IOSUD - Universitatea Politehnica Timişoa
Şcoala Doctorală de Studii Inginereşti

Transparent and secure management of activities carried out by teachers using blockchain technology

Doctoral thesis

Abstract for obtaining the scientific title of doctor at
University Politehnica Timisoara
in the doctoral field Computers and Information Technology

author inf. Silaghi Diana Laura

scientific supervisor Prof.univ.dr.ing. Popescu Daniela Elena

September, 2025

Abstract: *The evaluation of teachers in pre-university education remains heavily dependent on paper-based processes, which are fragmented, time-consuming, and vulnerable to document loss, inefficiency, and fraud. Despite the emergence of digital initiatives in education, existing systems lack integrated mechanisms for secure verification and traceability of professional documents across teachers' careers. To address this gap, the present thesis proposes a blockchain-based framework for the issuance and verification of diplomas, certificates, and attestations, thereby enabling the creation of a secure digital portfolio for each teacher. The proposed solution relies on two smart contracts, one dedicated to managing educational resources produced by teachers and another focused on credentials, both developed with built-in security mechanisms and cost optimization techniques. By leveraging zk-Rollup integration, the framework achieves a significant reduction in transaction costs on blockchain, ensuring scalability and suitability for large-scale adoption in education systems. Experimental results validate the feasibility and efficiency of the approach, demonstrating its potential to enhance transparency, trust, and credibility in teacher evaluation processes while supporting the broader digital transformation of educational administration.*

Even though teachers in the pre-university system undergo multiple forms of professional evaluation, ranging from annual assessment, to evaluation for obtaining merit-based recognition, or to evaluations carried out when teaching activities are restricted or workloads are adjusted, the evaluation process itself has remained largely traditional. Teachers are still required to compile extensive portfolios containing dozens or even hundreds of documents, all of which must be

manually verified by evaluation committees. This reliance on paper-based submissions places an enormous administrative burden on both teachers and evaluators, and has changed very little over decades, despite the digital transformation occurring in education. The persistence of such practices underscores not only inefficiencies but also vulnerabilities in ensuring fairness, transparency, and accuracy within evaluation processes.

A central issue stems from the heavy reliance on physical documentation, which must be repeatedly submitted for each assessment stage [1, 2]. Each evaluation demands a separate copy of documents, often reviewed by different committees operating under distinct criteria. Consequently, the verification process becomes both complex and labor-intensive. Committees must meticulously examine a wide range of diplomas, certificates, and attestations, not only to confirm their authenticity but also to assess their relevance for the evaluation at hand. In cases where hundreds of documents are presented by each teacher, the workload multiplies significantly, raising the risk of human error, inconsistencies, or overlooked details.

The diversity of documentation compounds the problem further. Teacher evaluations are not limited to formal academic diplomas or certificates obtained through university programs or accredited training. They also include professional development certificates, short-term training or micro-credentials, and numerous attestations issued by schools or inspectorates. These attestations typically certify contributions to extracurricular or community-based activities, such as mentoring students, coordinating competitions, supervising projects, or supporting specific groups of learners. In practice, this creates an overwhelming volume of documentation, each piece requiring careful scrutiny. The stakes are high, particularly in evaluations linked to merit grades, where recognition often entails financial rewards or career advancement opportunities. As such, the process demands exceptional rigor and precision, both to safeguard institutional integrity and to ensure that teachers receive recognition based on verified, authentic contributions.

Yet, challenges extend beyond volume and verification. Another significant issue arises when teachers lose access to their documents. This may occur when a diploma, certificate, or attestation is not issued promptly at the time of the activity, or when the original document is misplaced and a duplicate is required. The problem becomes more acute when the issuing institution no longer exists, a reality increasingly common in rural areas affected by declining student populations and school consolidations. In such cases, the teacher may be unable to provide official proof of professional activities, despite having carried them out. This administrative gap undermines the accuracy of evaluations and risks penalizing teachers for circumstances beyond their control. Furthermore, mobility within the education system, such as moving to a different school, exacerbates these challenges, as the continuity of document management is often fragmented between institutions.

