TECHNICAL AND VOCATIONAL TRAINING INSTITUTE

(FDRE TVTI)

DEPARTMENT OF INFORMATION TECHNOLOGY



A Research Submitted in Partial Fulfillment of the Requirements for the Degree of

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

By

Shishay Hadush

Student ID: MTR/718/13

Principal Advisor: Dr.Kibrom Tadesse

Addis Ababa, Ethiopia

June 2026

FDRE TECHNICAL AND VOCATIONAL TRAINING INSTITUTE

COLLEGE OF GRADUATE STUDIES

DEPARTMENT OF INFORMATION TECHNOLOGY

Title:

Blockchain-Based Educational Certification System: A Case of TVET Colleges in Eastern Tigray

By
Shishay Hadush

Supervisor: Dr. Kibrom Tadesse

A Research Submitted to the Department of Information Technology, College of Graduate Studies, FDRE Technical and Vocational Training Institute (FDRE TVTI), in partial fulfillment of the requirements for the degree of Master of Science in Information Technology.

MASTER OF SCIENCE IN INFORMATION TECHNOLOGY

By: *Shishay Hadush*

Student ID: MTR/718/13

Principal Advisor: Dr.Kibrom Tadesse

Addis Ababa, Ethiopia

June 2026

Declaration

I, Mr.Shishay Hadush, the under signed, declare that this thesis entitled**: "Blockchain-Based Educational Certification System: A Case of TVET Colleges in Eastern Tigray"** is my original work. I have undertaken the research work independently with the guidance and support of the research advisor. This study has not been submitted for any degree or diploma program in this or any other institutions and that all sources of materials used for the thesis has been duly acknowledged.

Declared by:

Name: _____

Signature: _____

Department: Information Technology, FDRE TVTI

Date: _____

This Research has been submitted for examination with my approval as the candidate's advisor.

Principal Advisor: _____

Signature: _____

Date: _____

APPROVAL PAGE

This is to certify that the Research entitled **"**Blockchain-Based Educational Certification System: A Case of TVET Colleges in Eastern Tigray**"** submitted by Mr. Shishay Hadush (ID No. MTR/718/13, in partial fulfillment of the requirements for the degree of Master of Science in Information Technology, has been examined and approved by the Board of Examiners of the Department of Information Technology, FDRE Technical and Vocational Training Institute.

Examination Role	Name	Signature	Date
Principal Advisor			
Co-Advisor (if any)			
Internal Examiner			
External Examiner			
Department Head, IT			
Dean, College of Graduate Studies			

Place: Addis Ababa, Ethiopia

Date of Final Approval: _____

Acknowledgment

First of all, I am thankful to the Almighty God for giving me good health and recovery. I could not reach this stage without His blessings and protection.

Secondly, I would like to express my profound gratitude to my advisor Kibrom Tadesse(PHD) whose timely encouragement and constructive criticisms made it possible for me to conduct this research successfully. I am extremely grateful to his motivation and advice that he played a significant role in the research process and completion.

I would also like to show my gratitude to the management and lecturers of the ICT Department of the Federal TVET Institute Ethiopia for their continuous cooperation during this research. Moreover, I am very thankful to the management and lecturers, students and human resource management practitioners of Edaga Hamus TVET College, Wukro TVET College, Adigrat TVET College, Edaga Hamus Town Woreda Office, Frewoin Town Woreda Office, Tsaeda Emba Woreda Civil Service Office, and Subuha Saesi Civil Service Office for their cooperation.

Finally, I am extremely thankful to my respected family members and close friends for their continuous encouragement, understanding, and support while conducting this research. Furthermore, I would like to express my heartfelt thanks to all those people who helped directly on this research.

Abstract

An emerging trend towards faked certificates became a problem to educational integrity worldwide . Eastern Tigray was known to be exposed to threats related to the conflict in that region, including destruction of credentials and counterfeiting of certificates Traditional methods of verification were deemed not sufficient as they posed a risk of both fraud and time-consuming process. It made the process of credentials' verification difficult to manage for everyone. In this context, blockchain technology offered a unique opportunity by providing an additional layer of protection due to the decentralized and encrypted ledger. As a consequence, this paper explores the application of blockchain technology to enhance the process of credential management in TVET colleges. Specifically, this research will discuss ways of preventing fraud and destruction, rapid access to verification data, and additional control over personal information that can be gained through the implementation of blockchain-based credential management solutions. Methodology used in this research is mixed and consists of qualitative interviews with TVET college's administration, IT specialists, and students, as well as quantitative analysis relying on the prototype of blockchain created using smart contracts.

Keywords: Blockchain, smart contracts, verification, Tigray TVET colleges

Contents

Declaration II

APPROVAL PAGE III

Acknowledgment IV

List of Abbreviation and acronyms iii

Application programming interface iii

Build and Build iii

Content identifier iii

Database iii

Degree chain iii

An open sources framework used in python for backend development iii

Design science research iii

A name of the research prototype iii

Non-fungible token standard is written in solidity language on the Ethereum blockchain iii

Standard can be used in the Sandbox, combinations of non-fungible, fungible, and semi fungible tokens iii

Ethereum Virtual machine iii

Istanbul byzantine fault tolerant iii

Interplanetary file system iii

JavaScript Object notation iii

Non fungible token iii

An open source cross platform java script run time environment used for server side code iii

Object relational mapping iii

Proof of authority iii

Proof of work iii

Rapid Application Development iii

A collection of libraries that allow development to interact with a local or remote ethereum node using HTTP, IPC, or web socket iii

1.1. Statement of the Problem 5

Specific objective 5

1.4. Research Question 6

1.5. Significance of the Study 6

1.6. Limitation of the Study 6

1.7. Scope of the Study 7

1.8. Organization of the study 7

Chapter Two 8
2. Review of Related Literature 8
2.1. Emergence of Blockchain in Education 8
2.2. Application in the TVET Sector and Resource-Limited Settings 9
2.3. Overview of Technical Basics of Distributed Ledgers 9
2.4. A Critical Look at the Missing Pieces 12
2.5. Structural and Systemic Limits in Blockchain Technology 13
2.6. The Consensus Engineering Landscape in Low-Resource Settings 13
2.7. Architectural Evolution: 14
2.8. Self-Sovereign Identity (SSI) and Student Data Ownership 14
2.9. Identification of the Core Research Gap 15
2.10. Conclusion 15
Chapter Three 20
Research methodology 20
3.1. Research Design 20
Comparative analysis vs manual process method 23
3.2. System Structure 25
3.3. Study Area, Target Population, and Stratification 27
3.4. Blockchain-Based System Design 28
3.5. Functional Components 31
3.6. Data Flow and Process Model 34
❖ Technical Snapshot (Ganache Testnet Metrics) 37
4. Unsurpassed Transparency and Provenance 39
5. Highly Resilient and Distributed Security Model 39
3.7. Development Tools and Environment 40
Selecting EVM 44
3.8. Evaluation Strategy 44
Chapter 4 49
System Development and Discussion 49
4.1. Development Environment and Tools 49
Summary Statement: 53
4.2. The Issuance & Verification Workflow 53
4.3. Core Subsystem Development 54
4.6. Results and System Performance Technical Validation 58
4.8. Discussion 60

N.B From the system implementation 62
Summary 62
CHAPTER 5 63
Conclusion and Recommendations 63
5.1. Summary of Findings 63
5.2. Conclusions 64
5.3. Recommendations 65
5.4. Future Work 65
5.5. Chapter Summary 66
Appendix 70
Appendex A: 70
Appendix F : Qustiones of the questioner 74
Part 2: General Certification Process and Issues 74
Appndix G: interview questions 74

Table of figures entries found

TABLE 2.1 PUBLIC VS PRIVATE BLOCKCHAIN PERMISSIONS(CANTILLO-LUNA ET AL., 2022) 9
TABLE 2.2. COMPARATIVE MATRIX OF BLOCKCHAIN CREDENTIALING FRAMEWORKS 17
TABLE 3.1. MAP OF DSR ARTIFACTS OF EDUBLOCK PROTOTYPE 23
TABLE 3.2. COMPARISON TABLE: EXISTING CERTIFICATION SYSTEM VS. PROPOSED BLOCKCHAIN-BASED EDUBLOCK SYSTEM 24
TABLE 3.6. TARGET POPULATION AND SAMPLE STRATIFICATION MATRIX 28
TABLE 3.3 SUBSTANTIAL TIME SAVINGS ACHIEVED THROUGH THE BLOCKCHAIN SYSTEM COMPARED TO TRADITIONAL MANUAL PROCESSES 39
TABLE 3.4. COMPLETE CORE TECHNICAL STACK COMPONENTS 44
TABLE 3.5. SUBSTANTIAL TIME SAVINGS ACHIEVED THROUGH THE BLOCKCHAIN SYSTEM COMPARED TO TRADITIONAL MANUAL PROCESSES 48
TABLE 4.1. GANACHE CONFIGURATION PARAMETERS 50
TABLE 4.3. TIME EFFICIENCY OF EDUBLOCK 52
TABLE 4.4. EMPIRICAL DESCRIPTION OF EDUBLOCK BLOCKCHAIN SYSTEM 53
TABLE 4.5. SMART CONTRACT DEPLOYMENT DETAILS 55
TABLE 4.6. SMART CONTRACT PERFORMANCE METRICS FROM OBSERVATION 56
TABLE 4.7. VISUALIZES THE SUS SCORE DISTRIBUTION, WHICH HELPS ILLUSTRATE HOW USABILITY PERCEPTIONS VARIED AMONG THE 10 PARTICIPANTS 58
TABLE 4.8. COMPARISON TABLE BETWEEN THE MANUAL CERTIFICATION SYSTEM AND THE EDUBLOCK BLOCKCHAIN-BASED SYSTEM: 60
TABLE 4.9. TECHNICAL EFFICIENCY (LOW LATENCY AND MODEST GAS COSTS) AND THE USABILITY OUTCOMES (SOLID SUS SCORE INDICATING ACCEPTABLE USER EXPERIENCE). 62

FIGURES ENTRIES FOUND

FIGURE 3.1. . MAPPING OF DSRM ARTIFACT LIFECYCLE FOR THE EDUBLOCK PROTOTYPE (IMAGE USING LLM)..... 25
FIGURE 3.2. SYSTEM ARCHITECTURE DIAGRAM(IMAGE USING LUCID CHART)..... 27
FIGURE 3.3. BLOCKCHAIN-BASED CERTIFICATE MANAGEMENT THROUGH SMART CONTRACTS FROM 30
FIGURE 3.4. CERTIFICATE ISSUANCE LIFECYCLE PIPELINE FROM (ASIF & HASSAN, 2023)..... 33
FIGURE 3.5. EDUBLOCK DATA FLOW AND PROCESS MODEL 34
FIGURE 3.6. TRANSACTION HASHES ON GANACHE 37
FIGURE 3.7. SECURE DECENTRALIZED VERIFICATION WORKFLOW(IMAGE USING LUCID CHART)..... 40
FIGURE 3.8. LOCAL ETHEREUM BLOCKCHAIN NETWORK USED IN EDUBLOCK 41
FIGURE 3.9. FRONT END AND BACKEND INTERACTION OUTPUT 43
FIGURE 4.1. 1 ROLE-BASED STAKEHOLDER ACCOUNT CONFIGURATION IN GANACHE..... 49
FIGURE 4.2. BLOCKCHAIN BLOCK MINING AND GAS CONSUMPTION DURING EDUBLOCK SIMULATION..... 50
FIGURE 4.3. AUTHORIZED COLLEGE CREDENTIAL ISSUANCE DASHBOARD..... 51
FIGURE 4.4.B. EDUBLOCK INTERFACE FOR NEW STUDENT REGISTRATION 54
FIGURE 4.4.A. EDUBLOCK INTERFACE FOR NEW STUDENT REGISTRATION 54
FIGURE 4.4. C HASH RECORD OF A REGISTERED STUDENT IN GANACHE..... 54
FIGURE 4.5. CONTRACT COMPILATION PROGRESS IN VISUAL STUDIO 55
FIGURE 4.6. COLLEGE PANEL OF EDUBLOCK SYSTEM..... 58
FIGURE 4.8. PERFORMANCE METRICS GRAPH 59
ACCEPTABLE USER EXPERIENCE)..... 62

List of Abbreviation and acronyms

API	Application programming interface
BNB	Build and Build
CID	Content identifier
DB	Database
DegChain	Degree chain
Django	An open sources framework used in python for backend development
DSR	Design science research
EDUBLOCK	A name of the research prototype
ERC-721	Non-fungible token standard is written in solidity language on the Ethereum blockchain
ERC-11 55	Standard can be used in the Sandbox, combinations of non-fungible, fungible, and semi fungible tokens
EVM	Ethereum Virtual machine
IBFT	Istanbul byzantine fault tolerant
IPFS	Interplanetary file system
JSON	JavaScript Object notation
NFT	Non fungible token
Node.js	An open source cross platform java script run time environment used for server side code
ORM	Object relational mapping
POA	Proof of authority
POW	Proof of work
RAD	Rapid Application Development
WEB3	A collection of libraries that allow development to interact with a local or remote ethereum node using HTTP, IPC, or web socket

Chapter one

1. Introduction

There have been several cases reported globally in regard to fake or falsified certification of educational qualifications. This phenomenon is compromising the validity of any education program as well as making the process of verification more challenging. When people manage to obtain credentials without attending relevant courses, it compromises the credibility of the educational process and makes it difficult for organizations to verify them (Carmichael & Eaton, 2023). For example 200,000 of Ethiopian civil servant which work in public and private institutions were spotted with false certification. have been instances of fraud cases where celebrities used counterfeit certificates (Garg, 2022; Yonas Abiye, 2019). In Tigray in one health bureau recruitment from 50 candidates 12 of them are rejected by the case of forged certification(*Letter5*, n.d.). From similar cases in different countries, one can note that this is indeed a global problem affecting the integrity of education and employment systems everywhere (Tolu-kolawole, 2025; *ንግድ ባንክ በሀሰተኛ የትምህርት ማስረጃ የተቀጠሩ ከ200 በላይ ሰራተኞቸን አባረረ - Wazemaradio.Pdf*, n.d.)).

