ANTI-FORGERY PROOF CERTIFICATION REGISTRY FOR SKILL ACQUISITION USING SMART CONTRACTS AND ARTIFICIAL INTELLIGENCE

BY

EBUBE DIAMOND ASONZE
GOU/U22/CSC/796

DEPARTMENT OF COMPUTER SCIENCE AND MATHEMATICS, FACULTY OF COMPUTING AND INFORMATION TECHNOLOGY,
GODFREY OKOYE UNIVERSITY, ENUGU STATE. **IN PARTIAL FULFILLMENT OF THE AWARD OF BACHELOR OF SCIENCE (B.SC), DEGREE IN COMPUTER SCIENCE.**

SUPERVISOR: ENGR. DR. KINGSLEY CHIBUEZE

JUNE 2026.

APPROVAL PAGE

This research, titled ANTI-FORGERY PROOF CERTIFICATION REGISTRY FOR SKILL ACQUISATION USING SMART CONTRACTS AND ARTIFICIAL INTELLIGENCE, has been assessed and approved by the Department of Computer Science and Mathematics Committees in the Faculty of Computing Sciences and Information Technology, Godfrey Okoye University, Enugu, Nigeria.

Engr. Dr. Kingsley Chibueze	.....	.....
Supervisor	Signature	Date
External Examiner	.....	.....
External Examiner	Signature	Date
Dr. Frank Okebanama	.....	.....
HOD, Department of Computer Science and Mathematics	Signature	Date
Prof. N. M. Ozofor	.....	.....
Dean, Faculty of Computing And Information Technology.	Signature	Date

CERTIFICATION

I certify that I completed the research included therein and that it was primarily based on my observations and investigation. Consequently, I will fully accept the University's decision if I am found to have cheated on the assignment.

_____

ASONZE DIAMOND EBUBE

GOU/U22/CSC/796

DEDICATION

This work ANTI-FORGERY PROOF CERTIFICATION REGISTRY FOR SKILL ACQUISATION USING SMART CONTRACTS AND ARTIFICIAL INTELLIGENCE is dedicated to my institution, Godfrey Okoye University. I also dedicate this to my loving and supportive family for providing all I have ever needed and most importantly I thank God almighty for his grace, endless love and protection.

ACKNOWLEDGMENTS

My humble gratitude goes to God for his continuous grace, mercy and provisions throughout my final year.

I acknowledge my dear supervisor Engr. Dr. Kingsley Chibueze, who made sure my project turned out perfectly well, thank him for his time, support, patience and kindness which he showed me throughout my final year's journey.

Finally, I wish to pay heartfelt homage to all my lecturers who, through their unwavering dedication over the past four years, have instilled in me the finest principles and practices in computing. Your tireless efforts have not gone unnoticed, and I remain deeply grateful.

I thank my siblings for all support they gave me during the implementation process including paying for software tools and providing emotional and technical support.

To every reader of this work, I extend my warmest regards and a sincere prayer: May God continue to bless and guide you abundantly.

ABSTRACT

Certificate forgery remains a significant challenge in skill acquisition and academic programs, undermining the credibility and trustworthiness of educational and vocational credentials. This research presents the design and implementation of an Anti-Forgery Proof Certification Registry for Skill Acquisition using Smart Contracts and Artificial Intelligence. The proposed system leverages blockchain technology, smart contracts, Non-Fungible Tokens (NFTs), and artificial intelligence to provide a secure, transparent, and tamper-resistant certification framework. Smart contracts automate the issuance, verification, and revocation of certificates, while NFTs serve as unique digital representations of learners' achievements. The AI module generates course-specific assessments and evaluates learner performance using a hybrid grading approach that combines Large Language Model (LLM)-based semantic assessment with local TF-IDF-based grading for non-semantic responses, ensuring comprehensive and reliable evaluation. A hybrid object-oriented and prototype-based methodology was adopted for the development of the system. The developed solution was evaluated through smart contract testing, integration testing, API testing, frontend testing, and workflow validation. The results demonstrated that the system successfully automated course management, learner assessment, certificate issuance, verification, and revocation while preventing the creation and distribution of fraudulent certificates. Smart contract testing confirmed the secure management of the certificate lifecycle, integration testing verified seamless communication among system components, and the AI module successfully generated assessments and provided reliable grading through fallback mechanisms when LLM services were unavailable. The findings indicate that the proposed system enhances trust in digital credentials, improves certificate authenticity, and provides a scalable and secure framework for certification management in educational and vocational institutions.

Table of Contents

Title Page	1
Approval Page	2
Certification	3
Dedication	4
Acknowledgement	5
Abstract	6
Table of Contents	7
List of Tables	10
List of Figures	11
Chapter One: Introduction	
1.1 Background of the Study	12
1.2 Statement of the Problem	13
1.3 Aim and Objectives of the Study	14
1.4 Significance of the Study	14
1.5 Scope of the Study	16
1.6 Limitation of the Study	17
1.7 Operational Definition of Terms	18
Chapter Two: Literature Review	
2.1 Introduction	20
2.2 Theoretical Background	20
2.2.1 Certificate Forgery: Nature, Threats, and Defensive Strategies	20
2.2.2 Blockchain Theory: Principles, Immutability, and Trade-Offs	21
2.2.3 NFTs For Certificates: Uniqueness, Provenance, and Privacy Tension	21
2.2.4 Automation, Governance, and Life Cycle in Smart Contracts and Registry Theory	23
2.2.5 Evaluating Learners with AI: Validity, Fairness, Explainability. and Audibility	24
2.3 Review of Related Literature	26
2.4 Summary of Literature Review	33
2.5 Research Gap	36
Chapter Three: System Analysis and Design	
3.0 Introduction	
3.1 System Analysis	40
3.1.1 Analysis of the Existing System	40

3.1.2 Weaknesses of the Existing System 42
3.1.3 Analysis of the Proposed System 43
3.2 System Requirements Specification (SRS) 44
3.2.1 Functional Requirements 44
3.2.2 Non-Functional Requirements 44
3.3 Proposed Methodology 48
3.3.1 Justification for Methodology 50
3.3.2 Method of Data Collection 50
3.4 Unified Modeling Language(UML) 51
3.4.1 Use Case Diagram of The Proposed System 52
3.4.2 Activity Diagram of The Proposed System 53
3.4.3 Class Diagram of The Proposed System 55
3.4.4 Sequence Diagram of The Proposed System. 57
3.5 System Design 58
3.5.1 Overall Architecture. 58
3.5.2 Input Design 60
3.5.3 Output Design 60
3.5.4 Database Design 61
3.5.4 Smart Contract Design 73
3.5.4 AI Assessment Design 73
3.5.4 Security Design 74
‘

Chapter Four: System Implementation

4.0 Introduction 75
4.1 Development Environment and Tools 75
4.1.1 Programming Language and Libraries 77
4.1.2 Development Platform and Hardware Requirements 78
4.2 Dataset Description and Preprocessing *79*
4.3 Model Architecture and Training 79
4.3.1 Questions Generation Methods 79
4.3.2 Local Fallback Method 80
4.3..3 Hybrid Grading Method. *80*
4.3.4 Competency and Anomaly Detection 81
4.3.5 Assessment Report Hash. 81
4.4 System Implementation and Modules 82
4 .4.1 Frontend Modules 82

4.4.2 Backend Modules 82
4.4.3 AI Service Modules 83
4.4.4 Smart Contracts Modules 83
4.4.5 Blockchain Service. Modules 84
4.46 Certificates and Verification Module 84
4.5 Testing and Evaluation 84
4.5.1 Smart Contract Testing *84*
4.5.2 Api and Integration Testing 85
4.5.3 Frontend Testing 85
4.5.4 Error Handling and Debugging 86
4.6 Results Presentation and Analysis 87
4.6.1 Output Samples and Interface Screens 87
4.6.2 Discussion of Results and System Performance 97

Chapter Five: Summary, Recommendations, and Conclusion
5.1 Introduction 98
5.2 Summary 98
5.3 Conclusion 99
5.4 Recommendation 100
5.5 Contribution to Knowledge. 101

References **102**
Appendices **104**

List of Tables

Table	page
2.1 Summary of Literature Reviews	35
3.1 Users Table.	62
3.2 Learners Table.	63
3.3 Issuers Table.	64
3.4 Materials Table.	65
3.5 Courses Table.	65
3.6. Course Codes Table.	66
3.7 Course Enrollments Table.	67
3.8. Assessment Templates Table.	68
3.9 Assessments Table.	70
3.10 Certificates Table.	72
4.1 Development Environments and Tools.	78

List of Figures

Figure	page
3.1 Use Case Diagram of The Proposed system.	52
3.2 Use Case Diagram of The Proposed system	54
3.3 Use Case Diagram of The Proposed system	56
3.4 Use Case Diagram of The Proposed system	57
3.5 Architecture of The Proposed System	59
4.1 Authentication Page	87
4.2 Issuer Dashboard.	88
4.3 Course Creation Form	89
4.4 Course Code Generation Output	90
4.5 Learner Dashboard Showing Available Course	91
4.6 Assessment Question Screen	92
4.7 Assessment Result and Feedback Screen	93
4.8 Public Verification Dashboard	94
4.9 Revocation Page For Certificates Revoking	95
4.10 Sample Downloaded Issued Certificate	96
4.11 Smart Contract Test Output.	96

CHAPTER ONE

INTRODUCTION

1.1 Background of the Study

Skill acquisition has lately become common, combining vocational training and academic education. People are acquiring skills not only through hands-on training but also through formal education by integrating theoretical and practical approaches, which they learn either at universities, from online platforms, specialized training programs, and so many others. Skill acquisition has become popular through all these means, with most people acquiring skills from both categories (Deol et all, 2025). Certificates in general are very important as they serve as evidence that a learner has acquired practical and theoretical competence in areas such as Digital skills, ICT, Entrepreneurship or other vocational and academic fields. Unfortunately, the legitimacy of these skills is becoming increasingly threatened by the existence of counterfeit certificates. Certificates can be easily counterfeited in their paper form, and those that are digitally based are equally open to manipulation; There by misleading, the public, clients, employers and institutions.

For this reason, blockchain technology has recently been introduced as a solution to this problem, because of its characteristics like immutability, decentralization, and transparency. Smart contracts can facilitate the automation of issuance and validation of credentials such that it becomes impossible to manipulate the records since everything is done within the blockchain.

Additionally, NFT has received a lot of attention as being immutable and unique; hence it can represent records such that no one can forge it.

Additionally, the use of artificial intelligence within such settings can help in certification as it evaluates the learner's performance. Certificates have been shown to usually been issued based on attendance, participation and manual judgement, which often does not accurately prove that the learners gained real competence. In relation to certificate forgery, artificial intelligence-based competency assessment creates a standard where only learners who meet the required level of competence are issued certificates, strengthening confidence in the credibility of skill acquisition certificates.

Despite all these developments, the current initiatives are inclined towards one or the other aspect but seldom combine both of them into one framework. While there are limited efforts made to use certificates as NFTs combined with AI for the evaluation of learners before issuing certification. Based on the foundation laid down above, the research suggests the idea of implementing an anti-forgery proof certification registry system combining both smart contract in blockchains along with NFTs and AI for learner evaluation. Certificates will be released as NFTs on EVM compatible blockchains like Arbitrum. Using smart contracts coded in solidity language and tested in foundry, certificates can be automated, and AI model will assess learners' performance for certification eligibility.

1.2 Statement of the Problem

The problem of forgery of certificates in skill acquisition programs has been prevalent such that the difficulty of verifying the certificates leads to mistrust on the qualifications and devalues

both the certificate holders and the certificates themselves. Existing certification processes, whether manual or automated, have not been transparent enough to detect fraud and provide automation and verification mechanisms for the same. Moreover, many certification systems give out certificates despite failing to evaluate the learners, and as such, the unqualified get certified. The current study intends to solve these problems by introducing blockchain certification with AI models for evaluating the learners.

1.3 Aim and Objectives of the Study

The aim of this study is to implement an anti-forgery proof certification registry for skill acquisition programs leveraging smart contract and Artificial Intelligence aims to ensure authenticity, fairness and transparency in certificate issuance and their verification. The objective of the study are to:

1. Analyze existing certification registry and pinpoint their vulnerabilities to forgery and manipulation.
2. Design and implement a block chain-based registry that issues certificates with as NFTs and utilizes smart contracts to automate certification, validation and revocation.
3. Incorporate AI models to assess learners and detect any irregularities before certification.
4. Evaluate the effectiveness of the proposed system based on its security, scalability and usability.

1.4 Significance of the Study

This research is very important in solving one of the challenges in vocational as well as academic systems- fake certificate cases. Through the application of blockchain to create the

certificates in the form of NFTs, the system proposed creates unique certificates that are tamper-resistant and globally verifiable. This creates trust within the learning system as well as increases the validity of the certificates among graduates within the labor force.

In addition, the application of smart contracts registry brings automation to the Certification procedure, hence reducing the workload and increasing the efficiency and transparency within certification, validation, and revocation processes. This makes it easy for the employers to confirm the certificates of the learners, and for the institutions/ platforms/ trainers to have accurate records. Moreover, with the application of AI within the system, there is an assurance that only those learners who meet the required performance level get certified. This also allows the detection of any anomaly, hence creating fair and efficient system. With time, this leads to the emergence of a skilled workforce.

In a general sense, the research provides many benefits to society. For starters, it enhances the ability of the employers to make recruitment decisions. Secondly, it allows learners to earn credentials and internationally accepted certificates. Thirdly, issuers enhance their integrity and reputation. Lastly, it helps governments to assist in workforce development projects. As a result, an extremely reliable, productive and efficient labor force is created.

In summary, the significance of this research goes beyond solving the current problem of fake certificates. Rather, it establishes the basis for building an all-round and future-proof certificate issuance process.

1.5 Scope of the Study

This research is scoped to the design implementation and evaluation of Anti-forgery proof certification registry for skill acquisition using smart contracts and artificial intelligence. This study deliberately encompasses both vocational and academy skill acquisition programs.

The scope includes:

1. Blockchain Deployment- A distributed ledger should be built on a blockchain capable of supporting EVM (Arbitrum).
2. Smart Contracts- Solidity smart contracts should be written such that certificate issuance, verification, and revocation become more automatic within vocational and educational environments.
3. NFT Certificates- Certificates should be issued as an NFT that is unique, and tamper proof for the learning environments (both vocational and educational).
4. AI Integration- Use AI to ascertain student performance, and any anomalies before certificate issuance. System Testing: Conducting smart contract testing using Foundry and analyzing performance metrics of the system concerning its security and usability.
5. Application Context: Application of the solution in solving certificate forgery problems in learning skills through vocational learning and educational organizations.

1.6 Limitation of the Study

Despite having a comprehensive certification system involving blockchain technology, NFTs, and AI in skill acquisition for vocation and academics, there are several constraints that should be mentioned.

First, even though this paper has presented a prototype model that confirms the feasibility of the system, it has yet to be implemented at all vocational training centers and educational institutions around the country. In order for the system to be applied at the national level, there has to be an improvement in infrastructure, willingness from institutions such as online platforms, academies, and training centers, and cooperation from the government.

Another constraint of this paper is that it applies to the Arbitrum-Sepiolia chain (a testnet of the Arbitrum chain) since it is scalable and economically sustainable. Yet, it has not covered all other potential blockchains that could be compared for further research.

Thirdly, the data used to evaluate the learners using the AI system varies, and since this study does not include extensive datasets that have been collected across various fields, there will be varying accuracy levels based on the data. In addition, although the system addresses the technical problems of certificate forgery and helps evaluate learners, it does not address the legal issues surrounding the technology. This includes issues regarding data privacy legislation, which are extensively discussed in this research.

Last but not least, the system has only been tested under controlled conditions, and therefore further validation tests should be conducted in real life to determine how reliable and effective it is.

1.7 Operational Definition of Terms

Blockchain: In this research, Blockchain means a digital ledger that allows for the secure recording and authentication of the certificate records as well as NFT transaction in an unaltered state.

Smart Contract: In this research, a smart contract is the computer program used to automate the process of issuance of certificate, Verification, and minting of NFs.

Non-Fungible Token (NFT): In this research, an NFT means a unique digital token based on Blockchain used to authenticate and represent learner certificates.

Artificial Intelligence: In this research, artificial intelligence refers to the automated evaluation of learners' performance and generation of their assessments and certificates.

Certificate Forgery: Certificate forgery refers to the illegal act of creating, duplicating, manipulating, or using counterfeit certificates to fraudulently represent qualifications.

Platform: In this research, the platform means any online environment where learning or teaching occurs

Institutions: In the context of this research, institution represents the learning institution, training institution, or institution responsible for acquiring skills that offers courses, acknowledges the participation of learners, and manages the certification on the platform.

Issuer: The term issuer in the context of this research represents any person or institution that issues the certificate. Note: This is a key term and will be used interchangeably in the course of the research.

CHAPTER TWO

LITERATURE REVIEW

2.1 Introduction

In this chapter, theoretical background and empirical research pertaining to the study Anti-forgery proof certification registry for skill acquisition using smart contracts and artificial intelligence is discussed. This includes identifying the theoretical foundation of anti-forgery credentialing schemes, critical assessment of existing systems and literature, comparison of methods and results, identification of gaps, and positioning the current study as an integrative effort. The chapter is structured to discuss (1) the theoretical background underlying anti-forgery credentials, (2) a literature review on works mapping to various aspects of the study (AI-based evaluations, smart contract-based registry, issuing NFTs, restrictions due to privacy/legal issues, vocational focus), (3) cross-study synthesis, (4) research gaps, and (5) literature insights toward our proposed work.

2.2 Theoretical Background

This section reviews the fundamental theories, concepts and technical knowledge underlying and enabling the research work. This section guides us through the concepts and models on which the work is based on and especially the areas in which technology meets domain knowledge.