This situation highlights a pressing need for a long-term, digital solution that can securely store, manage, and validate professional documents over time. Such a system must guarantee that credentials remain accessible and verifiable, regardless of institutional changes or administrative

restructuring. A secure digital repository would allow teachers to maintain lifelong portfolios of their professional development, accessible across different schools. At the same time, it would reduce administrative burdens for evaluators, who could verify documents quickly and reliably.

A further observation about current evaluation practices concerns their inherent temporal dimension. Teacher assessments are tied to specific time frames: one year for annual performance reviews, and up to five years for professional development cycles or evaluations for merit-based recognition. This means that the precise date of issuance of each diploma, certificate, or attestation is critical in determining whether the document falls within the relevant evaluation period. In the current system, which relies on physical documents, ensuring both authenticity and accurate time-stamping of credentials presents considerable challenges. Errors or uncertainties regarding the issuance date of a document can compromise the fairness of the evaluation process, creating grounds for disputes or appeals. For this reason, a solution is required that not only preserves the integrity of documents but also secures their temporal validity. Blockchain technology offers an innovative response to this challenge. By design, blockchain operates as an immutable ledger, capable of recording transactions in a secure and transparent manner. One of its core advantages lies in the ability to timestamp data at the moment it is uploaded, ensuring that both the content of the document and the exact time of its registration are permanently recorded. Once a credential is entered into the blockchain, neither the data nor its timestamp can be altered or erased. If an error occurs, a correction cannot simply overwrite the original entry, but instead, a new transaction must be created, preserving a complete history of modifications. This feature ensures integrity, traceability, and transparency, while also providing evaluators with absolute certainty regarding the issuance date of documents.

Beyond technical accuracy, blockchain also addresses concerns related to fraud [3]. Teacher evaluations often carry high stakes, especially when linked to financial incentives, promotions, or professional recognition. This creates the potential for misconduct, where individuals may attempt to submit falsified documents or obtain attestations for activities in which they did not participate. Such practices undermine the credibility of the entire evaluation system, disadvantaging teachers who comply with rules and eroding institutional trust. Fraudulent behavior is difficult to detect in paper-based systems, particularly when evaluators face overwhelming volumes of documentation. Blockchain, however, introduces structural safeguards: documents can only be issued to teachers' digital portfolios by accredited institutions registered as authoritative entities within the system. This eliminates the possibility of self-issued or falsified credentials and ensures that every entry originates from a trusted source.

Taken together, these challenges and opportunities highlight the transformative potential of integrating blockchain into teacher evaluation processes. Current practices, grounded in manual verification and physical documentation, not only generate inefficiencies but also expose the system to errors, administrative gaps, and fraud. By contrast, a blockchain-based framework would create a secure, transparent, and verifiable digital portfolio for each teacher, integrating timestamping, institutional accreditation, and immutable record-keeping. Such an approach would

not only reduce administrative burdens but also strengthen the fairness, accuracy, and credibility of evaluations. Ultimately, adopting such a system could play a decisive role in supporting the broader digital transformation of educational administration, aligning teacher evaluation with the standards of reliability and transparency increasingly expected in modern society.