Despite the universal nature of credential fraud, it is an especially pressing issue in the field of education and training within Tigray TVET. Due to the recent conflict in Tigray, many academic papers and official documents were destroyed or simply not found anymore, thus making it very hard to verify people's qualifications. As part of the civil service administration in the woreda sa/tsa/emba area, most records were destroyed (25% of all civil service and administrative documents, information from the expert of civil service office of woreda sa/tsa/emba) which made it impossible to confirm any candidate's academic success. Therefore, due to a decline in verification activities, the possibility of fraud was significantly higher which made it possible to produce counterfeit diplomas and certifications). Moreover, there have been cases of unauthorized institutions issuing certificates which did not meet necessary requirements. The sum of these weak points leads to credential fraud in Tigray that affects numerous administrative actions including delays in hiring, legal issues, and complicated promotion/placement processes. Some information shows that many people working in certain areas possess fake credentials (*Letter5*, n.d.) In order to solve the problem Blockchain provides a tamper-proof technology that lessens dependence on physical archives. Effective process through digital signature and smart contract that allows rapid verification of credentialing (Maroso et al., 2024). Digital credentials not only provide learners with better control and transparency but also offer the organizations and employers a dependable, efficient credentialing service (*BlockchainRevolutioninEducation_RG*, n.d.; Maroso et al., 2024). Moreover, blockchain technology can help prevent destruction of document integrity from conflicts by providing decentralized storage of credentialing documents (Carmichael & Eaton, 2023). It is becoming increasingly popular to use IT technologies like blockchain as the most promising solution to manage credentials. This level of corruption undermines the credibility of the assessment and proper accreditation of the TVET graduates' skills. Then the researcher sees the above studies constructing a blcockahin based educational certification prototype finds a solution for the problems existed in eastern Tigray TVET colleges. This research proposes a new model that utilizes blockchain technology for the efficient issuance and authentication of certification in TVET colleges within the Eastern part of Tigray. Instead of merely relying on paper work, this prototype uses smart

contracts to provide an environment in which data can be recorded and validated quickly and credentials can be revoked whenever necessary. One important issue that needs to be addressed at this point is whether a permissioned blockchain will be effective in the light of poor infrastructure and lack of reliable connectivity in the region.

1.1. Statement of the Problem

The existing system used by TVET colleges in Eastern Tigray is based on the traditional, centralized approach to credential management. All data about students is saved in a single, centralized office and, most importantly, is not backed up through modern cryptography methods such as encryption and no digital records at all. Since there is only one node/at college level storing the data, the entire system is highly vulnerable and prone to failures and destruction. Besides, it does not guarantee integrity of the records over long periods of time. Since all data storage is performed physically and in a centralized manner digitally, the trustworthiness of the information may be put into question in an unstable environment where physical destruction of records is highly possible without a way to prove the veracity of the lost data.

Finally, the procedure of credential verification is time-consuming and inefficient since no automated systems of asynchronous processes are used, making it hard for third parties to distinguish between authentic and fake certificates.

The national-level analysis has demonstrated that the absence of proper security mechanisms, including cryptography-based security schemes, has been one of the main causes of credential frauds and the emergence of fraudulent certification registry databases. Although the utilization of blockchain technology allows for the development of a solid basis for integrity checks based on mathematically provable techniques, all available blockchain technologies operate under the assumption of rapid and stable internet connection. This is hardly applicable in the case of the Tigray region.

Therefore, the research indicates an evident gap that requires addressing there is an urgent need to develop light-weight and permissioned blockchain technologies appropriate for deployment in regions such as Tigray. This problem has led to the creation of the study objective, which implies developing a decentralized trust model appropriate for the operational environment.

1.2. General Objective

Objective the study is to design and develop a blockchain based educational certification prototype for issuing and verifying certificates for Eastern Tigray TVET Colleges

Specific objective

1. Analyze the structure of cryptographic state anchoring and design permissioned ledger architecture (EduBlock) for TVET academic data, ensuring the system cannot be compromised through malicious changes or tampering.
2. Evaluate how decentralization improves verification by comparing system performance between manual verification using the centralized database and a hash-matching verification protocol, to determine whether verification latency can be reduced.

3. Identify engineering constraints of permissioned blockchain in a limited-resource environment by experimentally assessing key factors such as transaction confirmation times**,** transaction processing speed, and gas consumption of smart contracts**.**
4. Assess security constraints and opportunities by reviewing how decentralized access control can be implemented using role-based mechanisms embedded in smart contracts at the levels of regional authorities**,** TVET institutions, and individual students**.**

1.4. Research Question

1. How effective is it to use cryptographic technologies in order to ensure immutability and non-repudiation of TVET educational records in a centralized scenario through permissioned hybrid blockchain framework?
2. How efficient is the decentralized web-based hash matching technique in order to reduce the required time of verification and also tackle the issue of information asymmetry among the third parties when compared with traditional methods?
3. What are the drawbacks of transaction speed, efficiency, and gas fees in order to apply EVM-compatible solution in a simulation environment?
4. How effective are RBAC role modifiers through smart contract in order to grant administrative privileges?

1.5. Significance of the Study

This research contributes both practically and theoretically by delivering a tested solution to the problem of moving sensitive paper-based records to a decentralized, cryptographically secured digital format. The following sections assess the practical impact of this research according to four specific domains. Firstly, from the perspective of TVET regional administration and policy-makers, this research provides a functional implementation blueprint for decentralization and data governance. Role based access control authentication allows to whitelist regulatory bodies that's why it was from the benefits of Edublock , because it enables no any certification is issued improperly so it should be a model for another tvet colleges on the region and he country also.

Secondly, in terms of practical impact on the graduate and learning experience, this solution moves credentialing to the user-centered paradigm of data ownership. Immutability in the form of cryptographic hashes ensures that academic achievements are safely recorded regardless of any regional instability or damage to local infrastructure. Additionally the removal of any overhead or delay associated with paper-based record keeping allows for swifter entrance to the workforce. Thirdly, employers and verifiers gain a novel automated means of credential verification without the need for intermediaries, thus cutting down on recruitment costs and reducing information asymmetry. What used to take at least two weeks in some cases can

1.6. Limitation of the Study

Although this research provides functional baseline evidence for decentralized credentialing some technical, operational, and structural considerations need to be noted. The limitations of the infrastructure itself include the development of the system prototype as a local and permissioned blockchain solution deployed on an emulated Ethereum network (Ganache). This test version does not

exist as a public mainnet or decentralized network layer. Hence, the results related to execution costs, network latency, and node propagation time can only be measured within these infrastructural parameters and cannot serve as the basis for assumptions concerning its actual behavior in terms of these metrics in the real world. The limitation of the availability of empirical data is associated with the highly sensitive nature of credential fraud in the region and the closure of some of the institutions. Hence, participants' reluctance to disclose exact data about the number of fake certificates or the fraud networks prevented the use of comprehensive statistical data as an empirical source. In turn, administrative declarations served as more reliable data sources for research in this particular case. Another limitation of the technological type includes the potential subjectivity of opinions due to the lack of digital literacy among the administrative personnel.

1.7. Scope of the Study

Scope of the study is limited in one zonal administration of three tvet colleges of Edagaa Hamus, Adigrat, Wukro as a model for working of blockcahin based certification to apply in minimum infrastructural regions like Tigray . It was not extend wide to other educational levels, so it was only for TVET colleges.

1.8. Organization of the study

Chapter One describes the including the introduction part , background , statement of the problem ,objective of the study , research question , significance of the study, limitation of the study and organization of the study.
Chapter Two Literature review, including empirical studies, conceptual studies, and emergency of blockchain system for Tvet colleges.
Chapter Three describes the research methodology, the research design, study area, population, sampling techniques, data collection methods, and data analysis procedures used in the study.
Chapter Four presents the results and discussion of the study, including data analysis, system implementation, and evaluation of the blockchain-based certification system.
Chapter Five provides the conclusions and recommendations based on the findings of the study, along with suggestions for future research.

Chapter Two

2. Review of Related Literature

In this section, the current study reviews the previous researches, relevant models or frameworks, as well as technologies that have already been used to develop digital credential systems. The traditional paper-based credential system is burdened with numerous obstacles including long-term processes, expensive administrative processes, and high levels of fraud that are prevalent in this kind of management system (Turkanović et al., 2018). Particularly, the fraud risks that accompany traditional paper-based credential systems are particularly significant in developing regions like Tigray in which counterfeit degrees negatively impact not only the reputation of educational institutions but also prevent graduates from obtaining jobs and continuing their education (*The Global Rise of Fake Degrees : Six Major Scandals in 2024 Member Of Legal*, 2025). This study seeks to build a substantial knowledge foundation for its implementation. To do so, the relevant literature, as well as the methods and strategies that are used in the development of digital credential management and verification system, will be considered in detail. As it is obvious, the rapid advancement of blockchain technology has attracted great attention from various sectors including education due to its capability to solve several issues that arise in this area (Delgado-Von-eitzen et al., 2021; Sithandekile, 2025).

2.1. Emergence of Blockchain in Education

Emerging distributed ledger technology into the TVET colleges the student data will be managed gets transformed dramatically(Farabi et al., 2025). In a centralized certification system all student data are documented in one node or college which is owned by the college officer. But with the distributed technology data will be stored across different colleges at various geographic locations which means is student documents are not vulnerable for destruction and it was shifting the trust from institutions to the capacity of the network in securing transactions. In public blockchains such as Bitcoin are completely decentralized which mean is anyone can participate on the ledger and no one third person is intermediate on the transaction. The problem with public blockchains is the total loss of confidentiality, since grades and diplomas require strict confidentiality; fully public networks simply aren't built for this. When we see the private blockchains shift the rules to single entity or sometimes just a few known groups keeps hold of who gets in and how it runs (Heredia & Show, 2018) when tighter secrecy matters these setups tend to fit better.

Then let’s came into the attempt in creating a way for digital certification to exist within the blockchain broadcast by MIT. The system creates the integration between academic documents and blockcahin through the cryptography. The advantages of cryptography are of verifying something with a blockchain technology is that the information becomes tamper proof. As a result proof the verification process comes fast and with people who need them able to confirm things instantly (Rana & Gautam, 2023). Still looking closer at those first open designs reveal real world delays down line. Setting a strong login details on open and shared network and fees will add up fast because everyone pays to use the system and privacy to use the system and privacy settings might lack precision. Academic records need tighter safeguards than these platforms usually offer.

Today time a blockchain technologies used in various researches have a new direction, involving blockchain technologies where consent or permission is needed. Follow this example such as DegChain there is joint participation among several organizations, unlike in public blockchains. The privacy of data is guaranteed throughout the transactions, thanks to the manner in which data flows through. The performance remains constant despite any changes in demand. Responsibilities are shared by those participating. This technology can be applied to issues related to confidential educational records.(Shawon et al., 2021).

Table 2.1 Public vs Private Blockchain permissions(Cantillo-Luna et al., 2022)

Action	Public Chain		Private Chain	
	(Permission-Less)	(Permissioned)	(Consortium)	(Enterprise)
Chain Access	Everyone	Everyone	Group Owner	Group Owner
Transactions	Everyone	Owners & Validated Users	Owners & Validated Users	Administrator
Commit to chain	Everyone	Owners & subset of Validated Users	Owners & subset of Validated Users	Administrator

2.2. Application in the TVET Sector and Resource-Limited Settings

While traditional universities and colleges have spearheaded the testing of blockchain technology in early deployments, its deployment in the TVET industry is quite underdeveloped(Mihaljević et al., 2023). In vocational training facilities, qualifications must always be updated owing to the ever-changing nature of skill sets, modules, and certificates awarded (& Xu, 2024).

In places where there are few resources and infrastructure is already destabilized, the reason why one needs to choose a decentralized system has much more to do with preserving information than with anything else. Traditional central databases can suffer failures easily, leading to a permanent loss of records in cases of political unrest or technical difficulties (Zambrano-ortiz, 2025). Cryptographically distributed ledgers reduce this risk because they dispersing transaction information from different locations, to ensure that historical data for certification verification is accessible even in some locations signed any problem or destruction and network breakdowns.

2.3. Overview of Technical Basics of Distributed Ledgers

To justify adequate technical progresses for designing and developing the EduBlock system prototype, the architecture needs breakdown its cryptographic and algorithmic components.

2.3.1. Cryptographic Hashing and Data Architecture

The Decentralized credentialing ecosystem depends on one-way cryptographic functions in beginning the Secure Hash Algorithm 256-bit (SHA-256). Within this architecture, plaintext student metadata, institutional wallet, and regional private and credentialing keys are entered into the hashing algorithm to generate a deterministic, fixed-length 32 or 42-byte string, there are different bit distributions in hashing example UTF-8,UTF-16,UTF-32.but for the purpose of cryptographic hash in blockchain it was good to use UTF-8.

$H(x) \rightarrow \{0, 1\}^{256}$

The payload string (x) represents different fields of the Admin, college, and student Meta data. In a specific sequence based on the established format for avoiding confusion. The following descriptions are how a hashing is encoded in cryptography in smart contracts. Let one student have the following details ID, Name, training college, department, and issued date, then it was hashed by the following description as " the world standard for text" states(Daniels, 1993).

The following descriptions are the student Meta data representations on the local blockchain

x = f"{StudentID}{FullName}{CollegeID}{Department}{GraduationDate}"

It should be noted that each of these data is converted to UTF-8 string with a delimiter that cannot occur in these individual strings. In other words, using a cipher suit, the exact process for creating x is described below(McKay, 2019).

StudentID – Convert StudentID (for instance, S123456) to UTF-8 string.

FullName – Convert fullName (for instance, Berihu Hagos) to UTF-8 string.

CollegeID – Convert CollegeID (for instance, COL123) to UTF-8 string.

Department – Convert Department (for instance, Computer Science) to UTF-8 string.

GraduationDate – Convert GraduationDate (for instance, 2026-06-26) to UTF-8 string.

In other words, use a delimiter (for instance, a pipe) and concatenate all of these, for example,

(x = text {"S123456|Berihu Hagos|COL123|Computer Science|2026-06-26|3.75"})

The final result of this is used as an input for hashing, and therefore,

String memory X ="S123456 |Berihu Hagos |COL123 |Computer Science |2026-06-26; bytes32 certhash =H256 (abi.encodePacked(X))

The payload of our transaction sent to EVM is:

StorageState[certID] = certHash;

NB. Sources from the book of "Guidelines for the Selection, Configuration, and Use of Transport Layer Security (TLS) Implementations" (Daniels, 1993).

(H(x)), in this case, will represent the hash value of the 256 bit hash of the serialization of the data payload (x). This way, we can make sure that only the hash is recorded in the blockchain while storing the actual data fields' off-chain to ensure their privacy and strictly adhering to the off-chain philosophy. The on-chain cryptographic anchor hash allows us to verify the data without revealing any personal and confidential information. Mathematically speaking, it proves that data privacy can be ensured since all the data and personal data will remain off-chain(Marchesi et al., 2020).

Following to a consistent series technique, the different files can easily represent in its compact form. So it was the role of on-chain data storage.