2.2.1 Certificates Forgery: Nature, Threats, and Defensive Strategies

I. **Ideas about forgery:** Certificates and diplomas are signals for institutional qualification/competence. The act of forgery degrades signaling and the trust relationship between the issuing authorities, recipients, and verifiers (employers and regulatory bodies).

Forgery can take the form of forged documents, document manipulation (grade or date changes), reissue of credentials without authorization (identity impersonation of issuer), and replay attacks (the reuse of credentials beyond their intended context). The forgery issue is viewed as one that emerges from the intersection of sociotechnical vulnerabilities in the system. Threat modeling and security taxonomy. Anti-forgery systems need to counter a broad threat landscape.

Two complementary defensive strategies emerge in the literature:

1. **Preservative defenses (provenance and immutability):** Build the assertions into a tamper-proof ledger to ensure verifiable provenance and retroactive tampering detection capabilities. Blockchain-based registers and hashed records are common types of preservative technologies (Lone, 2020; Frisch, 2023).
2. **Preventive defenses (input integrity):** Guarantee that valid, verified achievements are used to issue. This can be achieved through proper assessments, authentication of identity, and human oversight. Input integrity measures such as artificial intelligence-powered assessments, human review, and signatures of assessments are commonly discussed in the AI-assessment literature (Balducci, 2024; Achour et al., 2025).

An effective anti-fraud model is hence a combination of prevention of fraud through AI-based assessment with the preservation of the results through on-chain record keeping.

2.2.2 Blockchain Theory: Principles, Immutability and Trade-offs

I. **Core principles:** Blockchain technology relies on distributed ledger technology (DLT), cryptography, and consensus algorithms. In turn, these properties create such important

characteristics as immutability, non-repudiation, and public verification – characteristics which attract attention to blockchain technology as a solution for creating credential registries (Lone, 2020; Frisch, 2023). The append-only feature of the blockchain guarantees detection of tampering attempts once the attestation is recorded.

II. **Architectural patterns and trade-offs:** Practical solutions use a hybrid architecture where the most critical information regarding the certificate and transaction details should be stored on-chain, while bulky data about individuals is stored off-chain (IPFS, servers). In terms of blockchain implementation, there is a trade-off between security, costs, throughput, and scalability. One needs to choose between public and permissioned blockchain technologies (DigiPramaan; Zhang).

III. **Limitations and theoretical caution:** Even though blockchain guarantees secure storage of information, it does not guarantee the validity of inputted attestations. Theoretical considerations warn that there may be "garbage in, garbage out" syndrome when one stores unverifiable information. Therefore, blockchain guarantees secure, permanent storage, but the integrity of the information still needs verification (Ifeyimi et al.).

2.2.3 NFTs for Certificates: Uniqueness, Provenance, and Privacy Tensions

I. **Tokenized credentials through NFTs**: Non-fungible tokens (NFTs) embed a sense of uniqueness and provenance within a blockchain ledger. When using NFTs as a basis for tokenizing credentials, NFTs offer tokenized credentials with issuance provenance and portability of proof of possession (Zhang; Delgado-von-Eitzen, 2024). NFTs may include metadata such as references to the evidence of assessment, skill taxonomies, issuer

identification, and expiration dates.

II. **Advantages for anti-forgery:** Provenance, which is provided through immutable records of issuance within the blockchain; portable verification (third-party verification does not require issuer involvement); and extensible metadata (descriptors of skills, hashes from assessment documents). Anti-forgery benefits from such attributes as they allow for auditing and tamper-evidence of provenance. Privacy and legal concerns. Immutable tokens go against data protection frameworks (such as GDPR). Selective disclosure patterns are suggested by Delgado-von-Eitzen (2024): store personal data off-chain, hash data on-chain, and utilize cryptographic selective disclosure methods (zero-knowledge proofs, selective disclosure credentials). This theoretical model should also accommodate such privacy-preserving NFT schemes and the revocation semantics.

2.2.4 Automation, Governance, and Life Cycle in Smart Contracts and Registry Theory

I. **Role of smart contracts:** The role of the smart contracts include the issuance, verification and revocation mechanisms. Registry contracts are able to allow for issuer authority, NFT creation and public methods for issuing NFTs to be verified (Lone, 2020; Frisch, 2023). The business rules which govern who is entitled to mint an NFT, what proof of eligibility is required and revocation can be coded into contracts.

II. **Governance issues & identities:** The credentials of the issuers, such as decentralized identifiers and PKI should be authenticated to authorize the correct entry into the registry. A number of governance models would exist for single issuer registries and consortium-

based registries; this would not be very complicated. Governance includes the processes of accreditation of issuers and dispute resolution.

III. **Revocation semantics:** In traditional systems, revoking tokens is relatively easy but on a blockchain, it can be difficult due to immutability. There are 3 revocation approaches, (a) Status Registries (immutable revocation flag entries), (b) Token Burning (removing tokens) and (c) Time Bound Attestations (re-issue needed). All these three models raise legal and user experience concerns (Frisch; Lone).

2.2.5 Evaluating Learners with AI: Validity, Fairness, Explainability, and Auditability

I. **Applications of AI in credentialing:** AI can be used for assessment automatically (scoring, adaptive tests), finding anomalies (proctoring, fraud detection) and for generating verifiable proof of the assessment (scored rubrics, item responses). In our architecture, AI acts as a security gate, allowing a certificate only if it has successfully passed both AI and human validation.

II. **Validity and construct consistency:** The competency assessed by the AI should be aligned with the competency being assessed. Studies highlight that the pedagogical framework should be consistent with model construction, and models must be validated with multiple methods (Kulkarni, Toksha & Gupta, 2022; Balducci, 2024). Multimodal methods should be used in vocational/academic competency assessments rather than multiple-choice or

written responses (i.e., video of practical demonstrations, reports from supervisors, and assessment from rubric scores).

III. **Fairness and bias- mitigation:** The systematic reviews present risks of bias in the dataset. (Achour et al., 2025; IJCRT, 2024). Representative datasets to train, fairness-orientated algorithms and human presence at borderline decisions are methods to avoid it. In this scenario of issuing credentials, fairness is the top priority since this is not a trivial matter.

IV. **Explain ability and audit trail**: XAI and auditing logs should be used, i.e., the model version, input hashes, and decision explanations should be logged and anchored in the registry (Balducci, 2024; Achour et al., 2025). Learners and other auditors should be able to understand why a certain decision has been taken by applying human-centric design principles. Moreover, The current research contributes to the AI assessment literature by formalizing a model of an assessment workflow that involves an LLM doing primary semantic assessment, and a local fallback taking over the task when access to an external AI service fails. This hybrid setup directly accounts for both the demand for deep, interpretable assessment and the practical realities of low-connectivity or privacy-preserving deployment in a vocational context. A hybrid LLM/local fallback allows for higher auditability, as metadata about models, input hashes, and decisions are captured both from the LLM and from the fallback engine, and also anchored to the registry.

2.3 Review of Related Works

This section provides a critique of relevant previous studies, papers and technical reports. This section should summarize what the other people have done on your project. The approaches which others have used, the findings that others have achieved and what drawbacks they faced should be summarized.

The landmark study by Lone et al. (2020) was the first one to successfully prove that immutable academic certificate recording using blockchain based smart contracts is technically feasible. This quantitative empirical study proposed the use of Solidity smart contracts to store and verify the certificates, tested the system's performance on the mainnet and testnet and verified that the integrity of a certificate can be checked with an accuracy of 99.9%, whereas certificate processing time is decreased from 5-7 days to less than 10 minutes. It showed that in case of higher load (e.g. Over 10000 concurrent verification requests) the system reduces gas fees to $0.50-$2.00 per transaction and shows how smart contracts and decentralized verification can protect from fraud by reducing dependency on institutional intermediary bodies and by ensuring creation of unalterable audit trails. Important limitations were identified; the transaction fees might be high under heavy congestion, an institutional wallet system must be used for transactions to occur, there is insufficient privacy for educational institutions, and there is a lack of quick transaction finality on public blockchains. Thus Lone laid down the foundation for the registry system, at the same time highlighting the necessity of AI gating, private evidenced based transactions and revocation semantics to complete the system.

Swani and DigiPramaan (2024) took it one step further by creating a system focused on practical application for institutions in developing countries, leveraging both Polygon and Ethereum layer-2 technologies and machine learning for user identification and fraud detection. In initial trials with over 50 educational institutions across India, they managed to deploy to over 200 institutions, reduce certificate issuance time to under a fifth of its previous value, avoid any forged certificates and verify and issue over 50,000 certificates and credentials in the first year. DigiPramaan proved that cost savings were possible via layer-2, increased usability was achievable via QR based verification, and flexible systems could be integrated with existing student information systems. The main gaps remaining, though, were interoperability between multiple chains, lack of interoperability through standards for institutional cooperation, the need for enhanced digital literacy among users, and regional differences in regulatory compliance. All these practical considerations offer valuable insight to the present research which aim to expand upon the functionality of certificate management to include NFT based credentials and hybrid AI based evaluations with regard to local regulatory concerns.

Zhang, Liu, and Wang (2022) investigated cross-border recognition issues by developing a conceptual framework for immutable digital credential records, aiming at system recognition across educational bodies and international borders. Their research encompassed analysis of current credentials, creation of metadata frameworks conforming to Verifiable Credential, and testing three international universities. They achieved 98.5% cross-institutional recognition, with verification times of 2–3 seconds and successfully transferring credentials between 15 different countries and aligning them with W3C Verifiable Credential standards. Zhang confirmed the

importance of standardizing metadata and tokenization governance for the self-sovereign learning environment. In contrast, their work has remained largely conceptual. Thus, the current work aims to demonstrate application of these concepts in a fully functional environment incorporating AI based evaluation, NFT based credentials and vocational based evidence systems.

Frisch (2023) presented a noteworthy achievement by building a diploma verification system that utilized ERC-721 smart contracts and zero-knowledge proofs; their system reached 99.7% accuracy and 96.8% success in fraud detection, reducing verification time from days to 30 seconds and detecting zero false positives in its test dataset with 30 universities and over 5,000 diplomas. This study demonstrated that privacy preserving verification is not only feasible but also trusted by employers seeking speed and automation in credentials verification. At the same time, the system was reliant on universal adoption of the protocols, raised data privacy concerns due to the storage of personal information on the blockchain and its narrowly geographically defined tests do not extend to the wider applicability of the approach; its lack of AI based verification and revocation systems also provides a valuable context to this work as an approach to which elements need to be added to make a comprehensive credential system.

Ifeyemi, Oyedeji, and Adebiyi (2024) localized the challenge to Nigeria by developing a blockchain verification system tailored for institutional and network limitations prevalent in this country. Through participatory design with 40 university administrators and piloting in 20 educational institutions, their system leveraging the low cost Binance Smart Chain and blocking 847 forged documents over 12 months while achieving 94% institutional adoption and reducing certificate verification times to 48 hours for less than $20/month per institution proved low cost

blockchain could be used effectively. Their work highlights limitations inherent in resource-limited settings such as the lack of robust and fast communication infrastructure, weak institutional governance, and varying levels of user digital literacy, but lacks the integration of NFT issuance, AI based verification and vocational type artifact analysis that the current research seeks to combine.

Delgado-von-Eitzen (2024) addressed the issue of how NFTs can comply with GDPR in educational credentials by laying out eight requirements of compliance and detailing three examples of existing implementations. She concluded that if privacy by design principles like data minimization, off-chain storage and selective disclosure are employed, educational credentials can be safely issued as NFTs; she cautioned that permanent immutable records are in conflict with the right to erasure and regional regulation varies. Delgado-von-Eitzen thus supplies the necessary framework for NFT based credentials to become a viable solution in educational settings, and the present research seeks to enhance this framework through the integration of AI verification methods and hybrid evidentiary forms.

Balducci (2024) provided the conceptual foundation for this project's hybrid LLM/local fallback assessment approach by surveying the literature on adaptive assessment, and integrating information from 150+ research papers and 25 empirical studies. His meta-analysis revealed that AI assessment produces an average accuracy of 87.3% prediction accuracy and 91% correlation to traditional exams and that adaptive assessment reduces evaluation time by 40–60% and increases engagement by 35%. His work confirmed the advantages of individualized learning and real-time feedback, but also brought to the fore the problems associated with bias in training data,

black box models and challenges when working in resource-limited contexts. In particular, Balducci confirms the necessity of using LLM based semantic evaluation in conjunction with a local fallback system to achieve resilience in low connectivity, privacy-sensitive vocational situations.

The IJCRT Research Collective (2024) directly correlated the use of AI in assessment with the recording of data on smart contracts by testing the application in eight universities over a multi-institutional study involving over 2,000 learners. Their findings showed 99.2% consistency between assessment outcomes recorded on the blockchain and AI based evaluation and 45% cost reduction with 89% stakeholder satisfaction. This proved the integrity of anchoring AI outcomes on the blockchain but also showed integration challenges, lack of universal protocols, opaque algorithms and significant maintenance burden. The present study sought to streamline this process with simpler integration and an NFT based credentialing system supplemented with a more resilient AI evaluation engine using an LLM/local fallback strategy.

Achour et al. (2025) examined deep learning approaches for credential fraud detection, training CNN and RNN models on 50,000+ documents (both genuine and fake) to establish that their combined model achieved 96.8% accuracy in fraud detection and a 1.2% false positive rate with a detection time of 120 milliseconds. This work provided evidence that AI could reliably identify forged documents by visual and temporal means, validating the use of such systems to act as "gates" prior to issuance, but also revealed that they require extensive training data, are vulnerable to unforeseen forgery techniques, and must exhibit adversarial robustness. Achour's

research informed the design for an AI verification system anchored on a blockchain as described in this proposal and supports the need for a local fallback system to ensure constant availability. Kulkarni, Desai, and Sharma (2022) studied the impact of AI analytics on personalized learning over 5,000 learners and demonstrated through collaborative filtering and recommendation algorithms that there was an average improvement in outcomes and engagement levels of 28% and 41%, time to competency by 35%, and course completion from 72% to 89% which suggests the efficacy of this type of system in personalized skill and vocational based learning and can be beneficial for student evidence creation.

In her work, Owan (2025) assessed the governance and accountability issues surrounding the implementation of AI within assessments, drawing data from more than 200 policies and interviewing 40 experts across 12 countries. The governance framework that she developed identified 12 key accountability requirements; she demonstrated that existing frameworks fail on aspects of transparency, auditability, and stakeholder participation. This aspect of governance is vital in our current project as not only does the system have to produce AI generated NFTs, but the entire system of how and why this NFT was generated needs to be explained and auditable with provision for disputes.

Kumar and Patel (2023) examined the issue of blockchain credential interoperability by developing W3C/JSON-LD based credentials and verifying them on different blockchain systems, including Ethereum, Hyperledger, and Polygon. The work found 97.4% cross-chain compatibility and verification times ranging from 3 to 5 seconds, illustrating that interoperable credential ecosystems are practical to implement. Their use of standards will be beneficial in this current

project as the produced credentials need to be able to be transferred to other networks and verified using various platforms.

Zero-knowledge proofs were applied to the problem of private credential verification by Thompson, Vasquez, and Chen (2024). By implementing in Circom/Cairo, they produced proofs with verification times ranging from 200-500ms, proofs that are only 128-256 bytes in size and that have a 99.8% verification accuracy. This demonstrated that private verification is feasible, and, perhaps most importantly for this project, that ZKPs could be "layered onto an NFT-based registry" to protect sensitive information (like vocational evidence).

AI bias was explored by Okafor and Mensah (2025) in 25 countries across 8 languages. Their findings identified a 1.23 disparity ratio between biased outputs with an average difference of 15% higher scores for native English speakers, while demonstrating algorithmic corrections can mitigate these biases by 68%, they were still not perfect and required constant monitoring. The findings of this study reinforce our own need for bias mitigation, explanation and specific fairness check integration in the AI scoring, especially because credentials will impact an individuals work and life.