The development of the proposed blockchain-based solution for teacher evaluation was guided by a series of well-defined objectives, as follows:

- The first objective focused on analyzing blockchain technology from theoretical perspective, establishing a solid foundation for its application in managing teacher credentials.
- The second objective explored practical implementations of blockchain across various sectors, identifying strategies to enhance data security, transparency, and efficiency, which informed its adaptation to the educational context.
- The third objective examined existing research, highlighting gaps in credential management, inefficiencies in verification, and reliance on physical documents, emphasizing the need for a secure and verifiable solution.
- The fourth objective addressed specific challenges in managing diplomas, certificates, and attestations, such as document loss, fraud, and administrative delays.
- The fifth objective focused on designing a blockchain-based framework that ensures secure, tamper-proof, and time-stamped registration of teachers' professional documents, enabling verified digital portfolios for educators, secure credential issuance by institutions, and efficient access for evaluators.
- The sixth objective focused on testing feasibility, scalability, and implementation through simulations, demonstrating the system's operational viability.
- The seventh objective evaluated the framework's impact on teacher evaluation, highlighting improvements in transparency, accuracy, and procedural efficiency.
- The eighth objective assessed security mechanisms, including access control, immutability, and resistance to unauthorized modifications, ensuring the framework's reliability in practice.

Together, these objectives provided a structured approach to designing, implementing, and validating a blockchain-based system that addresses long-standing inefficiencies in teacher evaluation while supporting a more secure, transparent, and credible educational administration.

Chapter 2 is devoted to addressing Objective O1, providing a detailed and comprehensive analysis of blockchain technology with a focus on its core principles, structural components, and security considerations. The chapter begins by establishing a clear conceptual framework through formal definitions of blockchain, portraying it as a decentralized and distributed ledger system capable of securely recording transactions across a network of participants without relying on a central authority.

A central component of blockchain functionality lies in its consensus mechanisms, which ensure the validity of transactions and the consistency of the ledger across distributed nodes. Chapter 2 provides an in-depth exploration of consensus algorithms such as Proof of Work and Proof of Stake, analyzing their operational principles, security implications, and energy consumption profiles. This section highlights how consensus protocols not only prevent double-spending and fraudulent activity but also impact network performance, scalability, and resilience to attacks. By examining the trade-offs inherent in each mechanism, the chapter establishes a critical understanding of how blockchain networks can maintain security while addressing practical performance constraints.

The discussion then turns to the layered structure of blockchain, which underpins its robustness and flexibility. Blockchain is conceptualized as comprising multiple interacting layers, including the data layer, network layer, consensus layer, and application layer. The data layer stores transaction records and cryptographic hashes, ensuring immutability. The network layer facilitates communication between nodes, while the consensus layer guarantees agreement on the ledger state. Finally, the application layer enables the development of smart contracts and decentralized applications, bridging technical infrastructure with functional use cases. This layered perspective provides readers with a holistic understanding of how blockchain operates as an integrated system.

To illustrate these principles in practice, the chapter examines the Bitcoin blockchain in detail. As the first widely adopted blockchain, Bitcoin serves as a model for understanding decentralized ledger structures, cryptographic security, and transaction validation processes. The architecture of Bitcoin is analyzed, including block formation, transaction structure, and the use of cryptographic hashing to link blocks immutably. Its operational model, centered around a decentralized network of miners executing Proof of Work, ensures that transactions are verified without reliance on a central authority, providing a foundational example of blockchain security and trust mechanisms.

Following Bitcoin, the chapter explores Ethereum, emphasizing its extended capabilities through smart contracts. Unlike Bitcoin, Ethereum allows programmable scripts to be executed on-chain, enabling automated and self-enforcing agreements that can support complex workflows, such as the issuance and verification of professional documents for teachers. The chapter details the operational mechanics of Ethereum, including transaction validation, block propagation, and state management. Smart contracts are examined thoroughly, focusing on their potential applications, programming considerations, and security challenges, such as vulnerabilities to reentrancy attacks or gas limit issues. Additionally, the chapter addresses Ethereum’s scalability challenges and current solutions, including Layer 2 protocols, sharding, and zk-Rollups, which aim to increase transaction throughput, reduce latency, and lower costs without compromising decentralization or security.

To achieve the objectives mentioned above, the thesis is structured in 8 chapters presented below.

Chapter 1 introduces the thesis by presenting the research context and motivation, outlining the objectives, and providing a detailed overview of the thesis structure.

