Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

Secure Academic Certificate Authentication and Tamper Detection Using Blockchain and Smart Contracts

Saba Alaa abdulwahhab
[*1] Cybersecurity Department, Tikrit University, Tikrit, Iraq,
saba.programmer12@tu.edu.iq

[*]*Corresponding author: saba.programmer12@tu.edu.iq*

Received: 31 Aug 2026	Accepted: 12 Sep 2026	Published: 25 Sep 2026

Abstract

world of information security, Blockchain Technology has gained a lot of importance in the recent past as it uses hashing algorithms like SHA-256, thereby enabling the contents of the registered information to be secure and resistant to modification. In the current research paper, an effort has been made to exploit the Smart Contract feature of Blockchain Technology for academic credential verification. A Smart Contract System for secure registration and verification of academic credentials has been designed, developed, and deployed using Solidity. The proposed system uses SHA-256 hashes to represent academic credentials without storing the complete documents on the blockchain. Access control is used to restrict protected operations to the authorized issuer, while credential verification is performed by comparing the generated hash with the registered hash. The system was evaluated using 100 simulated academic credentials, including 50 original and 50 modified credentials across five tampering scenarios. The experimental results showed a 100% tamper detection rate and 100% verification accuracy under the tested conditions. Credential registration consumed 92,388 gas units, while contract deployment and unauthorized access attempts consumed 22,841 and 2,461 gas units, respectively. The results show that the developed Smart Contract System can support secure academic credential registration and verification while detecting modifications to the tested credential information.

Keywords: Blockchain, Smart Contracts, SHA-256, Academic Credentials, Tamper Detection, Access Control.

1. Introduction

Academic certificates are used as evidence of educational recommendations when individuals apply for employment, and professional opportunities. Though, proving the authenticity of these credentials remains a challenge for educational organizations and employers. [1][2] .

Blockchain technology has been examined as an alternative approach for academic credential management and verification. Said et al. [1] indicated that blockchain can support certificate verification through immutability, security, tamper resistance, and reduced dependence on intermediaries. [1].

Smart contracts provide another component of blockchain-based systems to be executed according to programmed rules. A blockchain-based academic degree verification system proposed in [3], for example, used an Ethereum smart contract to systematize degree

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

verification while minimizing the amount of degree information required for the verification process. The ZKBAR-V system offered in [4] employs blockchain and zero-knowledge proofs to verify academic records however limiting exposure of the primary information.

Cryptographic hashes can reduce the academic information that must be maintained on the blockchain. Instead of recording an entire certificate. If the offered credential is modified, its newly generated hash will differ from the registered reference. Ifeyemi et al. [5] implemented this principle in a blockchain-based educational certificate verification system by storing certificate on the blockchain.

Even though these developments, academic credential verification continues to raise practical issues concerning unauthorized operations. Recent studies have then moved beyond certificate toward controlled and privacy-aware verification mechanisms [1], so [4] this paper has also examined Blockchain supported access control for detecting academic certificate fraud, showing the continuing interest in combining blockchain properties with certificate verification processes[6] .

According to these requirements, this paper offered a blockchain-based smart contract framework for secure and tamper resistant academic credential verification.. The proposed framework is valued through functional and access-control tests, controlled credential modification experiments, and gas-consumption analysis.

The main contributions of this paper are present as follows:

1. A blockchain-based framework is established for registering and verifying academic credentials using SHA-256 credential hashes.
2. A smart contract is applied to support credential registration and verification, with an owner-based access-control mechanism.
3. The tamper-resistance mechanism is calculated using 100 simulated academic credentials, including 50 intentionally modified records across five tampering scenarios: student name, degree/grade, graduation year, credential ID, and multiple-field modifications.
4. The framework is estimated through functional and access-control experiments involving authorized and unauthorized interactions, together with hash-based verification
5. The requirements of the implemented smart contract are examined through gas consumption measurements for contract deployment.

