain the tamper-resistant and fault-tolerant properties that constitute the main advantages of blockchain technology [15]. The system is expected to continue producing accurate verification results even in the presence of data modifications or disruptions in one of the network components.

The results of each testing scenario are subsequently analyzed to evaluate the effectiveness of blockchain as an active validation system in the context of digital certificates. With this approach, the evaluation not only focuses on the technical functionality of the system but also on its resilience to data manipulation, the consistency of validation results, and its ability to maintain user trust in document authenticity.

3. RESULTS AND DISCUSSION

This section presents the results of the implementation of the proposed blockchain-based certificate validation system, along with a discussion of its reliability, security, and overall effectiveness. The evaluation focuses on the system's ability to preserve data integrity, automatically detect document modifications, and provide an objective verification process that does not depend on a centralized authority. These aspects are critical, as digital certification systems require a high level of trust from both issuing institutions and end users. A similar approach has been adopted in several previous studies that emphasize the role of blockchain as a fundamental foundation for authentication and verification systems in digital credentials [11], [12].

The results obtained from the system implementation and testing are analyzed to examine the extent to which blockchain technology can fulfill these requirements within an academic environment. The discussion not only highlights the functional performance of the system but also explains how the proposed mechanism enhances transparency, reduces the risk of data manipulation, and strengthens trust in the authenticity of digital certificates.

3. 1 Implementation of the Blockchain-Based Certificate Validation System

The implementation results demonstrate that blockchain can function as an active validation mechanism in the digital certificate verification process, rather than merely serving as a storage medium. Unlike conventional approaches that rely on centralized databases or manual inspection, this system positions blockchain as the primary source of truth (single source of truth) in determining document authenticity. With this approach, the validity status of a certificate is not determined by a single entity, but by data that has been permanently and distributively recorded within the network. This concept aligns with distributed verification approaches that have been widely proposed in the development of modern digital credential systems [11].

In the developed system, the blockchain does not store certificate files directly; instead, it records only cryptographic hash values as unique representations of each document. This strategy is adopted to maintain storage efficiency without compromising security. Even the slightest modification to the document content will produce a significantly different hash value, enabling automatic detection of manipulation during the verification process [12], [13]. Accordingly, this mechanism not only functions as an authentication tool but also as a real-time data change detection system.

The integration of the mobile application, backend server, and blockchain network allows the validation process to be performed directly by users without the need to contact the issuing institution. Users simply scan the QR code embedded in the certificate to initiate the verification process, which is then followed by retrieving the corresponding hash data from the blockchain and comparing it with the hash value of the submitted document. This mechanism makes the verification process more objective, faster, and more transparent, while also reducing the potential for administrative errors that commonly occur in conventional systems [4], [11].

Furthermore, this approach has a positive impact on users' trust in the verification results. Since the validation data is derived from an immutable ledger, users can be assured that the displayed information cannot be altered unilaterally. This strengthens the role of blockchain not only as a storage infrastructure but also as a core component in the decision-making process regarding the authenticity of digital certificates.

3. 2 Results of the Certificate Recording Mechanism Implementation

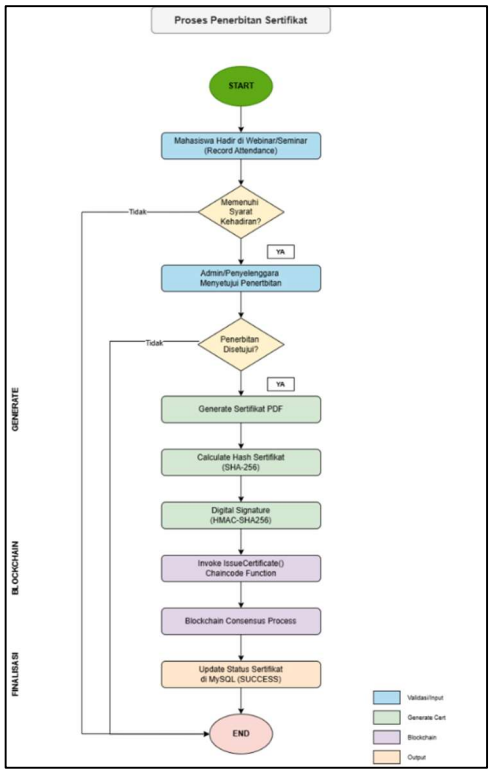

Figure 4. Certificate Recording Mechanism Based on Hyperledger Fabric

As illustrated in Figure 4, the certificate recording mechanism begins with the process of recording students' attendance at webinar or seminar activities. This attendance data is then verified based on predefined criteria, such as the fulfillment of participation requirements. If the requirements are not met, the certificate issuance process is not continued. Conversely, if the attendance criteria are satisfied, the administrator or organizer approves the certificate issuance.