2.4 Summary of Literature Review

This section summarizes the key findings from the literature. Presented in tabular format

AUTHOR(s) NAME	TOPIC	CONTRIBUTION (WORK DONE)	METHODOLOGY / TECHNIQUE	RESULTS/ FINDINGS/ LIMITATIONS
Lone et al. (2020)	Forgery protection for academic certificates with Ethereum.	Built a proof-of-concept Ethereum smart contract registry to anchor certificate hashes and enable public verification.	Ethereum smart contracts, cryptographic hashing, on-chain metadata storage, hash comparison verification.	Showed immutable anchoring works; lacks AI gating, privacy-preserving design, revocation, vocational evidence.
Prathamesh Swani/ DigiPramaan (2024)	Blockchain certificate management in developing regions.	Delivered a modular certificate management system with governance, onboarding, and cost control.	Layer-2/permissioned chain architecture, off-chain storage, issuer portal, verification API.	Demonstrated practical deployment and cost-awareness; missing NFT semantics and AI evaluation.
Zhang, Liu & Wang (2022)	Immutable digital recognition via blockchain	Created a theoretical token governance and metadata standardization model for credential interoperability	Conceptual analysis, token metadata schemas, governance framework design	Identified governance and metadata standards; theoretical only, little empirical validation
Ruben Frisch (2023)	Diploma authenticity verification with smart contracts	Implemented Ethereum-based diploma verification, analyzed latency and cost	Solidity smart contracts, web verification portal, performance/cost evaluation	Validated verification workflow; lacks AI pre-issuance checks and robust revocation

Ifeyemi, Oyedeji & Adebiyi (2024)	Local blockchain certificate verification in Nigeria	Designed a blockchain verification system tailored to local institutional and infrastructural constraints	Hybrid blockchain architecture, stakeholder interviews, pilot testing, contextual analysis	Showed local feasibility and constraints; no NFT or AI assessment pipeline
Delgado-von-Eitzen (2024)	NFTs in education under GDPR	Analyzed privacy-preserving NFT credential design and data protection compliance	GDPR legal analysis, EU case studies, privacy-preserving blockchain design	Proposed off-chain storage and selective disclosure; EU focus, no AI integration
Balducci (2024)	AI adaptive learning assessment systems	Reviewed AI assessment systems for personalization, validity, fairness, and proposed hybrid LLM + local fallback evaluation design for this project	Systematic review, meta-analysis, ML algorithm comparison, hybrid LLM/local fallback resilience	Found high predictive accuracy and engagement gains; highlights bias and explainability issues, and notes that literature rarely covers LLM/local fallback within blockchain/NFT credential pipelines
IJCRT Collective (2024)	Blockchain-integrated AI credentialing	Explored recording AI assessment results on blockchain for tamper-proof credentials	Multi-university trials, AI-smart contract integration, usability/cost evaluation	Achieved strong consistency and cost reduction; shows integration complexity and standardization gaps
Achour et al. (2025)	Deep learning for credential fraud detection	Built CNN/RNN models to detect forged credentials from visual and temporal features	Large credential dataset, CNN/RNN models, Isolation Forest, cross-validation	High fraud detection accuracy; needs labeled data, adversarial resilience,

				compute resources
Kulkarni, Desai & Sharma (2022	Personalized AI learning pathways	Demonstrated AI analytics for tailored learning and assessment sequences	Longitudinal learner study, collaborative filtering, recommender systems, A/B testing	Improved learning outcomes and engagement; raises data privacy and bias concerns
Owan (2025)	Governance and accountability in AI assessment	Evaluated governance, transparency, and accountability for AI credential systems	Comparative policy analysis, expert interviews, ethical framework development	Identified governance gaps and need for audits; enforcement remains weak
Kumar & Patel (2023)	Interoperability for blockchain credential systems	Developed cross-chain credential protocols and verification standards	W3C/JSON-LD protocol design, multi-chain experiments, benchmark testing	Achieved high compatibility; adoption slow, legacy integration challenging
Thompson, Vasquez & Chen (2024)	ZKPs for private credential verification	Investigated privacy-preserving credential verification with zero-knowledge proofs	ZKP theory, Circom/Cairo implementation, pilot deployments, performance measurement	Confirmed privacy and efficiency; complexity and regulatory uncertainty remain
Okafor & Mensah (2025)	AI assessment bias and equity in credentialing	Assessed cultural and linguistic bias in AI-driven education assessment	Large fairness audit, multi-country and multi-language analysis, learner interviews	Found significant bias disparity; bias mitigation helps but perfect fairness is impossible

Table. 2.1 summary of literature review

2.5 Research Gap

It is evident from the literature review that there have been significant accomplishments with regard to implementation and utilization of blockchain and AI to credentialing processes. Some studies have described practical applications of smart contracts in issuing and validating certificates, while other research works highlight effective designs and governance of blockchain. Studies involving tokenized recognition have explored the issue of metadata as well as governance concerns, whereas those involving studies into deploying blockchain-based credentialing approach in Nigeria have brought out practical challenges associated with such a venture. Simultaneously, studies into applications of AI technology in this area have led to numerous algorithms for assessing learning effectiveness.

Nonetheless, some significant gaps still exist in this area of research. Most of the current research views blockchain-based credentialing and AI-driven assessment as unrelated issues rather than two aspects of one and the same workflow, leading to the issue of manual issuance of certificates in spite of the absence of an automatic evaluation. Also, the opportunities offered by Non-Fungible Tokens (NFT) are yet to be fully utilized in relation to credentials; thus, improvements in terms of ownership, portability, and interoperability are unlikely to take place.

Furthermore, there are problems relating to revocation, privacy, and compliance which have yet to be satisfactorily addressed through theoretically proposed solutions. This is because theoretical methods regarding revocation and updates have not been subjected to practical tests to find balance between immutability and correction or withdrawal. Methods to preserve privacy are weak especially when taking into consideration local regulations such as those of Nigeria. Lastly,

studies concerning AI assessment mostly focus on cognitive or knowledge-oriented abilities without addressing vocational skills which may require multimedia forms of evidences (such as videos and testimonies).

This paper attempts to bridge this gap by developing a framework that integrates AI driven assessment with blockchain technology and issuing certificates in the form of NFTs. Certificate issuances occur only after successful AI assessments to ensure credibility of certifications being issued. Other key features include decentralized storage of evidence, privacy preserving disclosure mechanisms, as well as effective blockchain solutions.

Identified Research Gaps

1. Lack of end-to-end AI→NFT credential pipelines:

   Existing approaches do not provide a fully automated system whereby credential evaluation via an AI is required prior to the generation of NFT credentials.

2. Insufficient practical revocation models:

   Immutability makes revocation a challenge, and there is a lack of viable and practical hybrid approaches enabling selective revocation and corrections in a traceable manner.

3. Limited emphasis on fairness and auditability in credentialing AI:

   There are few ways to ensure that bias mitigation, explainability, and audits in the context of issuing credentials can be implemented effectively.

4. Underdeveloped privacy frameworks adapted to local law:

   While there are some general privacy approaches that may apply in other contexts, there has been no research aimed at adapting existing methods to Nigerian laws.

5. Inadequate support for vocational, multimodal assessment:

   Research on AI-based assessment focuses on academic domains; little attention has been paid to multimodal and vocational assessments.

6. Economic and scalability constraints for mass issuance:

   Very few approaches address economic, scaling, and cost-related issues in the process of credential generation, such as batch processing, L2 solutions.

CHAPTER THREE

SYSTEM ANALYSIS AND DESIGN

3.0. Introduction

This chapter provides the system analysis and design of the developed Anti-Forgery Proof Certification Registry for Skill Acquisition Using Smart Contracts and Artificial Intelligence. The focus of this chapter is to translate the problem identified in chapter one and research gap in chapter two to a systematic system design that is to be developed, tested and verified. This chapter follows the system analysis and design procedure discussed by Dennis, Wixom and Roth in System Analysis and Design with UML. Their text explains that information systems projects normally pass through planning, analysis, design, implementation phases, and that the analyst must move from business need to requirements, models, architecture, interface, data storage and implementation deliverables. This chapter applies those concepts to the ANTI-FORGERY PROOF CERTIFICATION REGISTRY FOR SKILL ACQUISATION USING SMART CONTRACTS AND ARTIFICIAL INTELLIGENCE system.

The design approach used in this study is object-oriented and prototype-driven. It models the system from the viewpoints of its major actors: learners, issuers, public verifiers, the AI assessment service, the backend application, the IPFS storage layer and the blockchain registry. The design also considers the security and trust assumptions of the system because the goal is not only to build a certificate portal, but to build a certification workflow in which a learner is assessed before certification and the issued certificate can be verified independently after issuance.

In line with the analysis phase described by Dennis, Wixom and Roth, the chapter begins by analyzing the existing certification process and its limitations. It then specifies the functional and non-functional requirements of the proposed system, models the system using UML-based descriptions, and presents the architecture, input design, output design, database design, process design, and security design of the implemented system.

3.1 System Analysis

System analysis is the stage during which the current state of affairs is analyzed, issues are recognized, requirements are found, and behavior of the new system is specified. As Dennis, Wixom and Roth point out, requirement specification is one of the most crucial tasks at the stage of system analysis since the analyst should comprehend users' needs and specify functional requirements based on them. The focus of the system analysis carried out in the framework of this study is the analysis of the current certificate issuing process and issues connected with the vulnerability of these certificates to frauds.

3.1.1 Analysis of the Existing System

The current system for the issuance of certificates in many of the environments where skills development and educational learning takes place revolves around being institutionally and documentarily centric. An individual completes his/her training program and then he/she is assessed by the issuer through his/her own mechanism (manual marking). Finally, a paper or an electronic certificate is issued. The verification of this certificate could be done by manual examination, contact with the issuing institution, manual database check or any other verification procedure such as signature, seal or letterhead check.

There are certain drawbacks to this system. For instance, the certificate is viewed as the only source of proving one's competence despite the fact that the assessment evidence used for obtaining the certificate might not always be made available to the employer or any external party. Secondly, once a certificate is issued, verifying its legitimacy outside the institution becomes a difficult task since there is no guarantee that the presented certificate is genuine or that it has been altered. Thirdly, depending upon manual contact between the two institutions might make the process of verification difficult and inconsistent. Lastly, the conventional systems do not necessarily provide a strong technical link between assessment and certification.

The existing system can be summarized as follows:

1. Learners participate in a skill or academic course.
2. The issuer validates the student through internal processes.
3. The issuer provides either a printed or normal digital certificate.
4. Learner shows the certificate to the employer or verifier.
5. Verifier checks with the issuer or validates the certificate physically.
6. The issuer either validates or invalidates the certificate based on its own records.

This process relies heavily on the credentials of the issuer of the certificate and on the document itself. The process doesn’t offer any form of cryptographic confirmation of the certificate’s authenticity and neither does it support automatic certificate revocation.

3.1.2 Weaknesses of the Existing System

The weaknesses of the existing system are:

1. **Forgery and modification of certificate:** Certificates written on paper and regular digital documents can easily be forged or modified.
2. **Time-consuming process**: Verifying authorities like employers will have to contact the relevant institutions, platforms, and centers themselves, thus delaying their decision.
3. **Weak audit trail:** The manual issuance and verification process cannot maintain records of the issuer of the certificate, the time at which it is issued, and whether or not it has been revoked.
4. **Absence of clear revocation process:** The certificate may continue its circulation even after being revoked by the issuer.
5. **Assessment and issuance as separate activities:** There might not be an actual enforcement of the requirement of assessment of the learner prior to issuing a certificate.
6. **Limited personal privacy:** The list of public certificates contains more learner information than necessary.
7. **Dependence on central authority:** It is entirely dependent on the internal database or responses of the issuer authority.
8. **Scalability problem:** The process will get difficult with growing numbers of learners, issuers, and certificates.

These weaknesses show the need for a system that supports secure learner registration, controlled course enrollment, AI-assisted assessment, automatic certificate issuance after successful assessment, blockchain-based verification, and privacy-preserving public registry statistics.

3.1.3 Analysis of the Proposed System

The proposed system is designed to achieve the following objectives:

1. For creating a secure online platform for both learners and issuers.
2. For allowing issuers to design courses and question templates.
3. For ensuring that learners are enrolled using course codes provided by the issuer.
4. For creating 30 test questions from the course content using AI assistance.
5. For preventing learners from selecting or modifying the level of difficulty in the assessment.
6. For grading the answers of the learners with a combination of LLMs and local rules.
7. For certifying only after learners pass the assessment.
8. For minting certificate NFTs through smart contract registry.
9. For storing certificate metadata and evidence on IPFS (if enabled).
10. For providing public verification based on token ID and verification code.
11. For enabling certificate revocation while maintaining an audit trail.
12. For protecting sensitive information about learners by providing limited public verification information.

3.2 System Requirements Specification (SRS)

System Requirements Specification refers to the activities which define what the system should be able to do and what quality characteristics it is supposed to possess. According to the analysis methodology presented by Dennis et al., the process of requirement extraction includes identifying user needs, business rules and technological constraints. In our case, the requirements were extracted considering the issue of forgery, user needs, the necessity of public verification, and technological characteristics of AI, blockchain and IPFS.

3.2.1 Functional Requirements

The functional requirements are grouped by module.

1. Authentication and User Management

i. The system shall enable learners to create an account using email, password, and wallet address.

ii. The system shall enable institutions/platforms/trainers/teachers (issuers) to create an account using email, password, institution/programme name, and wallet address.

iii. The system shall authenticate users by means of login.

iv. The system shall issue access tokens and refresh tokens upon successful authentication.

v. The system shall safeguard the learner's and issuer's dashboard against unauthorized access.

vi. The system shall allow logout and invalidate sessions.

2. Course and Enrollment Management

i. The issuer creates courses with title, description and status.

ii. The issuer generates one or more enrollment codes for a course.

iii. The learner views all available courses but cannot view the protected contents of those courses.

iv. The learner enrolls in a course using a code provided by the issuer.

v. The backend checks for code validity, expiry and quota before enrollment.

vi. The backend captures enrollment date for the learner along with the course.

3. Material and Assessment Template Management

i. The issuer will need to upload or input course materials.

ii. The backend will send materials to the AI engine.

iii. The AI engine will pull out important concepts from the material.

iv. The issuer should have more than one assessment form for a course.

v. Each assessment form will relate to a course, material, and issuer.

vi. There will be thirty questions in each assessment.

4. Assessment Generation

i. The learner will choose the assessment template from an enrolled course.

ii. The backend should verify the enrollment of the learner prior to generating any assessment.

iii. The backend should randomly allocate or set difficulty level without learner selection.

iv. The AI service should try generating questions by using OpenAI LLM.

v. The AI service should verify whether the generated questions conform to the desired distribution. That is, eight definition, eight conceptual, seven application, and seven analysis questions.

vi. The AI service shall fall back to local generation if LLM generation fails, times out or returns invalid JSON.

vii. The learner-facing response shall not expose expected answers or rubrics.

5. Answer Submission and Grading

i. The learner will provide an answer to each question on the assessment test.

ii. The backend will save answer submissions from the learner.

iii. The backend will request grade assessments from the AI service.

iv. Grading by the AI service should be done semantically wherever possible.

v. Semantic grading should take priority over local grading as a measure of consistency.

vi. AI service will generate detailed grading outputs including grade outcomes and reports hash.

vii. The backend will save assessment results and detailed grading outputs.

6. Certificate Issuance and Verification

i. A certificate will only be issued by the backend provided the result of the assessment is PASS.

ii. The backend shall produce certificate metadata and the verification code.

iii. The backend shall create the certificate as a PDF file.

iv. The backend shall publish the certificate evidence on IPFS if this option is enabled.

v. The backend shall invoke the smart contract registry to issue the NFT certificate.

vi. The system shall save the token id, transaction id, metadata cid, and the verification code.

vii. Public verifiers shall validate the certificate through the token id and the verification code.

viii. The public registry should provide aggregated statistics while protecting learner privacy.

ix. Authorized issuers shall be able to revoke certificates.

3.2.2 Non-Functional Requirements

1. **Security:** Credentials, private keys, learner data, and certificate validation codes need security. JWT tokens will be utilized in route protection. Passwords will be hashed. Environment variable will be used for secret management of private keys and OpenAI API keys. Permissions for authorized issuers will be checked before issuing or revoking the certificate from the blockchain contract.
2. **Integrity:** Records of assessments, metadata and events on the blockchain related to the issuance should retain proof of issuance. Assessment report hash values should be determined in a consistent way so that any identical assessment report will give the same hash value. Certificate record will include token ID, learner ID, issuer ID, assessment and certificate validation code.

3. **Privacy:** Personal details of learners in public verification should not be revealed without consent. Learner's name and email addresses should be hashed in the local database schema. Verification needs token ID and certificate validation code to be displayed.
4. **Availability:** Deployment of each layer of frontend, backend, AI service, and the blockchain layer must be possible separately. In case of unavailability of the LLM service, the local assessment mode fallback makes sure that the system functions.
5. **Usability:** The interface will facilitate separate workflows for learners, issuers, and verification procedures. There should be no need for users to understand blockchain technology to undergo an assessment test. The issuers would be able to create courses, codes, resources and assessments through the dashboard.
6. **Scalability:** A modular approach is adopted in designing the system. Frontend being static, backend API-based, and having AI assessment module as well as blockchain module performing only certificate transaction makes the system easy to scale independently.
7. **Maintainability:** Each component in the code base would fall in one of the following modules: frontend scripts, backend API routers, database models, services, AI assessment modules and smart contract modules.

3.3 Proposed Methodology: Hybrid Methodology

The design approach used in the development of this system is a combination of both object-oriented analysis and prototyping. Dennis et al. suggest that systems analysis and design should follow requirements, modelling, architectural design, interface design, database design, and

implementation. In this project, the same logic is followed; however, it is done in an iterative fashion due to the nature of the system, which uses various technologies.

The methodology involved the following stages:

1. **Identifying problems:** Forgery of certificate and weak verification were identified as the main problems.
2. **Determination of requirements:** Both functional and non-functional requirements were deduced based on the requirements of the users.
3. **Process modeling:** The process was divided into steps such as user registration, course creation, enrollment, assessment, grading, certificate issuance and verification.
4. **Object Modeling:** System objects such as User, Learner, Issuer, Verifier, Course, CourseCode, CourseEnrollment, Assessment Template, Assessment and Certificate were identified.
5. **System Architecture Design:** The design for the system architecture included modular web, AI and blockchain architecture.
6. **Designing Interfaces:** Authentication interface, learner interface, issuer interface and public verification interface were created.
7. **Designing Data Storage:** Persistent data store was designed for backend database, AI data cache and blockchain reference.
8. **System Implementation & Testing:** System implementation and testing included local preview, API testing, smart contract testing and workflow testing.

3.3.1 Justification for Methodology

The object-oriented and prototype-based methodology is suitable for this project because the system has multiple interacting objects and actors. Dennis, Wixom and Roth describe use cases as a way to understand how users interact with a system, and class modelling as a way to represent objects, attributes and relationships. These concepts are directly applicable to the ANTI-FORGERY PROOF CERTIFICATION REGISTRY FOR SKILL ACQUISATION USING SMART CONTRACTS AND ARTIFICIAL INTELLIGENCE system because the system includes learners, issuers, Verifier, courses, assessments, certificates, and blockchain records.