Finally, this paper is organized as follows. Section 2 reviews related work on blockchain-based academic credential verification. Section 3 explain the proposed methodology, smart contract implementation, experimental environment, and evaluation procedure. Section 4 discusses the experimental results. Finally, Section 5 conclusions and directions for future work.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

2. Related Work

Blockchain-based academic credential verification increasing attention as researchers seek to conventional certificate issuance and verification systems. Recent studies on paper have examined blockchain platforms, smart contracts, decentralized storage, digital signatures, privacy mechanisms, and cross-chain architectures for issuing, verifying, storing, and academic records.

Rustemi et al. [7]showed a systematic literature review of blockchain-based systems for academic certificate verification. The authors initially identified 1,744 publications and selected 34 relevant studies. The authors also indicated that research on blockchain-based academic credential verification was still at a evolving stage and identified several areas requiring further investigation.

Sultana et al. [8] present a framework that combines blockchain, smart contracts, and the InterPlanetary File System (IPFS) to address certificate fraud in the academic field. In the proposed framework, IPFS is used for distributed storage, while blockchain maintains information required for certificate verification.

Fartitchou et al. [9] suggested BlockMEDC, a blockchain and smart contract system for securing digital certificates in higher education.The paper demonstrates the application of blockchain technology to digital academic certificates within a higher-education environment.

Rustemi et al. [10] proposed the Diploma Integrity Authentication Record (DIAR), a blockchain-based system for generating and verifying academic diplomas. The paper designates a model and a layered architecture covering diploma generation, verification, and revocation.

Kabashi et al.[11] established a three-layer application for academic credential verification. Their architecture consists of a data layer, blockchain layer, and application layer. The data layer handles academic information, the blockchain layer provides the blockchain and smart contract functions required for recording and verification.

Said et al. [12]proposed a blockchain-based system for managing and verifying educational qualifications to counter certificate forgery. The author identifies disintermediation, immutability, tamper resistance, efficiency, and security as properties that make blockchain suitable for certificate issuance and verification.

Cardenas-Quispe and Pacheco [13] developed a degree-verification prototype using a hybrid blockchain network. It was implemented using Python and Docker with six blockchain nodes and included initial data registration, credential generation the proposed implementation provided authenticity and traceability of academic records.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

[14]proposed a secure blockchain-based framework for academic certificate authentication using Ethereum. The framework employs smart contracts to manage certificate issuance and verification, while cryptographic hashes are recorded on the blockchain to preserve certificate integrity and identify unauthorized changes.

A privacy-oriented approach was proposed through ZKBAR-V[15], a Zero-Knowledge Proof-enabled blockchain-based academic record verification system .Its main purpose is to allow academic credentials to be verified without revealing the underlying credential information. The authors designed the framework to provide privacy-preserving, immutable, and secure management of academic records .

Tran et al. [16] proposed DAVE-CC, a decentralized, access-controlled, and verifiable framework for cross-chain academic credential management. The study focuses particularly on decentralized trust, access control, privacy, and credential exchange across different blockchain environments.

Recent work has also moved from conceptual blockchain architectures toward practical implementations. Rustemi and Dalipi [17]extended the DIAR framework into a practical blockchain implementation for generating and verifying academic credentials. The authors describe the system as a means of digitizing academic documents while providing fast, secure, and cost-effective diploma verification.

The reviewed studies show several approaches to blockchain-based academic credential verification. Some works concentrate on system architecture and certificate management [8] –[11] , while others address broader qualification management[12] , practical blockchain prototypes [13] , resource and energy requirements[14], privacy-preserving verification [15], or cross-chain credential management [16]. More recent work has also examined the transition from conceptual academic credential architectures to implemented blockchain systems[17]. These studies use different combinations of smart contracts, IPFS, QR codes, digital signatures, decentralized identifiers, zero-knowledge proofs, consensus mechanisms, and cross-chain protocols.

