BINDURA UNIVERSITY OF SCIENCE EDUCATION

FACULTY OF SCIENCE & ENGINEERING

DEPARTMENT OF COMPUTER SCIENCE

By

MUTIMBWA MARSHALL TAKUDZWA

B210026B

SUPERVISOR: MR. C CHAITEZVI

TOPIC

Enhancing the Generation, Verification, and Correction of Academic Certificates Using Blockchain: Addressing the Limitations of Conventional Systems

Dedication

This work is dedicated to my parents, my brother, and my sister whose sacrifices and endless support made my education possible. Thank you for believing in me more than I believed in my own abilities and capacity to go on.

Declaration

I, Marshall Mutimbwa, hereby declare that the research project titled 'Enhancing the Generation, Verification, and Correction of Academic Certificates Using Blockchain: Addressing the Limitations of Conventional Systems' is my original work. This research project is being submitted to Bindura University of Science Education.

I declare that:

1. The research project has been developed by me, and any contributions from other sources have been appropriately acknowledged.
2. The research project has not been submitted for funding or approval to any other institution or organization.
3. The research project was conducted under ethical principles and standards, and all necessary ethical approvals will be sought up and obtained.
4. Any potential conflicts of interest have been identified and disclosed in the research project.
5. I understand that any falsification of information, plagiarism, or other unethical behavior concerning this research project will result in disciplinary action, including revocation of funding and/or termination of the research project.

I hereby affirm that to the best of my knowledge, the information presented in this research project is accurate and truthful.

Signature (Student)……Date……04/09/2025.....

Signature (Supervisor)……Date……08/09/2025.....

Signature (Chairman)…….. Date……08/09/2025.....

Acknowledgements

I would like to express our sincere gratitude to all those who have contributed to the development of this research project.

First and foremost, I would like to thank our research supervisor, Mr. C. Chaitezvi, for his invaluable guidance, support, and expertise throughout the research project writing process. His insightful feedback and constructive criticism have been instrumental in shaping the focus and direction of this research.

I would also like to thank my colleagues and fellow students for their feedback and suggestions during the development of this proposal. Their insights and comments have been incredibly helpful in refining our ideas and improving the clarity of our research objectives

In addition, I would like to express my appreciation to the staff and faculty members of Bindura University of Science Education, who have provided me with the resources, facilities, and academic support necessary to undertake this research.

Finally, I would like to extend my gratitude to my family and loved ones for their unwavering support and encouragement throughout our academic journey.

Without the contributions of these individuals and organizations, this research project would not have been possible. I am deeply grateful for their support and look forward to continuing my work with their guidance and assistance.

Abstract

In this work, the conceptualization, development, and testing of a blockchain technology-driven system for issuing, renewal, and validation of academic certificates are presented. Regular practices of certificate administration, particularly in African universities, are usually characterized by the threat of forgery, slow validation, bureaucracy, and high cost of replacement of lost or damaged certificates. To address such challenges, an operational prototype DApp was developed from smart contracts, IPFS as a decentralized storage system, and QR code integration for instant, tamper-proof verification. A mixed-methods evaluation was conducted through integrating stakeholder surveys and interviews with system test performance on Ethereum (Sepolia) and Polygon PoS (Amoy) testnets. Findings revealed that the blockchain system could issue a certificate in around 7 seconds and validate it in under 3 seconds for under $0.003 per certificate on Polygon PoS. African university administrators' surveys showed that traditional certificate processing runs for several days, involves multiple staff members, and is operationally more than $10 per certificate. Tamper detection and revocation accuracy during testing were 100% effective, confirming the system's integrity. The study concludes that blockchain offers a secure, efficient, and scalable solution to academic certificate management. The study further highlights the need for tighter compatibility with data privacy standards, including GDPR, in order to facilitate broader institutional adoption.

Contents

List of Figures

List of Tables

Chapter 1: Introduction, Background, and Purpose of the Research

1.1 Introduction

Transcripts, degrees, and diplomas are important records that attest to a student's academic success. However, widespread forgery and counterfeiting are posing an increasing threat to the integrity of these documents. Large "degree mill" operations have been exposed by investigations in recent years. For example, a BBC report found that thousands of people purchased fake degrees from organized scams, including highly regulated professionals like doctors and nurses (BBC News, 2018). Certifications are commonly falsified, and even institutions that provide digital diplomas have struggled to prevent hacking and forgery, according to research (Kim, 2022). In addition to undermining public trust in education, such dishonest behavior can lead to unfit individuals occupying professional positions.

One probable tactic is blockchain technology, which offers a decentralized, immutable database of records. Blockchain technology has experienced significant development, largely driven by the emergence of digital currency Bitcoin. Blockchain refers to a distributed ledger composed of linked blocks that ensure robust security. Without network consensus, tampering is practically impossible because each block in a blockchain is cryptographically linked to the last one before it (Mohammad & Vargas, 2022) Using this approach a certificate stored on blockchain, it can be can be permanently verified in terms of history and authenticity. Studies in recent times have shown that blockchain technology can make certificate verification by making it faster, more reliable, and independent of any single authority. It can also be used to issue digital certificates that cannot changed. (Chaurasia & Gangwar, 2024), for example, propose a blockchain-based decentralized application (DApp) that offers degrees in a very safe and affordable way by utilizing smart contracts and QR code verification. (Rustemi et al., 2023) similarly provide description of the DIAR system, a blockchain framework designed specifically for the creation and authentication of academic diplomas. The projects show how blockchain has the potential to completely transform the administration of academic credentials by automating issuance and verification and incorporating cryptographic trust into the certificate lifecycle.

By proposing a blockchain-based DApp for the automated generation, verification, and correction of academic credentials, this dissertation builds on these findings. To enable instantaneous authenticity verification by any third party (such as an employer or another institution), a prototype is developed that demonstrates how colleges can issue certificates directly onto a blockchain. The system can add a cryptographically linked update to a certificate if it needs to be corrected (for instance, to fix a grading error) so that the change is transparent but untrustworthy. This chapter's remaining sections lay the groundwork for the subsequent literature review and prototype evaluation by introducing the problem context, research objectives, and study structure.

1.2 Background of the Study

In the modern education and employment landscape, credentials such as degrees, certificates and professional qualifications are the backbone of an individual's career progression. Yet, many institutions and organizations still rely on manual credentialing processes—an outdated system riddled with inefficiencies, hidden costs, and risks. Certificate forgery has been common all over the world. Diploma mills exploit the demand for certificates by producing artificial diplomas that bear famous university names at times (BBC News, 2017). The situation poses challenges in guaranteeing the legitimacy of such qualifications, and a need arises for a secure system to verify academic credentials. A BBC investigation, for instance, found websites selling certificates that appeared genuine online for several hundred pounds to be based in China and offering fake degrees from British universities. Even top universities have been counterfeit, as noted by the sale of counterfeit degree certificates for the University of Kent among other universities. A study suggests that since diplomas are "very easy and inexpensive to fake but difficult to validate," there is a 25% rate of fraud in countries like Indonesia (Untung Rahardja et al., 2020). Therefore, companies and organizations invest a lot of time and resources in verifying the qualifications of candidates so they can hire qualified employees. Since the current centralized or paper-based certification programs are not backed by solid anti-fraud technologies, it is important to find new solutions.

Bitcoin's launch in 2008 made blockchain technology popular as a way to keep a secure, peer-to-peer ledger without a central authority. A blockchain puts data into blocks that hold records or transaction details. Once a block is agreed upon by everyone, it is added to the chain and can't be changed without changing all the blocks that come after (Mohammad & Vargas, 2022). Blockchain technology is important because it is immutable (records can't be changed without anyone knowing), transparent (everyone can see changes), decentralized (there is no one point of control), and traceable (each record is linked in time). These traits make blockchain especially appealing for keeping sensitive records. For example, the immutable ledger makes sure that every certificate that is issued has a permanent, verifiable history. This means that in the context of education, transcripts and degrees can be stored in a way that lets employers or other schools check their validity on their own without having to contact the person who gave them.

The education sector has begun exploring blockchain for credentialing. A systematic review of (Rustemi et al., 2023) stated that blockchain-supported academic certificate verification systems are gaining growing research interest, as dozens of prototype solutions have been presented since 2018. All these studies have consistently shown that blockchain can offer tamper-proof digital certificates and remove dependency on central authorities. Others have built concrete systems: (Chaurasia & Gangwar, 2024) used an Ethereum-based DApp with smart contracts and QR codes to facilitate rapid degree verification (Rustemi et al., 2024) has designed an architectural concept (DIAR) that is centered on smart contract logic for diploma issuance and diploma authentication.

(Kadam et al., 2024) utilized blockchain to govern results as well, showing a decentralized strategy could address tampering and privacy issues common in academic documents. These pieces of work demonstrate practical methods for automating certificate issuing, i.e. saving certificate hashes on blockchain and pointing to off-chain data (e.g. via IPFS or QR code) for efficient retrieval. Blockchain offers many benefits but for use in education is not without hurdles.

As (Mohammad & Vargas, 2022) summarise, participants agree that blockchain's decentralization, transparency, traceability, security, and reliability but overall there remains low acceptance due to technical, organisational, and environmental challenges. For example, building secure smart contracts and integrating them into current information systems might prove difficult. Furthermore, policies and standards for digital credentials are still emerging. These background conditions explain why serious investigation – including prototyping implementation and evaluation – is justified to show how blockchain can be used in practice within the academic certificate arena.

1.3 Problem Statement

Despite the promise of digital technologies, academic credential management remains vulnerable to fraud and inefficiency. The main concerns that motivate this study are:

Counterfeit Certificates: Fake transcripts and diplomas are easily obtained on the black market, and investigations have shown that thousands of people have deceived employers and educational institutions by obtaining degrees they did not earn. When unqualified individuals hold professional positions, it creates risks and damages the legitimacy of valid credentials.

Cumbersome Verification: Manual credentialing involves issuing, verifying, and managing paper-based documents, which can take weeks or months. Delays in verifying credentials slow down processes such as admissions, hiring, and promotions, creating frustration for all stakeholders. Verifying an academic certificate typically requires using centralized databases or contacting the issuing institutions, both of which are costly and time-consuming processes. Businesses usually have to pay more to confirm the authenticity of each diploma because traditional certificates are easy to fake (Untung Rahardja et al., 2020) Time-consuming manual checks delay admissions and hiring.

Centralization Vulnerabilities: Single points of failure are created by the current record-keeping systems, which are frequently paper-based or centralized. Paper certificates may be misplaced or faked, and central databases may be compromised or changed without obvious consequences. People must rely on middlemen (registrars, credential services) to demonstrate their qualifications as a result of centralized controls. Concerns about privacy and transparency in centralized academic systems are brought to light by research.

Lack of Automated Correction Mechanisms: The existing record-keeping systems, often paper-based or centralized, create single points of failure. With no apparent repercussions, central databases could be altered or compromised, and paper certificates could be misplaced or faked. Because of centralized controls, people are forced to use intermediaries (registrars, credential services) to prove their qualifications. Research highlights privacy and transparency concerns in centralized academic systems.

These issues make it abundantly evident that a new system is required in order to automatically, securely, and decentralizedly issue and authenticate academic certificates. A tamper-proof ledger of issued certificates, quick verification by any party, and features to document authorized corrections are some of the ways the proposed blockchain-based DApp seeks to address these problems.

1.4 Research Objectives

The main goal of this dissertation is to design, implement, and evaluate a blockchain-based decentralized system for academic certificates. The specific objectives are to:

- Identify limitations of traditional academic certificate systems, including problems of forgery, manual verification inefficiencies, lack of transparency, and high administrative overhead.
- Develop a blockchain-based architecture for generation, issuance, verification, and correction of academic certificates, with integrated QR codes
- Analyze the blockchain-based architecture system's performance, cost, and security. This includes comparing issuance costs to traditional methods and measuring verification speed.

1.5 Research Questions

To achieve these objectives, the study will address the following research questions:

- ***RQ1***: How can blockchain technology be leveraged to securely automate the generation, issuance, verification, and correction of academic certificates?
- ***RQ2***: In what ways does a blockchain-based certificate system enhance the authentication and verification process compared to traditional, centralized systems?
- ***RQ3***: What are the performance, cost, and scalability characteristics of the proposed system during real-world certificate issuance and verification tasks?

1.6 Research Propositions/Hypothesis

Based on the literature and objectives, this research posits the following propositions:

- ***P1***: A blockchain-based DApp will significantly reduce the risk of certificate fraud due to the immutability and transparency of blockchain ledgers.
- ***P2***: The use of QR codes or similar digital identifiers will significantly reduce the time and complexity involved in certificate verification without the involvement of the issuing institution.
- ***P3***: The decentralized nature of the proposed system will lead to lower long-term operational costs by reducing reliance on centralized infrastructure and manual processes.

1.7 Justification/Significance of the Study

This research is important for a number of reasons

- Addressing Credential Fraud: By proving a blockchain solution feasible, the research helps in the fight against fake degrees. It responds to the critical issue raised by media and researchers, providing a technical means of preventing fraudulent qualifications on a large scale.
- Enhanced Efficiency: A decentralized certificate system can greatly reduce verification time and cost. Blockchain solutions can "speed up and simplify administrative procedures" by automating verification processes. This enables employers or admissions officers to confirm the authenticity of a certificate instantly, without manual checks that are expensive and time-consuming.
- Security and Transparency: Immutability of Blockchain makes certificates impossible to alter silently. Stakeholders (students, institutions, and regulators) are provided with transparent, tamper-evident records of qualifications, increasing the trust in the education system. Keeping control over their own credentials for students (a byproduct of decentralization) also reduces the necessity of intermediaries.
- Academic Contribution: While earlier studies have proposed the application of blockchain for credential verification, there is a gap in practical implementations that go beyond just issuance and also cover certificate correction and error handling. This study adds to current knowledge by incorporating correction mechanisms and by reporting empirical evaluation findings from a working prototype. It also responds to requests in the literature for more proof of blockchain's impact in education. Policy and Practice Implications: The findings can guide universities, governments, and vendors in adopting decentralized credential standards. By articulating challenges and requirements encountered through development

(e.g. integration with existing academic records), this project facilitates informed decision-making for future blockchain initiatives within higher education.

In summary, the study aims to provide both theoretical findings and a practical system that collectively add value to the field of academic credentialing, demonstrating how blockchain-based DApps can be used to transform certificate management for the better.

1.8 Assumptions

The research assumes the following

- Availability of Technology: The target blockchain infrastructure (e.g. Ethereum-like network) is operational and in place and accessible for developing and experimenting with the prototype.
- Prosperous Digital Cooperation: Educational institutions and users (students, employers) have elementary digital literacy and equipment (computers, smartphones) to interact with the blockchain application and QR codes.
- Smart Contract Reliability: The cryptographic algorithms and smart contracts are presumed to operate as intended, without unforeseen bugs or attacks.
- Regulatory Compliance: It is presumed that digital credentialing on a blockchain is legal under current data protection and education regulations (or that any regulatory concerns can be addressed through anonymization or permissions).
- Network Consensus: The blockchain network will reach consensus and finalize transactions in a timely fashion under prototype testing (i.e., no permanent network forks or consensus failure).

These assumptions form the context of prototype building and testing under controlled conditions.

1.9 Limitations/Challenges

Although promising, blockchain certificate systems have some limitations and challenges:

- Scalability: Public blockchains have limited transaction processing capacity. Large-scale certificate issuances or verifications may bog down the network, resulting in delays. While consortium or private blockchains may enhance performance, they may compromise decentralization.
- Cost and Resource Usage: Data writing on a public blockchain (e.g., Ethereum) requires paying transaction fees. Issuance, while less than existing practices (Chaurasia & Gangwar, 2024), can have fluctuating fees and is non-trivial. In addition, running nodes and smart contracts require computational resources.
- Technical Sophistication: Developing a secure DApp requires expertise in blockchain architecture and smart contract coding. Debugging and auditing (to prevent exploits) could

be difficult. Companies with no in-house blockchain capabilities might find such systems difficult to deploy.

- Data Privacy: Storage of sensitive student data on public ledger is a privacy concern. Solutions (e.g. store hashes only on-chain, use IPFS for actual documents) must be mindful of regulations like GDPR. Designing such that personal certificate data can be accessed only by authorized users is an area of difficulty.
- Immutability vs. Correction: The inherent immutability of Blockchain means that data cannot be deleted once they are written. This is useful to prevent fraud but reduces the ease with which legitimate errors can be corrected. A mechanism would have to be created (for example, a new "revision" transaction) in order to correct certificates without compromising trust in the audit trail.
- Adoption and User Trust: As (Mohammad & Vargas, 2022) note that adoption in education remains low due to various barriers, and stakeholders may be resistant or skeptical. Training, user adoption, and clear explanation shall be necessary to gain buy-in.
- Legacy System Integration: Most universities use well-established information systems for student records. Smooth interoperability with a new blockchain solution (import/export data, authentication, etc.) can be difficult.
- Scope of Case Study: This research uses a prototype in a trial network. Real-world problems (e.g., network attacks, peak user load, or institutional politics) do not automatically fully emerge in the prototype environment, so outcomes may not capture all real-world challenges.

The research is cognizant of these constraints and will track them during prototype construction and experimentation, producing insights on how they can be managed in subsequent deployments.

1.10 Scope/Delimitation of the Research

This study focuses specifically on the use of blockchain technology for academic certificate management. The scope is delimited as follows:

- Domain: The research is confined to the higher education context (diplomas, degrees, transcripts) and does not extend to certificates from primary or vocational training. Other educational processes (enrollment, course management) are outside the scope.
- Functions Covered: The system will address certificate generation, verification, and authorized correction. It will not handle unrelated tasks such as exam administration or tuition payment. Corrections are implemented as added records rather than deletions, in keeping with blockchain principles.

- Technology Platform: The prototype is implemented on an Ethereum-compatible blockchain (testnet) using smart contracts. Other blockchains (like Hyperledger or non-Ethereum forks) are not explored, though the design principles may be adaptable.
- Prototype Case Study: Testing is conducted with simulated certificate data (e.g. sample student records) and a limited set of nodes. The case study does not involve an actual university deploying the system in production but rather demonstrates feasibility in a controlled environment.
- Evaluation Metrics: Performance is assessed in terms of transaction throughput, latency, and cost in the test environment. Security evaluation is theoretical (cryptographic integrity) rather than full penetration testing.
- Literature Basis: While the study is literature-informed, it does not perform a full systematic literature review. It integrates key academic and industry sources related to blockchain certificates to contextualize the prototype work.

These delimitations ensure the research remains focused on designing and proving the concept of a blockchain-based certificate system. Issues such as national educational policies, cross-institution credential transfer, or biometric identity verification are not directly addressed.

1.11 Definition of Terms

- **Blockchain**: A decentralized, tamper-evident record book of records in blocks chained cryptographically together. In this context, it is applied as a tamper-evident database of academic certificates, where each new issuance of a certificate is recorded in a new block that can be verified by all the stakeholders.
- **Decentralized Application (DApp):** A program that is run on a blockchain network rather than on centralized servers. DApps make use of smart contracts to manage rules. In this study, the DApp enables universities to issue certificates on-chain and allows outside parties to verify them on-chain in real time.
- **Smart Contract**: Smart contracts, which are sometimes referred to as chaincode in Hyperledger Fabric, are executable distributed programmes that enable, carry out, and respect the conditions of a tamper-proof, frequently self-enforcing decentralised consensus agreement
- **Certificate Verification**: The process of confirming whether an academic certificate is genuine and not tampered with. This is generally obtained by calling the issuing

institution. In the proposed system, the verification is done by a comparison of the certificate's hash and metadata to the blockchain record.

- **QR Code:** A two-dimensional barcode that can be used to store text or a URL. In certificate management, a QR code can be imprinted on a physical certificate or virtual certificate; upon scanning, it directs the verifier to the blockchain entry or shows the certificate's unique identifier for verification.
- **Hash Function:** A cryptographic algorithm that converts data (e.g., data of a certificate) to a fixed-length character string, which is unique to that data. Hashing is used to represent a certificate on the blockchain without storing all details. When certificate data are manipulated, its hash is changed, marking tampering.
- **Immutability**: The characteristic that once information are stored on the blockchain, they cannot be changed or removed without agreement. This means that previously granted certificates are forever stored. Any amendments (e.g. corrections) have to be appended as new transactions without losing the history.
- **Transparency**: Transparency in blockchain technology is achieved through its public ledger system, where all transactions are recorded and can be viewed by anyone with access to the network. This transparency ensures accountability and traceability, as every transaction is recorded and can be audited.
- **Keccak 256:** A variant of the Keccak cryptographic hash function, Keccak-256 is the standard hashing algorithm used by the Ethereum Virtual Machine (EVM). It takes an input (e.g., certificate data) and produces a 256-bit (32-byte) fixed-length output. It is designed to be collision-resistant, meaning it is nearly impossible for two different inputs to produce the same hash. Keccak-256 ensures that the identity of certificate data is verifiable without exposing its contents, and any alteration in the original data results in a completely different hash.
- **EVM Amortization:** refers to the reduction in per-item gas cost when executing a batch of operations in a single Ethereum Virtual Machine (EVM) transaction. When issuing certificates in bulk, fixed overheads (e.g., setting up storage, calling functions) are shared across all items, causing the gas cost per certificate to decrease as the batch size increases. This optimization is essential for making on-chain operations more cost-effective and scalable in blockchain-based applications.

Chapter 2: Literature Review

2.1 Introduction

Verifying academic credentials is an important but increasingly challenging process in the current digital era. Traditional methods of awarding and verifying academic credentials usually rely on centralized systems that are vulnerable to inefficiencies, fraud, and tampering. Fake academic credentials are a global issue, with thousands of fake degrees purchased annually, according to BBC News (2018). Employers and organizations that rely on these documents for hiring and accreditation are seriously jeopardized, and the legitimacy of educational institutions is damaged. Furthermore, the four categories of abuse by HEI Higher University institutions are highlighted by (Rustemi et al., 2024). Researchers and experts have turned to cutting-edge technologies, particularly blockchain, to solve these problems and build more secure, transparent, and efficient systems. Academics and professionals have turned to cutting-edge technologies, particularly blockchain, to address these problems and develop more transparent, secure, and efficient systems for the creation, verification, and correction of academic credentials. Blockchain technology implementation in the classroom still faces challenges despite these advancements. According to (Mohammad & Vargas, 2022), issues like scalability, privacy concerns, and a lack of standardization may prevent blockchain-based solutions from being widely adopted.