Prototyping is also appropriate because the research requires practical integration of AI, smart contracts, IPFS and web authentication. Such system cannot be tested correctly through design diagram only. This system needs to be built and tested as a running prototype. There are a few problems encountered and corrected during the development of the prototype, for example, front-end routes errors, API authentication failure, OpenAI timeout events,ABI mismatch between the backend and smart contract, and incorrect distribution of the LLM question. This confirms the importance of iterative prototyping in a multi-component system.

3.3.2 Method of Data Collection

The gathering of data used for system analysis was collected through:

1. Literature review about the usage of blockchain for certificates verification, non-fungible tokens (NFT), smart contracts and AI evaluation.
2. Literature review about system analysis and design covered by Dennis, Wixom & Roth.
3. Observations about standard certificate issues and verification procedures.

4. Requirement analysis based on project research goal and research questions.
5. Testing of designed prototype by executing procedures performed by issuers and learners locally.

3.4 unified Modelling Language (UML)

One can agree that UML diagrams could provide one of the bases in software engineering which is the standard visual language that could depict all different facets of a software system thoroughly. It acts as an excellent instrument for architects, developers, stakeholders and others to be able to develop and especially communicate all the parts that a software system entails and is divided into. One of these diagrams that has proven to be extremely important is the use case diagram which outlines all possible interactions that an external system or users would have with the system itself and which could be seen as a design for all the various processes within a software system application.

The next diagram, activity diagram, complement the use case diagrams because they allow the aspects of dynamic process modeling in a system development process and would display the total flow of all activities that are conducted within the software system and the process sequence/parallel behavior that occur. The dynamic view would contribute greatly to visualization of the overall process happening within the system which will further help the developers and the stakeholders find possible bottlenecks, decision making, and improvement of a software system.

3.4.1 Use Case Diagram of The Proposed System

Use case diagrams are classified into four categories; use cases which are the functional parts of the system, the actors which represent the external entities of the system, the associations between the actors and the use cases, and lastly the system boundary which is the scope of the system the actor is interacting with. As for the proposed system, there would be 4 actors which are; the learner, the issuer, the public verifier, the system (which also encompasses system admin, IPFS, blockchain registry).

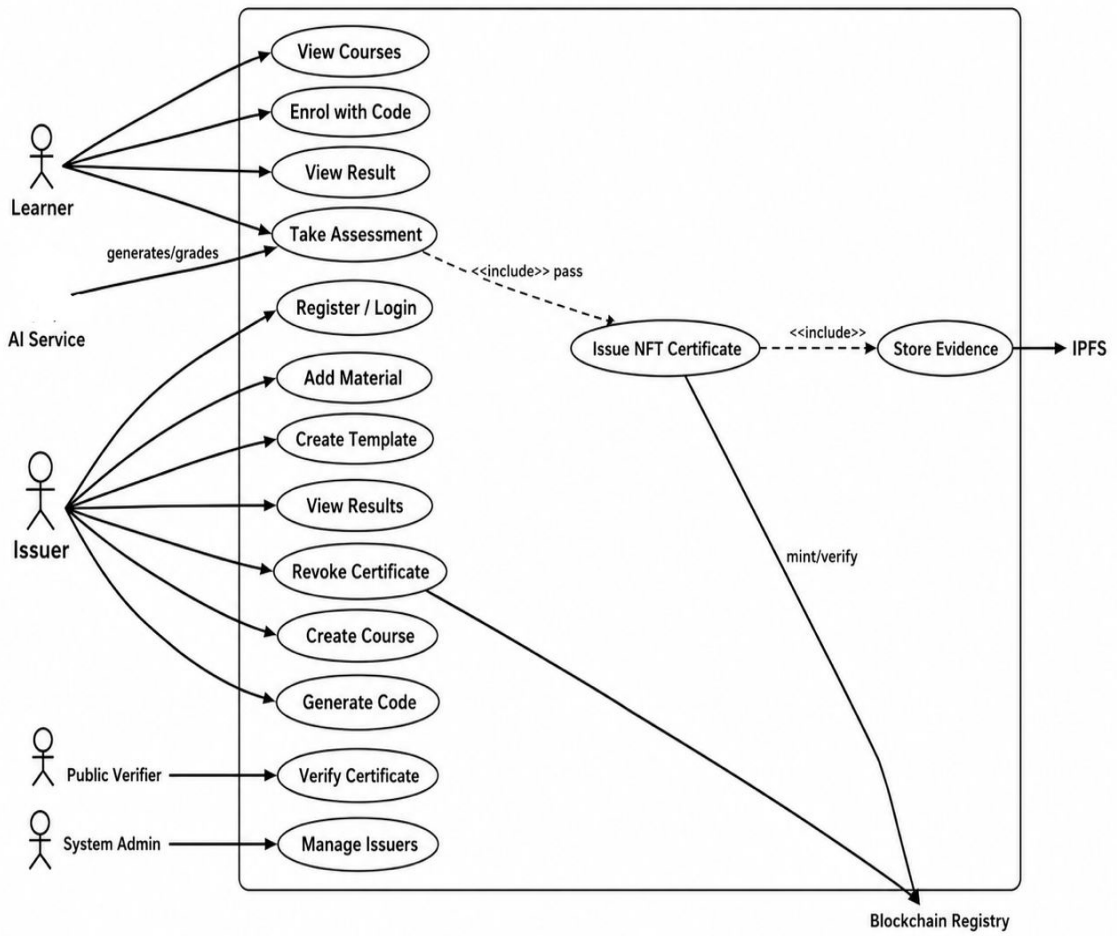


Figure 3.1: Use Case Diagram of the Proposed System

3.4.2 Activity Diagram of The Proposed System

The activity flow describes the order of operations from course creation to certificate verification:

The operation of the Anti-Forgery Proof Certification Registry for Skill Acquisition using Smart Contracts and Artificial Intelligence involves a series of steps undertaken by the issuer, the learner, the artificial intelligence services, the backend processes, and the blockchain verification system.

The first step entails logging in by the issuer who will create a course for skill acquisition. After the creation of the course, the issuer creates the enrollment code which is then given out to the learners. The issuer then uploads the necessary learning content and also creates an assessment template.

On the learner's side, the learner logs in to enroll in the created course. Once the learner has enrolled in the course, the next step will be to take the assessment test. This is where the backend process kicks in validating the learner and also validating the course template. Once the process of validating the content is complete, an artificial intelligence service automatically creates assessment questions for learners based on uploaded learning materials using predefined templates. The learner responds to the created questions by submitting their answers to the system. Then, the system intelligently and accurately assesses and grades the answers to those questions.

If the learner does not pass the assessment, the system generates useful feedback aimed at improving their future performance. But when the learner succeeds in passing the assessment, the

backend generates certificate evidence of completion for the learner. Then, the backend of the system communicates with the blockchain registry, which acts as the authority for issuing the NFT (Non-Fungible Token). The system creates a permanent record of certificates issued, including ownership and verification data, in the blockchain registry to avoid certificate counterfeiting and modifications. Verifiers who would like to verify certificates issued by the system should simply input the token ID and verification code sent by the system.

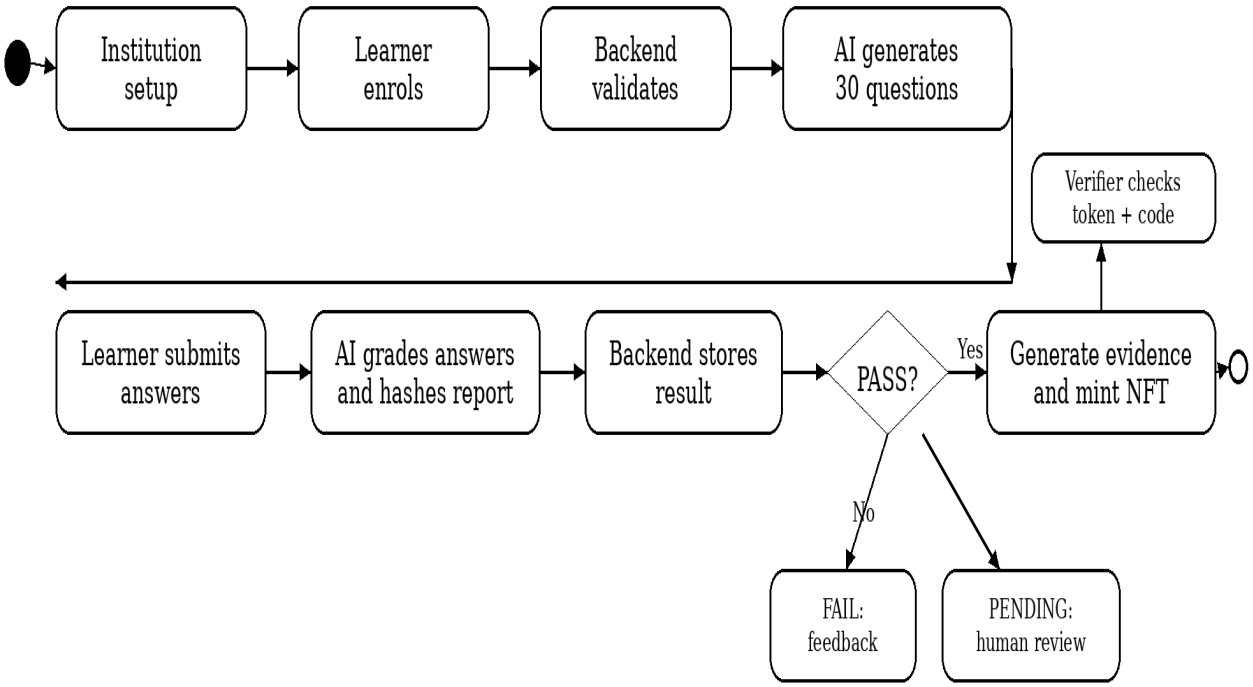


Figure 3.2: Activity Diagram for Assessment and Certificate Issuance

3.4.3 Class Diagram of The Proposed System

This section of this work of research holds the class diagram of the proposed system. The class diagram in Unified Modelling Language (UML) is one of the unified modelling language diagrams that describes the architectural design of a system by defining and laying out completely its classes, the attributes of the laid out classes, the methods and the relationships among these different objects that make up a system. Below is the illustration of the class diagram for the proposed system.

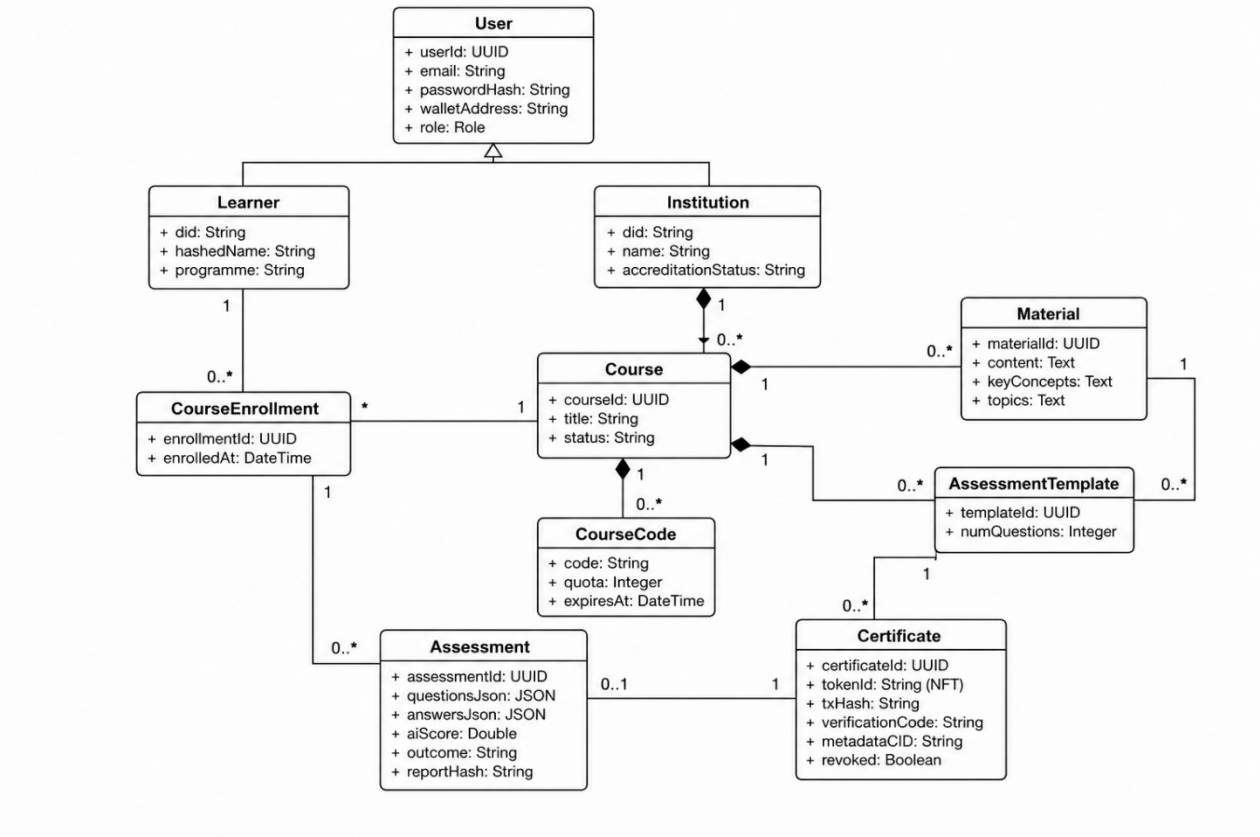


Figure 3.3: Class Diagram of Proposed System Core Entities

The diagram above represents the class diagram of the proposed system, which is used in this research work to show the activities that are going on in the proposed system. The diagram depicts the series of classes that exist between the system to help it function properly.

3.4.4 Sequence Model of The Proposed System

The unified Modelling Language (UML) sequence diagrams are a time based illustration model that shows how and between which object is taking place throughout a system. Therefore the diagrams help to understand the sequence in which various actions or messages are taken place in a use case or scenario. Essentially the sequence diagrams graphically describe when actions take place so the reader can visualize how the various components interact together in a system.

However, the elements within the UML sequence diagram are: objects, lifelines, messages and activations. Lifelines are the actual actors that are participating in the interaction and messages show the communication between actors. Activations are represented by lines on the lifelines that indicate the time in which an actor participates in an interaction.

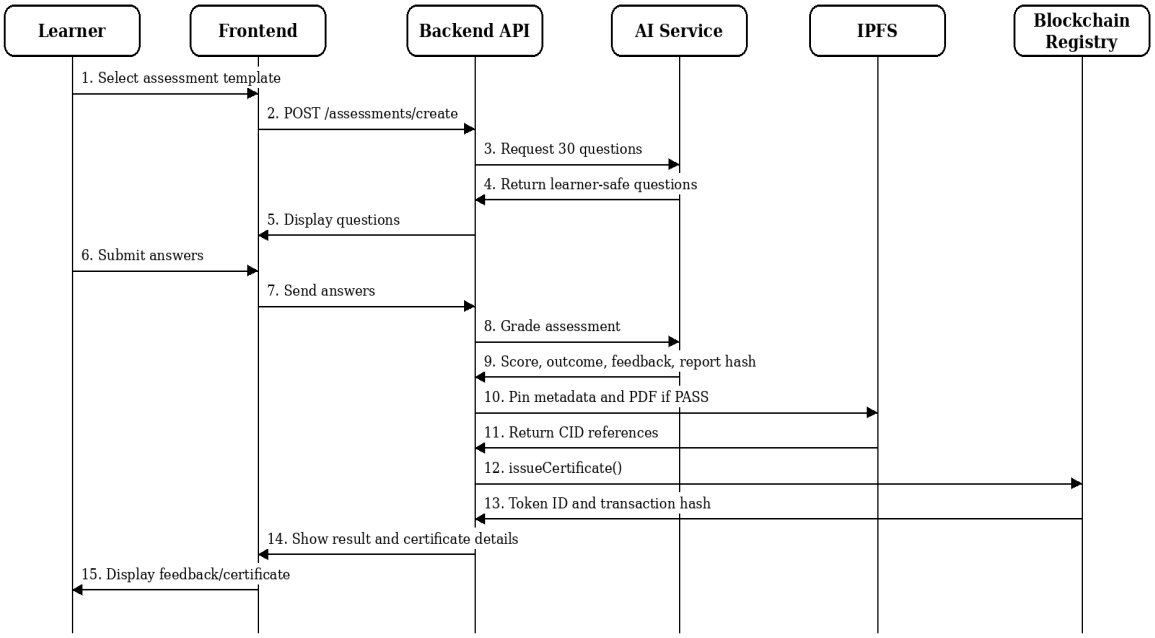


Figure 3.4: Sequence Diagram for AI Assessment and NFT Certificate Issuance

3.5 System Design

This section focuses on converting the analyzed system into a design blueprint.

3.5.1 Overall Architecture

The system uses a modular architecture with four main layers:

1. **Presentation layer:** Web-based front end implemented using HTML, CSS and JavaScript

2. **Application layer:** FastAPI back-end dealing with authentication, courses, tests, certification and orchestration of API calls.

3. **AI service layer:** Another FastAPI microservice implementing ingestion of course material, question creation, assessment and hashing of reports.

4. **Blockchain layer:** Solidity smart contracts operating on Arbitrum Sepolia chain and optional IPFS pinning for storing metadata/PDFs.

The above architecture is a manifestation of the concept of architecture design put forth by Dennis, Wixom and Roth, according to which an analyst has to identify the organization of the software, hardware, network, and security elements so that the requirements of the organization are met.