Chapter 2 addresses Objective O1 by providing a comprehensive analysis of blockchain technology, focusing on its components, principles, and security aspects. The chapter begins by defining blockchain as a decentralized and distributed ledger that records transactions across multiple nodes without the need for a central authority.

The types of blockchain are presented next. Public blockchains, such as Bitcoin and Ethereum, are open to all participants and rely on transparent consensus mechanisms to validate transactions. Private blockchains, in contrast, restrict access to authorized entities, providing a controlled environment that can enhance efficiency while maintaining certain levels of security. Consortium blockchains offer a hybrid model, where selected organizations collaboratively govern the network, balancing decentralization and control.

A central component of blockchain functionality lies in its consensus mechanisms, which ensure the validity of transactions and the consistency of the ledger across distributed nodes.

As the first widely adopted blockchain, Bitcoin serves as a model for understanding decentralized ledger structures, cryptographic security, and transaction validation processes. The architecture of Bitcoin is analyzed, including block formation, transaction structure, and the use of cryptographic hashing to link blocks immutably. Its operational model, centered around a decentralized network of miners executing proof-of-work, ensures that transactions are verified without reliance on a central authority, providing a foundational example of blockchain security and trust mechanisms.

Unlike Bitcoin, Ethereum allows programmable scripts to be executed on-chain, enabling automated and self-enforcing agreements that can support complex workflows.

Regarding scalability and congestion, Ethereum addresses through both Layer 1 and Layer 2 solutions. At Layer 1, sharding partitions the network into smaller, independent units called shards, each with its own validators, transactions, and smart contracts. This allows parallel processing and higher throughput.

Layer 2 solutions alleviate pressure on the main chain by executing transactions off-chain or on secondary layers while anchoring summary data on Layer 1. These include:

- state channels, which enable multiple off-chain interactions with only the final settlement recorded on Ethereum;
- sidechains, independent Ethereum-compatible chains with their own consensus mechanisms;
- Plasma, which leverages child chains to process high transaction volumes;

- rollups, which post compressed transaction proofs to Ethereum. Rollups are divided into Optimistic Rollups, assuming transactions are valid unless challenged, and Zero-Knowledge Rollups, which use cryptographic proofs for fast, secure verification [4].

Together, these solutions enhance scalability, reduce fees, and maintain network security.

Chapter 3 addresses Objective O2 by examining the practical implications of blockchain technology across a variety of sectors. This investigation encompassed an analysis of successful real-world implementations and identified best practices, which provided valuable insights into both the advantages and potential limitations of blockchain adoption. By studying applications in fields such as finance, healthcare, supply chain management, and governmental services, the research was able to highlight strategies for enhancing data integrity, transparency, and operational efficiency. These comparative insights informed the design of a blockchain-based solution tailored to educational settings, demonstrating how lessons learned from other industries could be adapted to improve the management, verification, and security of teachers' professional documents while addressing the specific challenges of the pre-university education system.

Chapter 4 addresses Objective O3 by examining current research on the management and verification of academic credentials [5]. The traditional model of a university providing a single, verifiable credential no longer fits the way people actually learn today [6]. They take a series of online courses, in-house training, and refresher courses held by educational institutions or organizations, but there are no systems to manage them. As a result, a learner's credentials are shaped by a combination of diplomas, academic certificates, qualifications in skills and competences, open recognition badges, and micro-credentials [7], together reflecting their educational background, skills, and achievements. Table 1 provides an overview of the key characteristics of credentials.