3. Methodology

This paper equipment a blockchain-based framework for secure and tamper-resistant verification of academic credentials. The method present a combines SHA-256 hashing with a smart contract to register credential information, control access to protected operations, and verify while a presented credential matches its registered record. The procedure covers smart contract implementation, functional and access-control testing, credential tampering, then gas consumption analysis.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

A. Proposed Framework

In this section proposed framework supports two main participants: institution and an authorized academic, then registers valid credentials, and a verifier, which checks the authenticity. Instead of storing the complete academic document on the blockchain, the framework produces a SHA-256 hash from the information and registers this value through the smart contract.

Through registration, and the authorized issuer generates the credential hash and submits it to the smart contract. The contract checks the sender's authorization before recording the information. During verification, the same hashing procedure is applied to the presented credential, and the result using hash is compared with the previously registered value. Any modification to the credential information produces a different hash and therefore results in a mismatch. The verification is show as

$$\begin{cases} Valid & H(D)=H_{stored}, \\ Mismattch, & H(D)\neq H_{stored} \end{cases} \quad (1)$$

Where D represent the academic credential (D) is its SHA-256 hash , and H_{stored} is the reference hash registered through the smart contract , it is reference hash registered through the smart contract , so figure 1 showed the proposed methods of blockchain based academic credential verification framework.

So figure 1 explains the main stages of the proposed method, from qualification issuance and hash generation to smart contract registration and verification. The unique credential information remains outside the blockchain, however its hash serves as the reference for detecting changes to the presented credential.

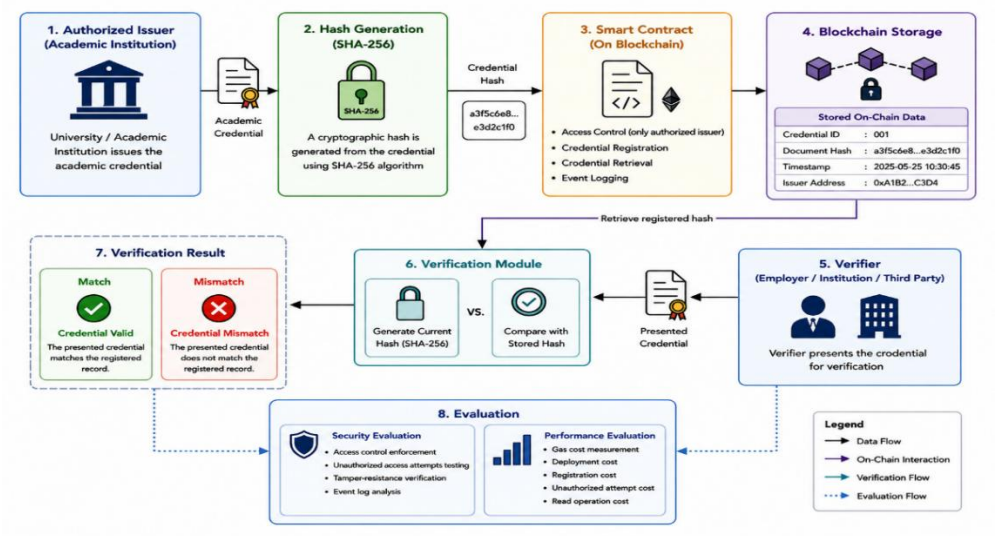


Figure 1: Architecture of the proposed framework.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

B. Smart Contract Implementation

The credential registry was executed in Solidity 0.8.x using the Remix IDE. The smart contract achieves credential registration, retrieval, access control, and transaction events. Credential hashes and registration timestamps are stored using Solidity. Protected the changing of state operations use the modifier, allowing only the approved academic institution to register credentials, however unauthorized transactions are reverted before changing the contract state.