2.3.2. Smart Contract Automation and State Transitions

The Ethereum Virtual Machine and conventional software configurations against other frameworks. In contrast to software frameworks like Node.js and Django, which run code in separate processes with CPU thread affinity, the EVM runs as a global virtual ecosystem and executing isolated code. Each participant node within a public or private blockchain performs the same EVM logic operations, thus ensuring consensus on a global scale. Distributed data modification relies on a key notion $\Upsilon(S, T) = S'$. The initial variable S stands for the current state of credential information; T refers to a protected collection of transactions, whereas the resulting variable S′ will be the new system state after performing the operation. The isolated nature of the runtime ensures consistency since, starting from the same initial state S, applying the same transaction list T to each node will yield an identical result S′ preventing discrepancies, synchronization issues, or malicious manipulations. The isolated runtime prevents access to any host operating system resources and thus, to the file system, local time references, or outgoing network connections such as HTTP. This ensures that no random behavior occurs while performing the verification. Hence, new real-time input data should use cryptography-enabled input mechanisms, which will be externally initiated via a bridge app built with Web3.js, leading to inherent dependency, often referred to as the Oracle Dilemma. The execution happens incrementally, and every small operation incurs some amount of gas cost. During execution, the process pays per operation performed, just like money put in a machine. This prevents infinite loops from crashing the system. Each instruction has a cost associated with it and is pre-determined. In the case of lack of resources midway through execution, everything stops. The process stops even before causing any mayhem.

In case a registrar transaction performs the state-changing function, it should have a maximum gas limit (gasLimit). The EVM utilizes the gas gradually while executing the contract opcodes:

[Solidity Entry: issueCertificate()]

├——> Opcode: CALLER (Identifies transaction origin) —► Consumes 2 Gas

├——> Opcode: SLOAD (Reads authorization state) —► Consumes 2100 Gas

└——> Opcode: SSTORE (Anchors SHA-256 state mapping) —► Consumes 20000 Gas

If the execution path runs out of gas mid-cycle, an Out-of-Gas runtime exception is triggered. The EVM immediately aborts execution, completely rolls back all modifications to the state tree to prevent data corruption, but still penalizes the calling identity by consuming the spent gas(Marchesi et al., 2020). This price constraint fundamentally justifies the hybrid architecture of the EduBlock system storing high-overhead string metadata off-chain within a relational SQLite database while minimizing on-chain execution to lightweight and fixed-size 32-byte (bytes32) SHA-256 cryptographic fingerprints (H(x)) inside the contract state mappings.

Component	What it represents mathematically	What it actually means in your EDUBLOCK Project
S	Old State	The ledger before a college issues a certificate. (Student balance/status is empty, exists, false)

T	The Transaction	The Web3.js payload containing the student's name, status, and IPFS image hash
ϒ (Upsilon)	The Transition Function	Your Ganache/Truffle blockchain network processing the transaction and verifying cryptographic keys
S′	New State	The updated ledger after the block is mined (Student status is updated, exists, true)

2.3.3. Decentralized Verification Pipelines

Old-style passes through some complexity procedures moving slow, jumping between paper mail and database searches as well as one signature after another. By cutting this problem new methods cut it down to one efficient moment. Someone outside the system hands encrypted data straight to a browser tool. That app runs a code fingerprint right there on the screen. After that the asked to the blockchain quietly through a lean communication line. When the number it made lines up with the inside memory then responds the answer for his question.

2.4. A Critical Look at the Missing Pieces

There are many blockchain architectures that come with different characteristics tailored for different uses. For example, public blockchains are open access and decentralized systems where everyone can join the network. The open access nature of public blockchain raises many security and privacy challenges, especially when it comes to certifications and data management. For example small rural college with weak infrastructure trying to incorporate a public blockchain together with larger and well-networked TVET institutions runs the risk of making confidential information exposed in a fully-transparent ledger(Grech et al., 2021). In addition, public blockchains attract many cybersecurity attacks, and any security breach may result in loss of confidential student and employer information. Some of the systems prefer using private blockchain platforms such as Hyperledger Fabric (Al-Breiki et al., 2020). Despite the number of studies that focus on different aspects of blockchain architecture, there are very few research studies that explore the use of blockchain architecture in TVET institutions. This paper attempts to fill this gap in literature by examining which blockchain architecture suits TVET colleges.

That approach can reduce transaction costs, but it also creates a closed environment. When the system administrator closes the system the external users like the government offices, auditors, and potential employers can easily verify the verification process. As a result organizations often resort to manual verification and document review process which are time consuming and can load to weeks of repeated exchanges. Furthermore, issues may arise with certain identity based methods, particularly regarding the secure storage of keys. This approach would require graduates to personally hold the keys needed to access their documents. However relying on graduate from conflict affected areas presents challenges, as their infrastructure may be unreliable and their skills may differ significantly

It is from this perspective that advantage of EduBlock provides a specialized blockchain solution to TVET institutions to solve this problem. It should be noted that unlike other blockchain networks that depend on costly mining activities, the Proof of Authority (PoA) consensus mechanism of EduBlock is compatible with the Ethereum Virtual Machine (EVM). In this way it becomes possible for validators in TVET colleges to validate transactions effectively and economically. It is evident that adoption of EduBlock technology in TVET can provide an effective avenue for obtaining secure and unalterable certification records. Nonetheless, an understanding of the integration of such blockchain technology needs more insight on the features of such technologies with regard to TVET institutions.

2.5. Structural and Systemic Limits in Blockchain Technology

One thing about using blockchain technology is it comes with certain issues. Figuring out how structures are made versus how they actually run matters a lot. The setup of blockchains shows four clear hurdles. These must be solved during the creation phase. Each piece affects performance in ways people often overlook. The reason most blockcahin networks operate very slowly lies in how the system checks for transaction. The process of reaching consensus among all nodes greatly reduces the efficiency of the system. All transactions must first reach far and wide before verification cans even take place. Time is involved because information has to travel to various distant locations. The capacity of the blockchain is greatly reduce since few transactions can be completed per second(Grech et al., 2021).

One challenge is when blockchains refuse to talk to each other and the Holders of an ethereum-based credential hits a wall sharing it on hyperledger or Corda networks. W3C's Which is the etheruem library used as a way or path that uses to communicate in common rules are necessary for verifiable credential when the data is registered once it is impossible to delete or alter it so by this function one is the problem of the right to forgotten (General Data Protection Regulation) the rules such as the right to erase personal traces. Names, addresses once posted stay fixed in place without escape and the separate storage setup becomes necessary for sensitive details and Linking happens through unbreakable codes tied back to entries on chain(Gonçalves et al., 2024).

Additionally it consumes a heavy electric power that the old blockchain uses. Using of massive electricity power is solved by the case of under Proof of Work rules so places without strong grids or advanced gear struggle to join equipment demands pile up alongside energy drains(Naser et al., 2022). This hurdle shape what was the challenge for using blockchain can do today is working around limits becomes part of using the system. So to work the blockchain fluently addressing those issues becomes necessary whenever anyone applies the system.

2.6. The Consensus Engineering Landscape in Low-Resource Settings

In some literatures Blockcahin is referred to as a ledger for transactions, while others refer to it as gatekeepers of trust in the protection of documents. The public Blockchain gives everyone a chance to have access however; a private blockchain gives access with restriction depending on the rules formulated earlier. The third type of blockchain that mixes both public and private is consortium. The researcher by the name Paul studied these types in 2021; years down the line, another researcher Zambrano-Ortiz did a follow-up study on the same (Zambrano-ortiz, 2025). When an authorized individuals attempt to access the system, it restricts the number of the people who can gain entry and

includes monitoring mechanisms to prevent unauthorized modification to the data. It is easier to prevent any misuse of information as all the details remain confidential, which makes accuracy crucial since mistakes will be duplicated once they are made. Therefore, in blockchain technology the traditional issue of trust in an individual or machine is replaced by code based decision making, since most actions are programmed directly into the system. In this context, access is restricted primarily to those predefined entities, ensuring that everyone has equal and controlled access private blockchain are often chosen by educational institutions to restrict and manage access to student records effectively.

It is not the case where all transactions become locked as hybrid chain systems emerge into the picture. There are features drawn from a public ledger aspect of the system, and another private ledger component. This becomes different as customized policies dictate the flow of information. As was noted by Sharma in 2024, such an aspect can be seen with the combination of both(Cantillo-Luna et al., 2022). Earlier, the works of Zheng and other researchers in 2017 also showed similarities (Zheng et al., 2017). Information that is restricted can only be viewed by authorized individuals alone.

In the event that the transaction becomes locked as the hybrid chains become available. Features of the public ledger, together with those of the private one. The whole process becomes different due to the customized nature of the rules governing information flow. According to Sharma in 2024, the two features mentioned above can easily apply here (Cantillo-Luna et al., 2022). Previous research carried out by Zheng and other scholars in 2017 also demonstrated similarities in terms of structure (Zheng et al., 2017). Restricted information can only be accessed by authorized individuals. The most recent type of blockchain that has proven very efficient is that of the consortia type, where several organizations work together and the information exchange is facilitated between organizations such as schools, accrediting agencies, as well as companies recruiting employees. As mentioned in 2023 by Vipie among other people (*Blockchain for TVET Credentialing in Tigray*, 2025). For the management of credentials shared blockchains have been increasingly becoming popular recently and these processes require safety and privacy as well as control measures. Private or consensual blockchains have been found useful in such cases while still giving way to multiple parties joining in the process of verification Safety, privacy, and tight control

2.7. Architectural Evolution:

To avoid the issues that arise due to scalability difficulties and strict data storage constraints on shared ledgers, modern research is shifting towards hybrid architectures. Large amounts of data such as complete certificate documents or data from deep learners uploaded directly into the memory of the blockchain cause its rapid filling. The maintenance costs skyrocket, and speed decreases significantly. Hybrid architecture solves these issues by dividing data storage between two separate layers. The first layer will be located on the chain and will only contain important cryptic data small yet highly secured. Crypto hashes consisting of thirty-two bytes are used to store data with statuses indicating whether a document is active or expired and verified issuer addresses(Chen et al., 2025)[i]. Large items such as student images and grades are stored off the chain in flexible databases like SQLite or distributed across different networks such as IPFS (Liu et al., 2021). Links are important here as well as off-blockchain data are linked directly to fingerprints on the blockchain.

2.8. Self-Sovereign Identity (SSI) and Student Data Ownership

Think of yourself as a person holding a little suitcase that holds all your certificates, achievements, and degrees. In the old days, getting access to your documents would require going through a cumbersome procedure of getting permission from the central office. However, imagine having the keys to open the lock on your own achievements. The new digital credentialing process changes how one should perceive ownership of information.

Under this new approach, the proof of your accomplishments will be always close at hand since everything will be stored in verifiable credentials. All your credentials and certificates will be in digital files available for sharing whenever you decide to. This means that no more institutional control of your data since everybody will be able to manage his/her information independently. Global regulations regarding the exchange of this data will be determined by the W3C community.

The principle behind this innovative technology is to trust people first. Now, everybody has an opportunity to have his/her own unique digital ID and the access keys. It means that now one will be the master of the information, having control over his/her data in a way nobody could dream of before.

2.9. Identification of the Core Research Gap

A new idea may a problem to adopt but it reveals something large. It points straight to the heart of what we're exploring. Integrating blockchain in to learning setups consider local needs instead of fitting global standards they target tech-heavy nations because places such as North America or Japan infrastructure is not integrated with our location, However they assume consistent power, connectivity because professionals control all processes. It is rarely investigated whether such networks operate amid adversity, such as post-war conditions, or in the heart of inaccessible villages.

In one known thing is quite common for concepts to remain mere thoughts rather than activities. In the context of Tigray's TVET system no any study is there about a blockchain based solution nor did any digital solution for the problem sign on the region. All descriptions are about on using blockchain to lock data permanently remain empty promises as nothing is being developed. Locally-conducted research produces theoretical information but never anything practical. There are no codes, smart contracts, or performance statistics. At this very moment, efforts are being made to address all these issues. Alongside all this comes EduBlock a practical solution that combines blockchains and which is based on the unique characteristics of the environment of eastern Tigray societal, technical and systematic.

2.10. Conclusion

A number of literatures support the decentralized ledger technology addresses several issues that plagued conventional credentialing systems. Additionally to distributed infrastructure they use SHA-256 hash codes for encryption purposes which used to protect from any alteration from identifying easily. The data stored once is unaltered and the Smart contract performs verification automatically hence it reduces fraud opportunities. The manual verification is no longer necessary because even in case of theft the documents will still be stored throughout the network.

Necessarily deployment of blockchain based technologies in regions like Eastern Tigray where public services are unreliable and renders open-source networks unsuitable as they require stable electricity,

high processing fees, and have throughput limitations. So the research suggests a private blockchain technology underpinned by Proof of Authority combined with decentralized data storage between internal server infrastructure and external blockchains. This approach significantly reduces the energy requirements and ensures constant performance moreover officials are in full control of user permissions. Despite slow adaptation to technological progress and lack of digital literacy in certain areas, the concepts outlined above determine the framework for implementation of EduBlock technology analyzed in detail below.