After approval is granted, the system automatically generates the certificate in PDF format. At this stage, the generated document is not directly stored on the blockchain; instead, it is first processed to produce a cryptographic hash value using the SHA-256 algorithm. This hash value serves as a unique representation of the document's content, such that even the slightest modification to the certificate will result in a different hash value. Furthermore, the system adds an additional security layer through a digital signature mechanism based on HMAC-SHA256 before the data is transmitted to the blockchain network.

The recording process on the blockchain is carried out by invoking the issueCertificate() function on the smart contract. The submitted transaction then undergoes a consensus phase, during which multiple nodes validate the transaction according to the predefined endorsement policy. This stage ensures that only data complying with the system rules can be permanently recorded. This mechanism reflects the principle of distributed validation, which is a core characteristic of Hyperledger Fabric [15].

Once the transaction is successfully approved, the certificate hash data is permanently recorded on the ledger. The recording status is subsequently updated in the operational database (MySQL) as an indication that the issuance process has been completed. With this workflow, blockchain does not merely function as a storage medium but as an active component that determines the validity of the certificate recording process.

The immutability property of blockchain guarantees that recorded data cannot be modified or deleted. This aspect is particularly important in the context of digital certification, as post-issuance data modification may reduce trust in the document. In addition, each transaction generates a unique transaction ID that serves as an audit trail, enabling the entire recording history to be transparently and verifiably traced [11].

These findings confirm that the implemented recording mechanism is not merely administrative but also functions as an active validation system. This approach differs from conventional systems, which typically perform passive recording without a distributed validation mechanism [3], [4].

3. 3 Results of the Blockchain-Based Certificate Verification Process Implementation

Figure 5. Blockchain-Based Certificate Verification Workflow

As illustrated in Figure 5, the verification process is designed to be independently performed by users through scanning the QR code embedded in the certificate. The QR code serves as an entry point that triggers a data request to the system, which is then forwarded to the backend to retrieve the corresponding certificate hash value from the blockchain network. This approach allows users to perform verification

without relying on the issuing institution, thereby increasing flexibility and user convenience [7].

After the hash value is retrieved from the blockchain, the system recalculates the hash value of the certificate document submitted by the user. These two hash values are then compared to determine the authenticity status of the document. If the hash values are identical, the certificate is declared valid. Conversely, any discrepancy indicates that the document has been altered or does not match the recorded data. With this mechanism, the validity decision is entirely determined by the data stored on the blockchain ledger, rather than by a centralized database [11].

The use of hash values as document representations ensures data integrity, as the highly sensitive nature of cryptographic hashes enables the system to automatically detect any form of manipulation [12], [13]. This approach is consistent with previous studies that emphasize the importance of hash-based verification as a tamper-detection mechanism in digital credential systems [14]. Accordingly, the verification process is not merely declarative but is based on objective cryptographic proof.

Figure 6. Certificate Verification Result Interface in the Mobile Application

Figure 6 presents the final outcome of the verification process in the form of a mobile application interface. The validation status is displayed directly to users as either valid or invalid, based on the result of the hash comparison between the submitted document and the data stored on the blockchain ledger. This information is presented in a concise and user-friendly manner, without exposing the underlying technical details of the process.

At this stage, the mobile application functions solely as a presentation layer and does not determine certificate authenticity. All validity decisions are derived from the hash comparison results obtained from the blockchain. This approach ensures that the verification outcome cannot be manipulated through either the client side or a centralized server.

These findings further reinforce the role of blockchain as the primary validation layer in digital certification systems, rather than merely as a storage medium [11], [12]. By positioning blockchain as the main source of truth, the system is able to provide a verification process that is transparent, objective, and auditable.

3. 4 Results of the Blockchain-Based Validation System Testing

System testing was conducted to evaluate the reliability of the blockchain-based certificate validation mechanism in detecting data modifications and maintaining information consistency. The testing focus was directed toward scenarios that represent real-world conditions, such as the verification of authentic certificates, modified certificates, and QR codes that are not registered in the system. In addition, tests were also performed by retrieving data from different nodes to assess the consistency of validation results in a distributed network:

Table 1. Results of the Blockchain-Based Certificate Validation System Testing

No.	Test Scenario	Expected Result	Actual Result
1	Authentic certificate	Valid	Valid
2	Modified certificate	Invalid	Invalid
3	Unregistered QR code	Invalid	Invalid
4	Data retrieval from different nodes	Consistent	Consistent

Based on Table 1, the test results indicate that the system is able to accurately and consistently classify the certificate status across all evaluated scenarios. Authentic certificates were correctly recognized as valid documents, whereas modified certificates were automatically detected as invalid. This outcome occurs because any alteration to the document results in a different hash value compared to the one stored on the blockchain ledger.