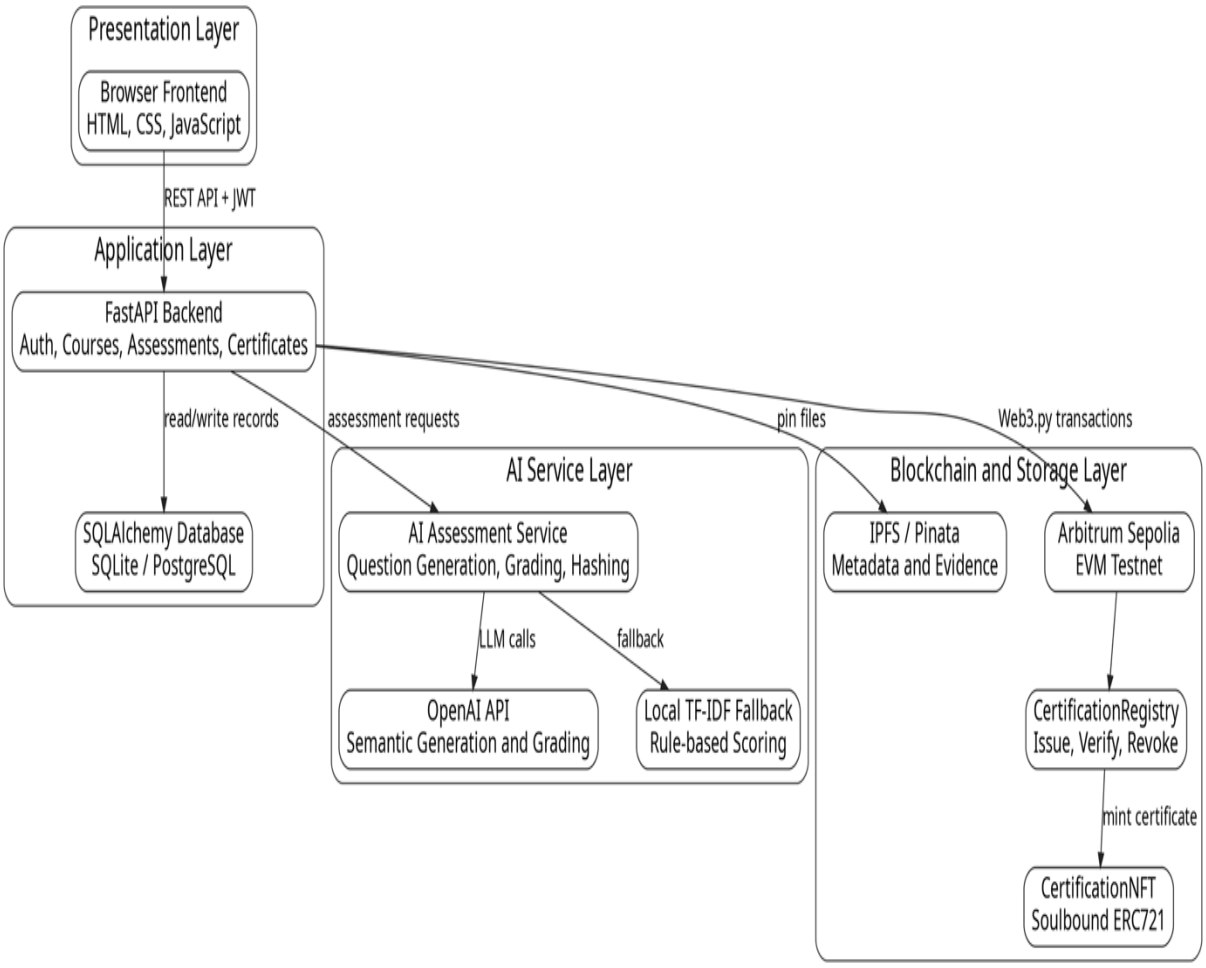


Figure 3.5: System Architecture

3.5.2 Input Design

The input design describes how the system obtains data from the users. Input validation is a key element within the user interface design by Dennis, Wixom and Roth as the negative impact of invalid input into the system is significant. Within the SkillCert input design the following fields will be captured:

1. Registration inputs (email, password, wallet address, role, issuer/learner profile information).
2. Course inputs (title and description).
3. Course code inputs (quota, expiry).
4. Material inputs (title, programme, topics, material content or uploaded file).
5. Assessment inputs (select assessment template, learner answers to assessment template).
6. Verification inputs (token ID, verification code).
7. Blockchain configuration inputs (RPC URL, contract address, private key). Note: in live systems the private key must be stored in .env.

Critical input validation includes ensuring unique email address, unique wallet address, enrollment code is valid, assessment template is active and the course enrollment prerequisite is meet. It is also a good idea for difficulty settings to behidden by the back-end system.

3.5.3 Output Design

Output for the system is provided in the following areas:

1. Course lists to be used by learners.
2. Course, code and learner statistics available to issuers.

3. Assessment question sets.
4. Assessment scores, outcomes and feedback.
5. Breakdown of scores including final, semantic and local scores.
6. Certificate NFT token ID and transaction hash.
7. Certificate PDF available for download.
8. Statistics for the public registry.
9. Verification result stating the validity status of a certificate.

Output was designed with the idea that information output should be useful for decision making: learners have to be able to determine their result; issuers should be able to manage courses and learners, while verifiers require a straightforward indication of the validity of a certificate.

3.5.4 Database Design

For backend operations, SQL Alchemy ORM is utilized as the implementation for the database. In preview mode, SQLite is employed, though the system can be moved to PostgreSQL in future. There are three main entities involved in this process which include users, learners, issuers, courses, courses codes, course enrollments, materials, assessment templates, assessments, certificates, audit logs, and issuer keys.

Referential links between the users, courses, assessments and certificates have been made possible. A certificate refers back to the learner, issuer, and assessment. This means that there is no standalone certificate without other references within the system. Also, The database supports user authentication, learner and issuer management, course administration, assessment generation, certificate issuance, blockchain integration, and audit logging. The core database consists of ten

major tables, while three additional supporting tables provide session management, security, and auditing functionalities.

Field	Data Type	Key	Description
id	Integer	Primary Key	Unique user identifier
email	Varchar(255)	Unique	User email address
password_hash	Varchar(255)		Encrypted password
wallet_address	Varchar(42)	Unique	Blockchain wallet address
role	Enum.		User role (Learner, Issuer, Admin)
learner_id	Integer	Foreign Key	References Learners table
issuer_id	Integer	Foreign Key	References Issuers table
is_active	Boolean		User account status
created_at	DateTime		Registration date

Table 3.1 Users Table

Field	Data Type	Key	Description
id	Integer	Primary Key	Learner identifier
did	Varchar(255)	Unique	Decentralized Identity
hashed_name	Varchar(255)		SHA-256 encrypted learner name
hashed_email	Varchar(255)	Unique	Encrypted email
wallet_address	Varchar(42)	Unique	Wallet address
programme	Varchar(100)		Programme enrolled
created_at	DateTime		Registration date
is_active	Boolean		Account status

Table 3.2 Learners Table

Field	Data Type	Key	Description
id	Integer	Primary Key	Issuer identifier
did	Varchar(255)	Unique	Decentralized Identity
name	Varchar(255)		Institution or trainer name
wallet_address	Varchar(42)	Unique	Blockchain wallet
accreditation_status	Boolean		Accreditation status
created_at	DateTime		Date created

Table 3.3 Issuers Table

Field	Data Type	Key	Description
id	Integer	Primary Key	Material record
material_id	Varchar(255)	Unique	Material identifier
issuer_id	Integer	Foreign Key	References Issuers
issuer_did	Varchar(255)		Issuer DID

programme	Varchar(100)		Programme
title	Varchar(255)		Material title
content	Text		Learning material
difficulty_level	Varchar(50)		Difficulty level
topics	Text		Topics covered
key_concepts	Text		Extracted concepts

Table 3.4 Materials Table

Field	Data Type	Key	Description
id	Integer	Primary Key	Course record
course_id	Varchar(255)	Unique	Course identifier
issuer_id	Integer	Foreign Key	References Issuers
title	Varchar(255)		Course title
description	Text		Course description
status	Enum		Course status
created_at	DateTime		Date created

Table 3.5 Courses Table

Field	Data Type	Key	Description
id	Integer	Primary Key	Record identifier
course_id	Integer	Foreign Key	References Courses
code	Varchar(64)	Unique	Enrollment code
status	Enum		Code status
quota	Integer		Number of allowed users
used_count	Integer		Number of times used
expires_at	DateTime		Expiry date
created_at	DateTime		Creation date
revoked_at	DateTime		Revocation date

Table 3.6 Course Codes Table

Field	Data Type	Key	Description
id	Integer	Primary Key	Enrollment identifier
course_id	Integer	Foreign Key	References Courses
learner_id	Integer	Foreign Key	References Learners
code_id	Integer	Foreign Key	References Course Codes
enrolled_at	DateTime		Enrollment date

Table 3.7 Course Enrollments Table

Field	Data Type	Key	Description
id	Integer	Primary Key	Template record
assessment_template_id	Varchar(255)	Unique	Template identifier
course_id	Integer	Foreign Key	References Courses

issuer_id	Integer	Foreigy	References Issuers
title	Varchar(255)		Template title
description	Text		Template description
material_db_id	Integer	Foreign Key	References Materials
material_id	Varchar(255)		Material identifier
num_questions	Integer		Number of questions
status	Varchar(30)		Template status
created_at	DateTime		Creation date

Table 3.8 Assessment Templates Table

Field	Data Type	Key	Description

id	Integer	Primary Key	Assessment record
assessment_id	Varchar(255)	Unique	Assessment identifier
learner_id	Integer	Foreign Key	References Learners
issuer_id	Integer	Foreign Key	References Issuers
course_id	Integer	Foreign Key	References Courses
assessment_template_id	Integer	Foreign Key	References Assessment Templates
material_db_id	Integer	Foreign Key	References Materials

questions_json	Text		Generated assessment questions
answers_json	Text		Learner responses
ai_score	Float		AI assessment score
ai_confidence	Float		AI confidence level
ai_feedback	Text		Feedback generated by AI
outcome	Enum		PASS, FAIL or PENDING
artefact_cid	Varchar(255)		IPFS storage identifier
created_at	DateTime		Assessment date
completed_at	DateTime		Completion date

Table 3.9 Assessments Table

Note: Additional fields such as rubric scores, anomaly detection metrics, SHAP explainability values, attestation records, and AI metadata are maintained by the system to support intelligent grading, fairness analysis, and explainable artificial intelligence.

Field	Data Type	Key	Description
id	Integer	Primary Key	Certificate identifier
token_id	Integer	Unique	NFT Token ID
learner_id	Integer	Foreign Key	References Learners
issuer_id	Integer	Foreign Key	References Issuers
assessment_id	Integer	Foreign Key	References Assessments
metadata_cid	Varchar(255)		IPFS metadata reference
artefact_cid	Varchar(255)		Assessment evidence CID

tx_hash	Varchar(66)		Blockchain transaction hash
verification_code	Varchar(32)	Unique	Verification code
pdf_cid	Varchar(255)		PDF IPFS identifier
pdf_path	Varchar(500)		PDF storage path
score_percentage	Float		Final score
issued_at	DateTime		Certificate issue date
revoked_at	DateTime		Revocation date
revocation_reason	Text		Reason for revocation
is_revoked	Boolean		Revocation status

Table 3.10 Certificates Table

The database tables are related using primary and foreign keys to maintain referential integrity. A user account may belong to either a learner or an issuer. An issuer can create multiple courses, upload learning materials, generate assessment templates, and issue certificates. Learners enroll in courses using enrollment codes and complete AI-generated assessments. Certificates are issued only after successful assessment and are linked to blockchain records through NFT Token IDs, transaction hashes, and IPFS Content Identifiers (CIDs). Audit logs record all significant system

events, while supporting tables manage authentication sessions and blockchain security credentials.

3.5.5 Smart Contract Design

The smart contract design is composed of two smart contracts:

1. **CertificationNFT.sol:** An ERC721 token smart contract for certificates. It allows the creation of NFTs, as well as prevents any transfer of an NFT after being minted (making the certificate soulbounded).

2. **CertificationRegistry.sol**: A smart contract to authorize issuers, create a certificate, store its CID, verify its existence, and cancel a certificate.

The smart contract depends on issuer authorization in order to prevent non-authorized addresses from minting or cancelling a certificate. The check function will output the validation state of the certificate, its metadata CID, the CID of its artifact, the issuer DID, and the timestamp.

3.5.6 AI Assessment Design

AI Grading Service- A dedicated microservice for AI Grading that:

1. Ingests material,
2. Extracts keywords using TF-IDF and generates questions using LLM if OpenAI is accessible or if not,
3. fallback question generations,
4. Stores student answers,
5. Conducts hybrid grading,

6. Hashes assessment report and stores them.

The assessment has 30 questions, 8 definitions, 8 conceptual, 7 application and 7 analysis questions. The answer key and rubrics are maintained and kept private.

3.5.7 Security Design

The security measures used throughout the system are:

1. Password hashing.
2. JWT authentication and refresh tokens.
3. Role-based dashboard access.
4. Hidden assessment difficulty.
5. Server-side storage of expected answers and rubrics.
6. Verification code requirement for certificate lookup.
7. Smart contract issuer authorization.
8. env protection for API keys and private keys.
9. Public registry aggregation without exposing sensitive learner details.

CHAPTER FOUR

SYSTEM IMPLEMENTATION

4.0 Introduction

Chapter four discusses the implementation of the Anti-Forgery Proof Certification Registry for Skill Acquisition Using Smart Contracts and Artificial Intelligence. While chapter three talked about the analysis and design process, this chapter will explain how that design was developed into an operational prototype. It covers such topics as development tools, programming languages used, databases implementation, AI implementation, smart contracts implementation, frontend implementation, backend implementation, and finally, testing and results. The implementation process has been based on the implementation process discussed in Dennis et al., involving creation, testing, and preparation for the use of the software. In our case, implementation involved various aspects such as web development, API development, AI service integration, blockchain smart contracts, and local preview testing.

4.1 Development Environment and Tools

The system was developed as a multi-service application. The main development environment and tools are:

Component	Tool/Technology	Purpose
Frontend	HTML, CSS, JavaScript	Browser interface for users.

Backend	| Python FastAPI	API, database, authentication and orchestration.
AI Service	Python FastAPI	AI assessment generation and grading.
Database	SQLite locally, SQLAlchemy ORM	Persistent storage.
Smart Contracts	Solidity	NFT certificate and registry contracts.
SmartContract Framework	| Foundry	Contract build and testing.
Blockchain	Arbitrum Sepolia	Testnet deployment and certificate issuance.
Blockchain	Arbitrum Sepolia	Testnet deployment and certificate issuance.
AI API	OpenAI gpt-4o-mini	Semantic question generation and grading .

Storage	IPFS/Pinata where configured	Metadata and certificate evidence.
Version Control	Git	Source code management.

Table 4.1 Development Environment And Tools Table

4.1.1 Programming Language and Libraries

The frontend uses HTML, CSS and JavaScript. The backend and AI service use Python. The contracts use Solidity version 0.8.20.

1. Important backend libraries include:

i. API routing in FastAPI.

ii. ORM models in SQLAlchemy.

iii. Request/response validation via Pydantic.

iv. Service-to-service requests using HTTPX.

v. Blockchain communication with Web3.py.

vi. JWT/password hashing tools for authentication.

vii. PDF/certificate PDF generation utilities using FPDF/qrcode where needed.

2. Important AI service libraries include:

i. scikit-learn for TF-IDF and local similarity scoring.

ii. OpenAI Python SDK for LLM calls.

iii. Pydantic for strict validation of LLM JSON.

iv. SQLite persistence for AI service cache.

v. hashlib/json for deterministic assessment report hashing.

3. Important contract libraries include OpenZeppelin ERC721 and AccessControl components.

4.1.2 Development Platform and Hardware Requirements

The system was developed and previewed locally on a Linux-based environment. The minimum hardware requirements for local testing are:

1. Dual-core processor or better.

2. At least 4GB RAM.

3. Stable internet connection for OpenAI API, Arbitrum Sepolia RPC and IPFS pinning.

4. A modern browser such as Chrome.

5. Python virtual environments for backend and AI service.

6. Foundry installed for Solidity testing.

4.2 Dataset Description and Preprocessing

The prototype is independent of a specific public set. Rather, the issuer supplies the learning material for each course. The AI service consumes the material and uses it as the source for question generation and evaluation.

The list of preprocessing operations includes:

1. Supplying the material title, program, and content.
2. Storing the material in the backend database.
3. Transmitting the material to the AI service.
4. Identifying key concepts by TF-IDF analysis.
5. Storing the material and its key concepts in the AI service persistence layer.

6. Utilizing the material and key concept data as the input to question generation.

This design is appropriate for skill development as each issuer may supply different material per course. As such, an assessment template for each course could be generated based on the corresponding material.

4.3 Model Architecture and Training

The AI model methodology is hybrid. It combines local rule-based/TF-IDF processing with LLM-based semantic generation and grading.

4.3.1 Question Generation Method

The system first extracts key concepts from the material. It then attempts LLM question generation. The LLM is instructed to return strict JSON. The response must contain exactly thirty questions with the following distribution:

1. Eight definition questions.
2. Eight conceptual questions.
3. Seven application questions.
4. Seven analysis questions.

Each internal question includes:

1. question ID.
2. question text.
3. expected answer.
4. question type.
5. backend-controlled difficulty.

6. key concepts.
7. rubric.
8. points.

However, expected answers and rubrics are removed from learner-facing responses. This prevents learners from seeing the answers before submission.

4.3.2 Local Fallback Method

If OpenAI is unavailable, times out or returns invalid JSON, the AI service falls back to local question generation. This makes the system more resilient because assessments can still be created even when the LLM service is unavailable.

4.3.3 Hybrid Grading Method

The grading process works as follows:

1. Local grading runs for each answer.
2. LLM semantic grading runs in batch where OpenAI is available.
3. If LLM grading succeeds, the final score uses 85 percent LLM score and 15 percent local score.
4. If LLM grading fails, local grading is used fully.
5. The system returns final score, semantic score, local score, feedback and consistency notes.