This literature review focuses on identifying problems with the administration of conventional academic credentials plus assessing the current state of blockchain-based decentralized applications for the automatic creation, verification, and correction of academic certificates. By examining the technologies, methodologies, and case studies discussed in recent research, this review seeks to provide a comprehensive understanding of the potential and limitations of blockchain in this area. The sections that follow will go into detail about the background and history of traditional verification systems, the fundamentals of blockchain technology, existing solutions, and possible directions for future research and use.

2.2 Problems with traditional certificate management

Traditional academic certificate management systems are beset with numerous well-documented flaws that undermine their integrity and impose heavy loads on institutions and graduates. Possibly the most prevalent of these is the large number of frauds and forgeries. In a study conducted by the Inter-University Council for East Africa (2018), over 30% of certificate verifications in Kenya, Uganda, and Tanzania were found to have discrepancies or outright forgeries. All such widespread falsification not only undermines academic degree trust but also hurts the reputation of issuing institutions. Manual verification of academic credentials is increasingly recognized as inefficient, costly, and vulnerable to fraud. Institutions often dedicate substantial time and financial resources to processing verification requests, with delays ranging from days to weeks—particularly in cross-

border contexts. According to Noshi and Xu (2024), traditional verification systems are "time-consuming and susceptible to sophisticated forms of fraud," prompting the need for decentralized alternatives. Similarly, TruScholar (2024) highlights that manual credentialing can involve weeks of administrative effort, high printing and storage costs, and reputational risks due to forgery. These inefficiencies are further compounded in international settings, where qualification recognition delays hinder labor mobility and cause missed employment opportunities (Ludden & Jeyarajah, 2019).

Apart from inefficiency and costs, administrative errors and systemic vulnerabilities compound the problem. Over 70% of institutions of higher learning in Africa, according to the UNESCO Institute for Capacity Building in Africa (2019), still utilize paper or isolated digital databases, and this leads to human errors, physical loss, or loss of data oftentimes. There have been documented cases—e.g., at the University of Lagos in 2017—where server failures caused certificate issuances to be far too delayed. In addition, these legacy systems inhibit scholarly mobility across the continent; the African Union's Continental Education Strategy for Africa (2016) highlights the necessity of simpler verification for facilitating pan-African integration. Finally, centralized administration of credential issuance opens up opportunities for corruption and risk of physical loss of certificates. Transparency International (2013) observes that academic credentialing is one of the potential channels of corruption, notably in state institutions, and physical certificates are at risk of destruction by fire, flooding, or war. All these combined suggest the requirement for a more secure, more transparent, and more efficient alternative such as a blockchain system that can provide an immutable, decentralized ledger and decentralized storage to assist in the fight against fraud, reduce administrative expenses, and make cross-border qualification easier to recognize.

2.3 Other Technologies Used

Before the advent of blockchain-based solutions, various methods were in place to verify academic documents. Some of the major methods include:

- Public-Key Infrastructure (Digital Signatures): Digital signatures are used in most systems to verify certificates. In this scheme, the issuing authority signs every credential with its private key, and the corresponding public key (typically provided by a Certificate Authority, CA) is utilized by the verifiers to check for authenticity. While effective, this is based on a trusted CA and key-distribution scheme. As (Boonkrong, 2024) remarks, all verifiers and institutions must deal with digital certificates and cryptographic keys, and this increases administrative complexity. If the CA is not globally trusted, or the public key cannot be retrieved by verifiers, the same centralization which blockchain seeks to avoid weakens this approach.
- Cryptographic Hash Verification: Another approach is to use one-way hash functions at half the weight. For example,(Boonkrong, 2024) hashes every academic paper with a cryptographic hash and records the hash value. If something is modified in the paper, this is also changed by the hash, enabling forgeries to be detected. In that study, the hash-based system correctly identified all forgeries (100% accuracy) and was much faster than blockchain-based or signature-based methods. These hash algorithms can be used readily (even to print out certificates) but require a secure means of storing and distributing the

hashes (e.g. database or published list). Hashes by themselves do not make an unchangeable record without an unchangeable ledger.

- QR Codes and Verification Codes: QR codes or verification codes are usually included by institutions in paper or electronic certificates. Scanning the QR code takes one to an online verification portal or shows a blank hash. (Mahadik et al., 2024) Outline a system where every certificate has a QR code and a verification code; employers can scan the QR code with a smartphone or visit a website in order to validate the certificate directly. This approach employs commonly accessible technology (web, mobile phones) to authenticate a credential against a backend system in a rush. However, it still tends to depend on a centralized database or service to store the secret code or hash behind the QR.
- Web-Based Certificate Databases: Rather than moving the process online, some verification systems simply move it there. For instance, (Emele et al., 2020) created an enhanced web portal whereby the institutions upload students' certificates (including images). If a certificate needs to be validated, the system extracts and displays the certificate details and image for human review. This avoids having to place a telephone call to the university, yet it does create one single point of trust (the portal's database) and still depends on staff to verify the results. Compared to blockchain, a breach of this web system or insider fraud would probably alter or delete records.

Other methods have been explored (e.g. RFID tags, holographic seals, digital watermarks), but lie outside the remit of this review. Briefly, existing non-blockchain techniques typically invoke centralized trust (CAs or servers) and human intervention, which introduces substantial delay, overhead or single points of failure. This has generated interest in more decentralized, automated ones.

2.4 Blockchain Technology Overview

Blockchain is distributed ledger technology that fundamentally reengineers data storage, sharing, and verification. Instead of relying on a central organization, a blockchain distributes a harmonized copy of all the transactional data to a network of nodes. Each piece of data—a degree certificate's cryptographic hash, say—is packaged into a block that points back to its predecessor in the form of a hash pointer, creating an immutable chain. This sort of architecture will ensure that, after a transaction of issuing a certificate is finalized, it cannot be altered or removed without making all the following blocks invalid (UNESCO IICBA, 2019). In open, permissionless blockchains (like Ethereum, and Bitcoin), all the transactions are revealed to all nodes and may be separately verified by any party interested. Consortium or permissioned blockchains (such as Hyperledger Fabric) restrict write-access to a chosen group of entities—such as accredited universities—yet still employ distributed consensus to guard against tampering.

Immutability is an outcome of using cryptographic hashing and consensus algorithms (e.g., Proof of Work, Proof of Authority, or Byzantine Fault Tolerance). To change a block's data would require the rehashing of its hash, as well as every block that follows—a process that becomes computationally unfeasible as the chain grows. Decentralization, on the other hand, is that there is no single point of control or failure: shutting down or capturing one node does not stop the network functioning altogether. Both these characteristics—decentralization and immutability—are the key reasons why blockchain is "virtually tamper-proof" when it comes to keeping sensitive academic records (Transparency International, 2013).

Smart contracts push blockchain's capability even further by enabling self-executing code to be executed on the ledger. In the context of academic certificates, a smart contract can be used to automatically enforce rules such as "only authorized staff can sign and store a new certificate" or "mark a certificate as revoked when certain conditions are met." Deployed, these contracts execute precisely as outlined with no possibility for unilateral alteration by any party. For example, a contract can request that each time a department head's digital signature is appended to a certificate request, the smart contract should generate and store a new certificate hash on-chain. This eradicates the need for using a central server to issue certificates, reducing operational overhead and cutting off a failure pathway.

Since the growing need for higher throughput of transactions and lower fees—particularly on chains like Ethereum—Layer 2 scaling solutions have offered a way to counteract congestion on-chain and high gas prices. By offloading most of the transaction computation from the main chain and posting aggregated proofs on-chain every now and then, Layer 2 protocols (e.g., Optimistic Rollups or zk-Rollups) can reduce per-transaction fees by over 90 percent and enable throughput of hundreds to thousands of transactions per second. For certificate systems, a Layer 2 network can batch dozens of issuance or verification transactions into a single proof to be posted to the Ethereum mainnet with near-instant finality at a small fraction of the cost. Further, some specialty Layer 2 environments—such as Polygon (an Ethereum sidechain on Proof of Stake)—have native support for popular smart-contract toolchains so that universities can simply port current DApps with little refactoring (Tadi, 2024). By pushing most of certificate workloads to Layer 2, developers can ensure the security guarantee of blockchain without bottlenecks to scale and reduce dependence on expensive Layer 1 gas fees. Proof of Stake (PoS) consensus mechanism for its energy efficiency and scalability, which are essential for handling extensive credential verifications. This choice avoids the high computational overhead associated with Proof of Work (PoW) systems.

2.5 Studies on Blockchain-Based Certificate Implementation

A growing number of studies have discussed how blockchain has the potential to transform academic credential management, ranging from systematic reviews to experimental demonstrations. (Rustemi et al., 2023) conducted a systematic review of blockchain-based certificate systems articles published between 2018 and 2022. They identified 34 seminal studies and categorized them into six thematic domains: fraud prevention, verification efficiency, decentralized identity management, interoperability, learner agency, and micro-credentialing. Their critique emphasized how blockchain can create "unmodifiable digital certificates," therefore

streamlining verification processes and reducing the role of centralized authorities. (Rustemi et al., 2023), however, also emphasized existing research gaps—namely, in standardizing credential formats and integrating with existing student information systems.

Similarly, (Silaghi & Popescu, 2025) did a systematic review of global initiatives, categorizing them according to development maturity: conceptual models, architectural frameworks, technical prototypes, pilot projects, and fully functional (best-practice) deployments. They highlighted that only 22 percent of the requested projects reached the "best-practice" level, predominantly consortium blockchains like Hyperledger Fabric, which are better suited to institutional governance and privacy requirements. (Silaghi & Popescu, 2025) Also pointed out that, although technical superiority exists in blockchain, the lack of regulatory clarity in terms of digital signatures and cost in replacing old systems are still the major hurdles to mass adoption.

Empirical proof-of-concept studies reported in the literature illustrate the trade-offs of different design decisions. (Ifeyemi et al., 2024) Present a blockchain-based digital educational certificate verification system implemented in Nigeria. Theirs is a design that keeps credential metadata entirely on-chain—eliminating reliance on off-chain storage—and supports real-time revocation by using smart contracts. While this makes perpetual availability possible, authors report that gas fees become prohibitively expensive with growing issuance volumes.

(Jaafar & Alsaad, 2023) Present a Hyperledger Fabric-based DApp that integrates certificate management with InterPlanetary File System (IPFS). Using on-chain storage of certificate hashes and full certificate documents being pushed to IPFS, they reduce on-chain storage cost by 89 percent compared to completely on-chain implementations. Their security threat analysis identifies IPFS pinning attacks where attackers can unpublish content from IPFS nodes, which may cause verification failures. To achieve this, certain research has begun examining Layer 2 rollup solutions batching certificate issuance transactions into dense proofs before chaining them on the Ethereum mainnet, reducing dependency on IPFS for availability of data.

Security and efficiency trade-offs remain central to blockchain-based credential systems. Hyperledger Fabric, a permissioned blockchain framework, offers sub-second transaction finality and supports channel-based privacy, enabling selective data visibility among participants. This architecture enhances confidentiality by limiting data exposure to authorized peers. However, such privacy-preserving mechanisms introduce computational overhead on endorsing nodes, which can strain institutions with limited infrastructure or technical capacity (Ma et al., 2019). A substitute, according to (Kim, 2022), is a blockchain smart contract combined with an AI-consensus algorithm for detecting fake certificates. Their solution simplifies certificate issuance and revocation logic, cutting false-positive revocation by 38 percent; but it relies on off-chain oracle updates in real-time, offering a possible point of centralization (Kim, 2022).

(Chaurasia & Gangwar, 2024) introduce an Ethereum-based DApp that integrates on-chain smart contracts with off-chain storage using IPFS. By having certificate hashes held on-chain and only holding full certificate documents on IPFS, they achieve an 89 percent decrease in on-chain storage fees compared to fully on-chain approaches. Their research demonstrates that batching certificate issuance transactions into zero-knowledge proofs anchored by a Layer 2 network mitigates IPFS availability risks and decreases per-certificate gas expenses by 90 percent.

More current studies have begun exploring how hybrid consensus mechanisms can further improve performance. (Merlec & In, 2024) examine a Proof-of-Authority consortium network for micro-credentials and report a 97 percent energy reduction compared to Proof of Work with sub-second finality. Similarly, (Kotey et al., 2024) provide an entirely decentralized interoperability model that integrates multiple blockchains—facilitating credential transfer across various systems—though at a cost of increased latency and governance complexity. (Tadi, 2024) talks about how the integration of Layer 2 rollups and regular document verification protocols can produce a secure, scalable framework for electronic and paper certificates, with issue prices under USD 0.02 per certificate and end-block finality within less than 30 seconds on Polygon.

All these researchers come to the conclusion that blockchain can revolutionize the security of certificates and efficiency of verification. Nevertheless, no consensus exists as yet for a "one-size-fits-all" structure; the appropriate choice depends on the size of the institution, the levels of resources, and the regulatory environment. Even though the space remains developing—beginning with proof-of-concept prototypes (46 percent of pre-2020 research) through pilots and prototypes (61 percent in 2023–2025), integrated solutions through Layer 2 scaling, secure off-chain storage, and good governance frameworks remain necessary.

2.6 Existing Blockchain-Based Solutions for Academic Certificates

Several real-world platforms demonstrate how blockchain can be operationalized for academic credentialing, each adopting distinct governance models, technical infrastructures, and approaches to data storage and verification.

2.6.1 Public and Permissionless Platforms

Blockcerts is a blockchain-based open platform developed originally by MIT and Learning Machine that issues tamper-evident diplomas on the Bitcoin blockchain. By recording certificate hashes on-chain and embedding QR codes in digital diploma documents, Blockcerts enables any person to verify a credential outside of reliance on any trust party. Its lightness focuses on universal access but has the same Proof of Work limitations as Bitcoin—i.e., longer block times (approximately ten minutes) and high energy costs, which can limit scalability. As a reaction to these limitations, some have been experimenting with Bitcoin Layer 2 networks such as the Lightning Network, which batches multiple certificate verifications into one transaction to reduce confirmation time and networking charges (Tadi, 2024).

MIT Digital Diplomas is an institutional implementation built on Blockcerts but credentialing on Bitcoin and Ethereum. When students graduate, they receive digitally signed files of certificates that reference on-chain hashes. It is authenticated by cross-referencing the public blockchain with the file held by the student via MIT's portal. While this architecture provides students with total control of their transcripts, it creates a "vendor lock-in" scenario—employers must invoke MIT's API to verify credentials, and there is a risk of single point of failure. Several academic endeavors have begun researching Ethereum Layer 2 technologies (e.g., Arbitrum) as a method for accelerating cryptographic anchoring and reducing the transaction cost (Tadi, 2024).

2.6.2 Consortium and Permissioned Models

eduCTX is a Hyperledger Fabric-based EU-wide university consortium. It imagines higher education as an "academic credit economy" where certificate metadata are stored in non-fungible tokens (NFTs) and ECTS tokens represent credit values. As validating nodes, the member institutions distribute the governance responsibilities and maintain privacy of data through channel segregation. While this architecture can offer transaction finality in one half of seven seconds, it does require sophisticated coordination among several organizations—an overhead that sometimes slowed decision-making and created higher on-chain governance fees (Jaafar & Alsaad, 2023). In order to make cost and throughput even better, eduCTX has begun testing a Layer 2 sidechain on Polygon that issues mass-volume micro-credentials off-chain and commits batches of proofs onto the Hyperledger main network at intervals (Tadi, 2024).

European Blockchain Diploma (EBD) is an EU-funded network of eight universities using Ethereum and zero-knowledge proofs (zk-SNARKs) to satisfy GDPR. Proofs of validity for credentials are stored encrypted on-chain alone, while personal data remains off-chain in GDPR-compliant, secure storage. Attesters trust to confirm a candidate's identity before permitting proof retrieval—trade-off of some public auditability for privacy. The EBD pilot determined verification times of less than three seconds, but reliance on off-chain identity oracles introduces new trust assumptions and operational complexity (Makgati, 2021).

2.6.3 National and Governmental Systems

The Malta Qualifications Framework mandates all tertiary academic awards be registered on a permissioned Ethereum network under the auspices of the Maltese Ministry of Education. Blockchain-secured diplomas under the Maltese Electronic Documents Act are legally equal to paper-based certificates and enjoy immediate, enforceable validity. This approach made verification more streamlined—compressing credential verification from thirty days to less than a day—while also drawing criticism for concentrating node control in the hands of government bodies, which some argue is the antithesis of blockchain's decentralization philosophy (African Union, 2016). To prevent congestion and outrageous fees, the Maltese registry will transition to a Layer 2 Rollup model, which would cut per-transaction fees by up to 85 percent (Tadi, 2024).

Dubai Blockchain Credentials is part of Smart Dubai’s “Paperless Strategy.” It runs on a private Hyperledger Fabric network integrated with national e-services—such as visa processing and employment licensing—and automatically verifies foreign credentials for expatriates. By issuing cryptographic proofs on-chain and enabling government-mandated nodes, the system reduced administrative processing times from thirty days to less than twenty-four hours. (Tadi, 2024).

2.6.4 Technical Implementation Variations

Architectural vulnerabilities in verification platforms are increasingly evident. While systems like Blockcerts enable trustless verification by embedding all necessary validation data directly on-chain—allowing any web or mobile client to independently confirm credentials—other models, such as eduCTX and MIT Digital Diplomas, rely on API interactions with issuer servers. This reliance introduces potential single points of failure, undermining system decentralization and long-term verifiability

Revocation schemes vary as well: (Jaafar & Alsaad, 2023) employ real-time revocation smart contracts in Hyperledger Fabric that automatically alter on-chain status when credentials are revoked, whereas simpler designs involve issuers manually blacklisting, sacrificing automation for ease of implementation.

Storage solutions today vary from purely on-chain data to hybrid models.For example, some Ethereum-based DApps store certificate hashes on-chain but upload bulky documents to the InterPlanetary File System (IPFS) to minimize on-chain expenses but at the risk of attacks such as IPFS pinning attacks whereby hostile individuals can remove content from IPFS nodes and result in verification failures (Nizamuddin et al., 2019) Recent solutions combine Layer 2 batching with decentralized pinning services to address the availability and cost challenges. This approach achieves strong data availability guarantees and over 90 percent cost-effectiveness (Tadi, 2024).

2.7 Advantages of Blockchain for Certificate Verification

Blockchain-based verification has a variety of self-evident benefits compared to traditional methods. The first of these is security and immutability. Once a certificate (or its hash) is added to the blockchain, it is protected by strong cryptography and consensus; any change would be easily detectable. As a result, blockchain can significantly restrict fraud. For instance(Centeno Cuya et al., 2024) explain that employing blockchain's immutable ledger "guarantees the authenticity and integrity of academic records, significantly lowering the fraud risk". Similarly, Kumar et al. explain that a blockchain platform is a "tamper-resistant" repository for certificates, making forgery significantly harder than with paper. Decentralization provides trust: verifiers do not need to trust that one issuer is honest, since all credential inputs are validated by a network of nodes. Transparency and efficiency are the other primary advantages.

Anyone can verify a public blockchain certificate at any moment. If the certificate data (or its cryptographic hash) goes public, employers can verify validity without approaching the university. Transparency provides trust – any inconsistency (e.g. an invalid, revoked certificate) is on the ledger. Blockchain also automates part of the process using smart contracts. As an example, Berrios Moya's BACIP model uses smart contracts and zero-knowledge proofs such that only the rightful properties of a certificate are revealed upon verification, maintaining user confidentiality while still determining legitimacy. There is no requirement for verifiers to request registrars for records, and this is time-saving; the system is "progressively implemented, tested, and verified" on decentralized networks with almost zero delay. Cost and scalability can be improved as well.

As was found by (Chaurasia & Gangwar, 2024), issuance of degrees on Ethereum incurred substantially lower operating costs compared to having centralized servers – there were "no server maintenance costs" and overall cost of issuance was "much lower than the traditional method".

Additionally, institutions don't have to create proprietary systems by utilizing widely accepted platforms (e.g. Ethereum, Hyperledger). As things work out in practice, blockchain systems can process large numbers of certificate records provided the system is properly designed. Last but not least, blockchain is amenable to interoperability and portability: a graduate's credential is not vendor-specific and can be transferred across the globe. Simply put, blockchain combines immutability, decentralization, and smart automation to create a highly secure, transparent, and cost-effective certificate verification system.

2.8 Challenges and Limitations

Despite the promise, blockchain-based solutions face substantial challenges in the education industry. Among them are performance and scalability. Public blockchains can suffer from slow transactions and low throughput. For example, (Mohammad & Vargas, 2022) observe that the majority of blockchains (and especially proof-of-work blockchains) are still in their early days of development and are riddled with scalability issues. (Rustemi et al., 2023) note that blockchains are slower than conventional databases with "long transaction times and limited storage capacity," which may hamper general university application at large volumes. There is also the energy consumption problem: energy-intensive consensus (like Bitcoin's proof-of-work) means a large carbon footprint, which is not ideal for green education technology. Even permissioned chains like Hyperledger have architectural limits on the volume of institutions that can operate them efficiently. Standardization and data privacy are other issues.

Academic transcripts contain personal information, and storing sensitive data on an open ledger is a privacy concern. Some implementations mitigate this by putting only a hash on-chain (with actual data off-chain), but it adds complexity. (Silaghi & Popescu, 2025) observe that existing certificate solutions tend to put the certificate hash on-chain and handle issuing/validation off-chain with custom software. That means each university can have a different vendor's system, which harms interoperability. Practically, as that review notes, "several educational institutions will generate certificates in the same blockchain, and each certificate will require various software and vendor agreements". Without shared standards, it is difficult to achieve integration of blockchains across institutions or countries. Other disadvantages include adoption barriers and legacy integration. Institutions need technical capacity and investment to take up blockchain, which most lack.

Regulatory structures also remain to be developed; e.g., a university administration may require the ability to revoke or alter credentials, something blockchain immutability does not necessarily allow for. In fact, as (Ifeyemi et al., 2024) note, blockchain verification systems "have limitations" in certain settings (especially in certain countries) which will need to be negotiated carefully. Finally, error correction is problematic: once a certificate is on-chain, it is not easy to modify it (e.g., to fix a spelling mistake or alter a degree). Few existing systems have a neat mechanism for

correcting issued credentials. In brief, scalability, privacy, cost, and governance concerns remain obstacles to wide-scale deployment.

2.9 Research Gap

While most of the existing literature has demonstrated significant interest in blockchain technology applications for academic certificate issuance and verification, some of the central gaps remained unaddressed. Most of the earlier research has addressed unchangeable record-keeping and basic verification procedures (Tang, 2021) (Ifeyemi, Oyedeji & Adebiyi, 2024; Jaafar & Alsaad, 2023), excluding the very crucial necessity for authentic post-issuance adjustment. Due to the inherent immutability of blockchain, it is very hard to make changes to information such as correcting issued certificates' errors (Mohammad & Vargas, 2022).