Table 2.2. Comparative Matrix of Blockchain Credentialing Frameworks

Literature Archetype & References	Consensus & Ledger Architecture	Metadata Storage Strategy	Security & Access Control	Primary Vulnerability & Operational Bottleneck	Additional Considerations
Public Layer-1 Systems (e.g., Early Ethereum / Bitcoin-anchored designs)(Liu et al., 2021)	Proof of Work (PoW) / Proof of Stake (PoS) on public permission less chains	On-chain storage of full student string records or massive transaction metadata fields	Asymmetric cryptography via public user wallets; lack of centralized institutional oversight, or lack of any official document.	Economic Volatility & Network Saturation: Extreme, unpredictable transaction fees (gas spikes reaching $6.25+ per mint) render continuous public deployment economically non-viable for public regional academic budgets	*Scalability issues; high energy consumption, low efficiency and poor scalability;limited control over transaction costs; lack of fine-grained access controls*
Decentralized Identity Frameworks (e.g., Atala PRISM / W3C DID implementations(Quispe & Pacheco, 2025)	Hybrid/Consortium networks optimized for public-key infrastructure (PKI) lookups	Off-chain digital credentials stored locally within individual user wallets; DIDs anchored on-chain	Multi-party cryptographic handshakes; cryptographic signature checking by verifiers	High User-Side Complexity & Key Management Friction: Requires end-users (students) to maintain complex mobile cryptographic wallets. If a device is lost or compromised in a resource-scarce environment, the credential chain breaks due to a lack of automated backup systems	*User onboarding friction; recovery mechanisms; reliance on external key management solutions*
Private Enterprise Ledgers (e.g., Hyperledger Fabric / Private Corda deployments(Feng et al., 2019)	Practical Byzantine Fault Tolerance (PBFT) or Raft consensus among closed nodes	Internalized state databases (e.g., CouchDB/LevelDB) synced securely among members	Strict Certificate Authority (CA) hierarchies and fine-grained channels for access	Lack of Public Verifiability & Centralized Isolation: The closed ecosystem completely restricts public verifiability. Third-party employers and international entities cannot query or authenticate credentials transparently without being granted explicit node access	*Limited transparency; reliance on trusted nodes; potential bottleneck in cross-institutional interoperability*
Proposed EduBlock Architecture	EVM-Compatible Proof of Authority (PoA) Consortium Network(Fobes et al., 2020)	Hybrid Model: Structural metadata in local SQLite via Sequelize ORM; 32-byte SHA-256 hashes anchored on-chain	Role-Based Access Control (RBAC) enforced via bare-metal Solidity modifiers (onlyAuthorizedCollege)	Consortium Node Dependency: Requires persistent local node replication across regional hubs (Adigrat, Wukro) to maintain Byzantine tolerance during localized internet drops	*Node dependency introduces operational complexity; potential latency; scalability considerations; governance of consortium membership*

Scalability & Throughput	Public chains often face throughput limits (~15 TPS for Bitcoin, ~30-100 TPS for Ethereum pre-sharding). Consortium models can scale better	Local storage and hashes enable high scalability; off-chain storage reduces on-chain load.	RBAC and node permissions allow flexible scalability within trusted network boundaries.	Cross-region synchronization latency; maintaining consistent state across hubs.	*Design should incorporate sharding or layer-2 solutions for future scalability*

	(Ante, 2020)with permissioned consensus but still face growth limits based on node count and Network design.	Zz\			
Interoperability & Standards(Buterin, 2016)	Public chains leverage ERC standards, W3C DIDs; private chains may lack standardized Interoperability.	Use of standardized DID methods (e.g., DID:ETHR, DID:ISO) can enhance interoperability across systems.	Authentication via cryptographic proofs; potential integration with federated identity systems.	Fragmented standards may hinder cross-system credential verification.	*Adopt open standards for future-proofing and broader ecosystem integration*
Governance & Compliance	Public networks have minimal governance; private/consortium chains require explicit governance policies.	EduBlock's governance via RBAC and regional node oversight.	Governance models should include audit logs, stakeholder consensus, and compliance checks.	Governance bottlenecks if stakeholder participation is limited or centralized.	*Implement transparent governance frameworks and audit mechanisms*
Operational & Maintenance(Cantillo-Luna et al., 2022)	Maintenance overhead varies; public chains require minimal management but are resource-intensive; private chains demand active node management.	EduBlock's hybrid model reduces on-chain data load but necessitates regional node upkeep.	Backup and disaster recovery protocols essential to prevent data loss.	Dependency on regional infrastructure stability; internet connectivity issues.	*Plan for automated backups, disaster recovery, and staff training*

Chapter Three

Research methodology

3.1. Research Design

In this research, Design Science Research (DSR) methodology has been adopted to systematically develop a blockchain enabled learning certification system called EduBlock that would be utilized in TVET colleges of the Eastern Tigray region.

There exist different methodologies that differ from each other in terms of their major strengths and constraints in developing systems when we say case studies provide an indepth context to phenomena and therefore help understand them, there is no guidance provided by case study for the creation of any artifacts. Grounded Theory revolves around the process of developing theories through data collection and analysis the outcome of this methodology is usually a conceptual framework rather than a system. An experiment involves testing some hypotheses under controlled conditions thereby facilitating the assessment of variables nevertheless this methodology cannot serve as guidance in building a system (Haoxing & System, n.d.). On the other hand action research includes collaboration in the process of problem solving with its emphasis on the change process it is not always organized in terms of artifact creation. (Peffers et al., 2007).

The DSR methodology will be ideal for this study due to its emphasis on producing a viable technology based solution to problems in the real world including forgery and ineffectual processes of verifying while at the same time making sure the solution is sound (Friedrich, 1996; Peffers et al., 2007). The model suggests that the study should progress following the order of problem identification goal setting artifact creation presentation evaluation and communication (Vaishnavi & Kuechler, 2007).

3.1.1. Problem Identification

The first step entailed an examination of the current practices of credential verification at the TVET institutions within eastern Tigray. Fixed format questionnaires as well as interviews were applied for obtaining information from staff tutors, past pupils, and other interested parties (see at the end of the appendix). The issues that emerged related to processing time, operational costs document , handling procedures verification techniques cases of counterfeit diplomas, problems associated with delays in record checking, and, more generally, file management and certification.

Further inquiry into the existing perception about the credibility of the present certificate verification process resulted in the discovery of conflicting perceptions concerning the authenticity from different stakeholders. The qualitative approach employed during the collection of data through interviews and experience sharing enabled identification of cases of fake credentials within the education sector. The discussions also brought out the capability of blockchain technology to address the issue through its security feature since it is known to all stakeholders. Even though not mentioned specifically, faster and easy verification process and improved transparency of records are other advantages identified by some interviewees. The privacy of personal information from users became an important challenge facing the system, together with problems encountered in users' interaction which became the main challenges

faced by the system. High cost of implementing the system and inadequate organizational readiness also came out as important issues. Lack of necessary skills became one of the most important barriers in everyday activities. Even though efforts towards using digital verification are being made, they always face the same predictable failure.

Lack of skills proved to be important enough in the day-to-day. Digital attempts exist but stumble in predictable places. Failures found here shaped core demands for EduBlock behind the scenes. Security needs took form based on real friction points uncovered early. Design choices later followed those unpolished truths closely.

3.1.2. Objective Definition

From what turned up during early analysis, the project set defined goals shaping how EduBlock would take form. Security was emphasized as well as transparency regarding how certificates would be processed dealing with problems that had already been identified. To combat any form of forgery security relies on the immutable nature of the blockchain technology meaning that once data is written there is no way of changing it. Verification will be easier thanks to fast response time and more reliability. Access will remain restricted, since only authorized individuals will view or modify data.

3.1.3. Designing and building artifacts

1. Artifact Design

The Edublock prototype uses the rapid application development much emphasis was put on rapid prototyping and constant refinement because of real feedback. The process is made up of three main parts of credential issuance, validation using block chain and front end design. Educational institutions are provided with ease of creating their digital diplomas thanks to the integration of the module into it.

Moreover, the digital audit checkes that the certificate is locked in its rightful place without swapping or tampering. Retrieving documents is easy because all an administrator needs to do is to press once and then verify twice hence no more piles of paperwork. Trust increases because everything is transparent to everybody. Schools feel relieved and brains are fresh.

2. Methodological Justification

While choosing the most appropriate software development process model for EduBlock several models were evaluated since when the researcher came to the conclusion that the Waterfall model is not suitable for the use in this context due to its rigidity and sequential. Hence in case of any necessity of changing the situation during the process of development becomes almost impossible. In addition to this the Agile model was not chosen due to its flexibility although it needs frequent meetings and regular sprint planning thus it will not be required to experiment and make errors with the end-user(Pargaonkar, 2023).

Therefore Rapid Application Development (RAD) became an optimal choice for us as it emphasizes prototyping and continuous updating. It works perfectly well for EduBlock project as we can develop the software gradually.

3. Development and Practical assessment

According to the RAD approach the development of EduBlock proceeded in a cyclic way involving prototyping testing and improving the prototype. In addition to the above-mentioned strategy we actively involved the target group the stakeholders including TVET administrator's lecturers and students. Feedback from the representatives (seven in number) was crucial in making sure that the platform is user-friendly and suitable for the learning environment.

EduBlock helps solve an important problem of the present day education sphere related to problems with verification of credentials. The issue is relevant for some regions in which there are challenges with obtaining diplomas and transcripts due to their unavailability or security concerns.

1. Stakeholder Requirements & Data Collection

To ensure EduBlock would meet the real-world certification process, we first sought users' needs and problems they encountered as well as their insights through our purposive questionnaires and interviews. College deans, finance core processors, teachers, and students in our study responded to our survey with the following three concerns: credential fraud elimination, faster verification, and data security.

2. Iterative Design Process

The development process was iterative. The researcher tries again and again the functionality of the system. Focusing on creating successive versions of EduBlock to grade up usability and system performance. This design phase was informed by a thorough review of existing central certification systems, ensuring that our architecture not only builds upon proven industry standards.

3.1.4. Demonstration

In order to demonstrate the main functionality of EduBlock, a prototype of the system was created in order to simulate scenarios of issuing and verifying certificates. Main scenarios that were demonstrated within the framework of the prototype include:

Certificate Issuance: The demonstration of issuing academic certificates involved simulating the procedure of creating the credential, hashing it and storing the information in the blockchain. Such a scenario demonstrated the efficiency of reducing the risks of forgery of credentials due to their secure storing.

Credential Verification: Stakeholders like employers, verifiers or students were shown the possibility to verify the credential by introducing necessary identifiers in order to show the efficiency and transparency of the system in terms of secure storing and efficient searching of academic credentials.

Revocation and Role Management: Other possible actions included revocation of certificates and managing of roles that could be performed with the help of EduBlock.

Overall, the demonstration showed what actions can be executed when using the system and how the work in such conditions can improve the efficiency, security, and transparency of the process of issuing and storing of credentials.

3.1.5. Evaluation

The assessment of whether the software prototype would be successful entailed the evaluation of usability, convenience, security and performance. In evaluating the usability, a few participants carried

out specific activities including performing actions such as creation of entries, access of documents, and verification of certificates. Positive signs were evident when evaluating interface friendliness, although some problems arose that might cause future poor performance in terms of the users' work process. On the other hand, the assessment of the security involved the implementation of ideas from blockchain technology, analysis of the threats before the use of the software and information from scholarly journals. It has been established that the software secures data, makes the information immutable and grants access based on user roles. The performance of the software could not be evaluated through testing because simulations such as issuing of certificates verifying them and carrying out transactions occurred. Although the performance at the initial level was acceptable some challenges arose during scale-up. User feedback was helpful in evaluating the suitability for vocational colleges in eastern Tigray.

Table 3.1. Map of DSR Artifacts of EDUBLOCK Prototype

DSR Cycle Step	Artifact / Output	Documentation
Problem Identification	Identification of credential verification challenges in TVET institutions in Eastern Tigray	Context and problem statement
Requirements Gathering	Stakeholder needs, system functionalities, security, and usability requirements	Stakeholder requirements & data collection
Design	System architecture, interface design, smart contract logic	System architecture and iterative design process
Development	EduBlock prototype development, implementation details	Artifact design and development process
Demonstration	Simulated scenarios of certificate issuance, verification, revocation	Demonstration of EduBlock's core capabilities
Evaluation	Usability, security analysis, performance metrics, stakeholder feedback	Evaluation results and discussion

Comparative analysis vs manual process method

Thus, the conclusions made based on the analysis indicate that the existing manual process of verifying participants credentials is highly time consuming and requires significant resources. Based on the interview data obtained during this research project the cost of verification is estimated at about 700 Birr per participant. Additionally, the manual method entails a lengthy workflow associated with delays varying between one to three months as the information from the questioner and takes only two weeks from the interview. This negatively impacts the quality-of-service provision as well as overall efficiency of TVET institutions operating in Ethiopia. Moreover, the manual approach is characterized by the risk of human error and low accuracy and reliability of verification, which may undermine the integrity of the entire process.

So, getting certified takes only about seconds with this new blockchain-based solution. However, it is important to note that it applies exclusively to this particular application. Normally the process takes much longer namely several months. Nonetheless blockchain solutions provide an unprecedented

opportunity to increase security, minimize costs and streamline certification processes. For instance, with a blockchain-based solution the verification can be completed within few seconds since it allows automation and decentralization of verification workflow. Thus, it facilitates the reduction of manual steps

Table 3.2. Comparison Table: Existing Certification System vs. Proposed Blockchain-Based Edublock System

Parameter	Existing System (Base Paper)	Proposed Blockchain-based Edublock System
Certificate Management	Manual or centralized records, as reported by participants	Decentralized and automated management through smart contracts, demonstrated in prototype settings
Security	Vulnerable to forgery, breaches, and unauthorized access based on participant feedback	Significantly enhanced security with tamper-proof blockchain encryption observed in prototype testing
Verification Process	Time-consuming, manual, often requiring third-party communication; verification times exceeded 90 minutes in reported cases	Prototype results show rapid verification, typically completed within approximately in seconds, indicating a substantial reduction in processing time
Reliability	Depends on the central issuing authority, as described by participants	Trustless system ensuring data integrity and authenticity through decentralized consensus, demonstrated in the prototype environment
Integration Support	Limited to Ethereum; lacks integration with existing college infrastructure	Designed for interoperability with college systems and chain-based platforms, as evidenced by prototype development

3.1.6. Communication

At the end, the experts from one college are pulled together reports and gathered around for discussions like a school project, honestly. They pulled information from system plans test runs and reviews, and these materials now point the way for future work on building and running the system, and some of them will see the completed application

1. Tools and Techniques

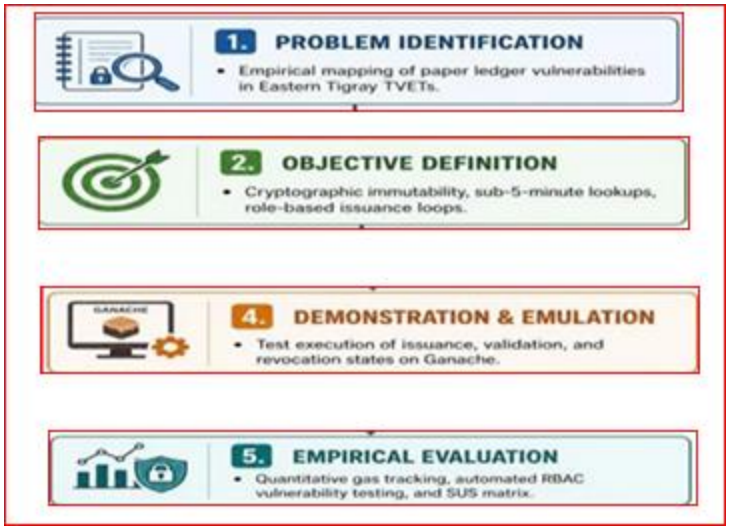
This prototype was created using many different tools and interfaces. Smart contracts were implemented using Solidity Truffle was used to code and Ganache started a local blockchain to test. Users communicated using Meta Mask or Ganache transaction wallet ID, ensuring safety. The custom dashboards simplified the process by providing visualization. Rather than sticking to paper documents only, he conducted interviews and questionnaires as well. System logs kept records of user behavior and actions throughout the practice trials, which were conducted in a virtual environment that simulated the real one. Having collected the data, he analyzed the users' statements and identified common themes.