Type of credential	***Description***	***Typical completion time***
Degree	Formal qualification for completing a full academic program	2-7 years
Diploma	Recognition for specialized or technical training	1–2 years
Certificate	Proof of completing a specific course or program	Weeks to 1 year
Micro-credential	Certification of specific skills or competencies	Hours to months
Digital Badge	Visual, shareable proof of a skill or achievement	Hours to weeks
Attestation	Formal declaration confirming completion of an educational activity or skill acquisition	Days to weeks

Table 1: Characteristics of credentials

The lifecycle of academic and professional credentials involves a series of distinct stages, beginning with the identification of learning goals and concluding with the practical use of the

awarded credential. Whether referring to degrees, certificates, micro-credentials, digital badges, or attestations, each type of credential follows a structured process that ensures the recognition of knowledge, skills, and competencies. Each step of the process presents potential risks related to fraud, verification, and data integrity, especially in traditional format.

Building upon established credentialing practices, printed diplomas can incorporate quick response (QR) code technology, embedding a digital layer that strengthens security and streamlines verification. This practice is already confirmed by some universities or countries that already apply QR codes on their diplomas [8].

Electronic documents offer convenience and efficiency, but this digital advantage comes with significant security risks. As these documents are accessed and transmitted through public channels, they are vulnerable to various cyber-attacks that can compromise their confidentiality, integrity, and authenticity. Such attacks include [9]:

- replay attacks, where legitimate data is delayed or repeated maliciously;
- man-in-the-middle attacks, where an attacker intercepts and alters communication between two users;
- impersonation attacks, where attackers pose as legitimate senders to trick recipients;
- compromise attacks, which involve unauthorized access to or alteration of the original data;
- masquerade attacks, in which an attacker uses a fake identity to gain unauthorized access to the document.

The most transformative approach examined in this chapter is the application of blockchain technology in the issuing and verification of academic credentials. Blockchain offers a decentralized, tamper-resistant, and transparent infrastructure for managing educational records. Credentials stored on the blockchain can be verified independently by any third party, fostering trust and interoperability across institutions. Platforms such as Ethereum, with its support for smart contracts, have been particularly influential in enabling programmable, automated credential systems that support lifelong learning and open recognition frameworks.

Chapter 5 is aligned with Objective O5, and introduces a blockchain-based framework designed to respond to the limitations of current document management practices by providing a structured system for recording attestations, certificates, diplomas, digital badges, and educational resources [10]. In doing so, it ensures that professional achievements are systematically preserved and accessible for evaluation processes, while maintaining efficiency and security through the integration of Layer 2 blockchain technologies.

The starting point of the framework is the classification of document categories that define a teacher’s evaluation portfolio:

- Attestations - Issued by the school director to recognize teachers' involvement in institutional activities, projects, or extracurricular programs.
- Educational resources - Created by teachers, including lesson plans, manuals, digital materials, and interactive classroom content, which reflect innovation and adaptability in modern pedagogy.
- Academic credentials - Certificates, diplomas, and digital badges awarded by certifying bodies and training institutions to validate teachers' expertise, continuous development, and formal qualifications.

We provided the bodies involved in the creation of these documents:

- School director emits attestations, since the activity is connected to the life of the institution because it involves the school's own students and takes place within its facilities.
- Teachers create a variety of educational resources, including lesson plans, teaching materials, and digital content, books, and manuals for classroom use.
- A professional training organization or certifying body issues certificates, diplomas or digital badges for specific professional development programs.

The workflow of the system, illustrated in Figure 1, ensures that attestations, certificates, diplomas, digital badges, and educational resources are securely issued, recorded, and verified. The process unfolds as follows:

1. Submission
    - An administrator accesses the decentralized application (dApp).
    - Relevant data is entered into a structured form.
    - Credentials are uploaded to IPFS, which generates unique content identifiers.
    - The transaction content includes both metadata and IPFS CIDs.
2. Off-Chain Processing (Polygon zkEVM)
    - The transaction is processed by the Polygon zkEVM sequencer in an Ethereum-compatible environment.
    - Transactions are collected and aggregated into batches for optimization.
    - The ledger is updated off-chain, ensuring high throughput with minimal latency.
3. Proof Generation (zk-SNARKs)
    - For each batch, a zk-SNARK validity proof is generated.
    - This proof cryptographically demonstrates that all transactions comply with Ethereum's consensus rules.
    - Proofs are compact and non-interactive, enabling efficient verification.
4. On-Chain Verification (Ethereum Mainnet)
    - The zk-SNARK proof and minimal calldata are submitted to an Ethereum smart contract.