Furthermore, the scenario involving unregistered QR codes was also handled effectively by the system, where verification requests were rejected due to the absence of matching records on the blockchain. This finding demonstrates that the system is not only capable of verifying document authenticity but also effective in preventing access to data that does not have a legitimate recording history.

The data retrieval tests from different nodes produced consistent outputs, confirming the data replication property of the distributed network. This characteristic represents one of the main advantages of blockchain technology, as it allows the system to remain reliable even when one of the nodes experiences disruption [15]. Consequently, the validation mechanism does not rely on a single point of failure.

Overall, the testing results indicate that blockchain in this system does not merely function as a recording medium, but also as an active component that directly contributes to maintaining the reliability, consistency, and objectivity of the digital certificate validation process.

3. 5 Discussion

The implementation and testing results indicate that blockchain can function as an active validation system rather than merely serving as a digital archive. By positioning the ledger as the primary source of truth, the system is able to determine certificate authenticity objectively without relying on centralized databases or manual inspection. This approach is consistent with the findings of several studies that emphasize the role of blockchain in enhancing trust and transparency in digital certification systems [11], [12].

Compared to conventional systems, the blockchain-based validation mechanism offers several key advantages. First, the use of hash values enables automatic detection of data modifications. Second, recording data on a distributed ledger reduces dependence on a single authority, thereby making the verification process more transparent and auditable. Third, the integration of QR codes simplifies the authentication process from the user's perspective [7].

Nevertheless, the proposed system also has certain limitations. Blockchain implementation requires a relatively more complex infrastructure compared to centralized systems. In addition, system performance is highly influenced by network configuration and endorsement policies. Therefore, the deployment of this system should be tailored to the scale and specific needs of the institution.

Overall, the combination of blockchain, smart contracts, and hash-based verification mechanisms forms a certificate validation system that is reliable, transparent, and resistant to manipulation. These findings are not only conceptually relevant but also practically applicable in modern academic environments.

4. CONCLUSION

This study successfully designed, implemented, and evaluated a blockchain-based electronic certificate validation system integrated with a mobile application. The developed system utilizes a private Hyperledger Fabric network and smart contracts as the core mechanisms for the automated and distributed recording and verification of certificates. This approach was designed to address the limitations of conventional systems that still rely on centralized databases and manual inspections, which are vulnerable to data manipulation and administrative errors.

By recording cryptographic hash values as unique representations of each document, the system is able to preserve data integrity without storing the entire certificate file on the blockchain ledger. This strategy has proven to be storage-efficient while maintaining accurate change detection capabilities. Even the slightest modification to the document content results in a different hash value, allowing manipulation to be automatically detected during the verification process.

The implementation and testing results indicate that the system is able to consistently distinguish between valid and invalid certificates across various testing scenarios. Authentic certificates were correctly identified as valid, whereas modified certificates and unregistered QR codes were automatically classified as invalid. In addition, data retrieval from different blockchain nodes produced consistent outputs, confirming the data replication characteristics of the distributed network. These findings demonstrate that the system not only functions correctly from a functional perspective but also exhibits a high level of reliability in a distributed environment.

The integration of QR codes into digital certificates enables users to independently, quickly, and objectively perform the verification process without having to contact the issuing institution. In this context, the mobile application serves only as a presentation layer, while the validity decision is entirely determined by the data stored on the blockchain ledger. This approach reinforces the principle that blockchain acts as the single source of truth within the system, rather than merely as a storage medium.

Overall, the findings of this study confirm that blockchain is not only relevant as a distributed recording technology but can also function as an active validation mechanism in digital certification systems. By positioning the ledger as the central authority for determining document authenticity, the system enhances transparency, reduces dependence on centralized authorities, and strengthens trust in the issued digital credentials.

Nevertheless, the developed system still has several limitations. The complexity of blockchain infrastructure, the relatively high network configuration requirements, and the limited scale of user testing remain challenges that need to be addressed. Therefore, future research may focus on system performance optimization, large-scale deployment testing, and the exploration of integration with digital identity systems and international credential standards.

With further development, this approach has the potential to become a reliable, secure, and sustainable solution for the management and verification of digital certificates in both academic and professional environments.