The evaluation of test scenarios and their analysis revealed performance indicators. These emerged when analyzing both the statements and system logs simultaneously.

2. Data Analysis

Moving on to the analysis stage where the results obtained were reviewed using the results obtained through the interviewing sessions, survey responses and the logs gathered from the simulations conducted. The investigator attempted to come up with recurring themes from the issues faced by the participants how the prototype could have been designed and the appropriate roles to be played. This was combined with information from the participant's suggestions to put the whole puzzle together. From there attention was directed to performance evaluation depending on the simulated scenarios.

Figure 3.1. . Mapping of DSRM Artifact Lifecycle for the EduBlock Prototype .



N.B image from layout of (Peffers et al., 2007)

3.2. System Structure

The system structure is organized based on the concept of a hierarchical structure, thus facilitating its operation and allowing convenient ways to improve the system without encountering any difficulties or inconveniences. There are three principal components in the architecture: the front end, back end, and smart contracts for communication with the blockchain. All of them have specific responsibilities. The backend does the most of the heavy lifting behind the curtains. Meanwhile smart contracts secure information and ensure that all data cannot be tampered with or modified. This design provides a number of advantages. In particular, system components can be updated and improved without affecting other aspects which greatly simplifies further development. Moreover, users are not involved in blockchain processes. They only experience the benefits provided by EduBlock services.

3.2.1. The Presentation Layer

This layer is responsible for user interactions with the program. It represents the user interface. College administrator, regional TVET administrators, and other users may request and manage certificates

analyze certificate status and properties etc. Various dashboards and reports can be implemented to observe current activities. Frontend connects to the backend to provide users with requested information.

3.2.2. The Application Layer

This should be viewed as the brain of the whole operation. This is where the backend API works, controlling all the logical workings of the system. It first validates any request received before communicating with the blockchain system. In other words, it is responsible for ensuring everything stays within the system parameters as far as security and reliability are concerned. Technologies such as Node.js have been applied to ensure its efficiency.

3.2.3. The Blockchain Layer (Smart Contracts)

This layer provides all essential security functions. Smart contracts ensure the certificate cannot be tampered with or changed. The rules state that the certificate should be issued only if all conditions have been met and are easy to verify by any third party. If needed, the certificate can be revoked using this layer of technology. Four interconnected smart contracts perform all tasks required to keep everything in check.

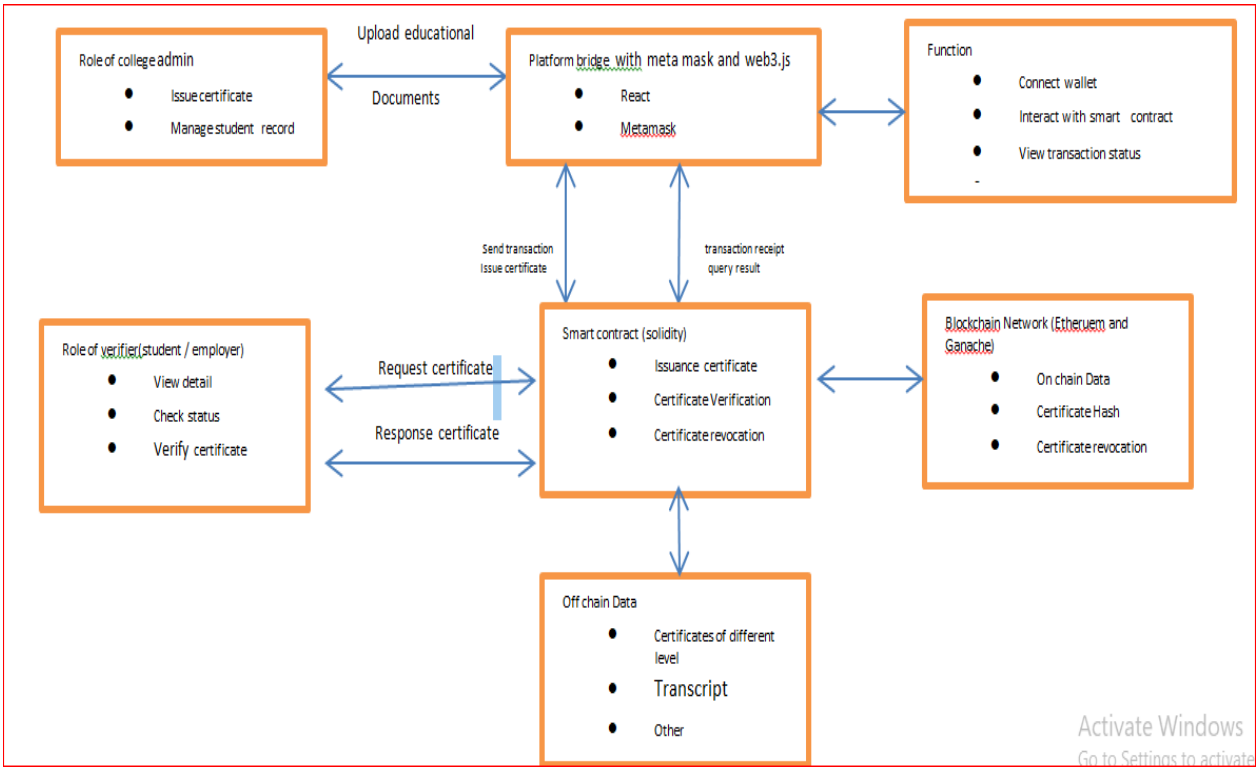
The system design ensures high safety, scalability, and trust. The layered design allows for easier maintenance without affecting other elements of the network, and EduBlock can be easily integrated with other solutions. In terms of functionality, the main aim is to provide users with an accessible but fully secure platform where the certificates cannot be tampered with. This is an extremely important advantage of the project, as it allows for safe and quick changes and additions. The changes do not affect existing functions of EduBlock, and it will continue to provide certificates protection services while increasing user trust.

That all becomes possible due to the well-planned structure that allows for dividing roles into four parts that operate independently from one another but at the same time collaborate in order to achieve certain tasks. Such structure allows for making changes in one part without affecting others. Namely, whenever information is being added, Issuance Contract generates fingerprints (a set of 32 bytes that cannot be decoded and stored). Actions are logged, and the entire process can be traced back. The process is protected at all times.

The hashes help in verifying the information on the blockchain; the process takes just several seconds and no personal information is shared. Should there be a need to revoke the certificate, the process is carried out via the use of Revocation Contract the latter ensures that certificates are only active while they need to be so. Security is ensured by means of key management and control. Different roles are associated with different keys. Access is granted only to authorized organizations that are able to manage certificates (issue them or revoke them); the process requires prior approval.

Breaking down tasks into individual elements makes them less cluttered and allows for faster completion. Every piece performs its own function, making any delay resulting from bottlenecks unlikely. All in all, it is a system that is quick, safe, and dependable.

Figure 3.2. System Architecture Diagram(image using Lucid Chart)



N.B image using the lucid chart

3.3. Study Area, Target Population, and Stratification

This study will be limited to only three leading TVET colleges that operate in Eastern Tigray region, namely Adigrat TVET College, Wukro TVET College and Edaga Hamus TVET College. Besides, the study will also consider four woredas/town administrations represented by civil service officials. Altogether, these organizations will comprise about 350 employees.

1. Geographical and Institutional Boundary

The study limited at three known TVET colleges of the eastern Tigray which is Edgahamus, Wukro, Adigrat colleges in eastern Tigray and also related with them are four local woreda offices involved through the interview. On these three colleges there are approximately 350 employees. Though spread out these places form a shared setting for the work being examined.

2. Participant Selection and Grouping Details

This population consists of the key stakeholders who are involved with the issuing, managing, and verifying of student credentials, such as the college staff (e.g. Admissions Officers, Academic Affairs personnel, Registrar's Office staff, IT Department members, Woreda-Level Human Resource Experts, and Core Process Handlers) who will be the main users of the digital credential system. They will use the digital credential system to process student applications, issue transcripts and degree certificates, maintain student records, and maintain the technical infrastructure for these functions.

Additionally, the students will be the primary beneficiaries of the digital credentialing system as they will depend on it to provide them with the ability to readily access, show, and verify their academic credentials (transcripts and diplomas) with employers, academic institutions and other stakeholders in a convenient manner. The ease of use and seamless integration of the digital credentialing system with current college operations are very important factors in providing students with a smooth and efficient user experience. In addition to the students, there are also external stakeholders (i.e. employers and verification agencies) who will require authentic and verifiable academic credentials in order to perform their respective roles. These external stakeholders will leverage the digital credentialing system to confirm the authenticity of student documentation, thus supporting employers' ability to make informed hiring decisions and streamlining their recruitment process. A purposive sampling will be employed to select a representative sample of 100 key stakeholders from three of the target colleges. See the table below.

Table 3.6. Target Population and Sample Stratification Matrix

Stakeholder Stratum Group	Sample Size (N=100)	Direct System Interaction Point / Research Role
College Registrars & Admissions Staff	6	To understand the administrative workflows, data entry challenges and user requirements from those directly managing student records.
IT Specialists & Network Handlers	20	To assess existing infrastructure, technical capacity and readiness for system deployment ensuring feasibility
TVET Instructors & Academic Deans	40	To gather insights on academic evaluation timelines, outcomes, and user needs within educational institutions.
Woreda HR Managers & Recruiters	15	To understand manual background verification processes and identifies friction points or inefficiencies.
Legal Experts & Compliance Advisors	19	To gain insights into forgery patterns and legal consideration informing security and validation features.

3.4. Blockchain-Based System Design

The EduBlock system uses blockchain technology to change the process of secured certification method. By moving from a central certification system to a decentralized ledger the system has three important features that make it more honest, transparent and easy to verify.

3.4.1. Core Design Principles Are

1. Data Immutability:

Whereas, in cases of systems, people managing the database have the power to alter or delete records, which may result in mistrust. In EduBlock, however, such manipulation or deletion cannot happen since codes of the certificates and the issuance records are stored on the blockchain itself. Once the information about the student has been entered in the blockchain, it becomes impossible to edit or delete

it. As soon as one tries to manipulate and edit the document, they will not be able to do so due to code mismatch and the document will become invalid.

2. Transparency and Traceability:

In EduBlock, transparency of the entire life cycle of each certificate is assured without invading personal privacy. Information regarding where each certificate comes from, who issues it, its date of issuance, and its validity is accessible to the public via blockchain explorers. This makes it more reliable than any record-keeping system in existence.

3. Decentralized Verification:

The system does not need an authority to verify certificates. Existing models often require contacting the issuing institution, which can be slow and may not always work. In EduBlock verification is done by asking the contract directly on the blockchain. The contract is a component on the system that enables you gives the correct information by validating a certification authenticity and status without any human interfere by making the verification process faster and trustworthy.

i. Smart Contract Functionality

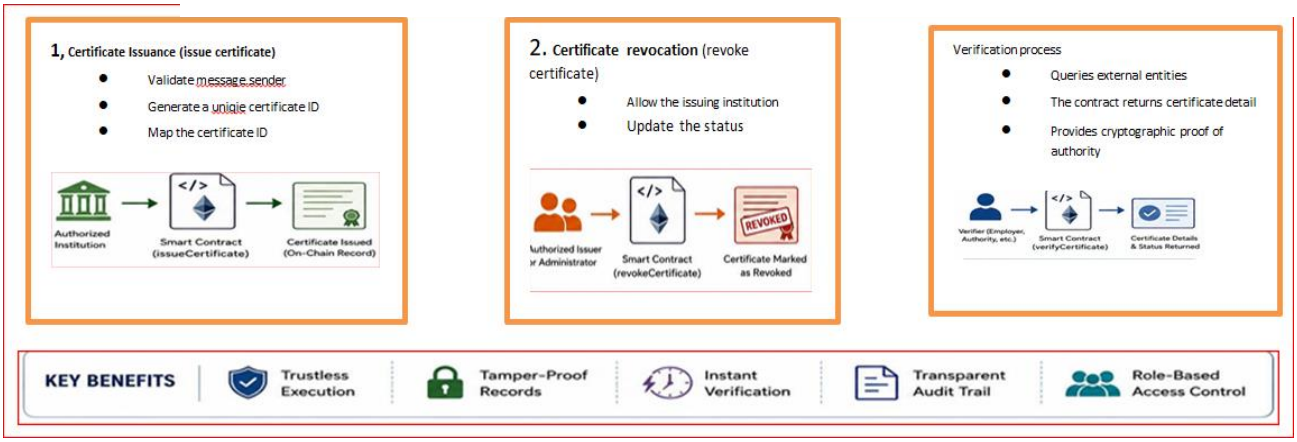
Smart contracts are the driving mechanism behind EduBlock's operation. The smart contracts are coded using Solidity.

Certificate Issuance: The issueCertificate function creates a certificate entry. The function ensures that the party sending the request is a recognized institution. After that, a unique identifier is created that involves making a hash value out of the certificate attributes and linking that hash value with the attributes of the students' identities and other data stored on the blockchain. This is done to ensure that only recognized colleges can create certificates and they are all unique.

Certificate Revocation: The process of revoking the certificate due to reasons such as misconduct will be enabled through the use of the revokeCertificate function, which allows authorized individuals such as the issuer of the certificate or the administrator to nullify the effect of a particular certificate. Rather than delete the record, the function updates the state of the contract by setting the status flag to cancel.

Verification Process: The verifyCertificate method enables those outside the network, such as employers and certification verifiers, to ask the smart contract about the status of a certain certificate by using the Wallet id as the input. As a result, the contract will provide relevant information regarding the certificate, proving its authenticity instantly the EduBlock. The technology utilized in the blockchain makes all this possible. Both the EduBlock system and the blockchain technology used work hand in hand towards making education certification credible and more transparent, as shown in the figure below.

Figure 3.3. Blockchain-Based Certificate Management through Smart Contracts form



ii. Platform Selection: Ethereum

Ethereum was selected from Non- EVM Networks (Solana, Cardano) by the following cases. They are faster transactions at a lower cost but do not support Solidity program which means that you would need to completely rewrite your program in a different language as well as a problem with the security, and you also lose the ability to use the rich ecosystem surrounding of Ethereum.

Layer-1s (BNB, Avalanche): You can use Ethereum code on these networks but you are losing the decentralization and security that comes from Ethereum's network which means you are no longer guaranteeing the data integrity that we want for security-minded credentials.