- Ethereum nodes verify the proof, finalizing the batch with Layer 1 security guarantees.
- The result is a tamper-proof, timestamped registration of credentials.

5. Verification and Access
   - Evaluators or institutions can verify documents by querying the blockchain.
   - The system checks metadata and IPFS identifiers against the registered transaction.
   - Any alteration attempt is immediately detectable due to blockchain immutability and cryptographic binding.

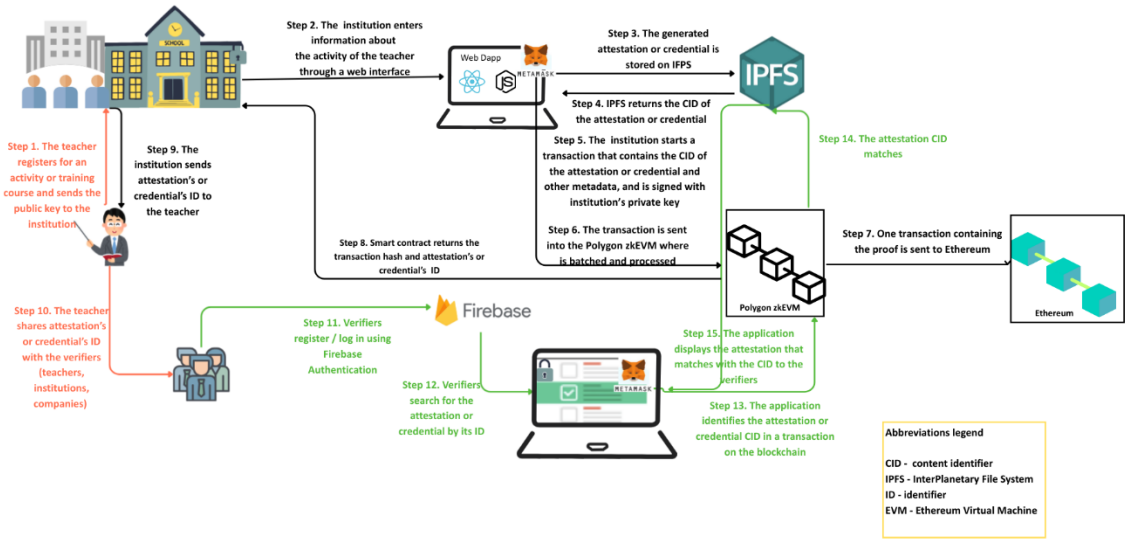

Figure 1: Overview of the proposed architecture of the issuing attestations or credentials.

The implementation of the proposed blockchain-based framework requires the integration of multiple tools and technologies, each serving a distinct role in the development, deployment, and operation of the system. The following tools were employed:

- Hardhat - Ethereum development environment for compiling, deploying, and testing smart contracts.
- Sepolia - Ethereum test network for simulating deployments without incurring real transaction costs.
- Polygon zkEVM Cardona Testnet - Layer 2 zk-Rollup environment for testing cost-efficient and scalable credential management.
- Metamask - Wallet for managing private keys and interacting with dApps.
- Alchemy - Blockchain node provider ensuring reliable connectivity to Ethereum and Polygon networks.
- Remix IDE - Online development environment for smart contract creation and debugging.
- Solidity - Programming language used for Ethereum-compatible smart contracts.

- Pinata - IPFS-based storage solution for uploading and managing decentralized educational resources.
- Visual Studio Code - Integrated code editor supporting multi-language development.
- HTML and CSS - Front-end technologies for designing the user interface of the dApp.
- Python - Back-end technology for handling server-side logic and blockchain interactions.
- Firebase - Authentication system providing secure access management for users.