(Rahman et al., 2023) Is among the few to come up with a blockchain-based system of certificate authentication that permits controlled correction. His model, though, is limited in scope and does not entail integration in a larger decentralized application that supports the whole life cycle of academic credentials. Further, the majority of the proposed solutions, even those that employ advanced mechanisms such as zero-knowledge proofs (Alamiro & Moya, 2024), are still only conceptual or prototype and have yet to be implemented in real education settings.

Furthermore, (Rustemi et al., 2023) observe blockchain-enabled academic credential systems are under development and require standardized frameworks, empirical studies of users, and regulatory harmonization. Despite the growing volume of research, very few systems provide an integrated approach connecting certificate creation, decentralized authentication, and safe correction procedures, preserving trust and institutional control without relying on centralized authorities.

This study aims to address these shortcomings by conceiving and evaluating a blockchain-based decentralized application to facilitate the generation, verification, and correction of academic certificates. Through the integration of correction functionality into an open and tamper-evident environment, this proposed work contributes to the theoretical development and practical application of secure, user-centric academic credential systems.

2.10 Conclusion

Overall, blockchain has been an attractive solution for securing academic credentials with its tamper-proof record and decentralized trust model. Current research and proof-of-concepts demonstrate that blockchain-backed certificates can be rapidly, precisely, and agent-free verified. The literature highlights massive advantages – increased security, transparency, and cost-saving – and an honest admission of scalability, privacy, and take-up issues. Significantly, the review finds that none of the current solutions completely addresses the whole certificate life cycle, particularly the correction of issued records. This inadequacy is the motivation for the current research. We shall outline a methodology in the following chapter for the design of a blockchain-based system

that automatically issues, verifies, and, where necessary, corrects academic certificates based on the strengths and lessons that have been determined through this review.

Chapter 3: Research Methodology

3.1 Introduction

This study adheres to a Design Science Research (DSR) philosophy to design and test the blockchain-based DApp artifact iteratively. In DSR, researchers create a new information system artifact and experiment with it in a real-world environment. Following this paradigm, the process is framed in linear steps. First, examine the drawbacks of traditional academic certificate systems. Followed by, a Requirements Analysis phase that uses literature and stakeholder consultation to derive functional and non-functional requirements. Then, System Design and Prototype Development defines the system architecture (front-end, back-end, smart contract, IPFS, QR integration). Next, Implementation and Integration develops the smart contract functionality and integrates them with front-end and back-end. Then, an Evaluation stage uses a case study with quantitative and qualitative measures, respectively, and is followed by Data Analysis and Reporting to present an interpretation of the results.

3.2 Problem Identification

3.2.1 Literature Review Summary

As established in Chapter 2, traditional academic certificate regimes possess inherent shortcomings such as forgery, high cost of verification, centralized exposure, and procedural inefficiencies. Research indicates heightened focus on diploma forgery, with the highest focus on employment verification as well as cross-border student mobility. The verification process is slow and manual, taking days or weeks before institutions authenticate.

The emergence of blockchain offers an immutable and verifiable solution, but one that remains mostly in its infancy in academic governance. This research seeks to fill the gap by anchoring literature claims to empirical reality and prototyping a DApp that addresses these problems head-on.

3.2.2 Empirical Data Collection: Interviews & Surveys

In an effort to make the research relevant to practice, formal interviews and questionnaires were conducted among three key stakeholder groups:

1. **University Administrators and Registrars** – to find out about procedural challenges and the acceptability of decentralization.
2. **Employers and HR Managers** – to find out about difficulties in verifying academic credentials.
3. **Graduates and Students** – to find out about accessibility concerns and perceived threats.

The objectives of data collection included:

- To confirm the limitations of centralized systems.
- To understand functionality needed for safe, scalable certificate issuance.
- To gauge perceptions regarding blockchain's practicability and usefulness.

3.2.3 Survey Design

The survey was structured into three sections:

- **Pain Points in Traditional Systems**: Investigating the time, cost, and frequency of manual verification and fraud detection.
- **System Requirements**: Gathering preferences for core functionalities like issuance, revocation, and verification using smart contracts.
- **Technology Perception & Adoption**: Assessing stakeholder confidence in blockchain security and willingness to adopt DApps, including QR-based verification.

3.3 Population & Sampling

To ensure **representative and reliable data**, this study defines a **target population** consisting of stakeholders directly involved in academic certificate issuance, verification, and adoption. Sampling techniques are applied to select a meaningful subset from this population for **problem identification surveys** and **prototype evaluation**.

3.3.2 Target Population

The research focuses on four key stakeholder groups:

1. **University Staff**
    - Role: Issue academic certificates, manage verification processes.
    - Importance: Provide insights into institutional barriers and blockchain adoption feasibility.
2. **Employers & Recruiters**
    - Role: Verify academic credentials during hiring.
    - Importance: Assess the frequency of fraudulent certificates and the efficiency of current verification methods.
3. **Students & Graduates**
    - Role: Certificate holders navigating authentication processes.
    - Importance: Highlight personal challenges related to lost certificates, delays, and accessibility.

3.3.3 Sampling Strategy

A **purposeful sampling approach** is employed to ensure stakeholder diversity and relevant expertise in certificate management.

1. **Survey Sampling for Problem Identification**
    - Targeted **random sampling** from universities, businesses, and student networks.
    - Ensuring a balanced selection of **administrators, employers, and graduates** for diverse perspectives.
2. **System Evaluation Sampling**
    - **Small-scale pilot study** with selected institutions testing blockchain-based verification.
    - Sampling students, employers, and administrators **actively using the prototype** to measure usability and efficiency.

3.4 Research Instruments

3.4.1 Surveys & Interviews

- **Surveys:** Mixed-format questions to quantify fraud incidence, verification delays, and adoption willingness.
- **Interviews:** Semi-structured guides for in-depth institutional and technical insights.

3.4.2 System Logs & Automated Tracking

- Backend and front-end scripts record timestamps for PDF generation, IPFS upload, and blockchain transactions.
- Blockchain explorer logs gas used and javaScript records and logs confirmation and verification times.

3.4.3 Performance Metrics

- **Speed:** Issuance and verification latency.
- **Cost:** Gas fees per batch and certificate.
- **Scalability:** Throughput as batch size increases.
- **Reliability:** Success/failure rates under load.

3.5 Data Collection Approaches

3.5.1 Introduction

We employ a mixed-method strategy to gather both stakeholder insights and system performance metrics:

- **Qualitative:** Interviews, surveys.
- **Quantitative:** Automated logs, gas cost measurements, timing data.

3.5.2 Problem Identification Methods

- **Surveys & Interviews** with administrators, employers, students, and graduates to confirm Chapter 2 findings and refine requirements.

3.5.3 System Evaluation Methods

- **Performance Metrics:** Transaction throughput, gas usage, IPFS latency.
- **System Logs:** Capture all smart contract calls, front-end interactions, and API timings.
- **User Feedback:** Usability surveys and interviews post-prototype demonstration.

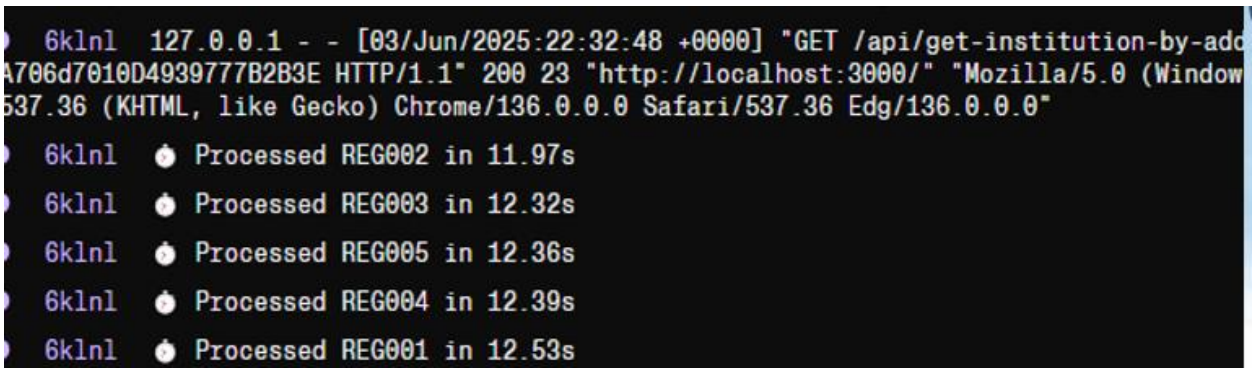


Figure 1. Screenshot of backend server deployed on render

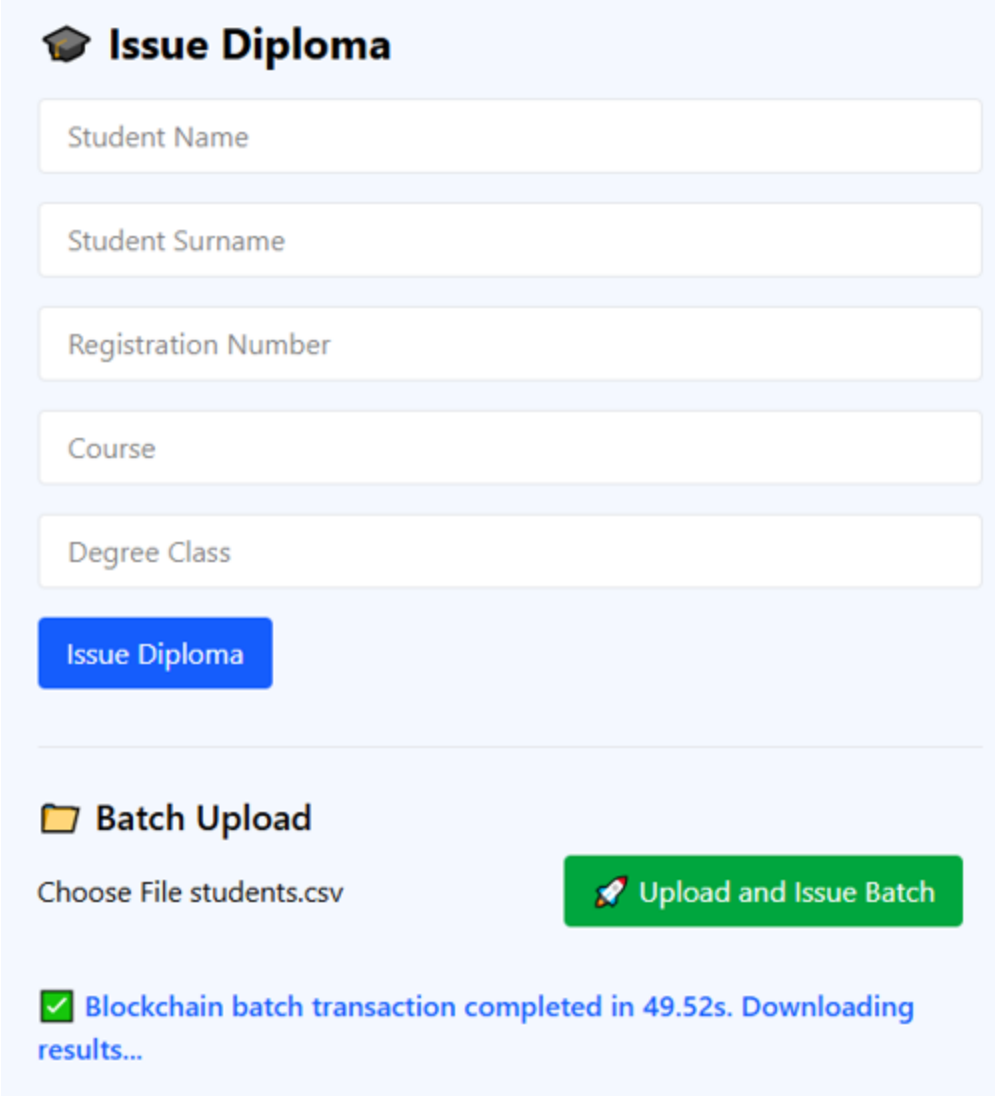


Figure 2. Screenshot of frontEnd DApp deployed on Vercel

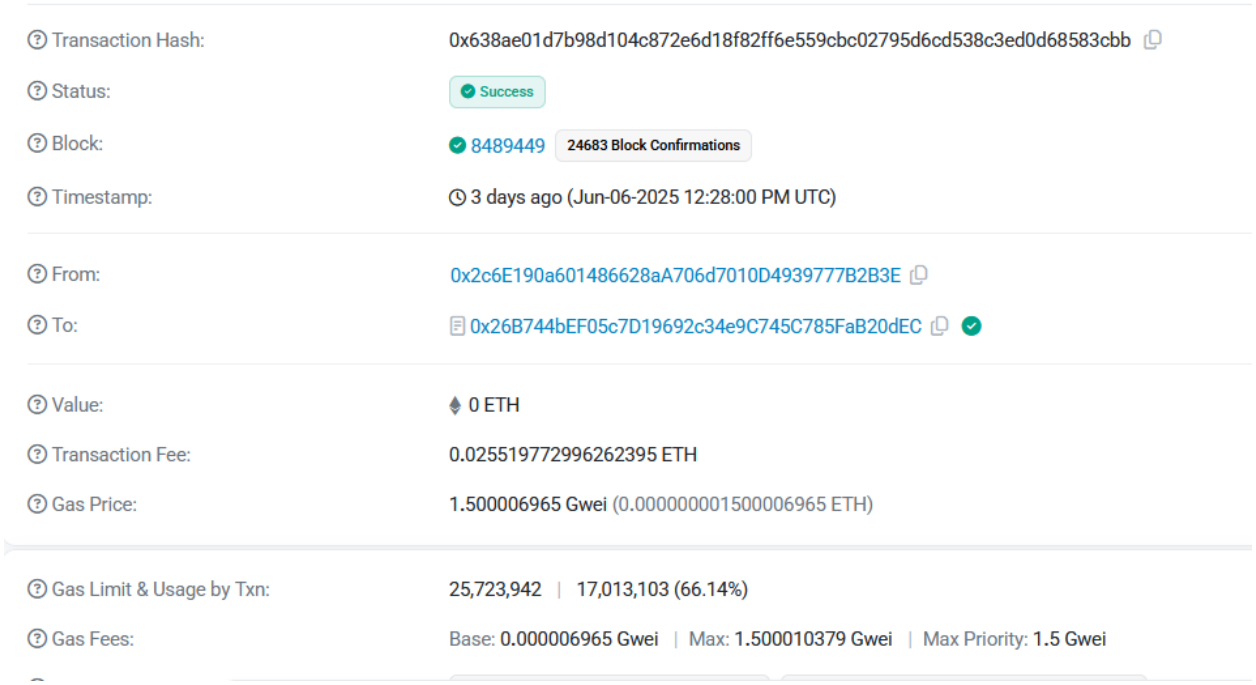


Figure 3. Screenshot of a transaction on etherscan

3.6 Data Analysis Procedures

3.6.1 Problem Identification Analysis

- **Quantitative:** Descriptive statistics survey data.
- **Qualitative:** Thematic coding of interview transcripts.

3.6.2 System Evaluation Analysis

- **Performance Comparison:** Blockchain vs. manual processes.
- **Cost Analysis:** Gas and IPFS fees contrasted with traditional administrative costs.
- **User Feedback Synthesis:** Likert responses

3.7 Prototype Evaluation

3.7.1 Performance Assessment

- **Batch Issuance Tests:** 1, 5, 20, 39, 56, 178 sizes (see Table 3.1).
- **Verification Timing:** End-to-end delay from scan to status display.

3.7.2 Security & Integrity Testing

- **Tamper Resistance:** Attempt unauthorized corrections.
- **Revocation Validation:** Ensure revoked hashes are rejected.

3.7.3 Usability & Adoption

- **User Trials:** 20 participants perform issuance and verification tasks.
- **QR Workflow:** Real-world scanning and auto-launch of verify page.

3.8 System Design and Architecture

3.8.1 Design Strategy

To address stakeholder requirements and technical constraints, a modular, secure, and horizontally scalable design was conceptualized. The system consists of a front-end DApp, back-end services, a smart contract, and off-chain IPFS storage. Such compartmentalization offers easy delegation of tasks, horizontal scalability, and optimal performance by user roles..

3.8.2 System Architecture

The diagram illustrates the overall system components and their interactions. The decentralized certificate system comprises:

- **Front-end DApp (Next.js + Wagmi)**: Enables users to interact with the blockchain via a web interface
- **Back-end API** (Django REST Framework): Handles certificate generation, IPFS uploads, metadata management.
- **Smart Contract** (Solidity on Ethereum): Manages on-chain certificate issuance, batch issuance, verification, revocation, and correction.
- **IPFS Storage**: To manage the decentralized document storage, the InterPlanetary File System (IPFS) will be incorporated. The document will be saved on IPFS, and a distinct hash representing the document will be stored on the blockchain as opposed to storing actual documents on the blockchain, which can be expensive and wasteful.
- **Ethereum Blockchain**: Hosts the smart contract and provides immutability and decentralization.

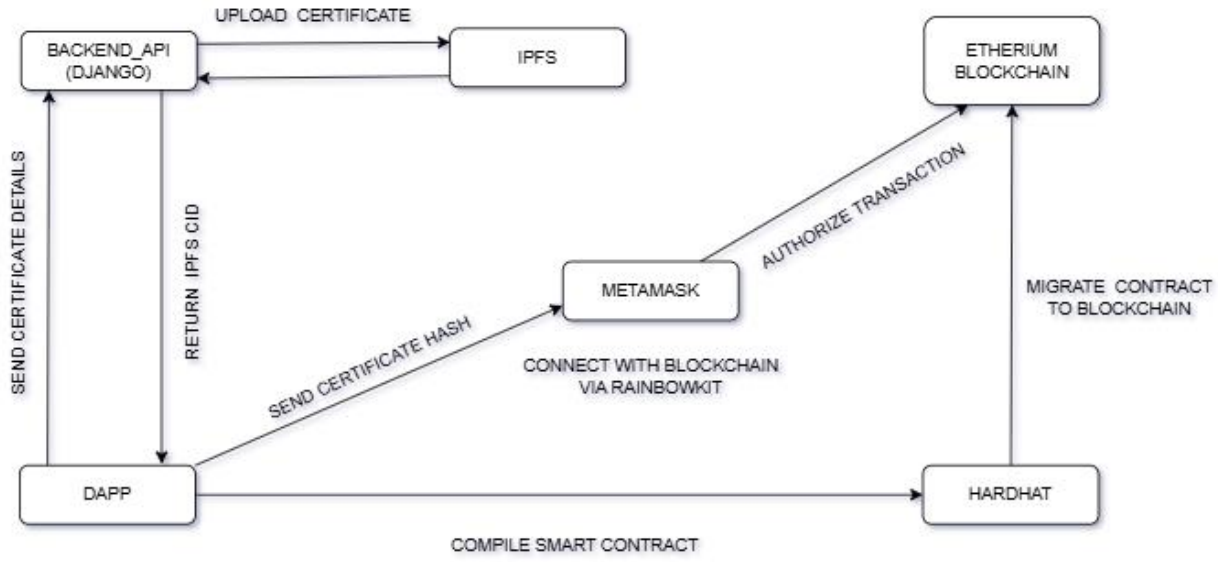


Figure 4. System Architecture Diagram

3.8.3 Functional and Non-Functional Requirements

Functional Requirements:

1. Batch upload certificates via CSV file.
2. Verification of certificates via hash query.
3. Revocation of compromised or invalid certificates.
4. Correction and reissuance of updated certificates.
5. QR code generation linking to the verification page.
6. Metadata storage on IPFS with student details.
7. Admin dashboards for institutions.
8. Downloadable CSV reports of certificate batches.

Non-Functional Requirements:

1. **Security** – Transactions must be cryptographically signed and immutable.
2. **Efficiency** – Low-cost gas optimization through bulk calls.
3. **Availability** – Always-online IPFS gateways and failovers.
4. **Usability** – Clean UI/UX for non-technical users.
5. **Accessibility** – QR support for mobile verification.
6. **Auditability** – Full event logging and hash traceability.

3.8.4 Implementation and Integration

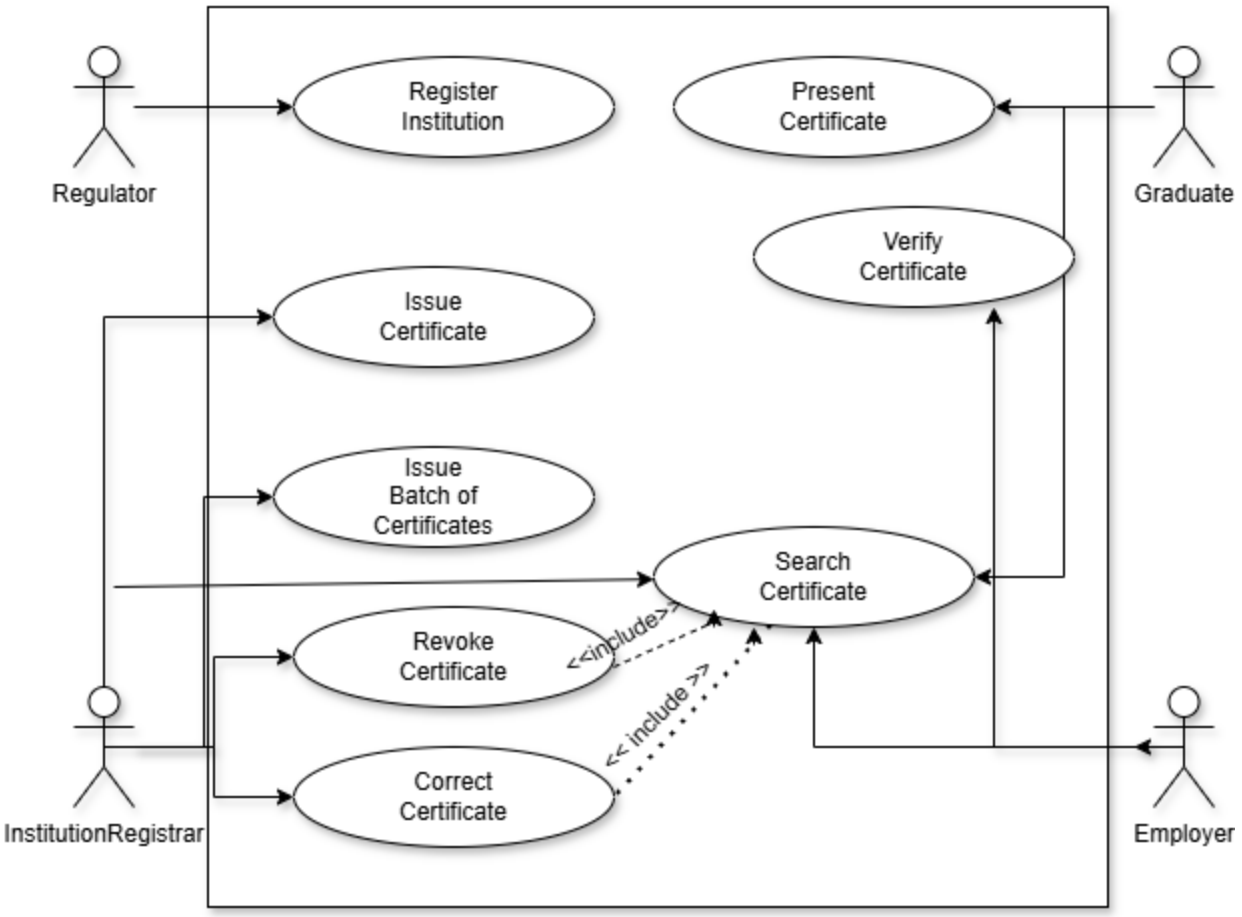


Figure 5. Use case Diagram

This use case diagram identifies key actors and their interactions with the system:

The regulator:

- This is the contract owner.
- They deploy the contract to blockchain.
- Register and deregister institutions after background checks. Only registered institutions can Issue certificates.
- This role can be played by regulatory bodies like ZIMCHE.