Mature DevEnvy: they are creates a good development ecosystem surrounding by etheruem and tools like Truffle, Ganache, and even VS code itself have plugins that allow for quick development, testing and deployment. There are also libraries like Web3.js and Ethers.js that make interacting with Ethereum easy.

Smart Contract Friendly: Bitcoin was designed as a peer-to-peer currency and isn't well suited for programmability but Ethereum on the other hand designed to allow developers to execute code on their network. It is Turing complete which means you can have complex data structures, state, and contract logic to handle all of the logic around the lifecycle of a certificate.

Standardized: Ethereum has community-wide agreed standards such as ERC-721 and ERC-11 55. We can use these standards to tokenize our certificates as NFTs on Ethereum and allow for interoperability with other educational institutions, wallets, and dApps in the future.

Uptime: Ethereum is the most popular smart contract platform. It has been battle-tested and provides great security, decentralization, and uptime. We will be using Ganache for our local testnet which allows us to mimic the Ethereum network for free while developing and testing our smart contracts. When we are ready to go live, we can deploy to a public testnet such as Goerli or Sepolia or one of the many

Layer-2's that exist today(Tredinnick, 2019) . As of right now, the system is designed to deploy to modern, active EVM testnets such as Sepolia or Holesky.

3.5. Functional Components

One component of the EduBlock system is a setup to handle the input, and the second one was validating the data process behind the door. And the third one was a picie of steps that manage how to transfer data into a blockchain. These components are work independently but still link together when needed. This independency makes the system easy for developing and maintaining of the system. When someone does something in the app, all detail about that person will be distributed to all the nodes. Each handoff makes sure actions turn into secure ledger entries without extra investigation.

3.5.1. Frontend Layer Presentation Interface

Behind the door there are complex processes stay hidden while users work through a clean straightforward interface. Instead of trying to know and costing with the code people see the human like interface which represented the code behind. This design enables someone to take action without knowing how blockchains actually run underneath. Ideas from Bolén in 2025 shaped part of this approach. The user interface panel makes the user to reduce the need to learn technical details which mean is easy usability.

1. Authentication and Authorization:

Who is allowed to access the system depends on the role whether they are administration of the TVET regional officer, TVET College, a student or a verifier and in general permissions are applied based on each users login identity and role based access checks. When a user performs an action on the shared network, he was communicating by his wallet id such as Meta Mask to help keep identity connection secure. But during the current stage of implementation the system relies on Ganache transaction code for testing and execution. In this step only users with approved digital address are able to issue or manage credentials, while all other addresses are restricted and cannot perform credential related actions.

2. Certificate Management Interface:

From the school's point of view, handling certifications becomes simpler through a built-in system that guides staff step by step. Instead of manual entries, digital forms capture learner information and class records smoothly. Once filled, these inputs trigger secure actions behind the scenes. A linked crypto wallet receives approval requests, signing off only after human confirmation. After validation, everything moves forward into the Edublock prototype without delays. For learners, tracking achievements feels straightforward thanks to clear navigation tools. Each qualification appears in one place, listed neatly with key facts beside it. Dates when items were recorded show up alongside unique identifiers for verification purposes. Extra background details sit just below, giving context without clutter. Nothing gets hidden or buried under layers of menus.

3. Verification Portal

Anyone needing proof - students, job providers, or certification authorities relies on this system. Start by typing a certificate ID or transaction hash on the verifier panel and then the full certificate data directly from the blockchain. The results display quickly and show the issue dates the issuer status of the

certificate and additional useful details. Each verification runs live so what you see matches exactly what is recorded on the blockchain.

3.5.2. Backend Layer Application Logic and API Gateway

Behind the screen a hidden system links what users see in their browser to the distributed ledger running in the background. This layer manages the off-chain steps and applies the required checks and rules before anything is saved permanently. It also process and organize the data first so the workflow stays efficient and reduces unnecessary costs. Only after everything is confirmed does it forward the information for final on-chain recording where updates are looked in permanently.

1. Check Requests and Apply Rules

Most of the errors are detected before any data is added to the blockchain platform. First, the platform checks for the information about the students like whether the ID number matches the format, and if the wallet ID in Meta mask or blockchain address matches the platform. Secondly, the platform checks the length of the keys to make sure they fit the space required in the smart contract. Duplicate or invalid input will be rejected by the platform right away, and the user will immediately know what the reaction will be.

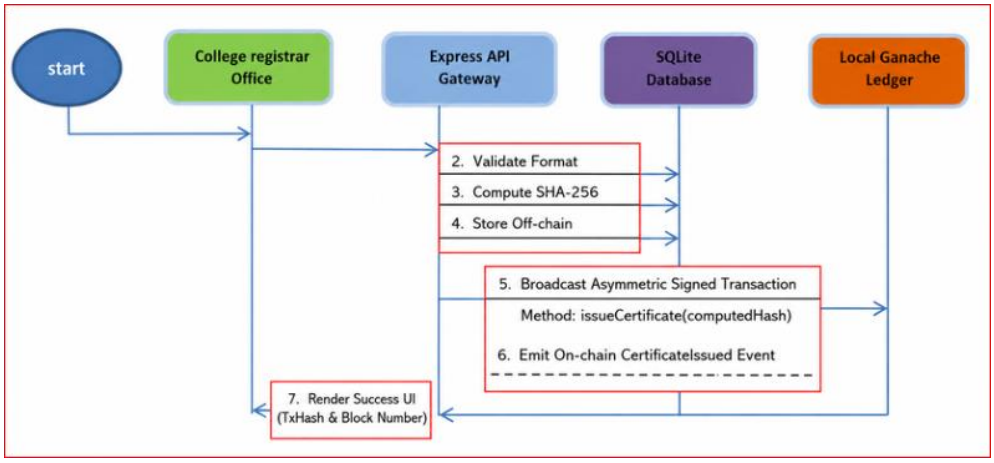
2. API communication using restful services

When the client requests information on the system, APIs manage and monitor how the front end or presentation layer is communicating with the backend and application layer. The request has a clear path and order that allows the system to respond quickly and efficiently. The client gets information on the certificate from pre-sorted records if they are available, or from the latest blockchain updates. This allows the system to respond quicker and with fewer delays. The rest of the processing occurs outside of the browser for an easier experience for the user.

3. Data Processing and Metadata Management

Most of the time, big files such as image PDFs linked to credentials don’t live on the blockchain itself. But, they get sent to distributed networks systems so IPFS handle that load. A hidden identifier forms once the file saved there a unique string called a CID. That code gets passed back through the system. Behind everything, software layers organize where each piece goes. Proof stays locked into the chain. What floats outside is still tied tightly by design thereby linking the immutable record to the full document. See the image below.

Figure 3.4. Certificate issuance lifecycle pipeline from (Asif & Hassan, 2023)



3.5.3. Blockchain Layer (Decentralized Ledger)

Trust was comes from the code than peoples, locking data safely across many computers at once, shared for the decentralized network. Shifting away from relying on a single administrator happens through math-based agreement rules built into the network system. This switch away from centralized control and trusting the distributed network has changed the way to verify information. Unlike traditional promises from people, it uses mechanisms that prevent any change from happening without the permission of other nodes in the network. For instance, data are cryptographically protected when they are submitted and recorded. Naz and team have written about this change in 2020(Al-Breiki et al., 2020).

1. Secure Data Storage and State Management

Every node keeps a copy of certificate records, and this procedure making sure nothing was altered. The mapping tools inside smart contracts link each certificate ID to its holder and current developments or changes. Because every machine holds the same information and one breakdown won't crash the system because they could not crash all nodes in different geographical areas. Copies spread across machines block attacks - no central target exists anymore.

2. Smart Contract Execution Engine

Inside the setup sits a smart contract execution engine handling the tasks spelled out in code using Solidity. Editing inside Visual Studio and it pushes live those digital agreements developer's design. One such agreement issueCertificate () validates fresh records onto the chain. Another ignores the outdated ones clean revokeCertificate() does just that. Then comes transfer ownership shifting control of specific credentials between parties seamlessly. Each piece runs only when conditions match the validation rule of the code. The whole mechanism stays active once launched, responding strictly to predefined triggers. No manual nudges needed after start. Rules baked into each function guide every move it makes

3. Validating Transactions and Reaching Agreement

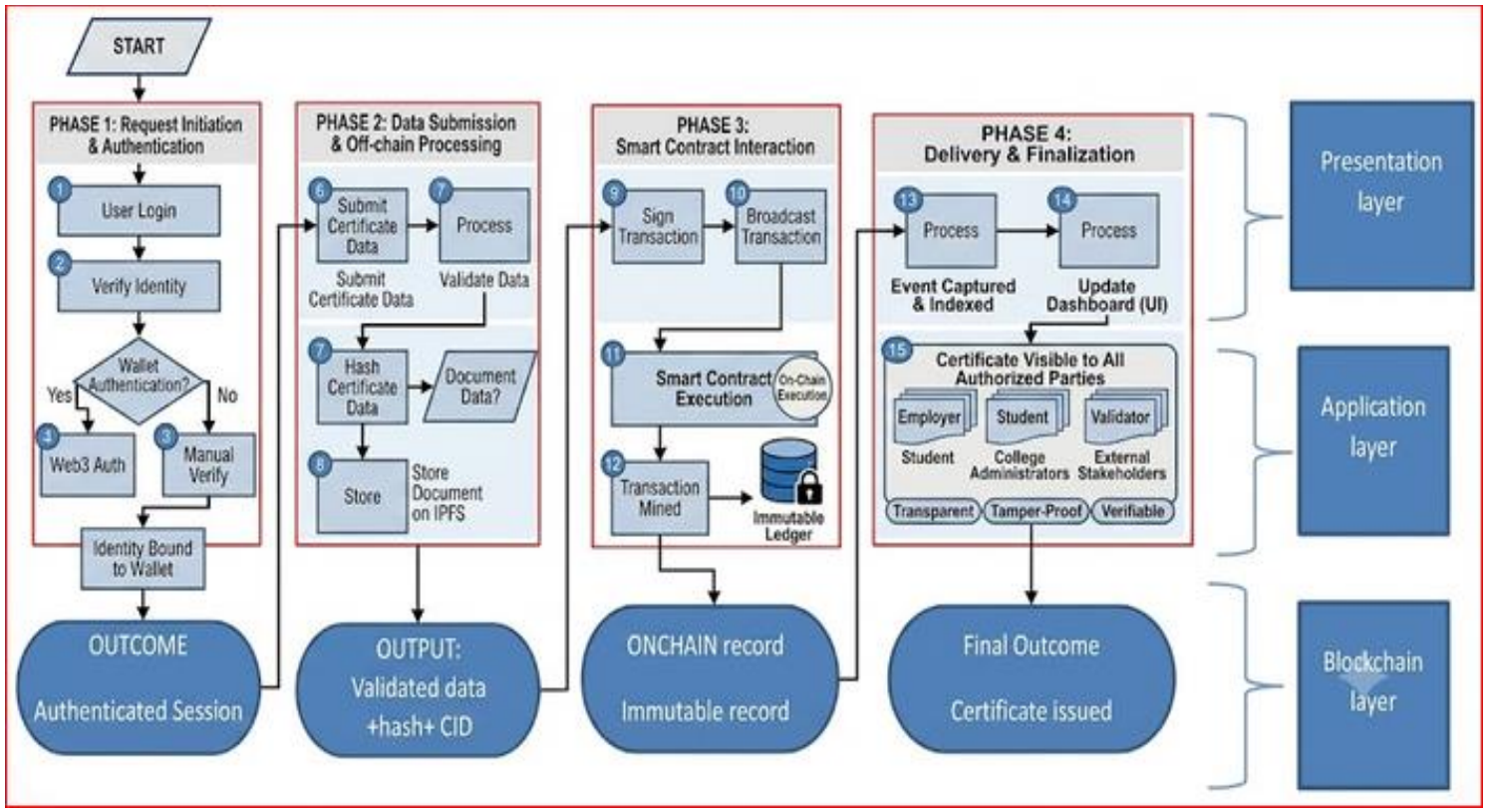
Whenever an event occurs on the blockcahin, someone needs to verify that it is valid and recognized by the system. To confirm its authenticity they compare digital signature a public key. Proof of who sent it.

On Ganache a tool that assist developers in creating applications, these verifications happen instantly. In live environments, however the network operates on the Etheruem main chain or sometimes on faster layer solution built above it.

3.6. Data Flow and Process Model

From the beginning EduBlock uses an organized flow driven by events to keep information accurate, traceable, and open. Data moves through three levels which discusses how it display, how it manage, and how it was stored permanently. Instead of mixing all the tasks and actions split clearly between issuing certificates and checking them later. User entries become fixed records once processed and each

Figure 3.5. EDUBLOCK data flow and process model



phase follows strict logic so trust stays built into every stage.

3.6.1. Certificate Issuance Workflow

The following process flow chart explains the end-to-end lifecycle of a credential ways, whereby the issuance process is evolved from a user input to a cryptographically secured chain transaction. The process follows a strict procedural order ensuring data integrity and authorization.

Phase I: Request Creation & Authentications

The entire lifecycle process starts at by the presentation layer which the identity authentication is performed. The process starts with a login initiated by the authenticated party an authorized individual

who holds an administrative right (for example, a TVET administration). This process uses two factors authentication approach, which ensures optimal security measures:

The traditional credential verification methods such as those involving login details and administrative access are employed to authenticate the authorized individual who could be a TVET administrator, and the credential verification procedure guarantees that the only person capable of authorizing a transaction would be someone qualified.

On the other hand the transaction also involves EduBlock authentication using Web3 wallets such as Meta Mask. This method utilizes blockchain technology whereby every transaction would be linked to a unique crypto-wallet address. In this manner only those who have wallet addresses that have been whitelisted would be able to sign off on the transaction. As you can see from the above image the progress is as follow in phase one.

1) This starts when the user logs into the presentation layer on the user interface panel
2) The system verifies the credentials entered.
3) The system determines whether a Web3 wallet is present?

3.1. The Yes Decision →the system makes an automated call to authenticate the user via the wallet, where he must sign a transaction.

3.2. The No Decision → the user has to follow the normal procedure of authentication (such as two-factor authentication).

4. The user is now bound cryptographically to an address in the blockchain. A college registrar logs in using their employee ID and is prompted to sign a transaction on their official MetaMask wallet. Then the outcome of this phase is an authenticated session established for a confirmed authorized entity.

Phase II: Data Submission and Off-Blockchain Processing

The transaction logic is implemented using the Blockchain Layer. The Application Layer creates a transaction request that triggers the issueCertificate() method within the smart contract deployed on the blockchain platform. In this process, the following protocol needs to be following points.