Chapter 6 discusses the results of the experimental evaluation of our blockchain-based system, focusing on both performance and cost metrics.

The core of our solution relied on two smart contracts: one dedicated to managing educational resources and the other to handling credentials.

We evaluated the contract's efficiency using a custom Python script, which use Web3.py together with the EthereumTester backend to simulate transactions and capture the exact gas used values. This tool allows developers to obtain a precise breakdown of the computational costs associated with different contract operations in a controlled environment, without incurring real costs on a real network. The results, illustrated in Figure 2, reveal a clear differentiation across functions: adding a teacher consumed 52973 gas, revoking a teacher only 31397 gas, while adding an educational resource required 188777 gas, and revoking it 51014 gas.

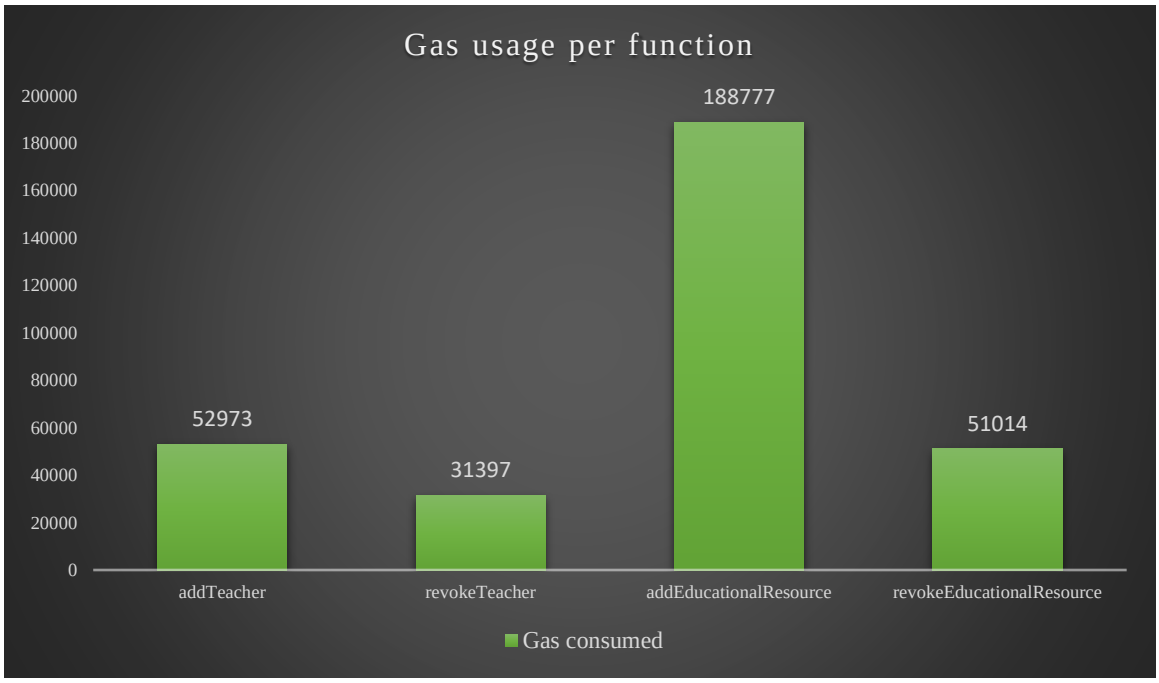

Figure 2: Gas consumed with different educational resources contract operations

To obtain a reliable estimation of transaction costs we conducted our experiments on the Sepolia testnet and on the Polygon zkEVM Cardona testnet. Transaction fees on Polygon zkEVM

Cardona are substantially lower than on Sepolia, with the Educational Resource contract costing approximately 0.056 USD and the Credential contract 0.066 USD, compared to 8.40 USD and 10.09 USD on Sepolia. This significant reduction in cost highlights the efficiency of Layer 2 solutions, making Polygon zkEVM particularly suitable for handling a high volume of transactions while maintaining affordability.