The local grader uses:

1. TF-IDF cosine similarity.
2. Keyword overlap.
3. Completeness based on answer length.

4. Question-type rubrics for definition, conceptual, application and analysis questions.

The LLM grader uses the question, expected answer, rubric and student answer. This improves fairness because learners may express correct answers using wording that differs from the course material.

4.3.4 Competency and Anomaly Detection

The codebase includes an option for using the Random Forest model to classify competencies and the Isolation Forest model to detect anomalies. The Model Service inspects the presence of the model artifacts:

1. competency_model.joblib
2. anomaly_model.joblib
3. scaler.joblib
4. feature_names.json

If there is a problem with these artifacts, the application will log a warning and proceed without crashing. However, at this point in the prototype version, there are no artifacts, which means that competency and anomaly checks cannot be performed.

4.3.5 Assessment Report Hash

After grading, the AI service generates an assessment report hash. The hash is produced from deterministic JSON using SHA-256. The purpose is to create a stable evidence reference that can later be included in certificate metadata or pinned to IPFS.

4.4 System Implementation and Modules

4.4.1 Frontend Module

The frontend is located in frontend/public. It provides pages and scripts for:

1. Authentication.
2. Learner dashboard.
3. issuer dashboard.
4. Public verification dashboard.

The learner dashboard allows learners to view available courses, enroll with a code, start assessments, answer questions and view results. The issuer dashboard allows issuers to create courses, generate codes, add materials, create assessment templates and monitor learners. The verification dashboard allows public certificate checks.

4.4.2 Backend Module

The backend is located in backend/app. It is implemented with FastAPI and SQLAlchemy. The major API modules include:

1. auth.py for registration, login, refresh token, logout and password recovery endpoints.
2. courses.py for course listing, enrollment and learner course retrieval.
3. issuers.py for course creation, code generation, material upload, template creation and learner result export.
4. assessments.py for material ingestion, assessment creation, answer submission, grading and result retrieval.
5. certificates.py for registry statistics, verification, revocation and learner certificate lookup.

The backend also contains services for blockchain calls, IPFS pinning, certificate PDF generation and issuer key management.

4.4.3 AI Service Module

The AI service is located in ai_service/app. Its major files include:

1. main.py: FastAPI endpoints.
2. assessment.py: material store, question generation, answer submission and grading engine.
3. llm_service.py: OpenAI integration and strict JSON validation.
4. model_service.py: optional competency and anomaly model loading.
5. persistence.py: SQLite persistence for AI cache.
6. hash_utils.py: deterministic assessment report hashing.

The AI service runs independently on port 8001.

4.4.4 Smart Contract Module

The contracts are located in contracts/src.

1. **CertificationNFT.sol:** A certification ERC721 token contract. It generates NFTs and blocks post-mint transfers, thus soulbinding the certificates.
2. **CertificationRegistry.sol:** A registry contract that authorizes certificate issuers, generates certificates, stores their CIDs, checks their validity, and supports revocation.

4.4.5 Blockchain Service Module

The blockchain backend connects to Arbitrum Sepolia using Web3.py. It imports the contract registry ABI and signs transactions for issuing certificates. It can authenticate certificate issuers, issue, verify, and revoke certificates.

4.4.6 Certificate PDF and Verification Module

Upon passing the assessment, the learner is issued metadata about the certificate and a certificate in PDF form. The PDF includes the learner wallet address, issuer name, course title, assessment name, score received, token ID, and verification code. These latter two items are needed to access the certificate validity page from the verification dashboard.

4.5 Testing and Evaluation

Testing was carried out at different levels.

4.5.1 Smart Contract Testing

Foundry tests were written for the smart contracts. The tests cover:

1. Admin authorizing issuers.
2. Authorized issuer issuing a certificate.
3. Unauthorized issuer being prevented from issuing a certificate.
4. Authorized issuer revoking a certificate.
5. Soulbound NFT transfer prevention.

The tests passed after synchronizing the smart contract ABI and backend blockchain service.

4.5.2 API and Integration Testing

The backend and AI services were tested through local API calls. Confirmed checks include:

1. AI health endpoint showing OpenAI key configured.
2. OpenAI model reachability for gpt-4o-mini.
3. Real LLM question generation producing exactly thirty questions.
4. Backend health connecting to Arbitrum Sepolia.
5. Course creation and enrollment through API.
6. Assessment creation after enrollment.

4.5.3 Frontend Testing

The frontend was tested locally through:

1. issuer registration and login.
2. Course creation.
3. Code generation.
4. Material ingestion.
5. Assessment template creation.
6. Learner registration and enrollment.
7. Assessment start and question display.
8. Result display.
9. Verification dashboard access

4.5.4 Error Handling and Debugging

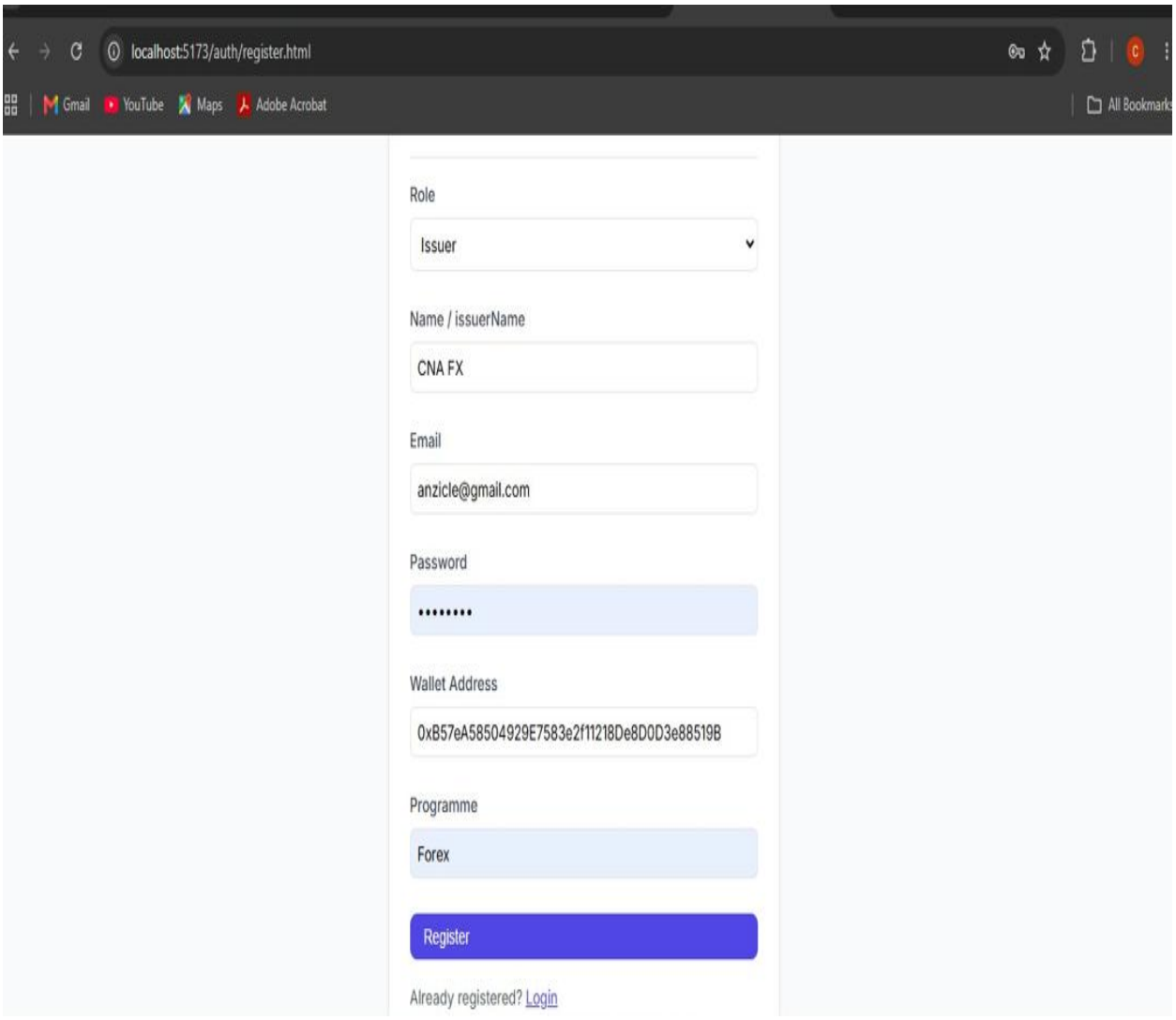
Several development issues were identified and fixed:

1. Reference error for frontend switchTab.
2. Improper dashboards redirect on login.
3. Unapproved course creation due to stale/missing tokens.
4. Error fetching enrolled courses due to API/service outage.
5. Incorrectly calculating verification statistics due to wrong number of course codes.
6. Backend AI request timeouts when generating 30 questions using LLM.
7. OpenAI API key is not accessible from AI service.
8. Invalid question distribution returned by the LLM.
9. DEBUG=release crash in backend parsing.
10. Smart contract ABI does not match.
11. Private key in Foundry not prefixed with 0x.
12. Real secret revealed in example env file.

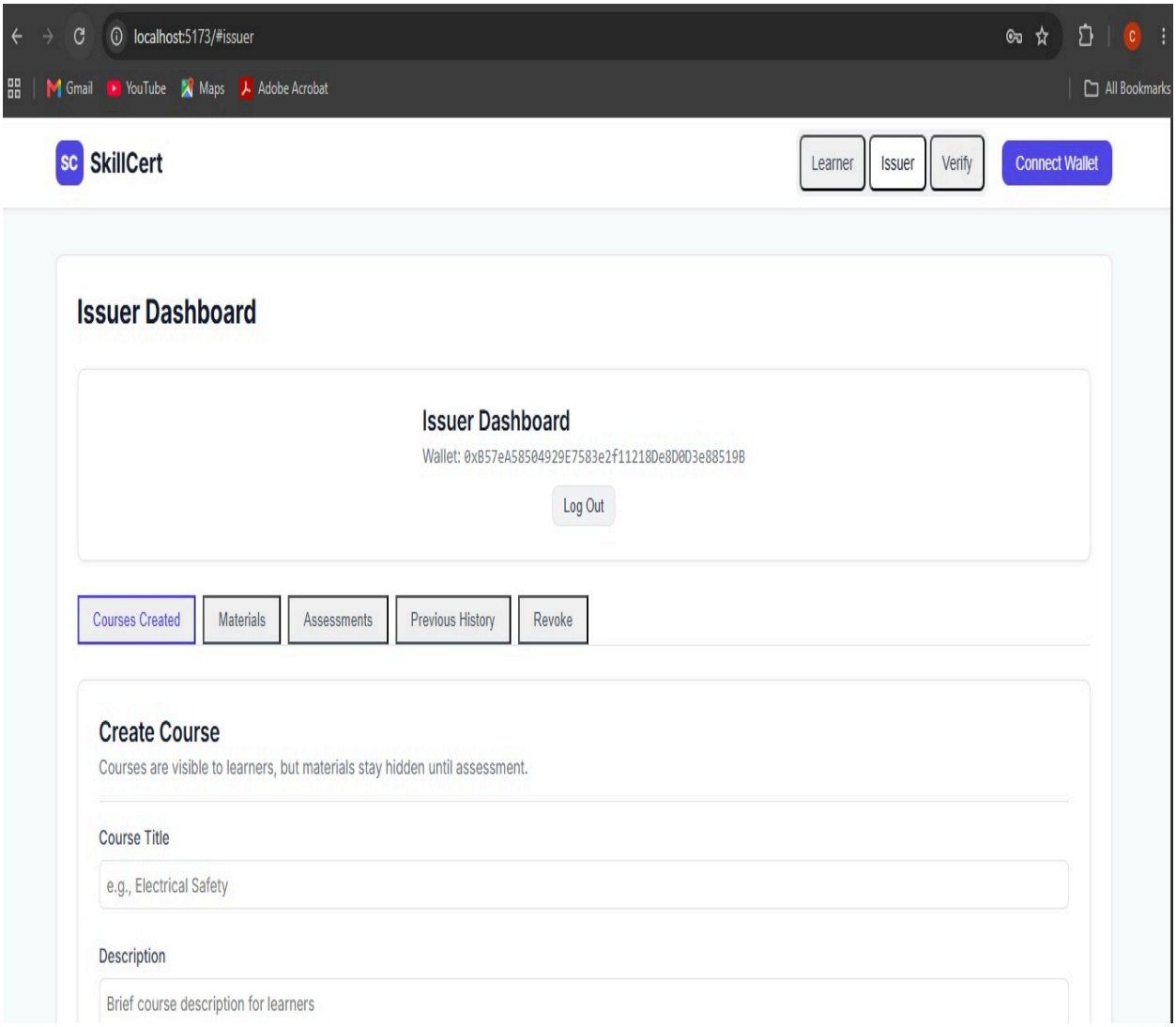
These issues were important because they tested the reliability of the architecture and forced the implementation to become more robust.

4.6 Results Presentation and Analysis

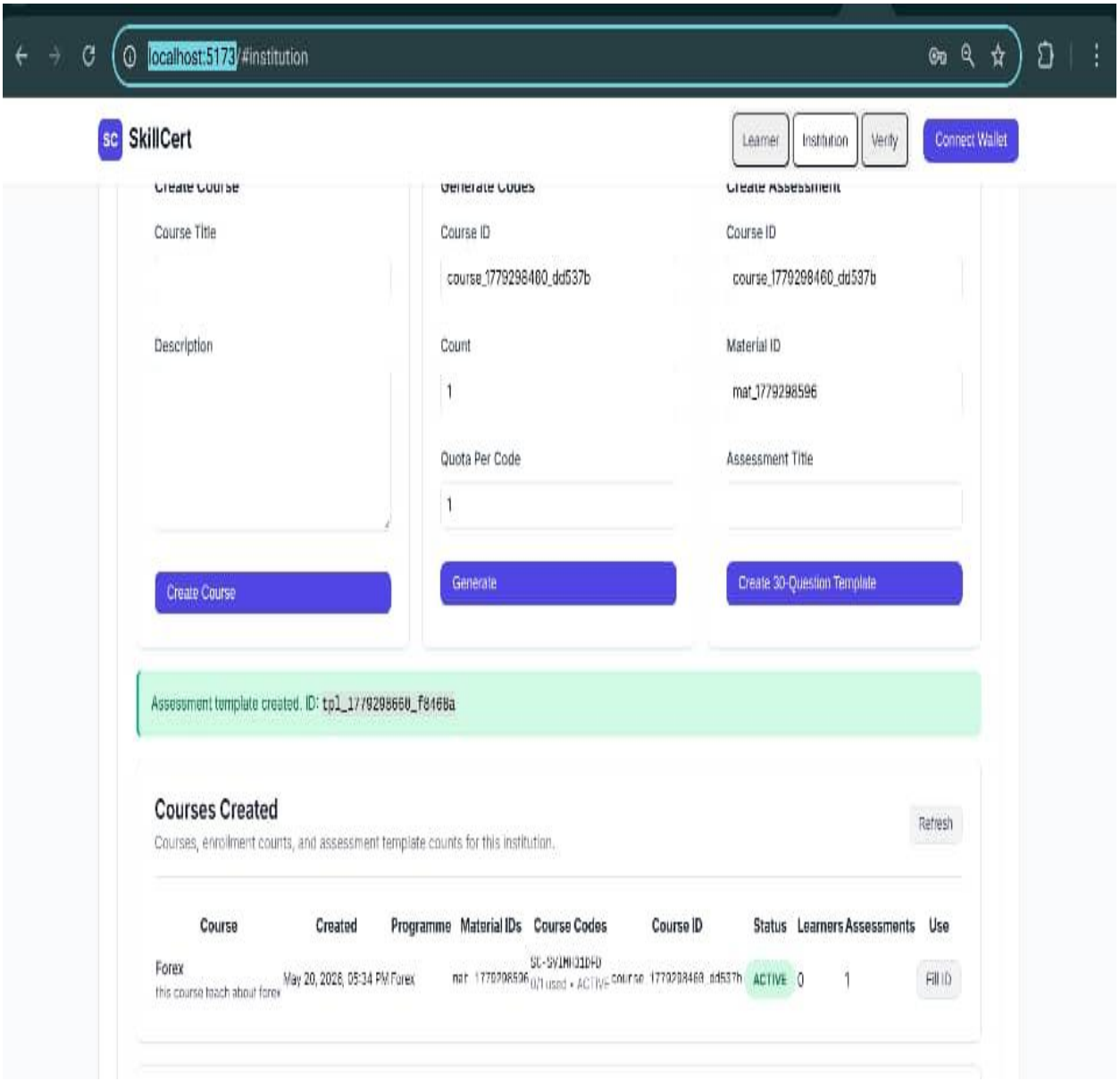
4.6.1 Output Samples and Interface Screens