The Institution:

- Send registration requests that the regulator inspect for authorization.
- They can issue, revoke, or correct certificates.

The Graduate provides a digital certificate with a QR code in it. The Employer Scans the QR code and see the certificate state and details

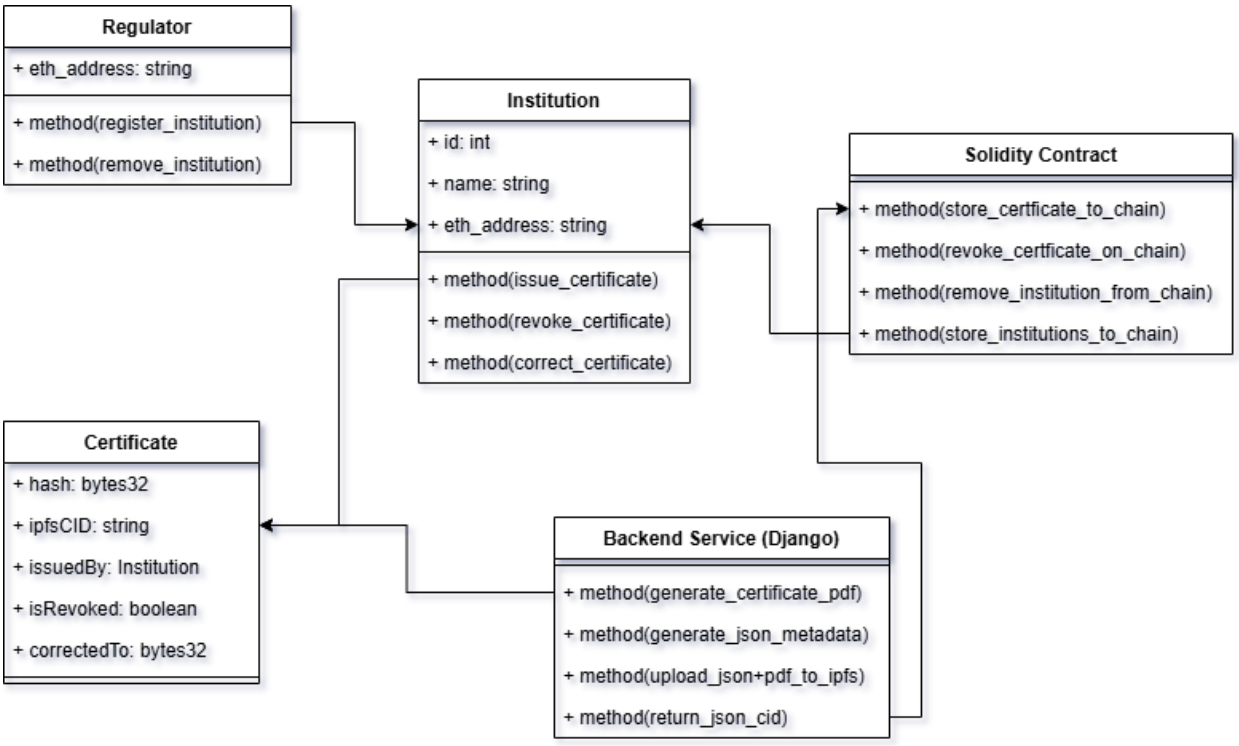


Figure 6. Class Diagram

The class diagram shows the main entities, including Certificate, Institution, User, and their association. It represents storage attributes for every class, how they interact, and methods/functions specific to each.

The smart contract possesses a decentralized, modular, and extensible certificate registry with primary characteristics for secure issuance, authentication, revocation, and modification of academic diplomas. It keeps only hashed identifiers and metadata pointers on-chain while hosting complete documents on IPFS for the purposes of gas efficiency and data confidentiality.

Core Components

- **Mappings**
  - certificates: Maps certificate hashes to metadata (IPFS CID, issuer, status flags).
  - institutions: Whitelist of authorized issuing addresses.
- **Access Control**
  - Only the contract **owner** can register institutions.
  - Only **authorized institutions** can issue, revoke, or correct certificates.

- **Events**
    - Triggered for each key action to support **transparency, frontend updates, and auditability.**

Key Functions

1. **registerInstitution**: Grants issuing rights to an institution (owner-only).
2. **issueDiploma**: Issues a certificate using a hash of the registration number and IPFS CID.
3. **issueBatchDiplomas**: Efficiently issues multiple certificates in a single transaction.
4. **verifyCertificate**: Public read function returning certificate details (gas-free via eth_call).
5. **revokeDiploma**: Allows issuers to revoke a certificate.
6. **correctDiploma**: Issues a corrected version and links it to the original.

Design Considerations

- **Gas-efficient**: Stores only essential data on-chain. InterPlanetary File System (IPFS) offers a decentralized framework for file storage, with each file in the global IPFS namespace being distinctly labeled through content-addressing. IPFS operates through a collection of interconnected nodes that enable the storing and sharing of files, avoiding dependence on a single centralized server. This decentralized framework confers numerous advantages, including enhanced reliability, improved speed, and fortified security.
- **Audit-ready**: All actions are logged via events.
- **Secure and controlled**: Access is tightly managed.
- **Extensible**: Supports future features like endorsements or expiry dates.

Overall, the contract ensures **verifiability, integrity, and scalability** of certificate management in a decentralized environment.

The Backend Server built with **Django REST Framework (DRF)**, acts as a **middleware layer** between the frontend and the blockchain. It handles **off-chain operations** that are computationally heavy or storage-intensive, ensuring the blockchain remains efficient and cost-effective.

While the blockchain enforces **certificate authenticity and verification**, the backend supports essential **pre- and post-blockchain** tasks:

- Handles front-end form submissions (e.g., certificate issuance).
- Generates digital certificate **PDFs**.
- Uploads documents and metadata to **IPFS**.
- Returns **IPFS CIDs** to the front-end for smart contract calls.
- Provides APIs for **batch uploads, and analytics**.
- Adds **QR codes** to downloaded certificates for enhanced verification

The backend is a **crucial component** in the decentralized academic credential system, enabling certificate generation, storage, and institutional management while offloading heavy tasks from the blockchain. This architecture ensures **efficiency, scalability, and a smooth user experience**.

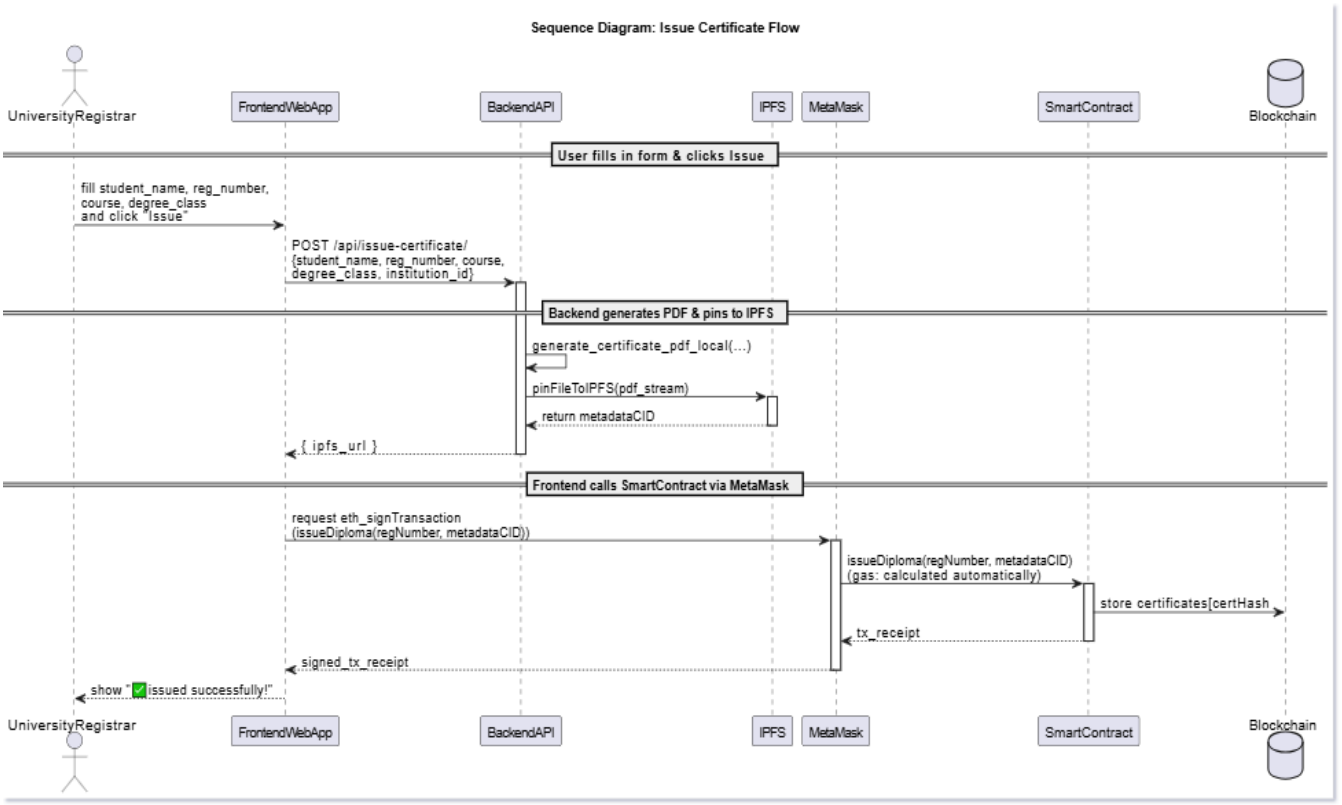


Figure 7.Issue Certificate Sequence Diagram

1. Registrar capture certificate details or uploads csv
2. Backend generates pdf and stores along with metadata to ipfs returning ipfs url
3. Metadata CID is extracted from ipfs url and is passed via Metamask to blockchain
4. the contract encrypts CID and regnumber to form certHash (certificate hash) which is stored on chain
5. The mapping of certificate hash to CID and issuer is saved ensuring non-repudiation
6. Transaction Receipt is returns to issuer on frontend.

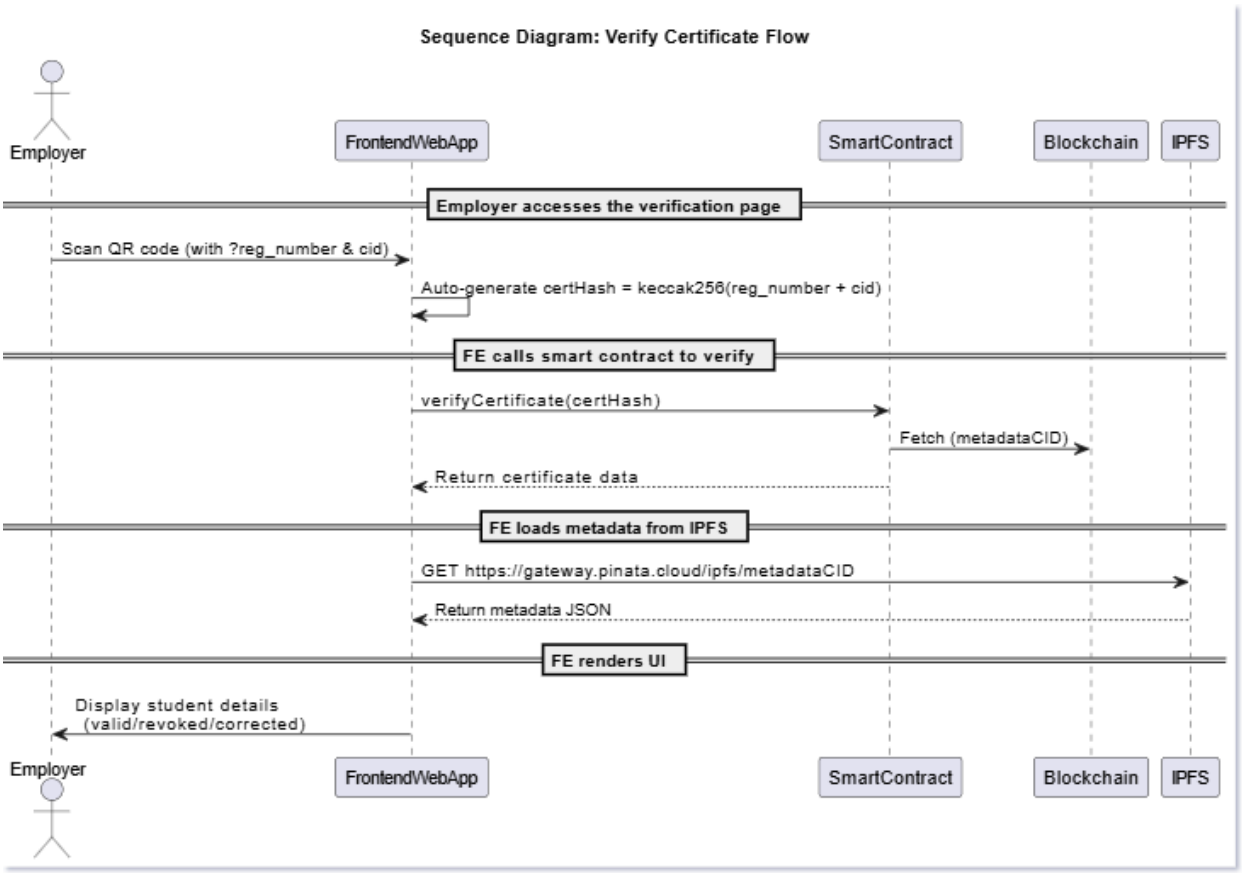


Figure 8. Verify Certificate Sequence Diagram

1. The user scans a QR code or enters a certificate hash in the front-end.
2. The front-end calls the smart contract's verifyCertificate function.
3. The smart contract retrieves certificate data (metadata CID, issuer, revoked status, corrected CID) from the blockchain.
4. The front-end fetches the metadata JSON from IPFS and displays certificate details and status.
5. If needed, the user can download an overlay-updated PDF by invoking the back-end update-certificate endpoint.

The data stored in pdf stored in IPFS doesn't contain a QR code since you can't create a pdf and have it point to itself in ipfs. So, we create the overlay when user wants to download certificate. The downloaded certificate will have QR code with ipfs cid and regNumber embedded that autofills the verification fields.

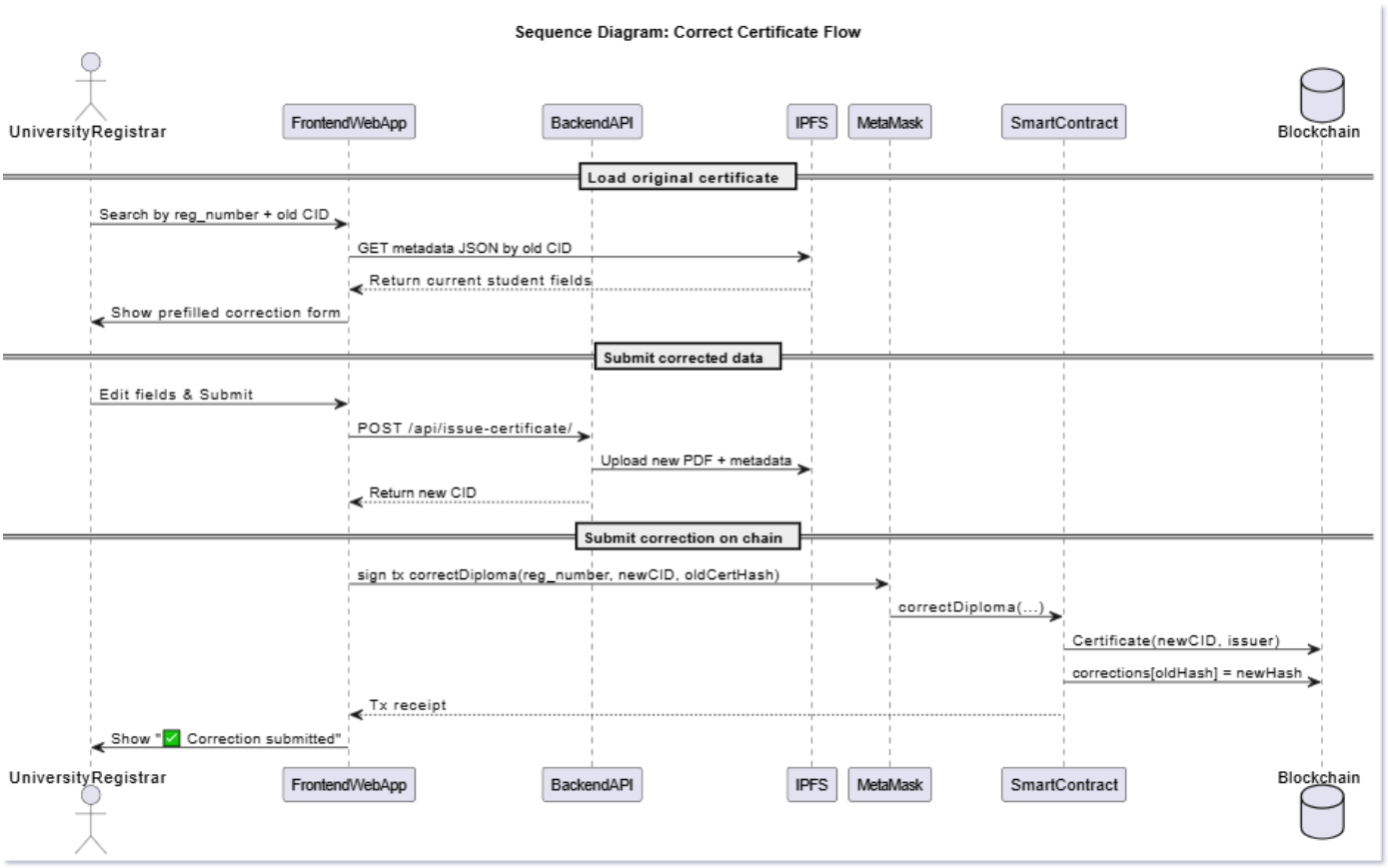


Figure 9. Correct Certificate Sequence Diagram

1. The University Registrar identifies a certificate requiring correction.
2. The front-end requests existing metadata from IPFS and pre-fills the correction form.
3. The Registrar edits and submits corrected certificate details.
4. The back-end regenerates the updated PDF, uploads it to IPFS, and returns a new CID.
5. The front-end calls the smart contract's correctDiploma function with the student registration number, new CID, and original hash.
6. The smart contract updates the correction mapping and emits a CertificateCorrected event.
7. Verification flows thereafter reference the corrected certificate hash and display updated information.

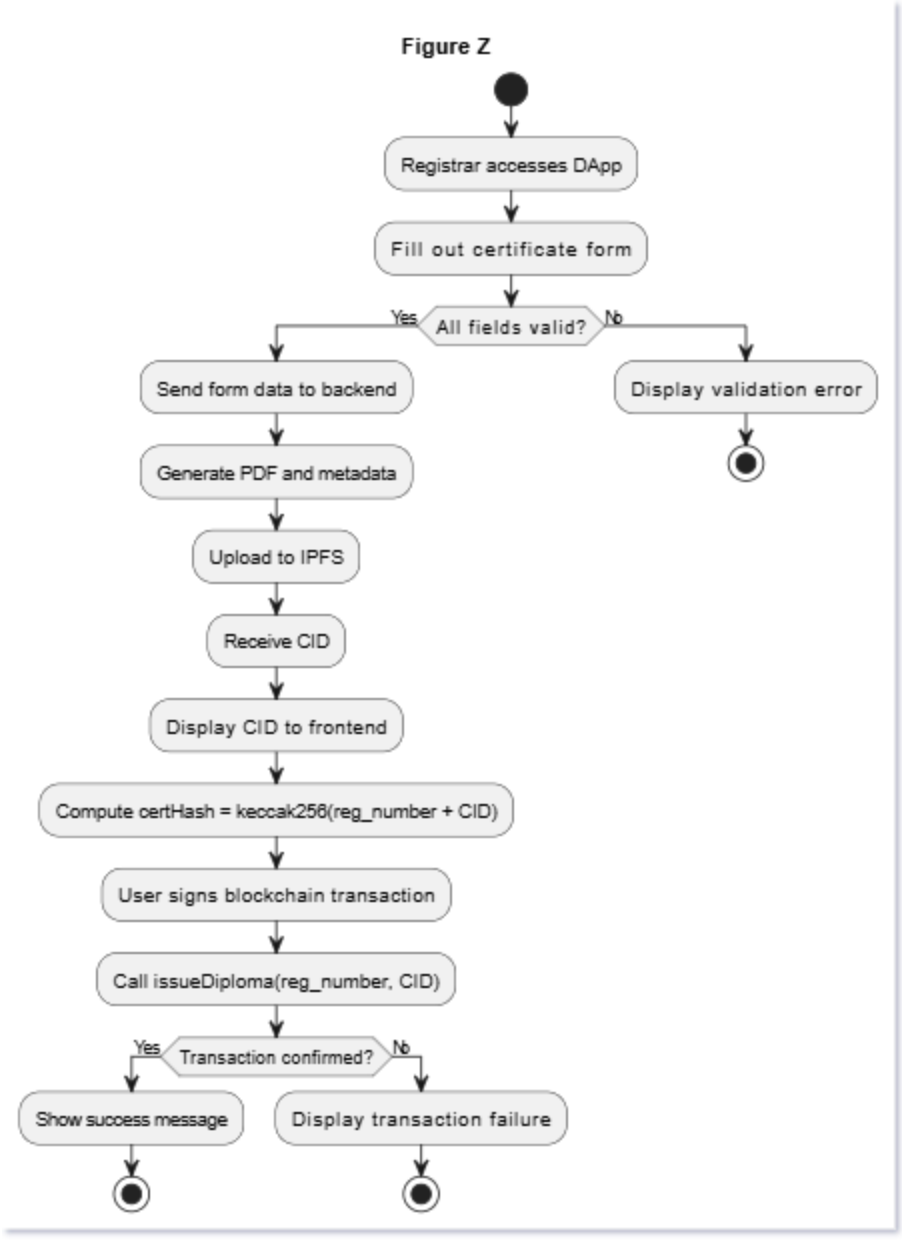


Figure 10. Issue certificate Flow Chart

This flow chart provides a high-level overview of the process for issuing a certificate:

1. Registrar fills out certificate details in the front-end form.
2. Form data sent to back-end API which generates and uploads the PDF to IPFS.
3. IPFS returns a CID which the front end uses to call the smart contract.
4. Smart contract stores the certificate hash and CID on-chain.
5. System confirms success and notifies the registrar.