Chapter 7 addresses Objective O8 by presenting a comprehensive analysis of the security mechanisms embedded in the smart contracts that form the foundational layer of our blockchain-based system. To assess the robustness of these contracts, we utilized SolidityScan, a specialized tool for evaluating smart contract security. Our analysis shows that the Educational Resource smart contract achieves a security score of 98.19/100, while the Credential smart contract attains an impressive 98.29/100, demonstrating a high level of protection against potential vulnerabilities. The chapter also details the strategies implemented to ensure data integrity, enforce strict access control, and mitigate common threats such as reentrancy attacks, unauthorized modifications, and duplicate entries, highlighting the reliability and trustworthiness of the system.

Chapter 8 provides a thorough summary of the research conclusions, emphasizing the original contributions of the thesis.

Bibliography

[1] "The methodology and criteria for awarding the merit-based distinction to teaching staff in public pre-university education in the 2025 session," [Online]. Available: https://www.edu.ro/sites/default/files/_fi%C8%99iere/Legislatie/2025/OMEC_3745_2025_Gradatie_merit.pdf. [Accessed 30 June 2025].

[2] "Modele de cereri și anexe pentru mișcarea personalului didactic în anul școlar 2024 - 2025," [Online]. Available: https://www.isjbihor.ro/resurse/modele-de-cereri/2306- modele-de-cereri-si-anexe-pentru-miscarea-personalului-didactic-in-anul-scolar-2024-2025. [Accessed 23 July 2025].

[3] D. L. Silaghi, "Blockchain-based Solution for Protecting Teachers' Copyrights on Educational Resources," in *International Conference on Engineering of Modern Electric Systems (ICEMES)*, Oradea, Romania, 2025.

[4] A. C. Artenie, D. L. Silaghi and D. E. Popescu, "Exploring the Synergy Between Ethereum Layer 2 Solutions and Machine Learning to Improve Blockchain Scalability," *Computers*, vol. 14, no. 9, p. 359, 2025.

[5] D. L. Silaghi and D. E. Popescu, "A Systematic Review of Blockchain-Based Initiatives in Comparison to Best Practices Used in Higher Education Institutions," *Computers*, vol. 14, no. 4, p. 141, 2025.

[6] E. Durant and A. Trachy, "Digital Diploma debuts at MIT," 17 October 2017. [Online]. Available: https://news.mit.edu/2017/mit-debuts-secure-digital-diploma-using-bitcoin-blockchain-technology-1017. [Accessed 26 May 2024].

[7] P. Boulet, P. d. Coëtlogon, É. Thébault and P. v. d. Velde, "Digital transformation of certificates issued by universities for European competitiveness," 6 March 2025. [Online]. Available: https://hal.science/hal-04979478/. [Accessed 12 August 2025].

[8] "Order no. 4634 of June 10, 2024," [Online]. Available: https://www.edu.ro/sites/default/files/_fi%C8%99iere/Legislatie/2024/Ordin_4634_2024.pdf. [Accessed 15 August 2025].

[9] H. R. Penubadi, P. Shah, R. Sekhar, M. N. Alrasheedy, Y. Niu, A. D. Radhi, M. Tharwat, J. F. Tawfeq, H. M. Gheni and Azmi, "Sustainable electronic document security: a comprehensive framework integrating encryption, digital signature and watermarking algorithms," *Heritage and Sustainable Development*, vol. 5, no. 2, pp. 391-404, 2023.

[10] D. L. Silaghi, A. C. Artenie and D. E. Popescu, "Optimizing Teacher Portfolio Integrity with a Cost-Effective Smart Contract for School-Issued Teacher Documents," *Computers*, vol. 14, no. 9, p. 395, 2025.