Client-Side Authentication: is the user sign into the wallet that uses a private key. The private key is required to sign the transaction. The signing of the transaction does not require any kind of digital signature; rather, it utilizes the cryptographic power of the private key to sign the transaction.

The Transaction broadcasting: The transaction signed using the private key is then broadcasted to the Ethereum platform (or to Ganache). In doing so, the transaction is validated as authentic by the blockchain, and the identity of the sender is authenticated through the private key inside the smart contract.

The contract execution: The mining of the contract occurs via miners or validators. The contract updates its internal state by updating the student's address with a unique Certificate ID and stores the corresponding metadata hash/CID inside the smart contract. Availability: The issued certificate will become available for viewing for students, college administrators, external authorities, and others.in

phase II the steps are continued from phase I by addressing the cryptography. The sequence steps are as follow

5. Submit Certificate Data → Process → Validate Data: The user submits the academic record data (e.g., a PDF images or raw JSON). The backend server validates the formatting (checking for null fields, invalid grade formats, etc.).

Hash Certificate Data & Document Data? (Decision): This decision process prepares data for two pathways. A cryptographic hash (e.g., SHA-256) is generated from the raw data.

6. The bulky document itself (the actual certificate image or JSON) is not stored on-chain or in the blockchain. It is pushed to a decentralized storage solution, like IPFS.
7. The decentralized identifier (CID) returned by IPFS is stored on the server's local backend (like a SQL database). The detail student data is, Student Name: Berhe Hagos; Department: ICT; Level: III and the onchian Meta data will be Hash Computation: The data above is hashed into a string like 00000FB3743092AE0bFCb2221D371911A771EdF499bD000000x2D55BcA30cDcdd1 844a4227989270eceb5468Cc0... The raw data record is stored on IPFS, returning the content identifier (CID) `QmYw...2d1a`.
8. Then the overall process is validated data + hash + CID a standardized package ready for blockchain anchoring. Then the next is phase III.

Phase III: Interact with smart contract and confirm transaction

Action begins at the application layer, building a call to trigger the `issueCertificate` smart contract. First step: confirming the user's wallet id, then the system links directly to that wallet so the transaction can be signed. Signing happens solely through the holder's private key. No extra digital signatures are required during this stage. Authentication completes once approval comes through each move follows a set path behind the scenes. Once approved it gets sent out across the network say Ethereum or Ganache. That system then examines the digital signature to verify whether it genuinely originated someone authorized to send such request, and only if this verification matches, indicate that the sender has proper access rights, does the process continue, without this validation nothing advances further and at this point., miners execute the smart contract code which results in the contract updating itself by adding a new entry into this record by this entry containing a unique certificate id that directly linked to the students wallet address mentioned earlier, with all these elements seamlessly connecting the scene. The detail steps in phase III that continued from phase II are

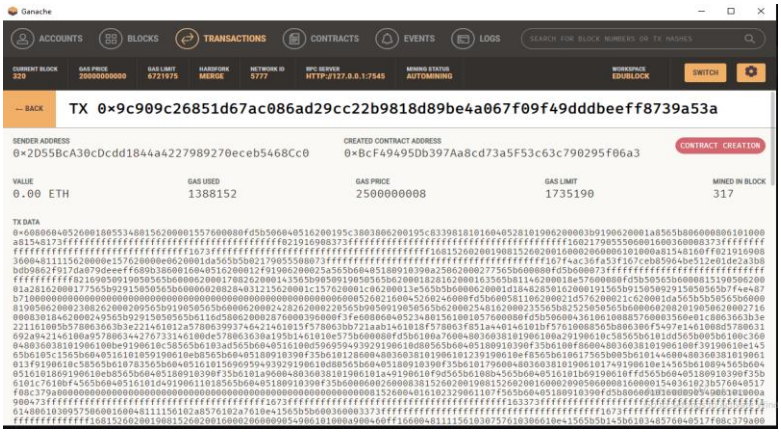
9. Using the cryptographic identity from PhaseI, the user authorizes the commitment of the Phase II data package.
10. The signed transaction is sent to the P2P network of blockchain nodes.
11. Smart Contract Execution→Transaction Mined: Network nodes process the transaction, calling the corresponding smart contract function (e.g., `issueCertificate(studentAddress, documentHash, IPFS_CID)`). A miner includes the transaction in a block.
12. The system signs and broadcasts the `issueCertificate` function call with the empirical data generated in Phase II: 00000FB3743092 ….5468Cc0 (data hash) and `QmYw...2d1a` (IPFS CID).

Phase IV: Delivery and Finalization

At this stage, the system sends a notification to the user to complete the certification process. The frontend dashboard changes in real time and the certificate is shown to the user along with the unique Certificate ID and the transaction hash. Thus, the user gets an audit trail to confirm the completion of the transaction on the blockchain.

13. A blockchain listener on the backend detects the `CertificatesIssued` event triggered by the contract in phase III. The transaction hash, block number, and CID are indexed for fast lookup.
14. The backend pushes a success signal to the front-end, updating the registrar's view.
15. The system can now render the final verifiable credential. A student uses the unique link to view their certificate. Then the outcome will be an employer or external stakeholder clicks a verification button. This triggers the on-chain validation process: fetching the document's anchored hash and comparing it to a freshly computed hash of the rendered data (confirming `Transparent, Tamper-Proof, Verifiable` status).

Figure 3.6. Transaction hashes on Ganache



❖ Technical Snapshot (Ganache Testnet Metrics)

To ground this in reality, here are the exact metrics from a successful certificate issuance transaction:

Sender Address: 0x2D55BcA30cDddd184a4227989270eceb5468Cc0 (Regional TVET Bureau)

Value: 0.00 ETH

Gas Used: 1,388,152

Gas Price: 2,500,000,008 (2.5 Gwei) *equivalent to roughly $6.25*

Gas Limit: 1,735,190

Mined in Block: #409

❖ Using Total Fee in USD = Gas Units × Gas Price × 10^{-9} × ETH Price

Then the cost is $6.25(this value is when the value of Gwei changed in to the dollar) fee using the above Ethereum network transaction cost, not a fee charged to the student for certification. In production, this actual network fee is covered by the service provider (such as Ethio Telecom or Safaricom) to keep the user experience seamless. And if there is any payment it should covered by the regional or institution.

3.6.2. Certificate Verification Workflow

Designed from the beginning up is for speed and transparency, thus this workflow allows any third party to make the verification a credential without ever needing to contact the issuing colleges. Beginning the query the verifier visits the public verification portal enters the unique certificate ID. Directs into the Blockchain query to ensure absolute accuracy and the application layer completely bypasses the backend database. Instead, it queries the smart contract's verifyCertificate() view function directly on the blockchain. The smart contract checks the student's wallet ID with the unalterable state of the student's ledger. The blockchain returns the student detail (student name, Students College, department and certificate issuing date, image of all certificate PDF which the student have) along with a validated code. The frontend instantly displays this data with a clear "Verified" visual indicator, offering instant cryptographic proof of authenticity.

3.6.3. Advantages of the Model

Transferring from the manual centralized system to a blockchain based process states that it was completely transforms how credentials are managed. By introducing distributed Ledger technology (DLT), the system provides three core developments from the traditional system because of not any system have been in Tigray also in Ethiopia specifically in TVET colleges.

1. Non Tampering Integrity

In a traditional documentation documents are alter by the officers or by the thefts easily because they are already stored on the shelf, so they are easily destructed, stolen, or altered but blockchain changes this entirely by using cryptographic hash is permanently written to the ledger and complete unchangeable. If anyone tries to change even a single alphabet or character of the certificate information the hash result will change entirely instantly exposing the result. This "write-once, read-many" setup ensures the academic records are definitive source of truth forever. So all student details are stored on the Ganache network, and hashed, which is changed into encrypted information.

2. Non-Repudiation

Credit for the public-key cryptography every single action in the system is fully accountable. Whether an institution is issuing or revoking a certificate and the transaction notifies using their unique wallet ID. This creates an assured digital identity and as a result issuing colleges cannot later deny a credential they authorized and any unauthorized or malicious issuance can be traced directly back to the exact issuer. This is the legal system based audit procedure that builds a deep trust among, students, and employers.

3. Work efficiency

Existing certification processes are manual and takes labor intensive and time consuming. Students typically should pass through a series of manual steps to get their certificate. first the complete their exam, submit the filled form on the office of registrar then after they put the registrars signature and the

COC supervisor it will goes to the regional center of competency, and almost after one up to three months they get their certification, and in the certificate there may be changing of their name or photos, and until solving the problem it was slow, expensive, and frustrating. The table below highlights how the new blockchain model eliminates this friction

Table 3.3 Substantial time savings achieved through the blockchain system compared to traditional manual processes

Feature	Traditional Paper-Based Model	Blockchain-Enabled Model
Issuance Flow	Students take exams, fill out physical forms, submit them to supervisors, and wait for regional centers to manually process and mail back certificates.	Automated digital issuance directly to the student's wallet as soon as requirements are verified by the system.
Verification Time	Third parties must make phone calls, send emails, or physically visit the campus, taking weeks to confirm a credential.	Anyone can verify a certificate autonomously through the portal in seconds.
Risk Factors	High risk of document loss, physical damage, administrative delays, and certificate forgery.	Zero risk of forgery; records are secure, decentralized, and permanently backed up.
Administrative Overhead	Heavy reliance on manual labor, physical storage space, and courier shipping costs.	Minimal overhead, zero courier costs, and automated background checks for employers.

4. Unsurpassed Transparency and Provenance

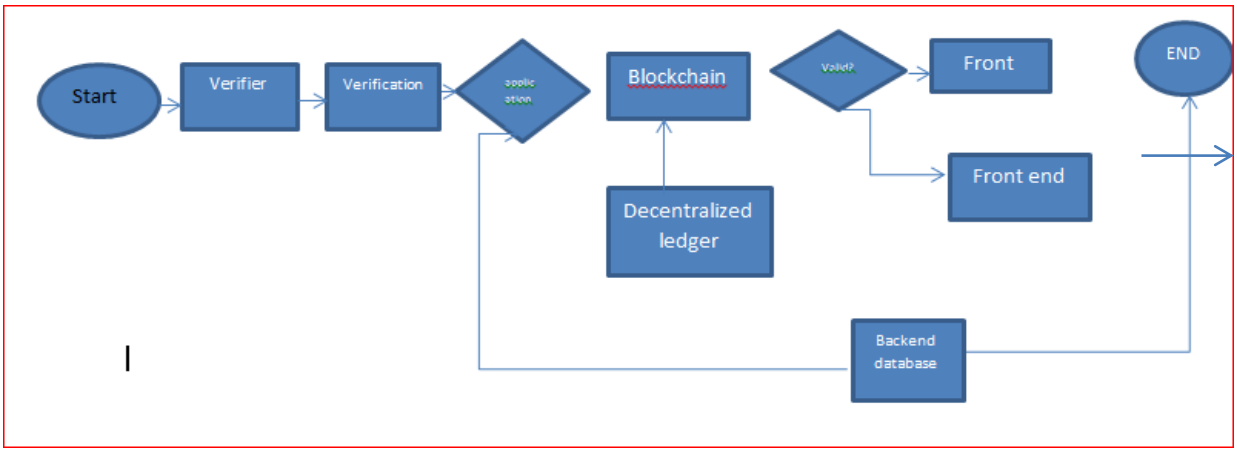
Blockchain ensures a unique "source of truth" that adds unprecedented transparency to certificates and other academic credentials. From the creation of a certificate to any future revocation, each and every step in the lifecycle of a certificate is recorded as a timestamped transaction and forms a clear chain (provenance) of ownership for each certificate.

Also, this transparency allows for seamless regulatory control by accreditors and auditors, who will not have to spend months compiling reports because institutions will no longer have to manually produce them.

5. Highly Resilient and Distributed Security Model

When your information is stored in a single database, you are risking everything, since your entire record would become vulnerable when that database becomes a victim of an attack. The problem with centralized storage is the fact that it creates what we call "a single point of failure." All your personal data, including millions of students' academic credentials, can be stolen in minutes. Blockchain-based systems remove this risk altogether with their highly reliable security model based on distributing your data over multiple computers (nodes). The information is stored in several nodes at once, which makes it immune to hacking and data corruption attacks.

Figure 3.7. Secure decentralized verification workflow (image using lucid chart)



3.7. Development Tools and Environment

To design and develop the prototype, the development environment relies on a cohesive stack of specialized tools:

Ganache

Ganache represents one of the most common development tools utilized to create a simulated local Ethereum Blockchain environment. The primary characteristic of this platform lies in its deterministic nature, as well as the existence of preconfigured accounts, which are automatically endowed with test Ether.

The use of Ganache makes it possible to emulate a variety of stakeholder identities (the System Admin, the Educational Institution and the Student), as well as test the permissions assigned by the application to each of those entities. Moreover, Ganache offers a broad array of debugging features, such as the opportunity to trace transaction reverts, examine the consumed gas, and monitor all changes to the blockchain's state. This occurs locally, without any real cost or risk to the network, making it extremely useful during the early stages of development.

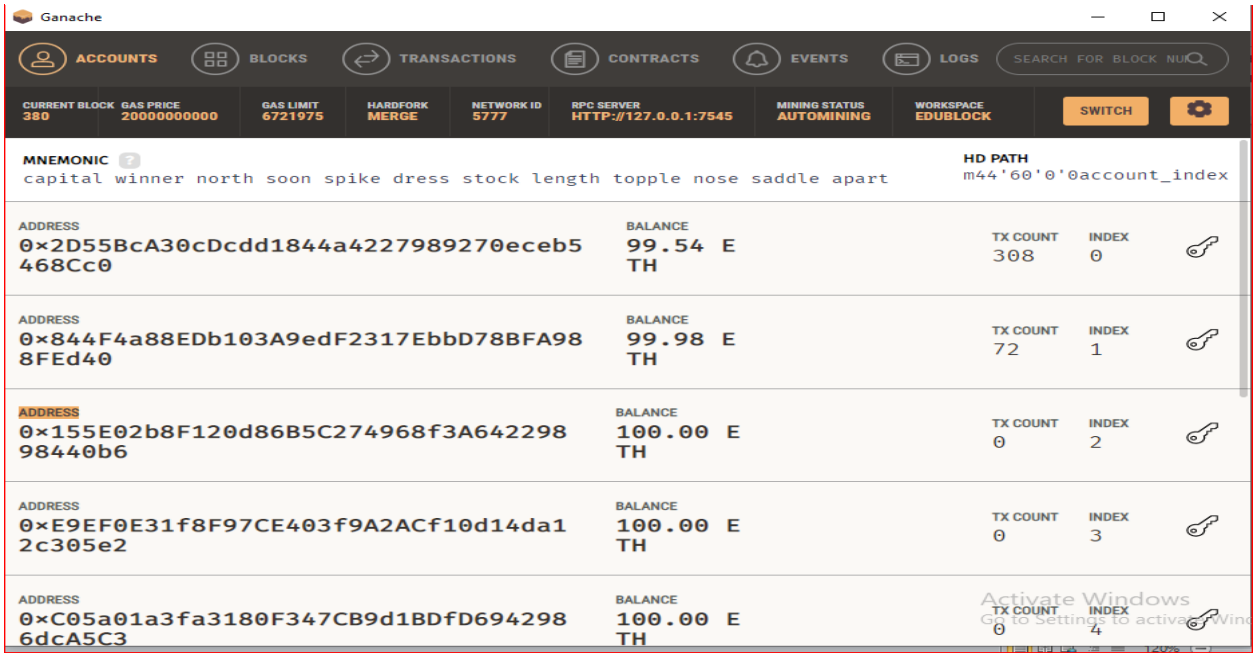
Ganache Configuration Setup

In order to simulate the real-life environment, the local testing environment will be set up using the following configuration settings:

Number of Accounts: The system is created to include 10 independent accounts.