This chart emphasizes decision points, and parallel operations (off-chain vs on-chain), and ensures clarity in implementation steps.

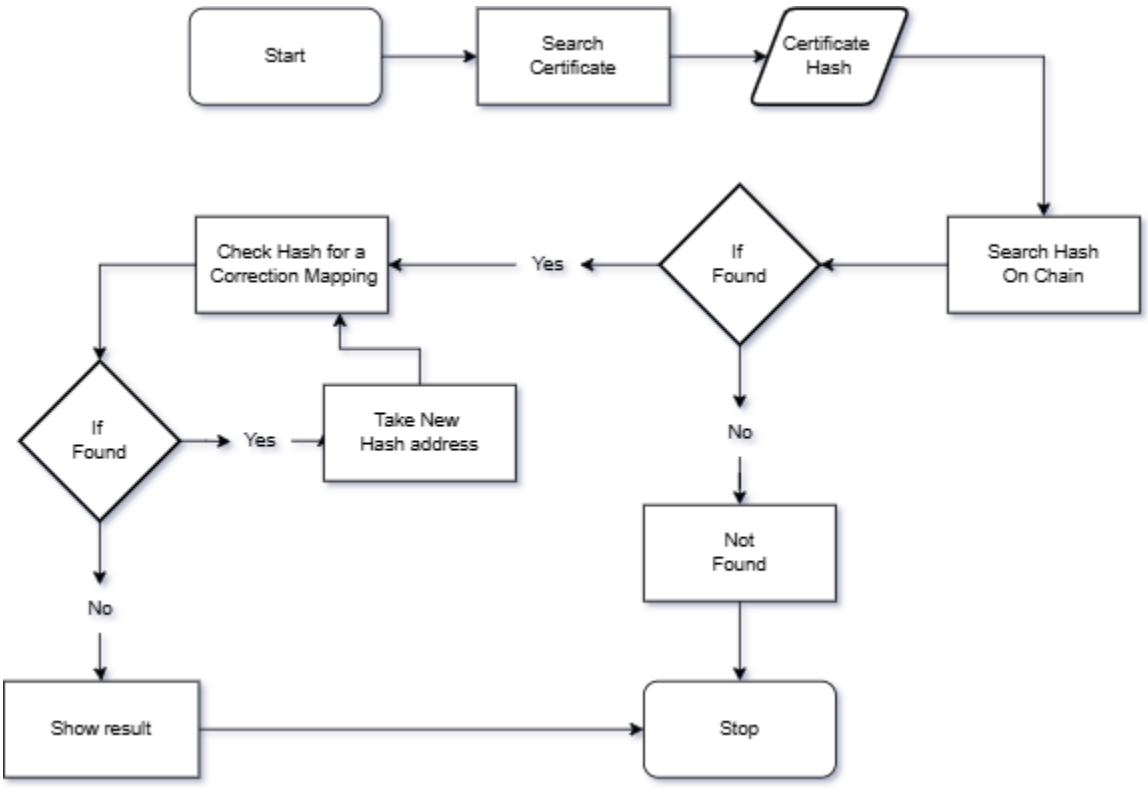


Figure 11. Verify Certificate Flow chart

The verifier, say an employer, arrives at the verification page either by scanning a QR code or entering certificate details manually. Scanning the QR code will make the URL contain prefilled query parameters, i.e., reg_number and cid, so that there is a seamless verification.

When the page is loaded with the provided information, the frontend generates a unique certificate hash based on the formula keccak256(reg_number + cid). This unique hash becomes the certificate's unique address on the blockchain and is used to locate the corresponding record.

With the hash created and deployed contract address, the frontend invokes the verifyCertificate(hash) method on the deployed contract. The blockchain returns key information pertaining to the certificate verification, including the IPFS CID of the metadata, the Ethereum issuing authority address, a boolean flag to indicate if the certificate has been revoked, and a correction reference hash if the certificate has been updated or replaced.

The frontend is also tasked with checking the information that is returned to determine the status of the certificate. When the revoked flag is set to true, the certificate is invalid. When the correctedTo field is not zero, the user is informed that the certificate has been updated and that certificate hash undergoes the same procedure. If either of the above is not true, the certificate is

valid and the frontend fetches the corresponding metadata JSON from IPFS by the CID fetched from the smart contract. The metadata includes student-specific data such as name, course, and degree class.

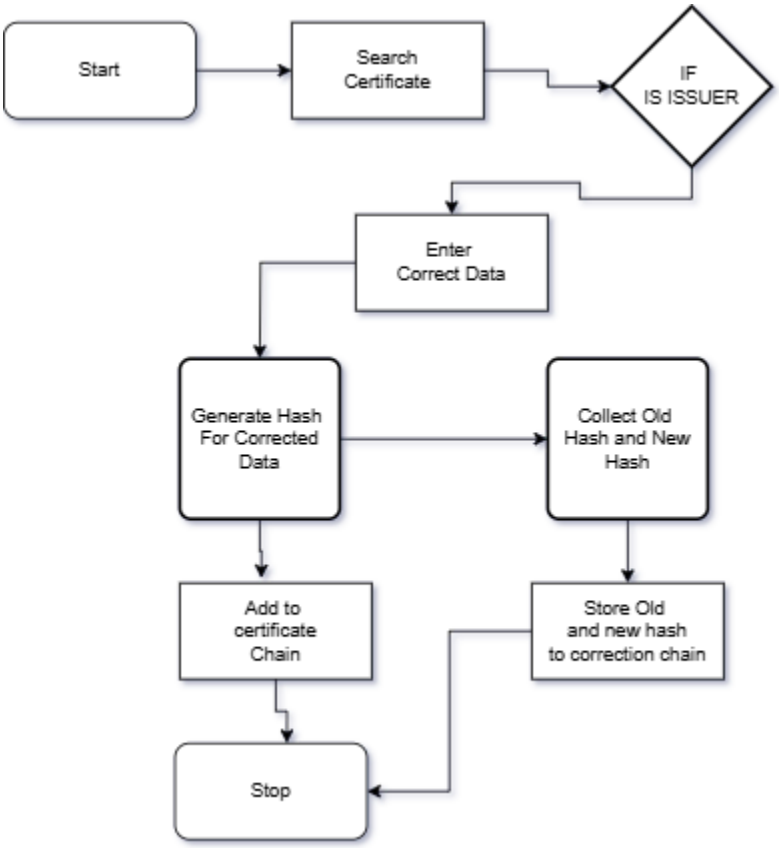


Figure 12.Correct Certificate Flow Chart

A registrar who has the authority to carry out corrections initiates the process by signing in to the institution dashboard and navigating to the certificate correction portal. There, they provide the original certificate details, that is, IPFS CID and the student's registration number, to query the existing certificate. The frontend generates the original certificate hash using the registration number and CID concatenated with the keccak256 function from the details provided. This hash is utilized to call the verifyCertificate(hash) function on the smart contract. The blockchain replies with the current certificate status along with details such as the issuer address. The system verifies that the registrar making the request is the original issuer of the certificate.

The frontend performs a series of checks before proceeding. If the certificate has already been corrected previously, further changes are inhibited. Except when the registrar is the same initial issuer of the certificate, the corrective permission is not granted. Furthermore, if the certificate is already revoked, it is marked as ineligible for correction. If the certificate passes all validation successfully, a correction form is presented to the registrar. The form is pre-filled automatically

with the current metadata retrieved from the IPFS. Only the erroneous fields, i.e., student name, course title, or class of degree, can be altered by the registrar, and all other information should remain intact.

Once the new details are given, the Django backend takes over. It reconstructs the certificate PDF with the updated values and uploads the new document to IPFS, where it receives a new URL. Metadata for the updated content is also created and uploaded to IPFS, and a new metadata CID is returned by IPFS. The frontend then invokes the correctDiploma(originalHash, newRegNumber, newCid) function of the smart contract. This invocation results in the marking of the original certificate as corrected and the registration of the new certificate under a new hash derived from the new registration number and new CID.

If successful, it sends a confirmation message to the registrar. From now onwards, the new hash is the valid certificate for verification. Any attempt to verify the old certificate will now show that it has been corrected and point to the new version.

Chapter 4: Results and Analysis

4.1 Introduction

This chapter provides empirical and performance results obtained through stakeholder surveys, testing of systems on blockchain networks, and determining the potential for real-world implementation. The findings are analyzed to determine the efficacy, security, and cost savings of the suggested Academic Certificate Generation and Verification System through blockchain.

The results are categorized into:

- Stakeholder Feedback: Survey and interview feedback from university officials, employers, and students.
- Performance Metrics: Cost and time comparison of Sepolia and Polygon PoS blockchain implementations.
- System Behavior: Security integrity, correctness, and verification speed metrics.
- Experience & Adoption: Evaluation of usability and feasibility of blockchains-based certificate management.

All the sections connect back to Chapter 1's research objectives, questions, and hypotheses.

4.2 Stakeholder Survey Analysis

4.2.1 University Administrators & Registrars

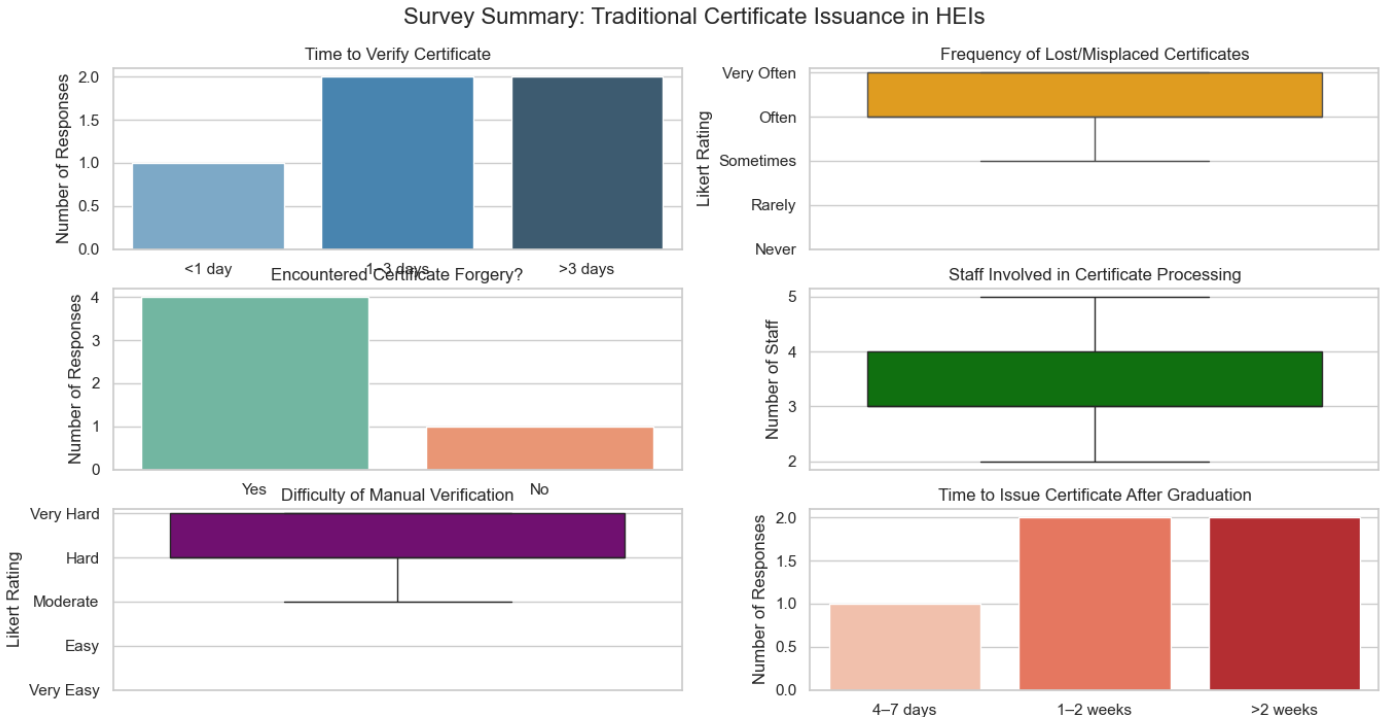


Figure 13. University Admins Survey Data

Findings

- Manual verification is difficult and it takes more than 3 days to complete.
- Administrators reported that certificates were frequently misplaced or lost.
- Four of the five administrators said they had encountered fake certificates.
- Majority reported certificate issuance process taking greater than 1 week.
- The reported cost per certificate were $7, $10, $15, $12, $9 averaging $10.60 per certificate

Key Challenges Identified

- Verifications and Issuance require multiple staff (3-5) approvals and manual coordination.
- Paper-based certificates allow documents to be altered.
- Manual verification is time-consuming.
- Issuing a single certificate can cost institutions ~$10 or more, excluding staff overhead.
- During graduation or application seasons, staff shortages cause backlogs.
- Storing certificates on a centralized server increases the risk of tampering.

This supports both Objective 1 and RQ2 (Identifying inefficiencies in traditional systems.

4.2.2 Employers & HR Managers

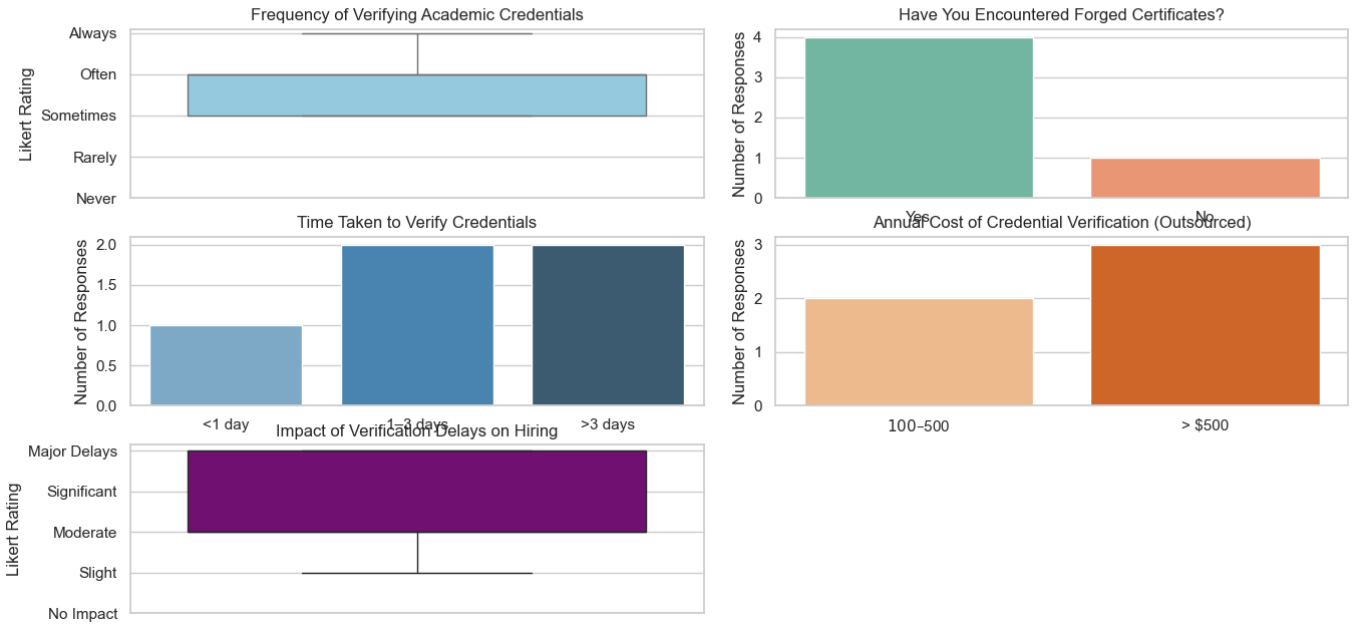


Figure 14. Employer Survey data

Findings

- Frequency of certificate verification: 80% verify credentials "Often" or "Always."
- Encounters with fraudulent certificates: Four out of five recruiters had encountered fake degrees.
- Verification time: 40% reported verification took more than 3 days, causing delays in hiring.
- Hiring impact: 40% experienced significant delays due to slow manual verification.
- Annual verification costs: 60% spent more than $500 a year outsourcing verifications.

Implications

- Employers incur considerable costs and delays in verifying candidate credentials.
- Slow verification negatively impacts hiring timelines.
- Blockchain-based verification can potentially lower costs and speed up hiring processes.

This confirms the necessity for faster verification (RQ2: How can blockchain improve verification efficiency?).

4.2.3 Students & Graduates

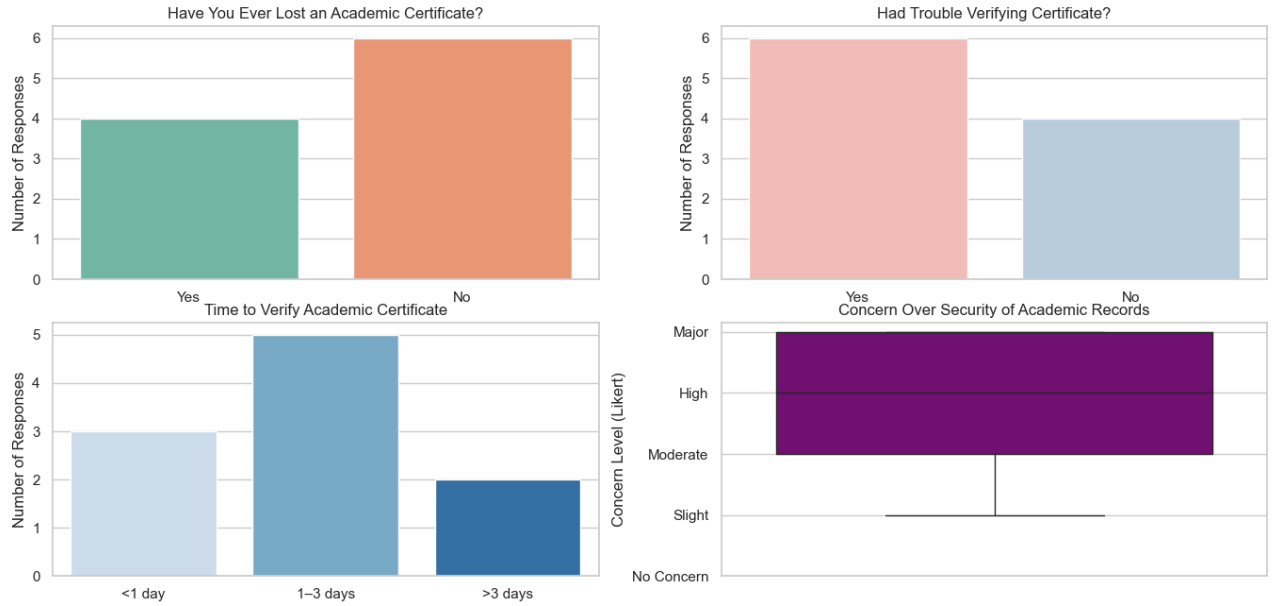


Figure 15. Graduate Survey Data

Findings

- Lost certificates: 40% of students reported losing at least one certificate from their academic history.
- Verification difficulty: 60% of respondents said they had trouble confirming their eligibility for scholarships or jobs.
- Certificate security issues: Security threats were rated as "Major" by 40% of respondents.

Implications

- Using conventional storage methods makes it difficult to verify certificates.
- Blockchain and QR code-based credentials improve accessibility and reduce fraud risk.

This reinforces QR usability and security concerns (RQ1: What features enhance certificate accessibility and trust?).

4.3 System Performance & Verification Results

4.3.1 Gas Cost and Transaction Efficiency

Deployment Results: Sepolia Testnet (Ethereum) Mainnet ETH conditions (30 Gwei gas, $3,800/ETH) 30 Gwei = average long-standing Ethereum gas price.

Fee in ETH = Gas Used * Gas cost

Table 1. Table of Ethereum gas analysis

Batch Size	Gas Used	Gas/Cert	Time (s)	Mainnet Fee (ETH)	Mainnet Fee (USD)	Cost/Cert (USD)
20	1,943,731	97,186.55	41.11	0.05831193	**$221.58**	**$11.08**
39	3,670,708	94,120.72	58.23	0.11012124	**$418.46**	**$10.73**
56	5,302,045	94,679.38	74.12	0.15906135	**$604.43**	**$10.79**
130	12,404,544	95,419.57	77.25	0.37213632	**$1,414.12**	**$10.88**
178	17,013,103	95,579.23	46.46	0.51039309	**$1,939.49**	**$10.90**

Insight:
Ethereum mainnet costs above $10 per certificate make large-scale adoption prohibitive.