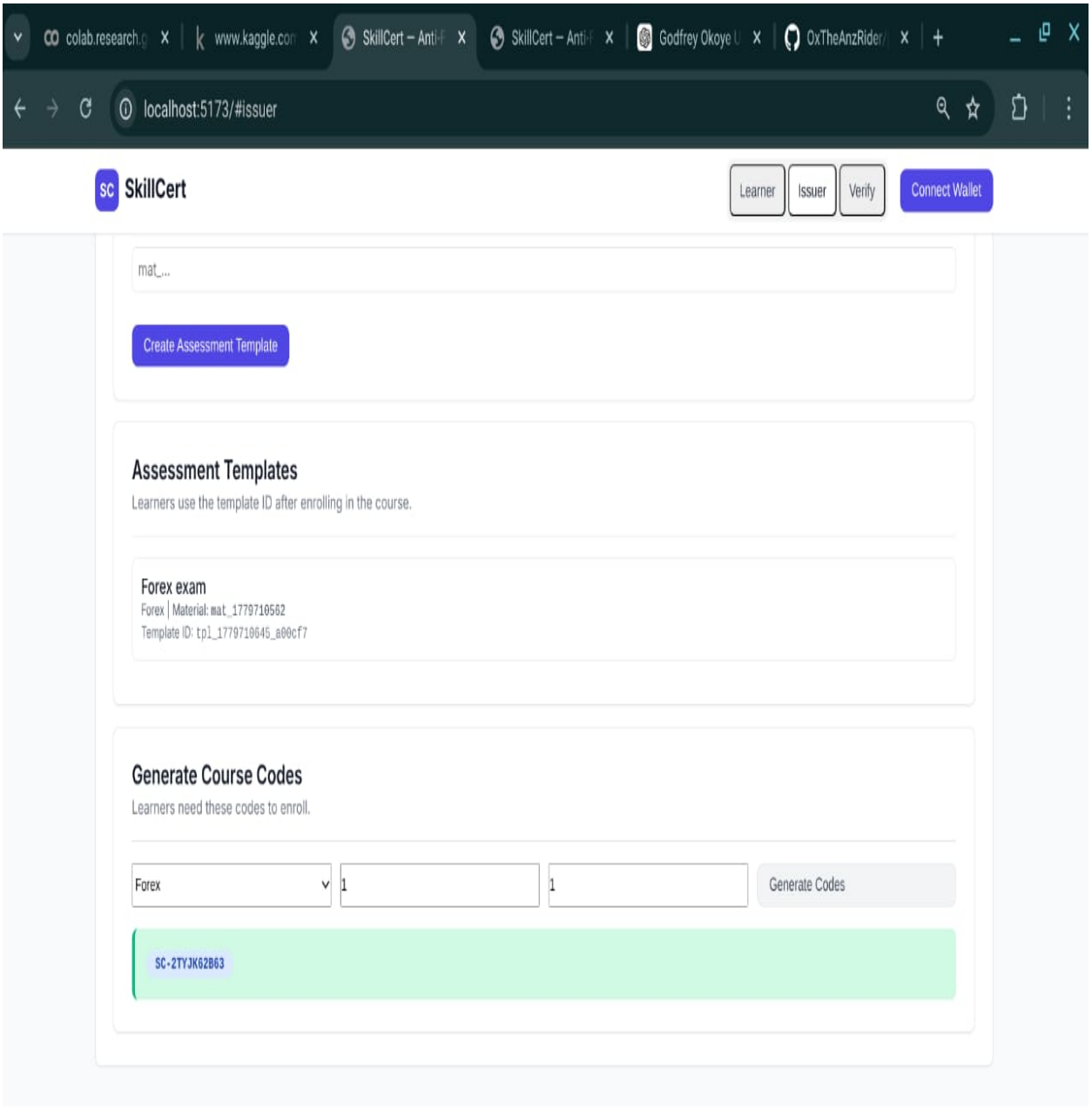
1. Figure 4.1: Authentication page.



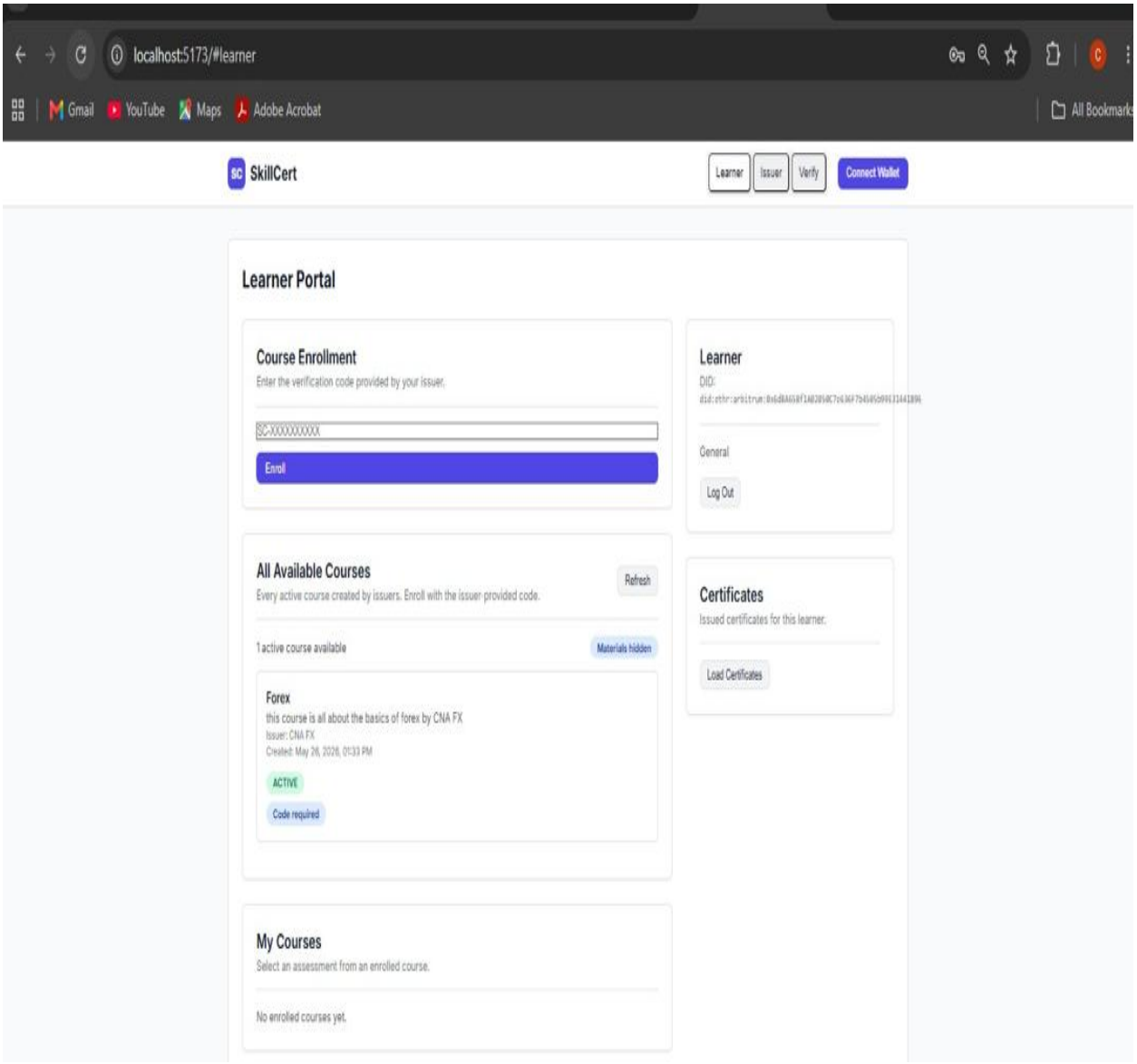
2. Figure 4.2: issuer dashboard.



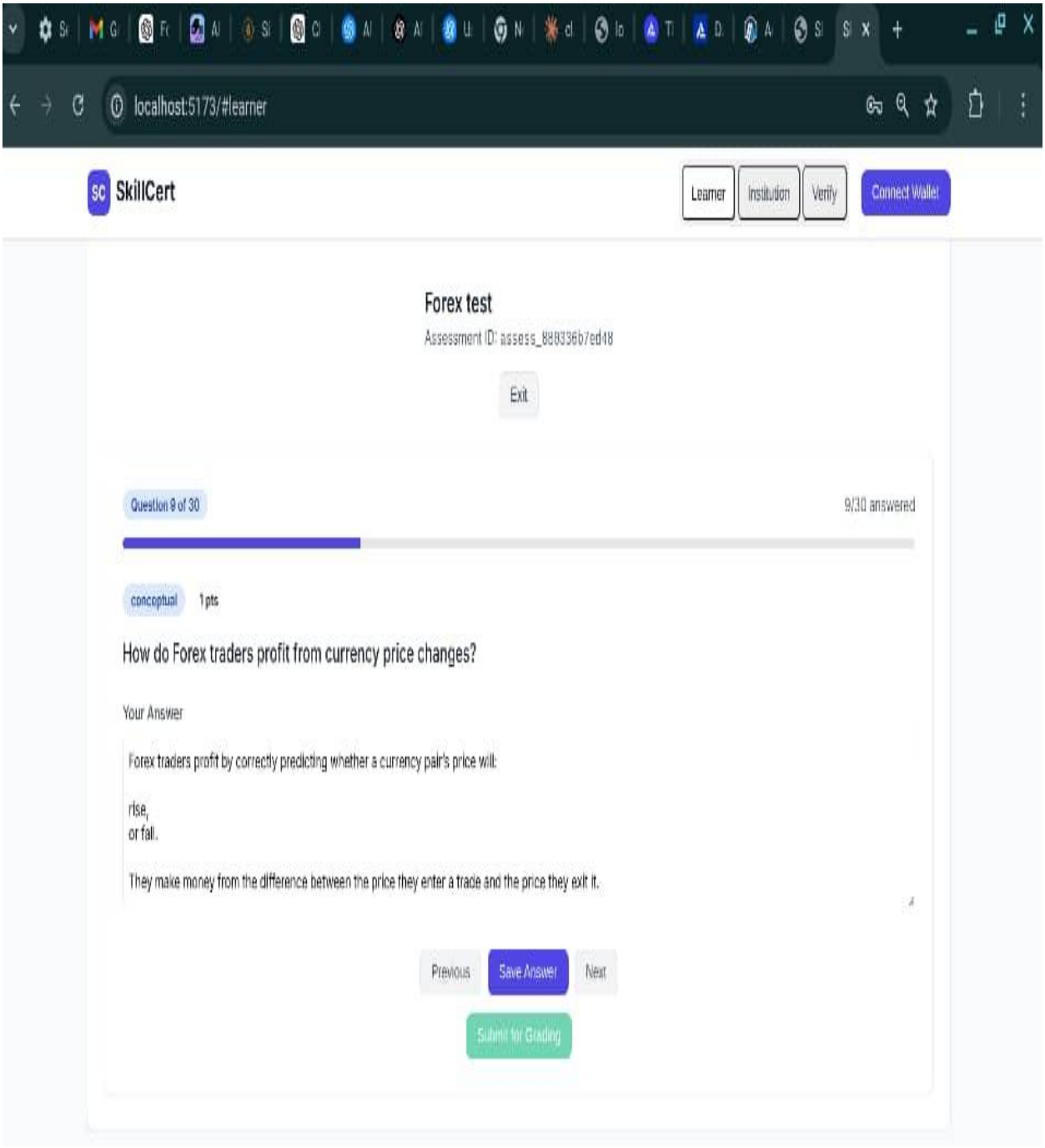
3. Figure 4.3: Course creation form.



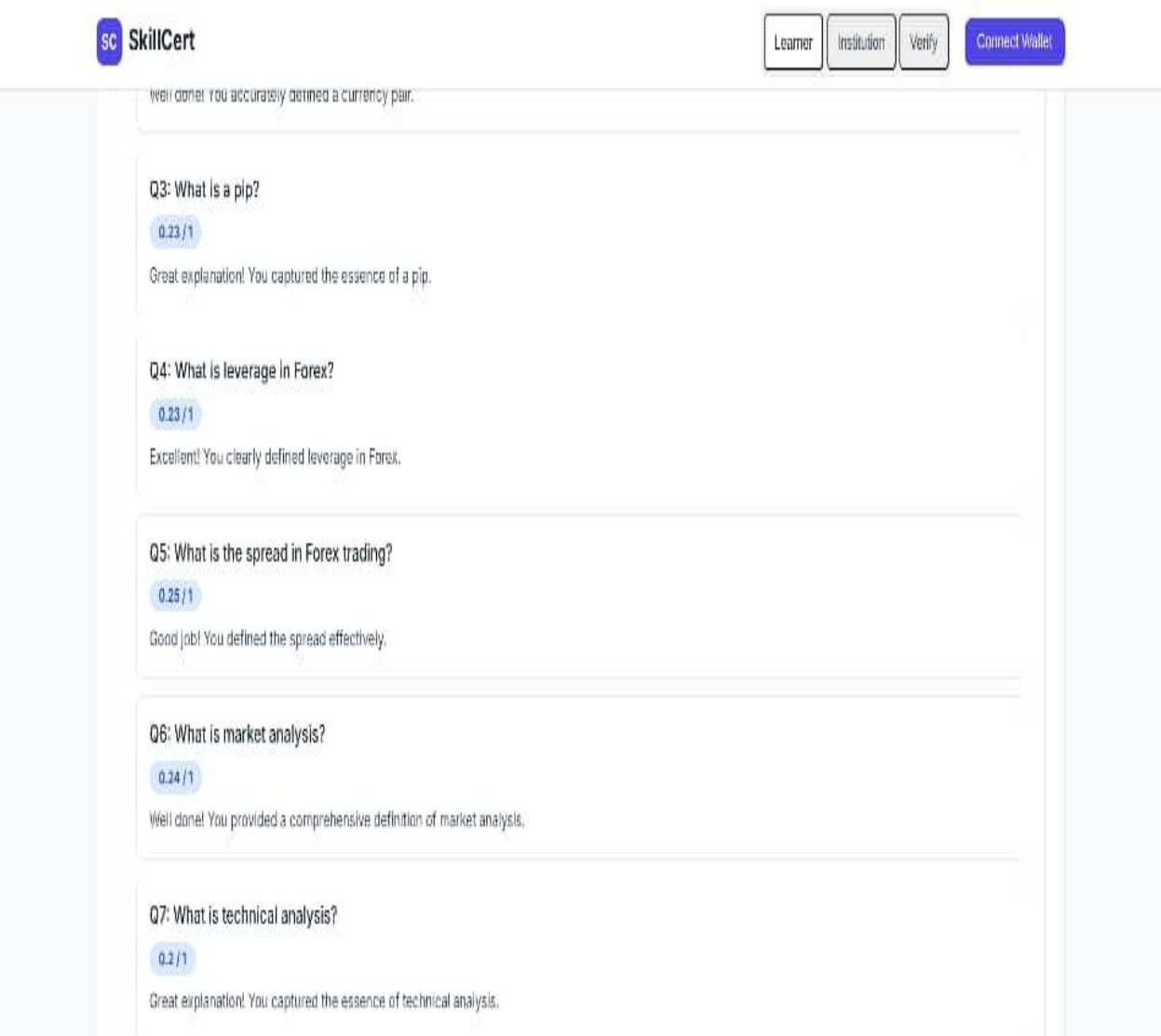
4. Figure 4.4: Course code generation output.



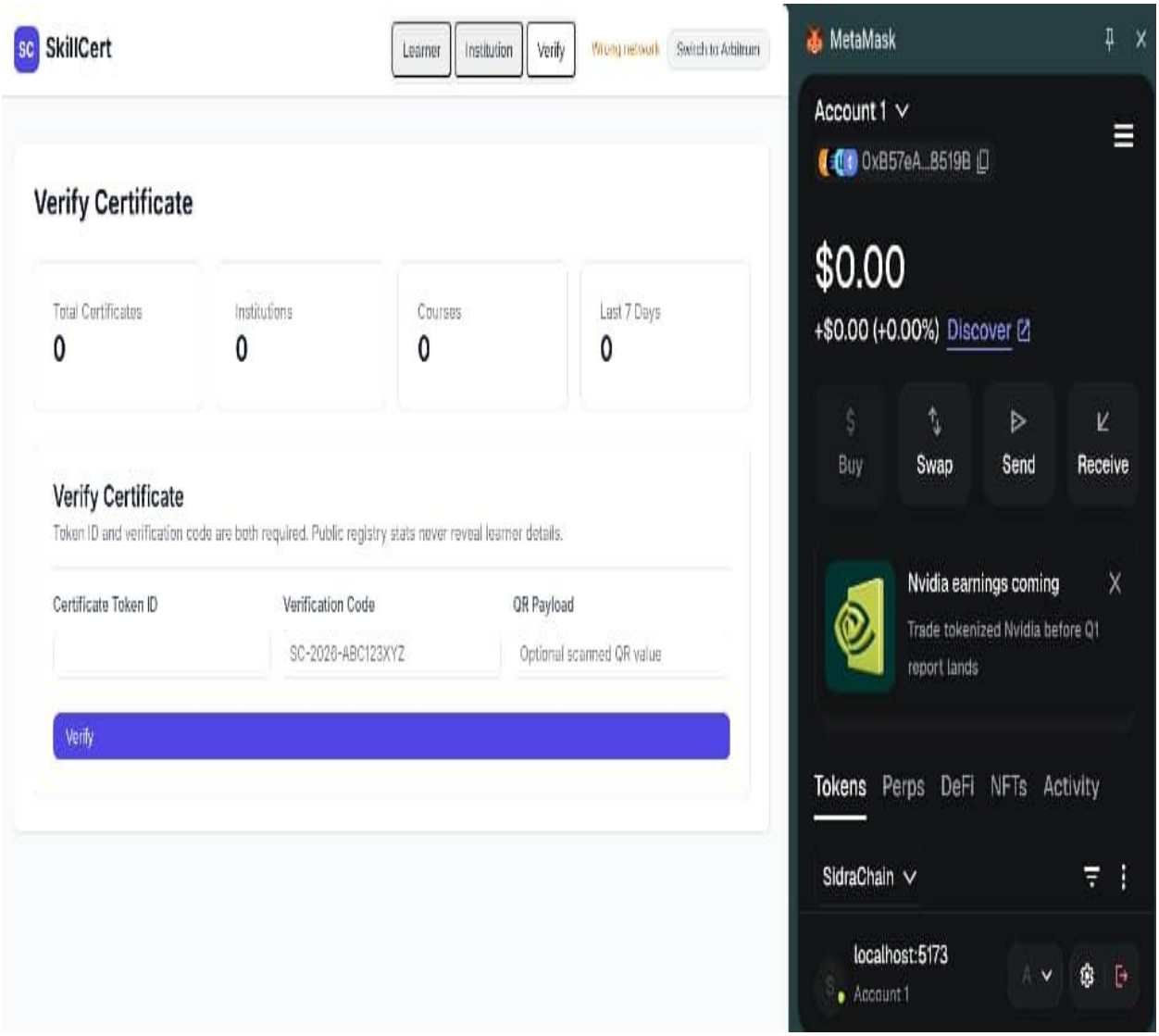
5. Figure 4.5: Learner dashboard showing available courses.