C. Experimental Environment

The smart contract was accumulated, deployed, and tested via Remix IDE, with Solidity 0.8.x, and the Remix JavaScript VM with many simulated accounts. Google Colab with Python were used to produce credential hashes, prepare tampering scenarios, and analyze the results. SHA-256 was used as the hashing algorithm. The experimentations performed on a computer prepared with an Intel Core i7 processor.

D. Functional and Access-Control Evaluation

The testing set correct credential registration and retrieval through transaction status and contract-state changes. The testing in the access control used owner and non-owner accounts to calculate the contract before and after applying the onlyOwner restriction. The tests tested whether unauthorized operations were rejected without modifying the registered state.

E. Tamper-Resistance Evaluation

An experiment was focused using 100 simulated academic credentials, it contain 50 original and 50 intentionally modified records. The modified credentials covered 5 tampering scenarios: student name, graduation year, degree/grade, credential ID, and multiple fields, with 10 records for each scenario. SHA-256 hashes of the modified credentials were compared with their original reference hashes to classify changes. Performance was calculated using the Tamper Detection Rate (TDR) and overall verification accuracy so table 1 present the experimental design.

Table 1. Tamper-resistance experimental design

Credential condition	Modification type	Number
Original	No modification	50
Modified	Student name	10
Modified	Degree/grade	10
Modified	Graduation year	10
Modified	Credential ID	10
Modified	Multiple fields	10
Total		100

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

F. Gas Cost Evaluation

Gas consumption was measured via the Remix implementation environment for contract deployment, record registration, unauthorized access. The recorded gas values were associated to estimate the computational requirements of the main smart contract operations.

4. Results and Discussion

The framework was calculated through functional testing, access-control testing, tamper-resistance experiments, and gas consumption analysis. The final results were used to examine the correct execution of detection of modified credentials ,the smart contract, restriction of unauthorized operations, and computational requirements of the main contract operations.

A. Access Control Results

Functional testing complete a credential registration and retrieval. Before applying the onlyOwner restriction, both owner and non-owner accounts could achieve the tested operation. After that apply the restriction, only the owner transaction succeeded, however the non-owner transaction was reverted without modifying the contract state, as brief in Table 3.

Table 3. Access-control evaluation results

Operation	Before Access Control	After Access Control
Owner operation	Successful	Successful
Non-owner operation	Successful	Reverted
Unauthorized modification	Possible	Prevented
State integrity	Vulnerable	Protected

The experiment indications that the onlyOwner restriction prevented the unauthorized account from performing the tested protected operation. So the credential registration and other protected state-changing operations remain under the control of the authorized issuer in the implemented framework.

B. Tamper Authentication Results

The experimental estimated 100 simulated academic credentials, it contain about 50 original and 50 modified records across 5 tampering scenarios. All credentials were verified, but all modified credentials were successfully detected, achieving a 100% tamper detection rate (50/50) and 100% total verification accuracy (100/100) under the tested conditions. Table 4 showed the results for each tampering scenario.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

Table 4. The results across the evaluated scenarios on Tamper detection

Tampering scenario	Tested	Detected	Detection rate (%)
Student name	10	10	100
Degree/grade	10	10	100
Graduation year	10	10	100
Credential ID	10	10	100
Multiple fields	10	10	100
Overall	50	50	100

Table 4 showed all 5 tampering scenarios were successfully detected because each modification produced a different SHA-256 hash from the registered reference. The 100% detection rate applies only to the simulated credentials and predefined modifications evaluated in this experiment.

C. Gas Consumption Analysis

Gas consumption measured for the main smart contract operations. Credential registration recorded the highest consumption at 92,388 gas units, however contract deployment required 22,841 gas units. The rejected unauthorized transaction consumed 2,461 gas units. The read operation did not require transaction gas in the adopted execution environment because it not modify the contract state. Figure 2 present the result analysis of gas consumption.