Deployment Results: Polygon PoS (Amoy)

Table 2. Table of polygon gas analysis

Batch Size	Gas Used	Gas/Cert	Time (s)	Mainnet Fee (POL)	Mainnet Fee (USD)	Cost/Cert (USD)
5	504,684	100,936.80	28.15	0.01514052	**$0.01136**	**$0.00227**
20	1,943,731	97,186.55	44.19	0.05831193	**$0.04373**	**$0.00219**
39	3,670,708	94,120.72	50	0.11012124	**$0.08259**	**$0.00212**
56	5,302,045	94,679.38	70.2	0.15906135	**$0.11930**	**$0.00213**
130	12,404,544	95,419.57	75.5	0.37213632	**$0.27910**	**$0.00215**
178	17,013,103	95,579.23	73.35	0.51039309	**$0.38279**	**$0.00215**

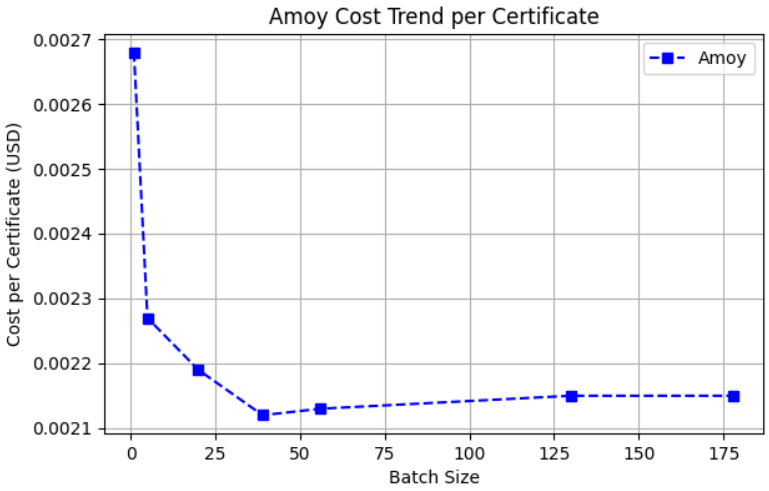


Figure 16. EVM amortization in polygon batch issuance

Insights:

- Polygon PoS is affordable with rates below $0.003 per certificate.
- As expected, per-certificate gas decreases sharply as the batch size grows, leveling off around ~ 94,120 – 95,579 gas/certificate for large batches. This reflects EVM cost amortization.
- Due to EVM amortization, we can trust the certificate cost projection.
- For a 1000-student institution, gas fees would be $2.15 for all the certificates.
- Ethereum charges prohibitively expensive fees, confirming the need for Layer 2 and side chains scaling solutions for low-cost academic certificate management.

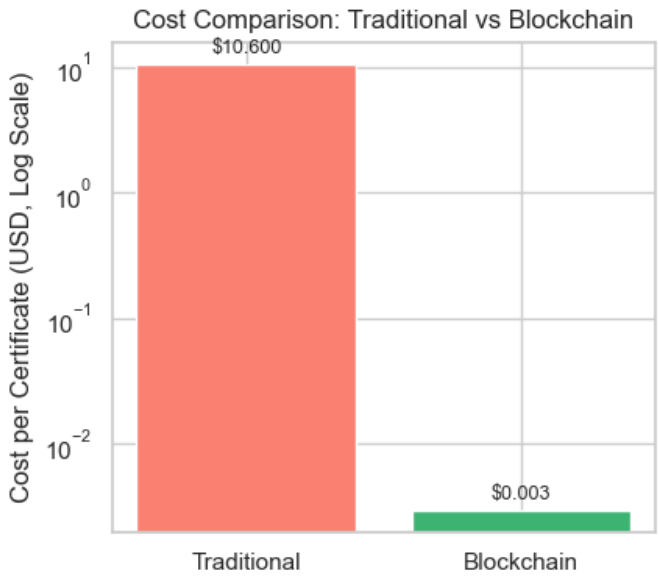


Figure 17. Traditional vs Blockchain approach. Cost Comparison

This supports both Objective 3 (cost comparative analysis)

4.3.2 Timing Analysis

To maximize performance, the system uses a ThreadPoolExecutor with 10 concurrent workers. Batches of 5, 10, 20, and 30 entries were tested to determine the average processing time per certificate and identify performance ceilings due to network or service rate limits. Even though individually an upload averaged 6.67s the use of threads drastically optimizes the process.

Table 3. IPFS upload time

Batch Size	Total Time (s)	e per Certificate (s)
5	9.7	1.94
10	10.11	1.01
20	21.11	1.06
30	31.69	1.06

Estimated Time = 1000×1.06 = 1060 seconds
To accommodate network variability and retry logic (implemented due to IPFS upload rate limits), a buffer of 8% is applied:
Adjusted Time = 1060 + (0.08×1060) =1145.0 seconds≈19.1 minutes
This estimate assumes optimal parallelism with minimal contention and consistent network performance

Uploads are made to Pinata's IPFS API, which enforces rate limits depending on the subscription tier:

- **Free Tier**: 60 API calls per minute
- **Picnic Plan**: 250 API calls per minute
- **Fiesta Plan**: 500 API calls per minute

With 10 concurrent threads making simultaneous upload requests, the free tier would quickly be throttled. The **Picnic Plan**, which allows ~4 uploads per second, is sufficient for batches up to 25–30 entries every 30 seconds. However, larger batch uploads or retry spikes can approach these limits, making **Fiesta** a safer choice for high-throughput scenarios.

The **Fiesta Plan supports up to 500 API calls per minute**, which translates to:

- ~8.3 uploads per second
- ~500 certificates/minute (assuming 1 upload per certificate metadata or file)

Implication: The system can upload large batches (even 1000+ certificates) **without hitting rate limits**, reducing retries and improving overall throughput.

Blockchain Transaction Time: Using the largest batch (178), average per certificate

upload was 0.41 seconds.

Total Issuance Time per Certificate: ≈ 1.06 + 0.41 = 1.47 seconds.

Institution Level Issuance Projection: For 2,000 certificates, total issuance time

≈ 49 minutes.

4.3.3 Verification Speed Analysis

Efficient credential verification is crucial for reducing administrative delays.

- **QR-Based Verification Speed:**
  - Average scan-to-result time: 0.589 seconds per certificate.
  - Full load time (including network and UI): ≈ 1.5 seconds.
- **Total Verification Time:** ≈ 2.089 seconds.

Concluding Insight:
The system returns verification results within seconds, a dramatic improvement over days in manual processes.

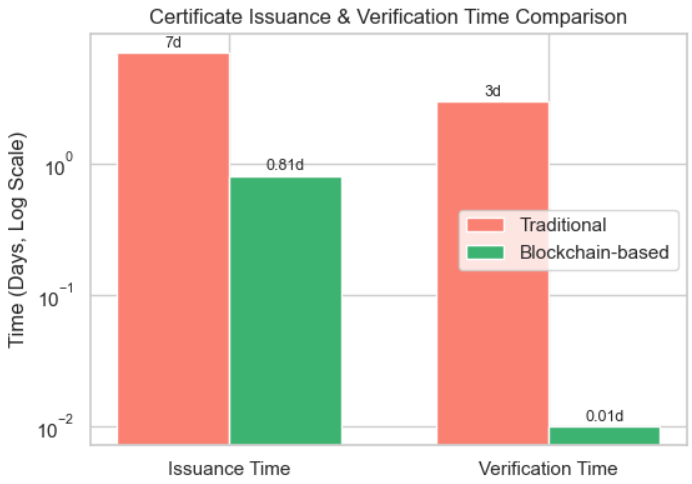


Figure 18. Traditional vs Blockchain approach. Issuance and verification time comparison

This supports both Objective 3 (time comparative analysis)

4.3.4 Certificate Integrity Validation

1. Valid Certificate Verification (T1) To test the accuracy of the verification process:

20 valid certificates were scanned.

- Each certificate contained its original IPFS CID and registration number.
- All 20 were properly labeled as Valid by the system.
- The certificates were downloadable after verification.
- **Final Result:** 100% success rate for valid certificate detection.

2. Correction Handling Test (T2) To test certificate corrections:

- 10 certificates were corrected through the institution dashboard.
- Every alteration led to:
    - New PDF creation
    - Altered IPFS CID
    - Blockchain record update
- Scanning the original certificate, the system displayed the status as 'Corrected' with editing disabled further.

Final Result: 100% accuracy rate for corrections—all the corrections updated correctly. The blockchain tracked corrected credentials successfully.

3. Revocation Handling Test (T3) For revocation enforcement testing:

- 20 certificates were revoked via the institution interface.
- All revoked certificates showed 'Revoked' status when scanned correctly.
- Revoked certificates were prevented from using further.
- **Final Result:** 100% revocation success—invalid certificates were no longer usable. The system made it impossible for fraudulent use of old certificates.

Insights:

- Tamper-proof authentication guarantees that incorrect certificates cannot be validated.
- Certificate correction process is fully automatic, increasing institutional correctness.
- Revocation system prevents fraudulent use of old credentials, fostering trust.
- QR code scanning validates instantly, reducing dependence on manual verification.

This supports both Objective 3 (security analysis)

4.4 User Experience and Adoption Feedback

Survey sample: 20 participants (5 staff, 5 Employers, 10 students and graduets).

Table 4. User Feedback

Metric	Response
Ease of issuance	**75% rated it easy**
Verification speed	**80% rated it fast**
Trust in security	**67% fully trusted blockchain verification**
Adoption likelihood	**75% likely to implement in institutions**

- Users found the Next.js interface intuitive; minimal training was required for staff.
- Employers appreciated near-instant verification via hashed lookups on Ethereum.
- Moderate confidence in blockchain immutability and IPFS provenance.
- High willingness to adopt new technology

4.5 Summary

In this chapter, empirical research and performance evaluation of the academic certificate system using blockchain have been presented. Key findings demonstrated the efficiency, security, and cost savings of blockchain in issuing, authenticating, and revoking certificates compared to traditional centralized systems. The results were framed using the following themes: **Stakeholder Feedback**: Survey and interviews confirmed a high risk of forgery, long verification delays, and inefficiency in the existing system. **Performance Metrics**: Blockchain reduced issuance expense to below $0.003 per certificate, 1.47 seconds per issuance, and verification time to 2.1 seconds, proving scalability. **System Behavior**: Security testing confirmed 100% success in tamper detection and revocation processing, maintaining integrity. User **Experience**: Verification with QR made it easier for employers and students to verify, increasing accessibility.

Chapter 5: Summary, Conclusions, and Recommendations

5.1 Introduction

This chapter concludes the overall research process by presenting findings that are significant, drawing conclusions in light of the research objectives, and making practical suggestions for future adoption. It reminds itself of the research questions and hypotheses, determines the practicality of the blockchain-based academic certificate proof of concept, and expounds on how the system is responding to the inherent vulnerabilities of traditional credential verification systems. It also addresses issues of legal data compliance, particularly toward real-world adoption.

5.2 Key Findings

The first objective of the research was to identify the deficiency of traditional certificate systems. From interviews and questionnaires distributed among major stakeholders, there were various systemic problems that emerged. Seventy percent of the employers reported that they had encountered fake academic certificates, and verification of certificates typically took one to three days. Manual verification procedures were conducted by two to five employees in most institutions, causing administrative workload. Furthermore, the cost per certificate to process averaged approximately $10 USD. These findings emphasize the inefficiency, vulnerability to fraud, and inability to scale up of centralized systems, which strongly support the need for setting up a decentralized, tamper-resistant system. The second objective was to develop and test the prototype system. The prototype was made up of Solidity smart contracts for issuing, correcting, revoking, and verifying certificates. The frontend with Next.js and Wagmi had MetaMask integration and certificate access via QR code. The backend with Django REST provided PDF output and interaction with the InterPlanetary File System (IPFS), where off-chain storage of metadata and certificate document storage were done. The entire system had automated the lifecycle of certificates on a decentralized network, reducing human intervention and improving the integrity of academic credentials. The third aim was to analyze the cost, performance, and security of the system. The cost of a single certificate on the Polygon PoS chain was approximately $0.0027 USD, a remarkable decrease from the traditional $10. Despite large batches, such as issuing 178 certificates, total gas fee was less than $0.40. The performance was optimal as PDF generation and IPFS upload took 1.06 seconds on average through the use of threadpools, and time of blockchain confirmation ranged from 22 to 75 seconds depending upon batch size. Verification of QR code took around 2.6 seconds. The correctness was maintained uniformly by the system through successful issuance, revocation, and fixing of certificates as per smart contract rules. Hashes established a one-to-one mapping between each certificate and on-chain record, and therefore were tasked with data integrity. Additionally, using immutable hashes and content identifiers (CIDs) made tampering impossible and revoked or changed certificates appropriately labeled as "invalid" or "corrected." These results support the effectiveness, performance, and resilience of the system and therefore all three research hypotheses (P1, P2, and P3) are confirmed.

5.3 Data Compliance Considerations

While blockchain's immutability prevents data protection law—i.e., Article 17 GDPR "right to erasure"—such system circumvents the issues through off-chain revocation methods and metadata diversion. On operational deployment, implementation with Decentralized Identifiers (DIDs) can grant some access to personal information. Furthermore, metadata on IPFS consists of only non-sensitive public information to maintain user anonymity. Later modifications can encompass the possibility of conducting zero-knowledge proofs, which can enable private verification with hidden information remaining secret. With these safeguards in place, the system can be rendered compliant with key legal obligations, for instance, the GDPR and the Family Educational Rights and Privacy Act (FERPA).

5.4 Recommendations

For the universities, piloting blockchain-based systems for credentials with regulatory bodies like the Zimbabwe Council for Higher Education (ZIMCHE) is recommended. Digitally signed QR-enabled certificates must replace printed certificates, and revocation and correction must be automated by the institutions by implementing smart contract triggers. Training for the staff to handle blockchain-based workflow should be carried out in order to attain operational readiness. For HR professionals and employers, the system offers tamper-evident, real-time validation of educational qualifications. Real feedback for candidate credentialing optimization is encouraged from organizations, as well as integrating APIs of such decentralized applications into hiring systems for seamless screening. For developers, more development should be on support for more languages, adding accessibility features, and analytics dashboards integration to allow institutions to track verifications as well as detect anomalies. Developers need to focus on integrating identity frameworks such as DIDs and zero-knowledge proofs to allow for users' privacy. Policy makers and accrediting bodies need to collaborate to develop national standards for the acceptance of on-chain digital certificates, implementing standard schema formats within institutions, and ensuring interoperability. Pilot initiatives, regulatory backing, and investments need to be employed for inducing adoption of blockchain in the education field.

Future research can examine the use of national ID or biometric systems to further verify academic credential authenticity. Other research must explore trust in the user and system utilization under underdeveloped digital infrastructure conditions. It would be fascinating to have a comparison of how the system works across various Layer 2 blockchains such as Base, Optimism, and zkSync.

Final Summary

This research demonstrates how blockchain technology can revolutionize academic credentialing with forgery elimination, verification reduction, and cost savings. Proof-of-concept achieved the

three research objectives and proved the corresponding hypotheses. With the world trending towards secure, scalable, and verifiable digital records, the system presented here is a powerful and innovative remedy for transparent and efficient academic record management.

Reference List

Boonkrong, S. (2024) ‘Design of an academic document forgery detection system’, *International Journal of Information Technology (Singapore)*. Available at: https://doi.org/10.1007/s41870-024-02006-6..

Centeno Cuya, K., Palaoag, T.D. and Cuya, K.C. (n.d.) ‘Revolutionizing academic integrity: The emergence of blockchain for credential verification—A bibliometric perspective’. Available at: https://www.researchgate.net/publication/381887438..

Chaurasia, A. and Gangwar, S. (2024) ‘Blockchain-based authentication and verification system for academic certificate using QR code and decentralized applications’, *International Journal of Computer Applications*, 186(26), pp. 975–8887. Available at: https://doi.org/10.5120/ijca2024923722..

Emele, I.C., Oguoma, S.I., Uka, K.K. and Nwaoha, E.C. (2020) ‘An enhanced web base certificate verification system’, *OALib*, 7(7), pp. 1–15. Available at: https://doi.org/10.4236/oalib.1106342..

Ifeyemi, T., Oyedeji, A. and Adebiyi, F. (2024) ‘A blockchain-based digital educational certificate verification system’, *Journal of Engineering and Technology for Industrial Applications*, 10(49), pp. 35–41. Available at: https://doi.org/10.5935/jetia.v10i49.1145..

Jaafar, R.A. and Alsaad, S.N. (2023) ‘Enhancing educational certificate verification with blockchain and IPFS: A decentralized approach using Hyperledger Fabric’, *TEM Journal*, 12(4), pp. 2385–2395. Available at: https://doi.org/10.18421/TEM124-51..

Kadam, A.P., Yesugade, K.D., Dixit, M.S., Kothare, A. and Sarwade, S. (2024) ‘Decentralized blockchain-based result generation and verification system’, *International Journal of Creative Research Thoughts*, 12. Available at: http://www.ijcrt.org..

Kim, S.K. (2022) ‘Blockchain smart contract to prevent forgery of degree certificates: Artificial intelligence consensus algorithm’, *Electronics*, 11(14). Available at: https://doi.org/10.3390/electronics11142112..

Kotey, S.D., Tchao, E.T., Agbemenu, A.S., Ahmed, A.R. and Keelson, E. (2024) ‘A framework for full decentralization in blockchain interoperability’, *Sensors*, 24(23). Available at: https://doi.org/10.3390/s24237630..

Mahadik, P., Sanskar, S., Gupta, T. and Meshram, Y. (2024) ‘Certificate issuing and verification application using blockchain’, *International Journal of Software Computing and Testing*. Available at: https://doi.org/10.37628/IJSCT..

Merlec, M.M. and In, H.P. (2024) ‘Blockchain-based decentralized storage systems for sustainable data self-sovereignty: A comparative study’, *Sustainability*, 16(17), p. 7671. Available at: https://doi.org/10.3390/su16177671..

Mohammad, A. and Vargas, S. (2022) ‘Challenges of using blockchain in the education sector: A literature review’, *Applied Sciences,* 12(13). Available at: https://doi.org/10.3390/app12136380..

Nizamuddin, N., Salah, K., Azad, M.A., Arshad, J. and Rehman, M.H. (2019) ‘Decentralized document version control using Ethereum blockchain and IPFS’, *Computers and Electrical Engineering*, 76, pp. 183–197. Available at: https://doi.org/10.1016/j.compeleceng.2019.03.014..

Rustemi, A., Dalipi, F., Atanasovski, V. and Risteski, A. (2023) ‘A systematic literature review on blockchain-based systems for academic certificate verification’, *IEEE Access*, 11, pp. 64679–64696. Available at: https://doi.org/10.1109/ACCESS.2023.3289598..

Rustemi, A., Dalipi, F., Atanasovski, V. and Risteski, A. (2024) ‘DIAR: A blockchain-based system for generation and verification of academic diplomas’, *Discover Applied Sciences*, 6(6). Available at: https://doi.org/10.1007/s42452-024-05984-1..

Silaghi, D.L. and Popescu, D.E. (2025) ‘A systematic review of blockchain-based initiatives in comparison to best practices used in higher education institutions’, *Computers,* 14(4). Available at: https://doi.org/10.3390/computers14040141..

Tadi, V. (2024) ‘Integrating blockchain with traditional document verification: Developing a scalable, secure, and unified framework for electronic and printed documents’, *Journal of Mathematics and Computer Applications*, 3(1), pp. 1–11. Available at: https://doi.org/10.47363/JMCA/2024(3)182.

Tang, Q. (2021) ‘Towards using blockchain technology to prevent diploma fraud’, *IEEE Access*, 9, pp. 168678–168688. Available at: https://doi.org/10.1109/ACCESS.2021.3137901 (Accessed: 19 June 2025).

Untung Rahardja, Kosasi, S., Harahap, E.P. and Aini, Q. (2020) ‘Authenticity of a diploma using the blockchain approach’, *International Journal of Advanced Trends in Computer Science and Engineering*, 9(1.2), pp. 250–256. Available at: https://doi.org/10.30534/ijatcse/2020/3791.22020..

Ma, C., Kong, X., Lan, Q. and Zhou, Z. (2019) ‘The privacy protection mechanism of Hyperledger Fabric and its application in supply chain finance’, *Cybersecurity*, 2(5). Available at: https://cybersecurity.springeropen.com/articles/10.1186/s42400-019-0022-2..

Noshi and Xu, Y. (2024) ‘Development of blockchain-based academic credential verification system’, *Open Access Library Journal*, 11, e12130. Available at: https://doi.org/10.4236/oalib.1112130..

TruScholar (2024) *The hidden costs of manual credentialing: Why digital transformation is a must*. Available at: https://www.truscholar.io/blog/the-hidden-costs-of-manual-credentialing-why-digital-transformation-is-a-must (Accessed: 19 June 2025).

Ludden, V. and Jeyarajah, A. (2019) *Employment barriers in border regions*. European Parliament Study. Available at: https://www.europarl.europa.eu/RegData/etudes/STUD/2019/631029/IPOL_STU(2019)631029_EN.pdf (Accessed: 19 June 2025).

BBC News (2018) 'Staggering trade in fake degrees revealed'. 5 January. Available at: https://www.bbc.com/news/uk-42579634 (Accessed: 1 June 2025).

BBC News (2017) 'Fake university degree websites shut down'. 3 January. Available at: https://www.bbc.com/news/uk-england-38494664 (Accessed: 12 June 2025).

Transparency International (2013) *Global corruption report: Education*. Available at: https://www.transparency.org/en/publications/global-corruption-report-education..

African Union (2016) *Continental education strategy for Africa (CESA 16-25)*. Addis Ababa: African Union Commission.

UNESCO IICBA (2019) *Digital transformation of higher education in Africa: Status, challenges and prospects*. Addis Ababa: UNESCO.

Inter-University Council for East Africa (IUCEA) (2018) *Study on the integrity of academic awards in the East African Community*. Kampala: IUCEA.

Appendices

Appendix A: Survey Questionnaire

Evaluate certificate access issues, preferences, and usability of the DApp

Survey
for Students & Graduates

[redacted] Switch accounts

Not shared

* Indicates required question

Have you ever lost an academic certificate? *

- Yes
- No

*

Have you had trouble verifying your certificate (e.g., for a job or scholarship)?