Acknowledgment

The authors would like to express their sincere gratitude to the Faculty of Computer Science, Universitas Esa Unggul, for the academic support and facilities provided throughout the course of this

research. Appreciation is also extended to the academic supervisors and colleagues who offered constructive feedback during both the system design phase and the manuscript refinement process. Their contributions were invaluable in ensuring that this study was completed systematically and in accordance with scientific writing standards.

5. REFERENCE

[1] C. Gayathri, M. Rani, P. Sai Kumar, M. D. Mushaarof, B. Tech, and T. S. Reddy, "Decentralized Certificate Authentication with Blockchain Technology," 2025. [Online]. Available: www.ijerst.com

[2] D. Setiowati *et al.*, "A Blockchain System for Digital Sertificate Verification On E-Learning," *Kumpulan jurnaL Ilmu Komputer (KLIK)*, vol. 08, no. 3, 2021.

[3] N. and Y. Xu, "Development of Blockchain-Based Academic Credential Verification System," *OAlib*, vol. 11, no. 09, pp. 1–20, 2024, doi: 10.4236/oalib.1112130.

[4] A. Djajadi, K. S. Lestari, L. E. Englista, and A. Destaryana, "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*, vol. 16, no. 1, 2023.

[5] H. Wijayanto and P. M. Waliyullah, "Aplikasi Verifikasi Sertifikat Berbasis Website Menggunakan Blockchain," *Jurnal InFact Sains dan Komputer*, vol. 8, no. 02, pp. 35–42, Aug. 2024, doi: 10.61179/jurnalinfact.v8i02.586.

[6] A. R. Febriansyah, Nazulasari, and N. Ramadhona, "OPTIMALISASI SMART CONTRACT UNTUK SISTEM SERTIFIKASI DIGITAL PADA PUBLIC BLOCKHAIN," 2024.

[7] N. K. Noorhizam, Z. Abdullah, S. Kasim, I. Rahmi, A. Hamid, and M. Anuar, "INTERNATIONAL JOURNAL ON INFORMATICS VISUALIZATION Verification of Ph.D. Certificate Using QR Code on Blockchain Ethereum," 2023. [Online]. Available: www.joiv.org/index.php/joiv

[8] L. Van Tan and P. M. Hung, "Driving Digital Transformation in Certificate Management: A Blockchain-Based Solution for Vinh University," *International Journal of Information and Education Technology*, vol. 14, no. 1, pp. 119–124, 2024, doi: 10.18178/ijiet.2024.14.1.2031.

[9] M. R. Hidayat, D. Gusman, and H. Adeswastoto, "Portal E-Sertifikat dengan QR Code Menggunakan PHP dan MYSQL," *Jurnal Pengabdian Masyarakat dan Riset Pendidikan*, vol. 1, no. 1, pp. 13–26, Sep. 2022, doi: 10.31004/JERKIN.V1I1.1.

[10] A. Bhise, C. Pardeshi, M. Vajale, P. Bhongale, S. Shirke, and M. Jagtap, "Blockchain Based Certificate Validation System," 2025. [Online]. Available: www.ijfmr.com

[11] R. A. Jaafar and S. N. Alsaad, "Enhancing Educational Certificate Verification With Blockchain and IPFS: A Decentralized Approach Using Hyperledger Fabric," *TEM Journal*, vol. 12, no. 4, pp. 2385–2395, Nov. 2023, doi: 10.18421/TEM124-51.

[12] S. P. Dash, A. K. Jena, and D. K. Murala, "A Hyperledger-Based Secure Framework for Academic Certificate Authentication Using Blockchain," *International Journal of Safety and Security Engineering*, vol. 15, no. 6, pp. 1185–1195, Jun. 2025, doi: 10.18280/ijsse.150610.

[13] T. Rahman, S. I. Mouno, A. M. Raatul, A. K. Al Azad, and N. Mansoor, "Verifi-Chain: A Credentials Verifier using Blockchain and IPFS," Jul. 2023, [Online]. Available: http://arxiv.org/abs/2307.05797

[14] S. Oknora Firza and F. Ilmu Komputer, "Teknologi Blockchain dalam Keamanan Sertifikat Menggunakan Smart Contracts dan Distributed Ledger pada Platfrom Edutech," 2024.

[15] B. Zhong, H. Wu, L. Ding, H. Luo, Y. Luo, and X. Pan, "Hyperledger fabric-based consortium blockchain for construction quality information management," *Frontiers of Engineering Management*, vol. 7, no. 4, pp. 512–527, Dec. 2020, doi: 10.1007/s42524-020-0128-y.

[16] A. Farabi, I. Khandaker, J. Ahsan, I. K. Shanto, N. Jahan, and M. J. Khan, "ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh," Oct. 2025, [Online]. Available: http://arxiv.org/abs/2508.05334