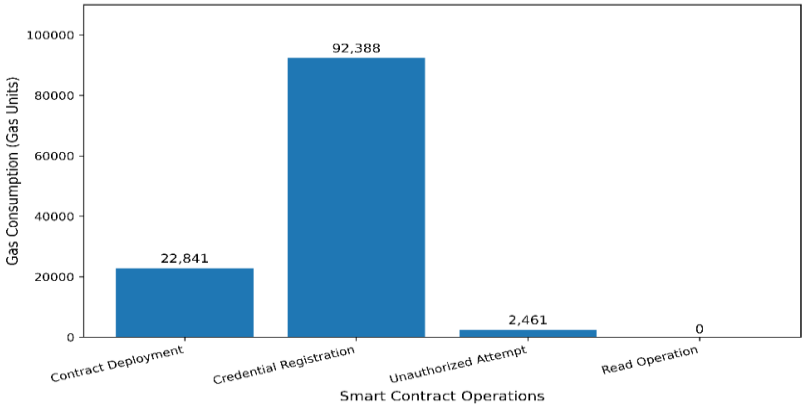


Figure 2: Gas consumption of the evaluated smart contract operations.

As proved in Figure 2, credential registration required the highest gas consumption because it includes persistent modification of the contract state. but the , unauthorized transactions consumed less gas because they were completed by the access control mechanism before modifying the protected state, however read operations required no transaction gas in the environment. The results confirmed that the framework successful credential registration and verification, disallowed the tested unauthorized operations, and detected all predefined credential modifications. Storing credential hashes rather after that complete documents reduces the amount of credential information maintained on chain. While the experiments

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"

Gharyan University Journal of Engineering Science (GUJES)
ISSN (3105-4560)
Website: http://journals.gu.edu.ly
email: gujes@gu.edu.ly

were conducted using the Remix JavaScript VM, the reported gas values represent the accepted environment and should not be considered actual transaction costs on a public blockchain network.

5. Conclusion

The framework offers an approach to improving academic credential verification by utilizing a blockchain-based system. This paper present a smart-contract-based implementation using SHA-256 hashing was developed for credential registration and verification. The framework restricts protected operations to the authorized issuer and verifies credential integrity by comparing the generated hash with the registered reference hash. Access-control testing moreover displayed that unauthorized state-changing operations were rejected after applying the onlyOwner restriction. The gas analysis prove the registration required the highest gas consumption among the evaluated operations because it modifies the stored blockchain state. The proposed framework may be used as a practical tool for academic credential verification and can be further extended for use by academic institutions. For real-world application, future work may consider real academic credential data and deployment on a public blockchain environment.

References

[1] P. Khandelwal, R. Johari, V. Gaur, and D. Vashisth, “BlockChain Technology based Smart Contract Agreement on REMIX IDE,” in 2021 8th International Conference on Signal Processing and Integrated Networks (SPIN), IEEE, Aug. 2021, pp. 938–942. doi: 10.1109/SPIN52536.2021.9565983.

[2] N. El Madhoun, I. Dionysiou, and E. Bertin, Eds., Blockchain and Smart-Contract Technologies for Innovative Applications. Cham: Springer Nature Switzerland, 2024. doi: 10.1007/978-3-031-50028-2.

[3] M. Gurunathan, M. A. Mahmoud, I. L. H. Alsammak, and S. S. Gunasekaran, “Development of Smart Contract Blockchain Integrated Model (Lightblock) for IOT Applications,” 2025, pp. 269–287. doi: 10.1007/978-3-031-75091-5_15.

[4] E. Sivakumar, K. J. Singh, P. Chawla, and G. Ganesan, “RBEDH: A Decentralized Role-Based Event Driven Hybrid Framework for Smart Contracts,” IEEE Access, vol. 13, pp. 74781–74798, 2025, doi: 10.1109/ACCESS.2025.3554630.

[5] T. Zaidi, M. Usman, M. U. Aftab, H. Aljuaid, and Y. Y. Ghadi, “Fabrication of Flexible Role-Based Access Control Based on Blockchain for Internet of Things Use Cases,” IEEE Access, vol. 11, pp. 106315–106333, 2023, doi: 10.1109/ACCESS.2023.3318487.