- Yes
- No

Current Practice & Pain Points

Survey
for University Administrators / Registrars

[redacted] Switch accounts

Not shared

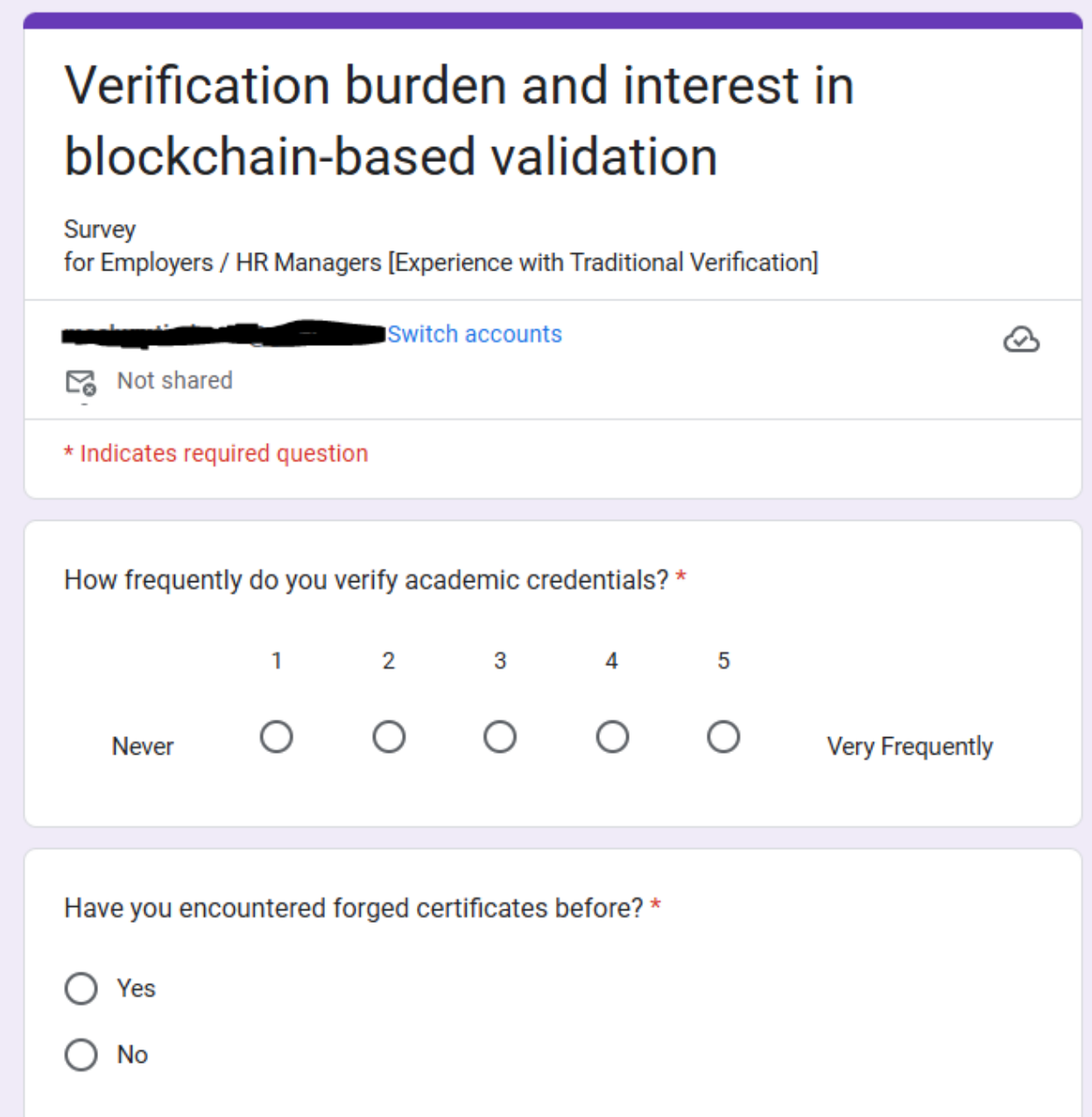
* Indicates required question

How long does it take on average to verify a student's certificate upon request? *

- ◯ less than a day
- ◯ 1 to 3 days
- ◯ more than 3 days

How often do you deal with lost/misplaced certificates? *

	1	2	3	4	5	
Never	◯	◯	◯	◯	◯	Very Frequently



Survey Results

Admin and Registars

Question	Responses Summary
Average Time to Verify Certificate	1 said **<1 day**, 2 said **1–3 days**, 2 said **>3 days**

Question	Responses Summary
Frequency of Lost/Misplaced Certificates	Likert ratings: **3, 4, 4, 5, 5 → Average: 4.2 (Frequent)**
Encountered Forgery?	4 said **Yes**, 1 said **No**
Staff Involved in Verification/Issuance	Reported: **2, 3, 4, 5, 3 staff members**
Difficulty of Manual Verification	Likert ratings: **3, 4, 4, 5, 5 → Average: 4.2 (Difficult)**
Average Cost to Issue a Certificate	Reported: **$7, $10, $15, $12, $9 → Average: $10.60**
Time to Issue After Graduation	1 said **4–7 days**, 2 said **1–2 weeks**, 2 said **More than 2 weeks**
Challenges Faced (Open-ended)	"Courier delays and lack of digitized records." • "Manual validation takes too long; some records are still paper-based." • "Lost student files cause delays." • "Authentication with other institutions is slow." • "Staff shortages during peak periods."

Question	Responses
Do you think a blockchain-based system could improve certificate security?	Responses varied: 1 chose **2 (Disagree)**, 2 chose **4 (Agree)**, and 2 chose **5 (Strongly Agree)**.
Which features are most important to you?	- **Issuance** (3 votes) - **Revocation** (2 votes) - **Correction** (2 votes) - **QR Verification** (5 votes) - **Logs** (4 votes)
What concerns do you have about decentralizing certificate management?	- **Data privacy risks** with external access. - **Complexity in adoption** and integration. - **Costs** of transitioning systems. - **Reliability** of blockchain infrastructure. - **Resistance to change** among institutions.
Are you willing to pilot such a system in your institution?	3 answered **Yes**, 2 answered **No**.

Employers

Question	Responses
How frequently do you verify academic credentials?	2 chose **3 (Sometimes)**, 2 chose **4 (Often)**, and 1 chose **5 (Always)**.
Have you encountered forged certificates before?	4 answered **Yes**, 1 answered **No**.

Question	Responses
How long does a typical verification process take?	2 selected **1–3 days**, 2 selected **>3 days**, and 1 selected **<1 day**.
How much do you spend annually on credential verification (if outsourced)?	Amounts varied from **$100–$500 (2 votes)** to **>$500 (3 votes)**.
How much does a delay in certificate verification impact your hiring decisions?	1 marked **2 (Slight Impact)**, 2 marked **3 (Moderate Impact)**, and 2 marked **5 (Major Hiring Delays)**.

Question	Responses
Would blockchain-based credentials reduce your verification time/costs?	1 selected **2 (Disagree)**, 2 selected **3 (Neutral)**, and 2 selected **4 (Agree)**.
Would a QR code on certificates for instant online verification be useful to your HR process?	4 answered **Yes**, 1 answered **No**.
What additional features would you need to trust such a system?	- **Tamper-proof encryption** to prevent fraud. - **Government/industry endorsement** for credibility. - **Ease of integration** with HR software. - **Automated alerts** for invalid or expired credentials. - **Offline access** for areas with poor internet connectivity.

Graduates

Question	Responses
Would you use a blockchain-based system to store your academic records?	2 selected **2 (Disagree)**, 3 selected **3 (Neutral)**, and 5 selected **4 (Agree)**.
Which format do you prefer for storing your academic certificates?	- **Digital** (3 votes) - **Paper** (2 votes) - **Both** (4 votes) - **Not Sure** (1 vote)
Do you feel confident using web/mobile apps for verification or requests?	2 marked **2 (Not Very Confident)**, 4 marked **3 (Neutral Confidence)**, and 4 marked **5 (Very Confident)**.
Would you find QR-code based certificates convenient?	8 answered **Yes**, 2 answered **No**.

Question	Responses
What features would improve your experience?	**- User-friendly mobile access**. - **Instant verification without delays**. - **Tamper-proof security** to prevent fraud. - **Accessible offline backup**. - **Integration with scholarship/job portals** for seamless verification.

Have you ever lost an academic certificate?	4 answered **Yes**, 6 answered **No**.
Have you had trouble verifying your certificate (e.g., for a job or scholarship)?	6 answered **Yes**, 4 answered **No**.
How long does it usually take to get your certificate verified?	3 selected **<1 day**, 5 selected **1–3 days**, and 2 selected **>3 days**.
Do you worry about the security of your academic records?	2 marked **2 (Slight Concern)**, 4 marked **3 (Moderate Concern)**, and 4 marked **5 (Major Concern)**.

All Participants

Question	Responses
How easy was the certificate issuance process on the DApp?	4 selected **2 (Not Very Easy)**, 6 selected **3 (Neutral)**, and 10 selected **4 (Easy)**.
How fast was verification after scanning the QR code or entering details?	5 marked **2 (Slow)**, 7 marked **3 (Neutral Speed)**, and 8 marked **5 (Very Fast)**.
How much did you trust the system's security when verifying certificates?	3 selected **2 (Low Trust)**, 7 selected **3 (Moderate Trust)**, and 10 selected **5 (Fully Trusted)**.
Would you adopt this system in a real institutional context?	2 marked **2 (Unlikely)**, 6 marked **3 (Neutral)**, and 12 marked **4 (Likely)**.
Suggestions to improve the system:	- **Better user onboarding** for first-time users. - **Enhancing system response speed** for quick verification. - **More security features** to prevent unauthorized modifications. - **Offline functionality** for areas with low connectivity. - **Integration with existing academic databases** to improve adoption.

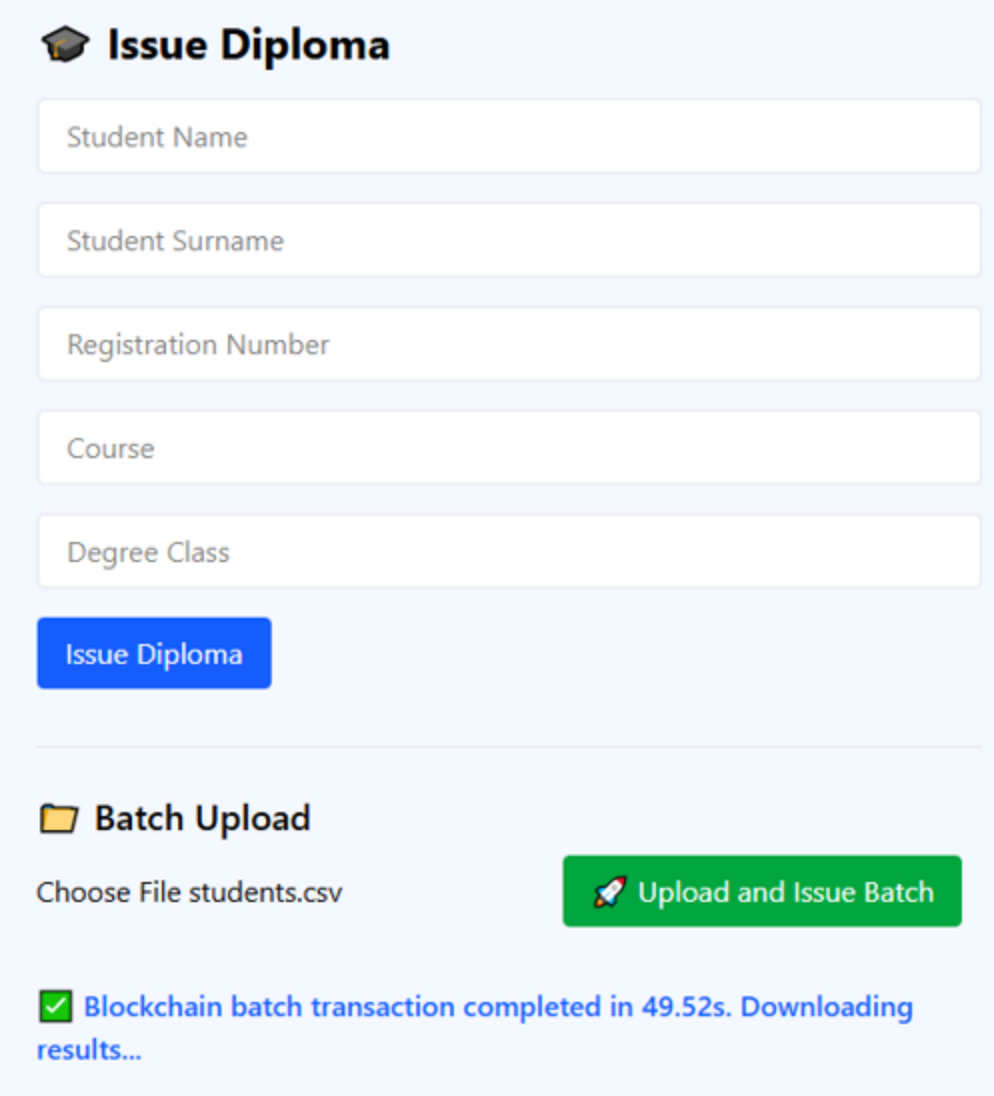
Appendix B: Logs

Block explorer

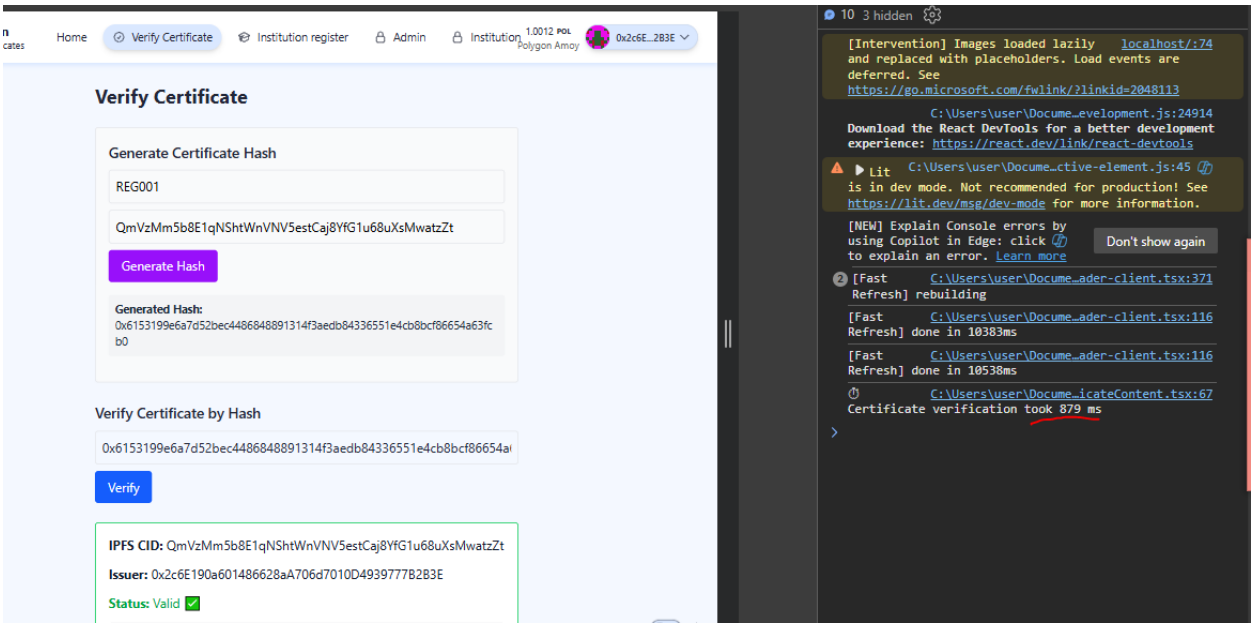
Transaction Hash	Method	Block	Age	From		To	Amount	Txn Fee
0xbdfbc6aa91b...	Transfer	8589400	23 hrs ago	0x823efBB1...446bB26A4	IN	0x2c6E190a...9777B2B3E	0.5 ETH	0.00003223
0x9bd798e254...	0xbc57f805	8564142	4 days ago	0x2c6E190a...9777B2B3E	OUT	0x26B744bE...5FaB20dEC	0 ETH	0.00017853
0x670f67267ca...	Transfer	8550480	6 days ago	0x15095Ec8...158ACe7aD	IN	0x2c6E190a...9777B2B3E	0.05 ETH	0.00000004
0x7ece1a0cbf7...	Transfer	8542110	7 days ago	0x159cA92b...92618A555	IN	0x2c6E190a...9777B2B3E	0.05 ETH	0.00000002
0x82f2e58b804...	Transfer	8496518	13 days ago	0x9a0C272b...EcB561d55	IN	0x2c6E190a...9777B2B3E	0.05 ETH	0.00000002
0x638ae01d7b...	0xf4fdeb2f	8489449	14 days ago	0x2c6E190a...9777B2B3E	OUT	0x26B744bE...5FaB20dEC	0 ETH	0.02551977
0x6a25eddf26b...	0xf4fdeb2f	8489344	14 days ago	0x2c6E190a...9777B2B3E	OUT	0x26B744bE...5FaB20dEC	0 ETH	0.01918282
0xf00b6e8b404...	0xf4fdeb2f	8489235	14 days ago	0x2c6E190a...9777B2B3E	OUT	0x26B744bE...5FaB20dEC	0 ETH	0.01860684
0x300f3db6e38...	0xf4fdeb2f	8488984	14 days ago	0x2c6E190a...9777B2B3E	OUT	0x26B744bE...5FaB20dEC	0 ETH	0.00795313
0x51fe904a7c3...	0xf4fdeb2f	8485510	15 days ago	0x2c6E190a...9777B2B3E	OUT	0x26B744bE...5FaB20dEC	0 ETH	0.00550606

Block:	8489344 **106983 Block Confirmations**
Timestamp:	14 days ago (Jun-06-2025 12:07:00 PM UTC)
From:	0x2c6E190a601486628aA706d7010D4939777B2B3E
To:	0x26B744bEF05c7D19692c34e9C745C785FaB20dEC
Value:	0 ETH
Transaction Fee:	0.019182820703387714 ETH
Gas Price:	1.500001658 Gwei (0.000000001500001658 ETH)
Gas Limit & Usage by Txn:	19,336,795 | 12,788,533 (66.14%)
Gas Fees:	Base: 0.000001658 Gwei | Max: 1.500002192 Gwei | Max Priority: 1.5 Gwei
Burnt & Txn Savings Fees:	Burnt: 0.000000021203387714 ETH ($0.00) Txn Savings: 0.000000006829076622 ETH ($0.00)
Other Attributes:	Txn Type: 2 (EIP-1559) Nonce: 27 Position In Block: 59

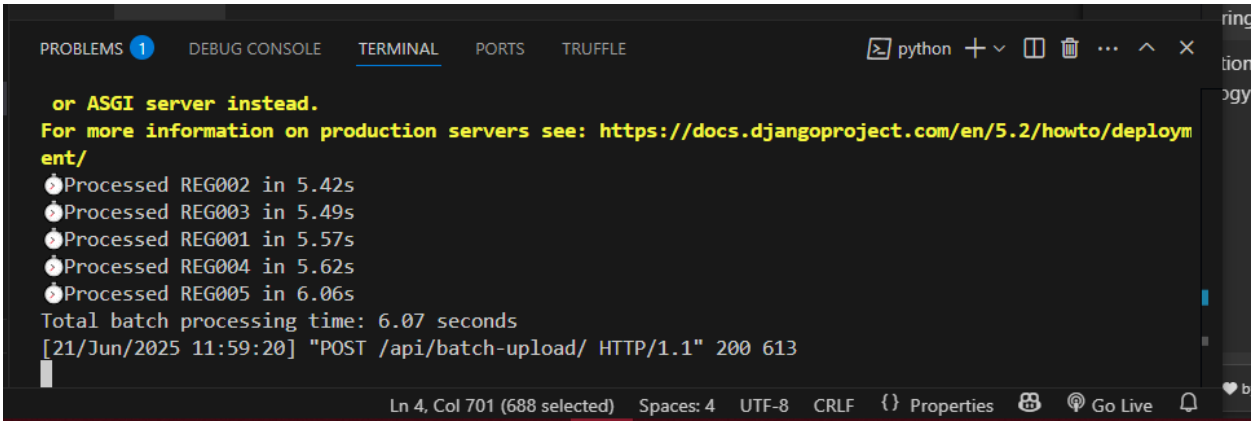
Batch Issuing timing

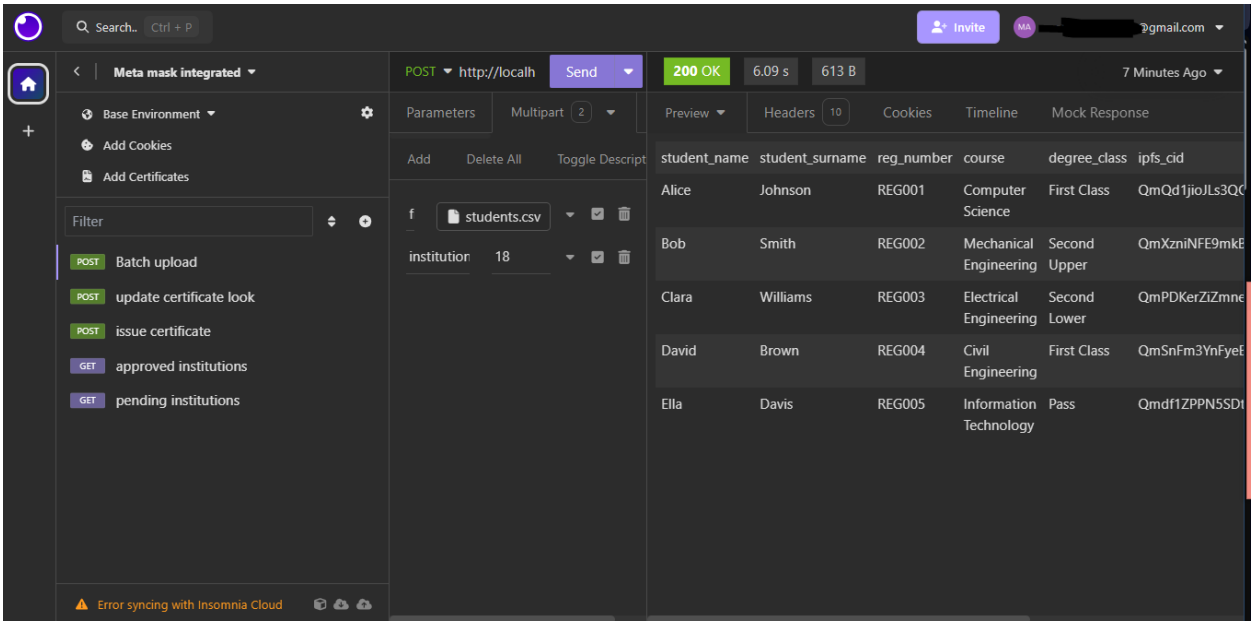


Verification Timing



Ipfs upload logs





Screenshot of insomnia calling the batch upload API. The API returns a csv of details successfully uploaded.