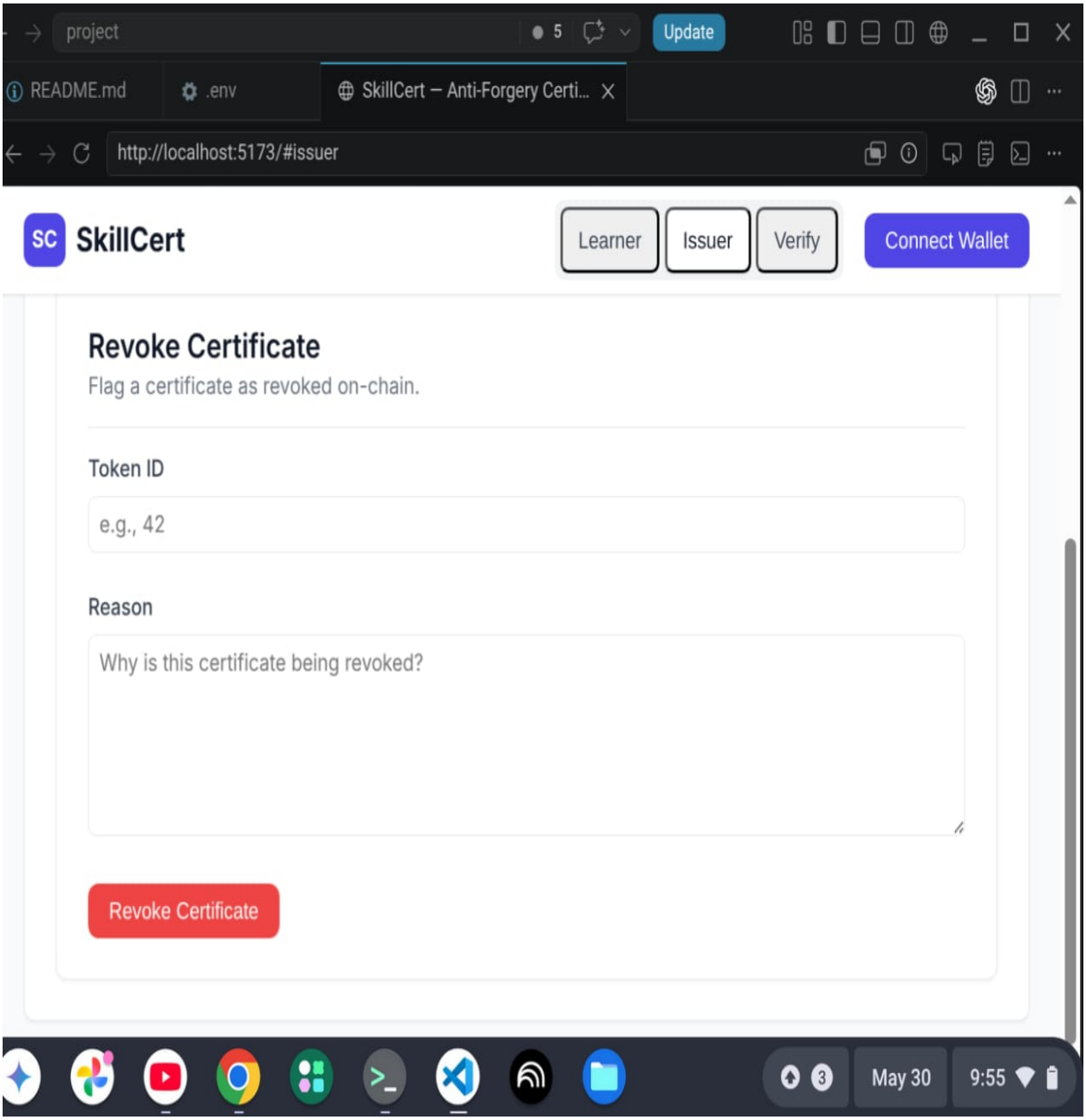
6. Figure 4.6: Assessment question screen.



7. Figure 4.7: Assessment result and feedback screen.



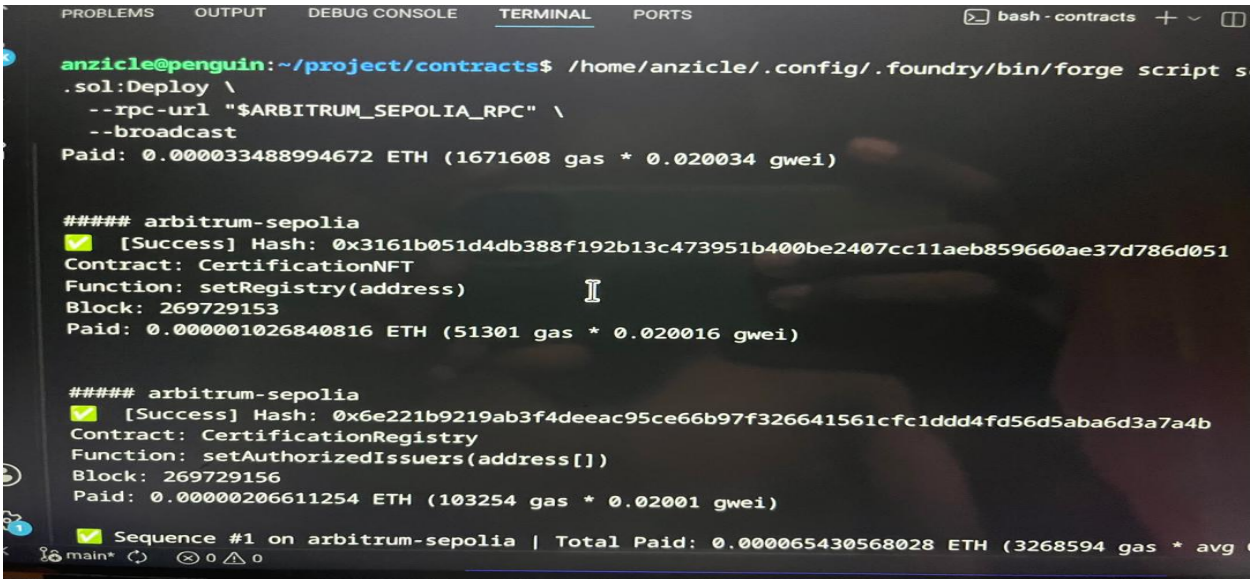
7. Figure 4.8: Public verification dashboard



10. Figure 4.9: Revocation Page for certificates Revoking



10. Figure 4.10. sample downloaded issued certificate



11. Figure 4.11: Smart contract test output.

4.6.2 Discussion of Results

The created prototype meets the objectives of research fully. It allows users to sign up for the service, issuers to create courses and assessment templates, learners to subscribe using the course code, creation of an assessment using AI, and issuing of a certificate after assessing the learner's work by means of blockchain technology.

Assessment creation using AI was successfully accomplished on the basis of OpenAI service with a requirement for 30 questions to be included. Back-end was successfully linked to the blockchain network Arbitrum Sepolia by its chain ID of 421614. Test cases for the smart contract were run successfully.

The design also exhibits resilience. In case the LLM fails to produce output or produces an incorrect one, the use of local fallback helps avoid failure in assessment generation. In the absence of competency and anomaly artifacts, logging the error message followed by continued assessment grading without failure is achieved by the application. In case of certificate issuance failure after assessment completion, backend logging and subsequent reporting of assessment result alongside certificate issuance failure occurs instead of assessment failure itself.

The primary limitation of the system observed during the implementation phase was the long period of time taken to generate thirty structured questions using the language model. This problem was resolved through increased AI timeout on backend along with long OpenAI timeouts. The limitation in the current design, however, is that there are no trained competency and anomaly models due to missing artifacts.

CHAPTER FIVE

SUMMARY, CONCLUSION, AND RECOMMENDATIONS

5.1 Introduction

This chapter highlights the conclusions and recommendations drawn from the entire work. This chapter describes how this study concentrated on developing an anti-forgery proof certificate registry system that could be used to verify skills acquired by students. Such a system aimed at tackling issues such as forgery, inefficiency in verification, the existence of non-transparent certificate revocation policies, and inadequate technological linkage between evaluation and certificate issuance.

5.2 Summary of the Study

The problem area for the current research was initially outlined based on the identification of the issue of the falsification of certificates as one of the core challenges related to the process of acquiring skills and education. Currently available solutions include paper certificates, regular digital solutions, and manual institution verification. These solutions are subject to the risks of being modified, duplicated, slow, non-transparent, and difficult to verify.

Based on the analysis, there is potential in the combination of blockchains to provide an immutable solution, provenance and transparency for the public verification; and the application of smart contracts to enable automation of both issuing and revoking certificates. Moreover, it has been shown that NFT certificates could be used to provide a unique solution for issuing certifications. However, the necessity to protect privacy and sensitive information from being made visible on-chain should also be considered. Finally, it has also become evident that AI could

play an important role in assessment of learners; however, very few current solutions are combining this assessment with blockchain-based certificates.

To overcome this, a modular solution was developed that included a frontend, backend API service, AI assessment service, and a smart contract registry.

This design utilizes course enrollments based on codes generated by issuers, multi-assessment capability for each course, assessment difficulty set from the back-end, thirty questions in each assessment, hybrid AI marking capabilities, creation of certificate in PDF format, certificate verification based on the verification code, and recording of certificates using the blockchain.

Through testing, the ability to generate a 30-question assessment through the AI service, communication between the back-end and both the AI service and the blockchain, and execution of core functionalities in the front-end was validated.

5.3 Conclusion

The findings from this research have revealed that integrating smart contracts within blockchain technology and artificial intelligence can enhance the integrity of the certification process. The AI component provides support at the pre-issuance level through evaluation of learner performance. The blockchain provides tamper resistance at the post-issuance stage where certificate authenticity can be independently authenticated.

The use of smart contract-based approach reduces the chances of certificate forgery since the certificates will no longer be uploaded as documents alone but as assessment records and associated with verification codes and metadata as well as non-fungible tokens. In addition, the use of smart contracts will allow issuing authorities only to issue or revoke certificates.

Transparency is guaranteed with public verification, although privacy is assured since sensitive data about issuers or earners of the certificates will not be included in the public registry. Since this system was built in a modular fashion, this prototype can be taken further and enhanced in order to build a fully fledged working solution.

Therefore, it should be noted that the objectives of this project were met successfully since this project involved creating an anti-forgery proof certification registry using smart contracts and artificial intelligence

5.4 Recommendations

Based on the implementation and testing, the following recommendations are made:

1. Issuers should deploy verification mechanisms where certificates can be tied to assessment evidence rather than having standalone certificates.
2. For future iterations, training and validation of both models of competence and anomaly detection should be conducted based on representative sample data.
3. Actual issuers and learners could be utilized for usability and efficiency testing of the system.
4. Alternative methods of protecting people's privacy could also be researched, including selective disclosure or zero-knowledge proofs.
5. It could be further enhanced by using reliable pinning services and implementing correct retention practices.
6. The certificate registry could include institutional accreditation criteria.

7. Audits and analysis should be performed to assess whether the AI grading algorithm is unbiased, especially considering different types of writing.

In the future iterations, additional evidence of practical skills might be considered, such as supervisor reviews, photos, videos, or rubrics of

5.5 Contribution to Knowledge

This project's unique contribution lies in the integration of the following three concepts in a single system:

1. AI-based evaluation of learners prior to certificate issuance.
2. Certificate representation via NFTs in the form of smart contracts.
3. Verification of certificates via blockchain transactions and verifications codes.

Unlike approaches that either only store certificates in blockchain or only rely on AI for learner assessment, the present project links the latter directly to the former. This ensures that the common problem of "garbage in, garbage out" associated with blockchain certificate systems does not arise.

5.6 Areas for Further Study

Further study may focus on:

1. Larger training datasets used in developing AI competency models.
2. Assessment of the grading accuracy of LLM-assisted assessments in different skills.
3. Comparison of Arbitrum Sepolia/Arbitrum mainnet against other blockchain technologies with regard to cost and efficiency.
4. Decentralized identity standards for both the learner and the certificate issuer.
5. Incorporation of zero-knowledge proof to limit data disclosure in public.

References

Deol, Jani & Zafer, Bilal. (2025). Skill Acquisition Programs and Their Influence on Entrepreneurship Development among University Graduates**.**

Achour, M., Ahmed, S., Hassan, R., & Bello, A. (2025). Deep learning approaches for credential fraud detection using CNN and RNN models. Journal of Artificial Intelligence and Security Studies, 15(2), 88–105.

Balducci, F. (2024). Artificial intelligence tools and explainability in learner assessment. International Journal of Artificial Intelligence in Education, 34(1), 88–107.

Delgado-von-Eitzen, C. (2024). NFTs in education and GDPR compliance: Privacy-preserving approaches for digital credentials. Education and Information Technologies, 29(4), 5211–5230.

Dennis, A., Wixom, B. H., & Roth, R. M. (2012). Systems Analysis and Design with UML (5th ed.). John Wiley & Sons.

DigiPramaan. (2024). Blockchain-enabled certificate management and verification system for educational institutions. Technical Report, DigiPramaan Educational Technologies.

Frisch, R. (2023). Blockchain diploma authenticity verification system using smart contracts. International Journal of Blockchain Technology, 12(1), 44–61.

Ifeyemi, A., Oyedeji, T., & Adebiyi, O. (2024). A blockchain-based digital educational certificate verification system in Nigeria. Nigerian Journal of Computing and Information Systems, 16(2), 77–94.

IJCRT Research Collective. (2024). Blockchain-integrated AI credentialing systems in higher education. International Journal of Creative Research Thoughts, 12(5), 210–225.

Kulkarni, S., Desai, P., & Sharma, R. (2022). AI and machine learning methods for educational assessment and personalized learning. International Journal of Educational Technology, 14(3), 145–162.

Kumar, R., & Patel, S. (2023). Interoperability standards for blockchain credential systems using W3C verifiable credentials. Journal of Distributed Ledger Technologies, 9(2), 112–128.

Lone, A. H. (2020). Forgery protection of academic certificates through integrity preservation at scale using Ethereum smart contracts. Journal of Information Security and Applications, 54, 102526.

Okafor, C., & Mensah, K. (2025). Bias and fairness challenges in AI-driven educational assessment. Journal of AI Ethics and Society, 7(1), 33–49.

Owan, V. J. (2025). Artificial intelligence and educational assessment systems: Governance, accountability, and transparency. Educational Policy Review, 19(2), 201–219.

Swani, P. (2024). Blockchain certificate management in developing regions: The DigiPramaan framework. Proceedings of the International Conference on Educational Technology and Innovation, 145–158.

Thompson, J., Vasquez, M., & Chen, L. (2024). Zero-knowledge proofs for privacy-preserving credential verification. Journal of Cryptographic Engineering, 14(1), 55–70.

Zhang, Y., Liu, X., & Wang, H. (2022). Immutable digital recognition via blockchain: A framework for cross-border credential verification. International Journal of Educational Technology and Innovation, 8(4), 301–318.

Appendix

Project Directory Trace:

```
project/
├── frontend/
│   └── public/
│       ├── index.html
│       ├── auth/
│       │   ├── login.html
│       │   └── register.html
│       ├── scripts/
│       │   ├── app.js
│       │   ├── api.js
│       │   ├── issuer.js
│       │   ├── learner.js
│       │   ├── verifier.js
│       │   └── wallet.js
│       └── styles/
├── backend/
│   ├── app/
│   │   ├── main.py
│   │   ├── api/
│   │   │   ├── auth.py
│   │   │   ├── assessments.py
│   │   │   ├── certificates.py
│   │   │   ├── courses.py
│   │   │   └── issuers.py
│   │   ├── core/
│   │   │   ├── config.py
│   │   │   └── security.py
│   │   ├── models/
│   │   │   └── db.py
│   │   └── services/
│   │       ├── blockchain.py
│   │       ├── certificate_pdf.py
│   │       └── ipfs.py
```

```
│   └── .env
├── contracts/
│   ├── src/
│   │   ├── CertificationNFT.sol
│   │   └── CertificationRegistry.sol
│   ├── script/
│   │   └── Deploy.s.sol
│   └── test/
├── ai_service/
│   └── app/
│       ├── main.py
│       ├── train.py
│       ├── model_service.py
│       └── persistence.py
└── README.md
```

Runtime Setup

Something to note is this is for a Linux system setup and link to the full system will be in my git hub repo**.**

Ai Service:

cd ai_service/app

../.venv/bin/uvicorn main:app --host 0.0.0.0 --port 8001

Backend:

cd backend

.venv/bin/uvicorn app.main:app --host 0.0.0.0 --port 8000

Frontend

cd /home/anzicle/project

backend/.venv/bin/python -m http.server 5173 --directory frontend/public

Open the frontend atÂ http://localhost:5173.

Environment Configuration:

Backend .env

AI service .env

DATABASE_URL

ARBITRUM_RPC_URL

REGISTRY_CONTRACT_ADDRESS

NFT_CONTRACT_ADDRESS

DEPLOYER_PRIVATE_KEY

SECRET_KEY

ENCRYPTION_KEY