[6] K. Soumya, K. S. Sharat, and N. Sreenivas, “Academic certificate fraud detection by Web-based intelligent access control system: An effective role of Blockchain technology,” Int. J. Inf. Manag. Data Insights, vol. 6, no. 1, p. 100386, Jun. 2026, doi: 10.1016/j.jjimei.2025.100386.

“Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License”

[7] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "A Systematic Literature Review on Blockchain-Based Systems for Academic Certificate Verification," IEEE Access, vol. 11, pp. 64679–64696, 2023, doi: 10.1109/ACCESS.2023.3289598.

[8] S. A. Sultana, C. Rupa, R. P. Malleswari, and T. R. Gadekallu, "IPFS-Blockchain Smart Contracts Based Conceptual Framework to Reduce Certificate Frauds in the Academic Field," Information, vol. 14, no. 8, p. 446, Aug. 2023, doi: 10.3390/info14080446.

[9] M. Fartitchou, I. Lamaakal, K. El Makkaoui, Z. El Allali, and Y. Maleh, "BlockMEDC: Blockchain Smart Contracts System for Securing Moroccan Higher Education Digital Certificates," IEEE Access, vol. 13, pp. 39152–39175, 2025, doi: 10.1109/ACCESS.2025.3546177.

[10] A. Rustemi, F. Dalipi, V. Atanasovski, and A. Risteski, "DIAR: a blockchain-based system for generation and verification of academic diplomas," Discov. Appl. Sci., vol. 6, no. 6, p. 297, May 2024, doi: 10.1007/s42452-024-05984-1.

[11] F. Kabashi, H. Snopçe, A. Luma, and V. Neziri, "Trustworthy Verification of Academic Credentials through Blockchain Technology," Int. J. Online Biomed. Eng., vol. 20, no. 09, pp. 51–64, Jun. 2024, doi: 10.3991/ijoe.v20i09.48999.

[12] S. H. Said, R. S. Sinde, E. M. Kosia, and M. A. Dida, "A Comprehensive Blockchain-Based System for Educational Qualifications Management and Verification to Counter Forgery," IEEE Access, vol. 13, pp. 31562–31589, 2025, doi: 10.1109/ACCESS.2025.3542545.

[13] M. A. Cardenas-Quispe and A. Pacheco, "Blockchain ensuring academic integrity with a degree verification prototype," Sci. Rep., vol. 15, no. 1, p. 9281, Mar. 2025, doi: 10.1038/s41598-025-93913-6.

[14] S. Narvekar, S. Patil, P. Motghare, T. Panaskar, and R. Pawar, "A Secure Framework for Academic Certificate Authentication on Ethereum Blockchain," in 2025 IEEE International Conference on Blockchain and Distributed Systems Security (ICBDS), IEEE, Oct. 2025, pp. 1–6. doi: 10.1109/ICBDS67396.2025.11377304.

[15] J. A. Berrios Moya, J. Ayoade, and M. A. Uddin, "A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System," Sensors, vol. 25, no. 11, p. 3450, May 2025, doi: 10.3390/s25113450.

[16] T.-D. Tran, H. P. G. Bao, N. T. Cam, and V.-H. Pham, "DAVE-CC: A decentralized, access-controlled, verifiable ecosystem for cross-chain academic credential management," J. Inf. Secur. Appl., vol. 94, p. 104238, Nov. 2025, doi: 10.1016/j.jisa.2025.104238.

[17] A. Rustemi and F. Dalipi, "From Concept to Practice: A Blockchain-Based Solution for Secure and Efficient Academic Credentials in Higher Education," IET Blockchain, vol. 6, no. 1, Jan. 2026, doi: 10.1049/blc2.70030.

"Articles published in GUJES are licensed under a Creative Commons Attribution-Non Commercial4.0International License"