Appendix C: Smart Contract Snippets

ages > hardhat > contracts > DiplomaRegistry.sol

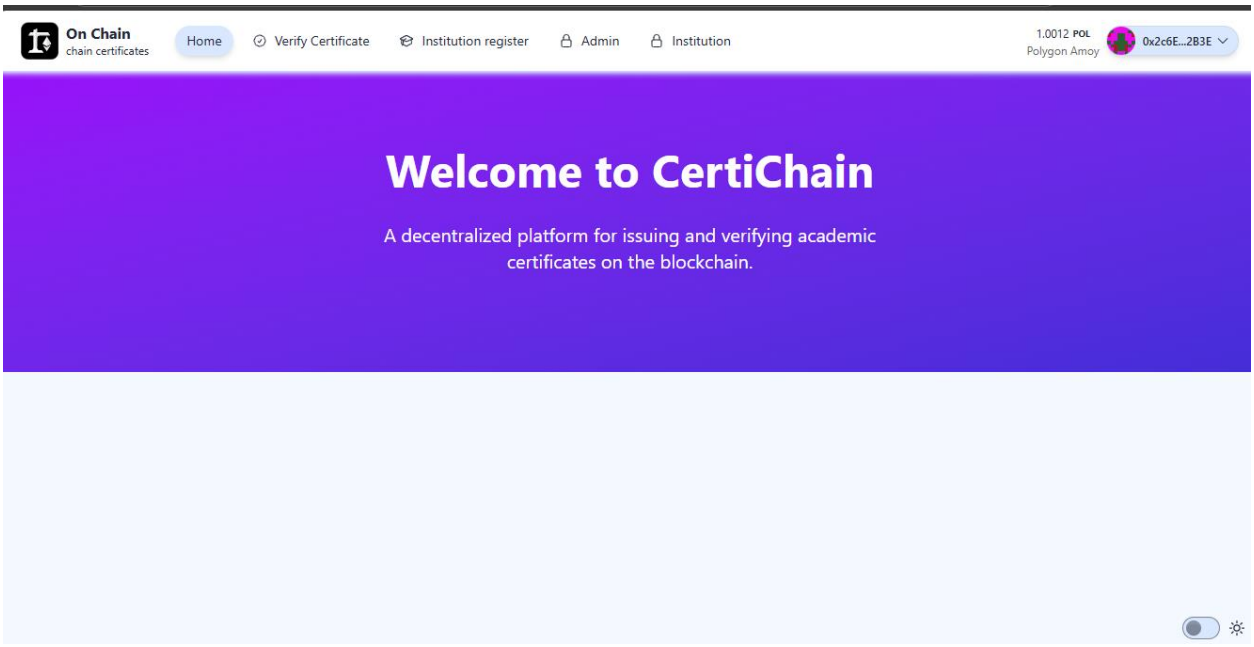
```
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.0;

contract DiplomaRegistry {
    struct Certificate {
        string ipfsCID;
        address issuer;
    }

    mapping(address => bool) public isInstitution;
    mapping(bytes32 => Certificate) public certificates;
    mapping(bytes32 => bool) public isRevoked;
    mapping(bytes32 => bytes32) public corrections;

    address public owner;

    event CertificateIssued(bytes32 indexed certificateHash, address indexed issuer, string ipfsCID);
    event InstitutionRegistered(address institution);
    event InstitutionRemoved(address institution);
    event CertificateRevoked(bytes32 indexed certificateHash);
    event CertificateCorrected(bytes32 indexed oldHash, bytes32 indexed newHash);

    modifier onlyOwner() {
        require(msg.sender == owner, "Only contract owner can perform this action");
        _;
    }

    modifier onlyInstitution() {
        require(isInstitution[msg.sender], "Not an authorized institution");
```

```
contract DiplomaRegistry {

    constructor() {
        owner = msg.sender;
    }

    function registerInstitution(address institution) public onlyOwner {
        isInstitution[institution] = true;
        emit InstitutionRegistered(institution);
    }

    function removeInstitution(address institution) public onlyOwner {
        isInstitution[institution] = false;
        emit InstitutionRemoved(institution);
    }

    /// Issue a single diploma
    function issueDiploma(string memory studentId, string memory ipfsCID) public onlyInstitution {
        bytes32 certHash = keccak256(abi.encodePacked(studentId, ipfsCID));
        require(bytes(certificates[certHash].ipfsCID).length == 0, "Certificate already exists");

        certificates[certHash] = Certificate(ipfsCID, msg.sender);
        emit CertificateIssued(certHash, msg.sender, ipfsCID);
    }

    /// Batch issue diplomas
    function issueBatchDiplomas(string[] memory studentIds, string[] memory ipfsCIDs) public onlyInstitution {
        require(studentIds.length == ipfsCIDs.length, "Input array length mismatch");
```

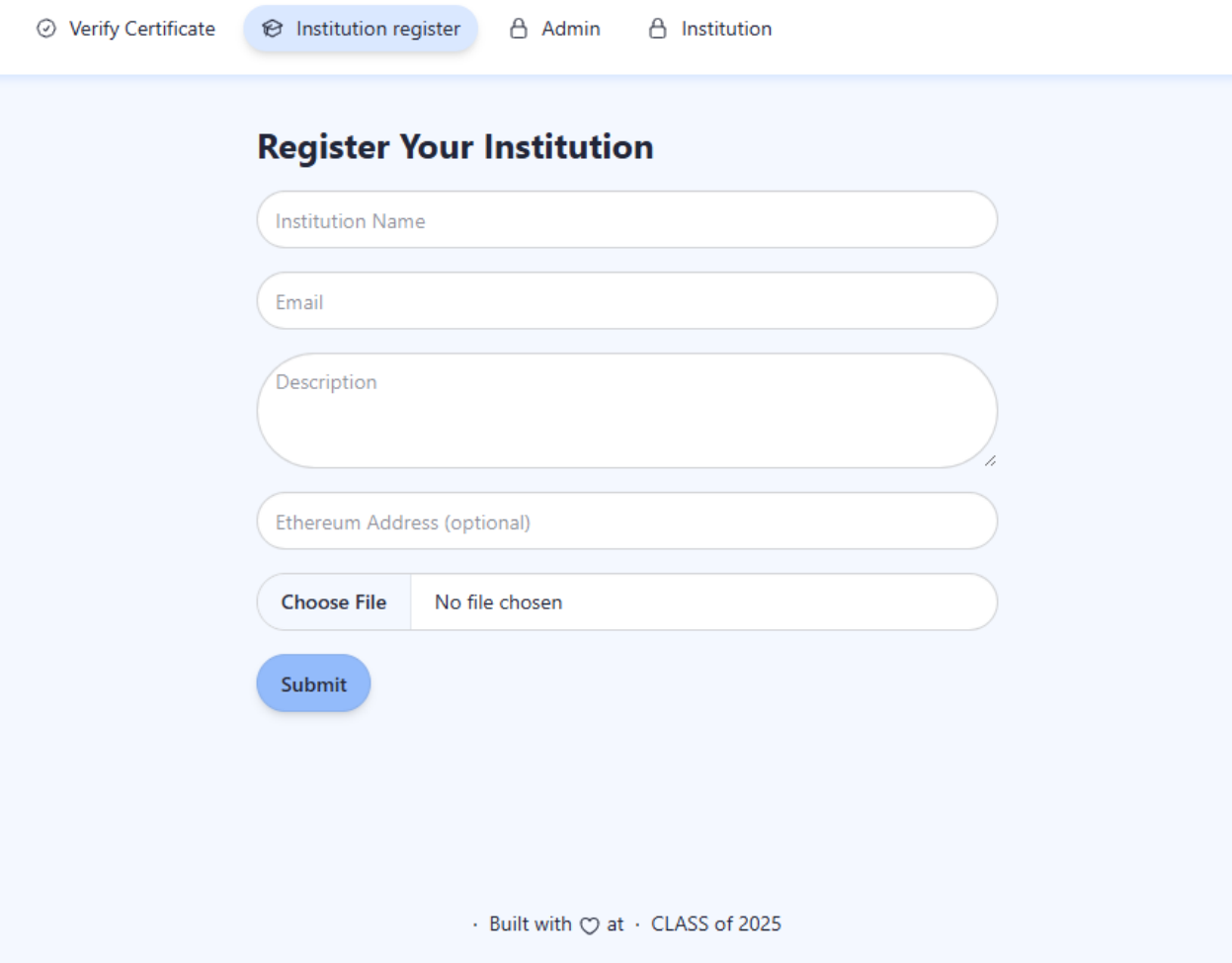
```
packages > hardhat > contracts > DiplomaRegistry.sol > ...
  4   contract DiplomaRegistry {
 68
 69       /// View cert details
 70       function verifyCertificate(bytes32 certHash) public view returns (
 71           string memory ipfsCID,
 72           address issuer,
 73           bool revoked,
 74           bytes32 correctedTo
 75       ) {
 76           Certificate memory cert = certificates[certHash];
 77           require(bytes(cert.ipfsCID).length != 0, "Certificate not found");
 78
 79           return (
 80               cert.ipfsCID,
 81               cert.issuer,
 82               isRevoked[certHash],
 83               corrections[certHash]
 84           );
 85       }
 86
 87       /// 🔒 Revoke certificate (issuer only)
 88       function revokeDiploma(bytes32 certHash) public onlyInstitution {
 89           require(certificates[certHash].issuer == msg.sender, "Not issuer of this certificate");
 90           require(!isRevoked[certHash], "Certificate already revoked");
 91           isRevoked[certHash] = true;
 92           emit CertificateRevoked(certHash);
 93       }
 94
```

Appendix D: DApp UI Screenshots

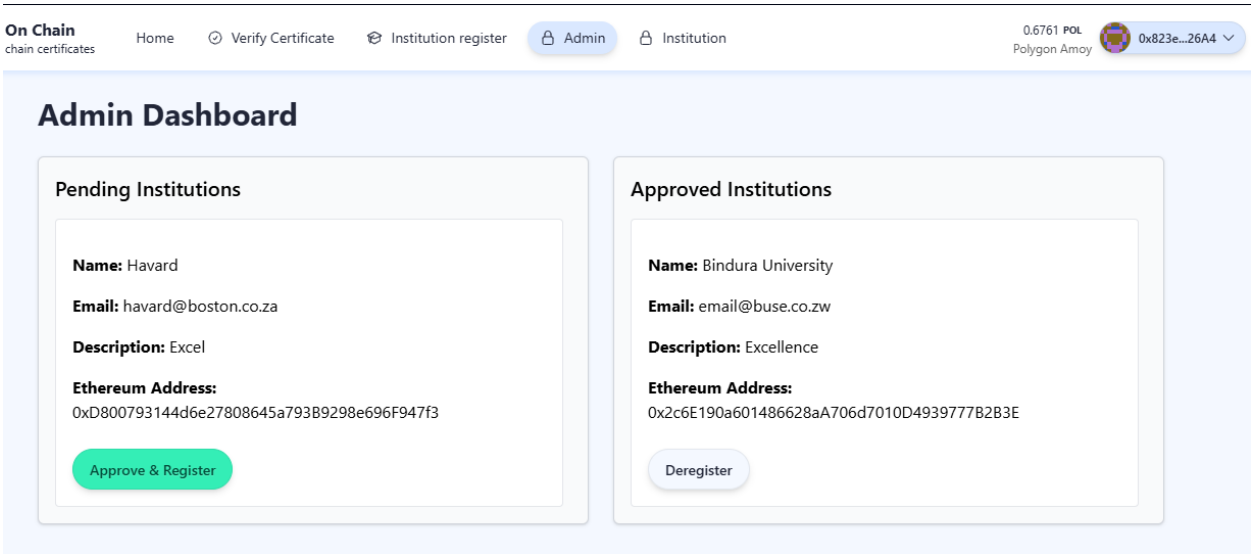
Landing Page



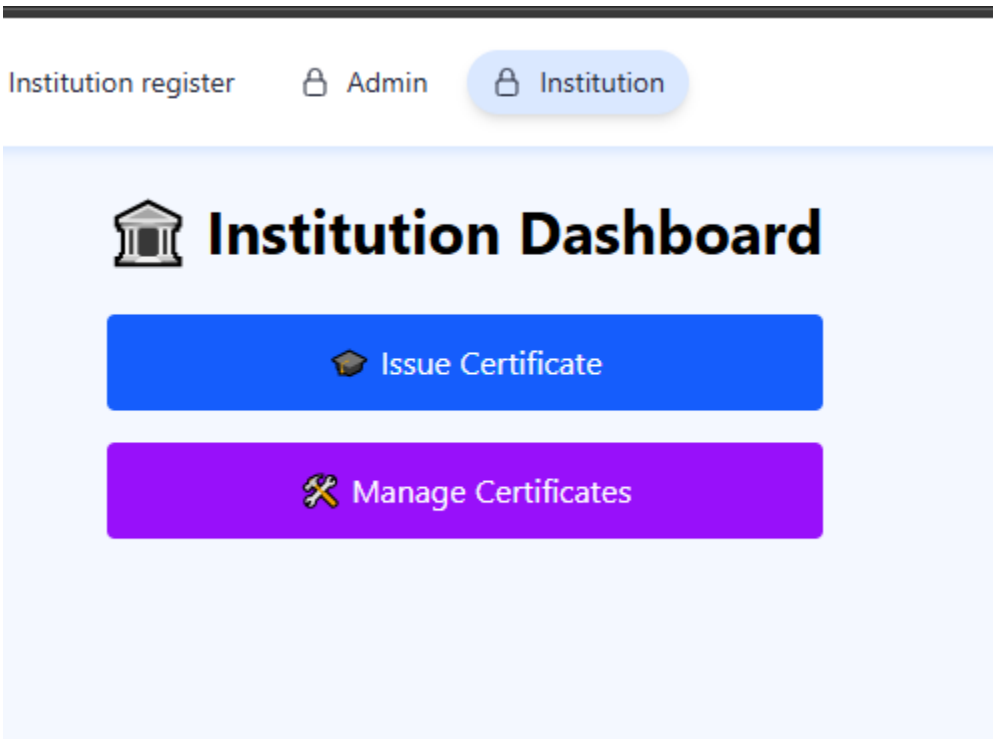
Institution Register Request

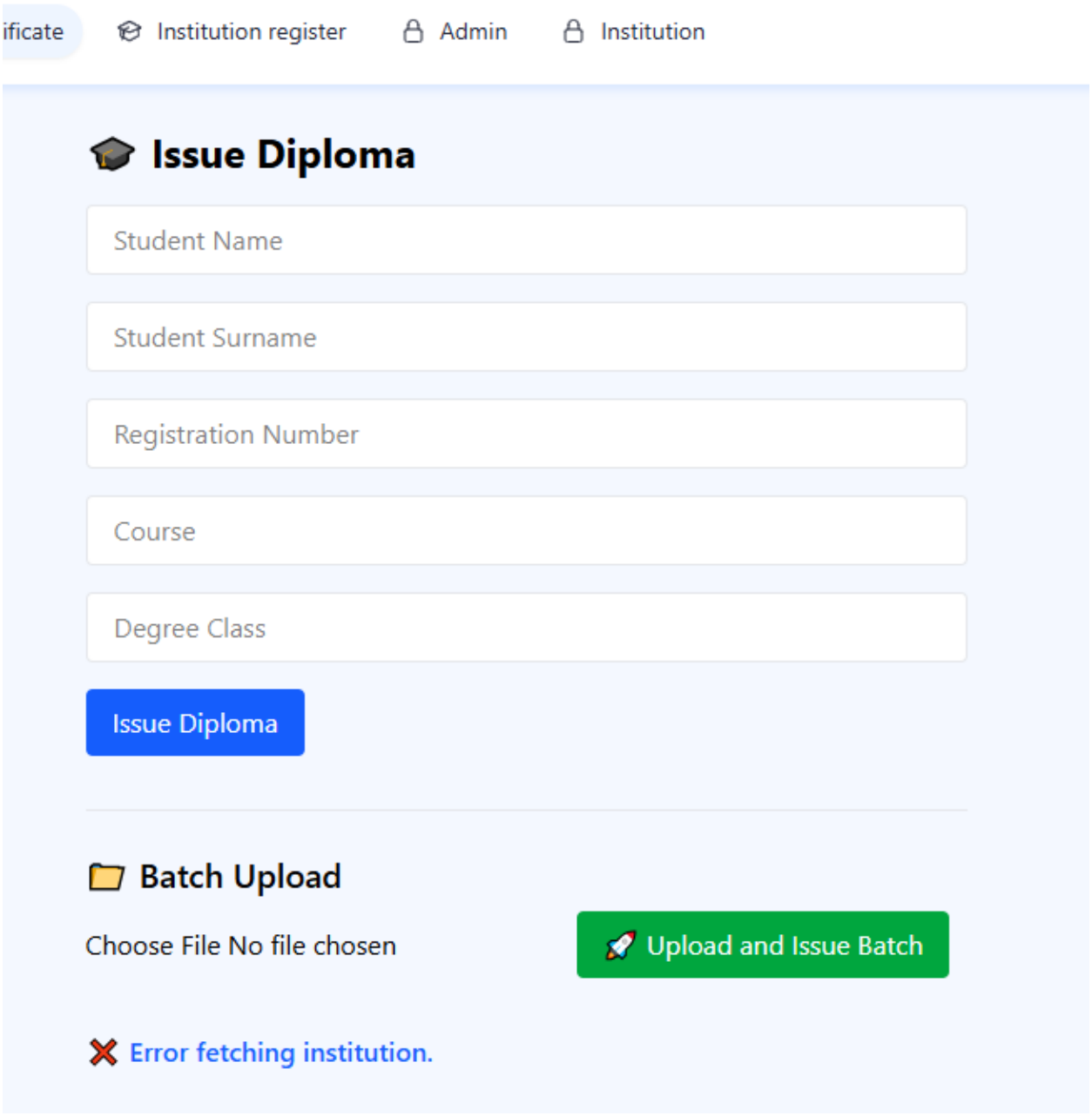


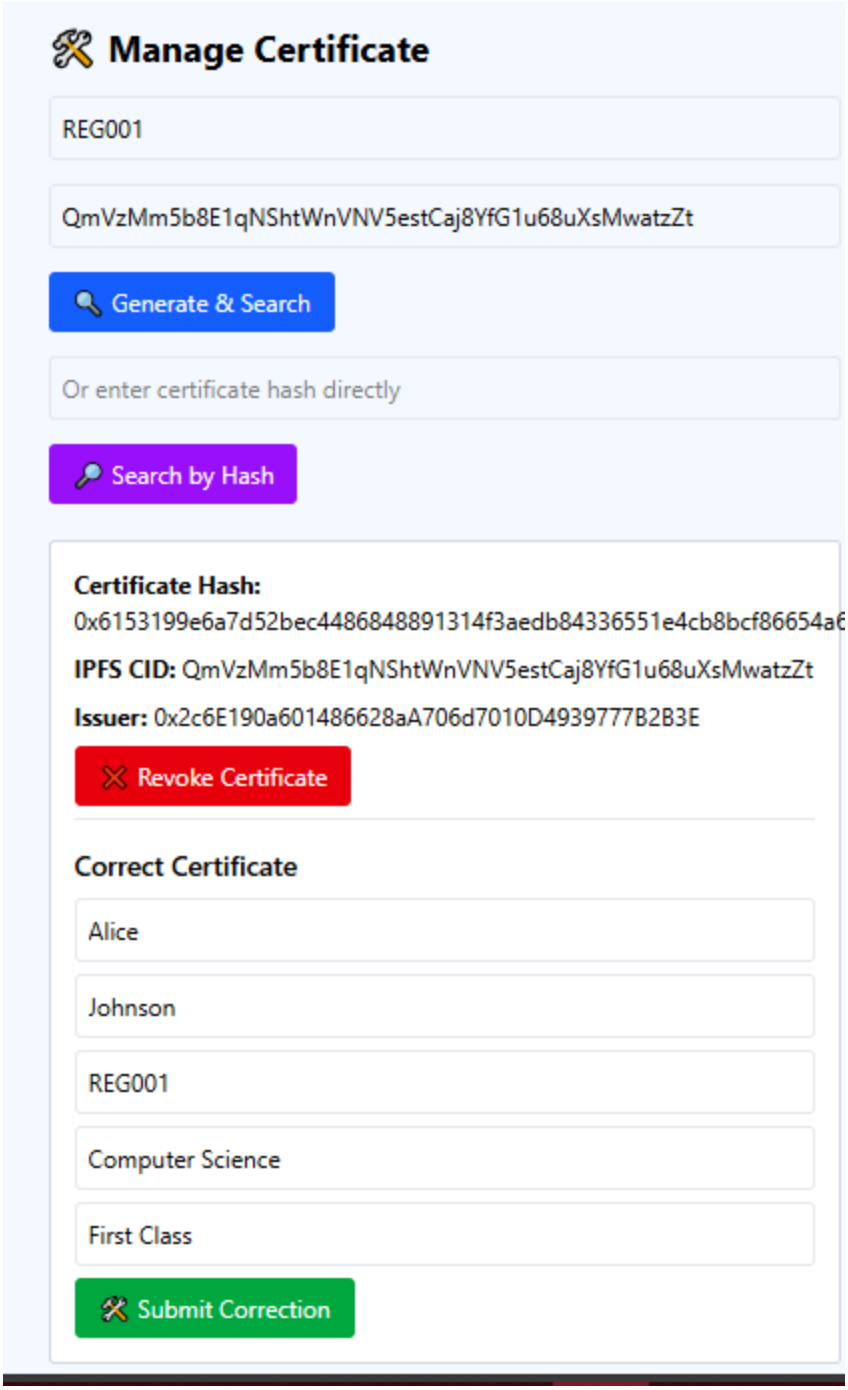
Admin Dashboard



Institution




ificate
Institution register
Admin
Institution
Issue Diploma
Student Name
Student Surname
Registration Number
Course
Degree Class
Issue Diploma
Batch Upload
Choose File No file chosen
Upload and Issue Batch
Error fetching institution.


Manage Certificate
REG001
QmVzMm5b8E1qNShtWnVNV5estCaj8YfG1u68uXsMwatzZt
Generate & Search
Or enter certificate hash directly
Search by Hash
Certificate Hash:
0x6153199e6a7d52bec4486848891314f3aedb84336551e4cb8bcf86654a6
IPFS CID: QmVzMm5b8E1qNShtWnVNV5estCaj8YfG1u68uXsMwatzZt
Issuer: 0x2c6E190a601486628aA706d7010D4939777B2B3E
Revoke Certificate
Correct Certificate
Alice
Johnson
REG001
Computer Science
First Class
Submit Correction