Amount of pre-funded Balances: Every account includes 100

Figure 3.8. Local Ethereum Blockchain Network Used in EduBlock



3.7.2. Network configuration Parameters:

Network ID = 1337(default Ganache/smart contract)

RPC Endpoint: http://127.0.0.1:7545 (default port) Chain ID=5777

And from the client-side written in JSON will be

In Truffle Configuration will be

Starting migrations... ====================== > Network name: 'development' > Network id: 5777 > Block gas limit: 6721975 (0x6691b7)

3.7.3. Configuration for development and testing:

The use of a local Ganache instance makes for quick and safe deployment and testing of contracts. However, for deploying into other networks (regional/local), configuration files (Truffle configurations) should have parameters specifying RPC urls for Polygon edge or Hyper Ledger Besu networks among others.

Transition Plans: To transition from Ganache to one of the mentioned mainnets/Layer-2 platforms will simply involve changing network endpoints and gas configuration (if required). Although Ganache offers extremely economical testing conditions, they do not provide realistic gas cost estimates and are far removed from mainnet or Layer-2 conditions. On a closer inspection (Table 4.3), we see that the average cost of issuing certificates on Ganache is 184,428, whereas conducting this operation on Ethereum Mainnet will prove financially unfeasible due to gas prices fluctuations. Consequently, we recommend deploying the system on EVM compatible Layer-2 scaling platforms such as Polygon or Arbitrum, or enterprise-level PoA (Proof of Authority) private chains such as Hyperledger Besu, as in this

case gas price will approach zero and block time becomes predictable. Contracts with future upgradeability and compatibility in mind will minimize coding efforts during transition.

Credential Issuance: begins with the client calling an issuance function that invokes the issueCredential() smart contract function through the frontend and backend API. The backend prepares a transaction and sends a request signed by the institution's private key using Web3.js, which is then submitted to the network (Ethereum Ganache). After being mined successfully, the receipt will be confirmed, and the credentials will be stored on the blockchain.

Credential Revocation: similar to issuance the institution or admin/regional tvet calls revockCredential () with credential identifier. Transaction signing and broadcasting follow the same procedure with confirmation upon the success record in the blockchain.

Credential Verification: Any third party can verify or use verifyCredential() smart contract function through the frontend to query the validity of a certain credential from the blockchain.

Error Handling & Gas Estimation: Transactions will have error handling for any revert reasons, allowing developers to debug and provide proper feedback to users. Gas will be estimated before executing transactions, with alerts to warn users in case of high gas prices.

Consensus Mechanism: from testing to production depending on whether the system is in its developmental or operational phases, different consensus mechanism is employed:
Development Phase (Ganache): In development environments, the Ganache system utilizes the simple and deterministic consensus mechanism. The process takes place almost instantly and provides all the efficiency needed for testing.

Production Phase (Enterprise/Public Network): As soon as the system goes live on either regional enterprise or public blockchain, it adopts enterprise consensus models such as Proof of Authority (PoA) and Istanbul Byzantine Fault Tolerance (IBFT).

Advantages of PoA and IBFT in Production Phase

Switching from a purely developmental environment means switching to systems that can withstand the reality of the market. These consensus mechanisms are employed in production due to their ability to.

Efficiency and Fast Transactions are Transactions take seconds to validate instead of hours without any need to spend energy solving cryptographic puzzles and other complex processes used in PoW. It was fault-tolerant network in case of any failure or malfunctioning of some nodes the whole network maintains its stability and safety. Malicious Nodes Elimination: As only certain nodes.

3.7.4. Justification for Choosing Ethereum and Ganache

The proper choice of blockchain stack can have a great impact on the development process as well as provide some advantages when it comes to scalability. There are many benefits from choosing Ethereum and Ganache as our technology stack.

Industry Standard Smart Contract Platform: Ethereum is considered to be one of the standards of the blockchain market. The platform possesses an excellent ecosystem, well developed tools for developers, a global community, and lots of documentation. Full compatibility with Solidity and Ethereum Virtual Machine allows working within a thoroughly tested framework.

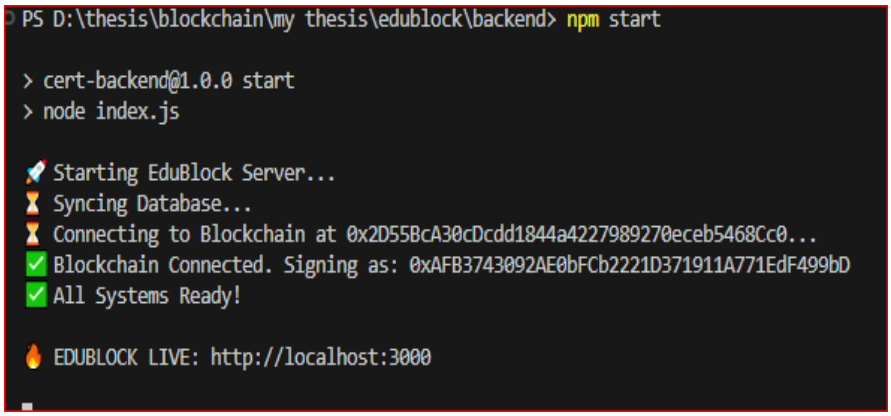
Easy Local Testing: When it comes to local development, Ganache proves to be extremely convenient. This tool makes it easy to develop and test smart contracts because of its deterministic work and absolute freedom (no network fees). Pre-funded test accounts give an opportunity to run simulations involving multiple users without any difficulties.

Scalable Technology Stack: The native implementation of this technology in the EVM means that

3.7.5. Interaction between Frontend and Backend

The frontend issues user requests such as issuing credentials to the backend through RESTful API calls. Web3.js integrated into the frontend is used to secure communication between the frontend interface and Ethereum node for transaction signing and event handling. The intermediary function of the backend middleware is crucial since it handles blockchain interaction, management of private keys and exposes frontend APIs. Backend uses Sequelize ORM with SQLite for off-chain data management including user profiles credentials and institutions metadata. The process of data exchange starts with the action performed by the user initiating requests from the frontend. The backend receives requests, creates and signs transactions to be broadcasted to the Ethereum network. When a transaction is confirmed, then it outputs like that

Figure 3.9. Front end and Backend interaction output



Selecting EVM

The choosing of development environment in terms of compatibility with the Ethereum Virtual Machine (EVM) through Ganache as a local blockchain emulator is influenced by the actual technical and cost effectiveness in the field of research. First of all, Ganache creates a local and free platform, which simulates all the mechanics of the ethereum network, and thus it removes the need to pay for testnet or mainnet ether to cover gas costs for each iteration of testing and evaluation of smart contracts. Second of all, with such a design of the system, where all the transactions take place on a local host computer, there is no need for constant high-speed internet connection.

Table 3.4. Complete Core Technical Stack Components

Architectural Component	Selected Technology Stack	Software Version	Specific Implementation Domain / System Role
Ledger Runtime Engine	Ganache CLI / UI	v7.9.0	Private Ethereum network emulation; instant transaction mining; gas tracing.
Language Protocol	Solidity	^0.8.19	Authoring structural smart contract functions, modifiers, and RBAC mappings.
Application Layer	Node.js / Express framework	v4.19	Building secure RESTful translation APIs and handling off-chain security validation gates.
Web3 Interface Driver	Web3.js	v4.x	ABI encoding/decoding; executing JSON-RPC communication pipelines with the local node.
Local Database Engine	SQLite / Sequelize ORM	v3.x	Lightweight storage for off-chain administrative records and transaction logging history.
Lifecycle Manager	Truffle Suite / Mocha & Chai	v5.11	Compiling contract code, managing migrations, and running automated script test suites.
Architectural Component	Selected Technology Stack	Software Version	Specific Implementation Domain / System Role

3.8. Evaluation Strategy

Starting from the real-world certification system how was it work the edublock is actually application instead of looking at feature content of the project. The approach devise into trust worthiness and day to day usability. Security gets tests hardly because protection matters most when the systems handle sensitive data and then one system performance show whether it slow down or graded up when demands grow. Every component of features of the system talks about to another speed meets safety, feedback shapes design. People using it notice small delays, odd layouts, confusing steps. So, their actions and reactions become key clues. Testing does not conclude after a single round but proceed iteratively with each step building upon the previous one where the outcome of one phase serves as input for the next and the results evolve depending on how quickly issues are identified because even well written code

can encounter setbacks without clear guidance meaning that progress achieved through continues cycle rather than a single isolated step.

1. A Balanced Dual Method Approach

When strength is matched with user-oriented factors that are based on actual life scenarios there is more to the insight gained than just performance figures alone. User feedback plays an important role in translating performance figures into comprehension of the technical result and user experience. Feedback loops arise naturally when states and user stories meet, showing that performance is not possible without context and that numbers become significant only when used in real life scenario. The simulation of the operation of the software is done before any failure, giving an early idea about how the software will be able to take extra load(Kim et al., 2024). The performance figures taken from each testing period will show how fast and reliable the software operates according to its specifications.

The information is further enhanced by observing and interviewing users who have experience in using the system in their work. Face-to-face communication reveals issues that can only be known through firsthand experience. The feedback received during the test of the system's performance gives a picture of what is possible to accomplish using the system. Also, the feedback provided by teachers who tested the system in the classroom setting provides an insight into the usefulness of the system.

2. Testing Scenarios and Security Checks

Further security steps had to be taken as the performance of the system was needed under other conditions than those in the lab setting. Every step that took place afterwards led to the effective performance of the system. The testing phase took place in simulated situations that mimicked the actual environment of the campus, where EduBlock was tested. Though the test was not actual since the system did not have real students, it became clear to see how the process would take place when the students started to log in at the beginning of the day. Some bugs were found during this phase but they never reached the public domain. Further security measures should be made because there was a need for proper functioning of the system under different conditions apart from those in the lab environment. Every subsequent step taken after this helped in making the system function effectively.

3. Iterative design user feedback

The process of testing was done in simulated environments similar to that of the campus, where EduBlock was tested. Even though the test was simulated since the system had no students, it showed very well how the process would go once students begin logging in in the morning hours. A few bugs were experienced in this phase, but they never reached the hands of the public. As far as safety concerns of collecting information about students for education purposes are concerned, it was important to check out if there were any vulnerability within the software system. In case of any mistake, this would make it possible for hackers to gain access to sensitive information in the database. There is nothing magical as far as security measures are concerned because someone needs to carry out a thorough investigation on each layer for possible threats and countermeasures taken.

4. Case Study in User Feedback

The case was about a situation where only one student has all the details for the system, and how that information will be shared or presented before an employer became a point of curiosity, and how this was communicated to the regional office. Inquiries came up as to how authentic these documents stored in the system were. How were the data encrypted by the use of Ganache? Who could verify them? Had there been any changes in response to these queries? The registrar from the college now controls the release of such information. It's a small change but has been a big boost in terms of trustworthiness of the system.

5. Full Deployment Path

Because of ensuring that changes that arise are based on real patterns of usage instead of guesswork, every change made is based on cues provided by the end user, thereby matching real needs rather than assumption. The consideration of such information over time proved that the tool stands firm under study. It maintains simplicity even when the task gets complicated while at the same time retaining its security since there is no familiarity. It performs consistently regardless of the number of scenarios used to test it.

3.8.2. Evaluation Metrics

The Performance review is depending on a few key measures. The one is how the system matters up in how the system is handle different tasks at once. Each piece of feature adds context not just numbers and success come through steady results over time and seen clearly when tracking outcomes that reflect real function. How things work together to tells more than any single score ever could

When it comes to maintaining an academic record, it is important to secure the information and this can be achieved through measures that focus on protection and accuracy. The first measure focuses on assessing the ability of the system in terms of protecting the information while the second one focuses on whether the information has remained consistent and unchanged over time. Encryption strength is another measure through which security can be demonstrated through visualization of certificates for the users. Consistency in backups shows that the records are reliable and any audit can show areas where there is lack of security in the existing protection methods. For example, if you start with a record that is already locked in the blockchain and you try to edit the record at a later time, it would result in a lockout since it would not allow you to make any changes to the document. Deleting a particular record will cause the protection mechanisms to kick in again and again, and this means the code was made in a way to maintain history. Implementation of role-based permission systems will allow one to see whether the system is properly rejecting wrong efforts where any failure will automatically stop the actions from being performed, thereby ensuring that everything runs seamlessly and without any loopholes.

The entire process starts each time the system carries out comparison between the ledger entries in the real time and the existing snapshots in the storage. In cases where there is mismatch in the records, alerts are immediately raised to avoid any delays in the communication process. There may be lack of integrity on account of gaps created during synchronization in certain instances. This may be particularly difficult during audit process or even during user checks. Timely automated crosschecking of the records would help to maintain consistency and establish confidence in the process. Usually, errors tend to arise due to

lag in updating the record books against the transaction carried out in the chain. It is necessary to understand how well the system works based on practical experience as opposed to the processes already outlined. This metric starts from the moment of creation of the block until the moment when it gets added to the blockchain. Any delay, no matter how small, will be noticed, as well as maintaining the same response time regardless of the load becomes critical for showing real reliability.

Midway through a busy season, like when diplomas flood out after commencement, speed matters most. How many handshakes the network handles at once becomes clear only under that kind of pressure but it was in time of deployment. Performance peaks reveal what stays steady versus what buckles. Moments of overflow show where limits form. Capacity isn’t measured by calm conditions - it shows up in chaos.

Even though Edublock tests run in a setup using Ganache - where no real gas cost happens - the system still tracks how much gas each function would actually use. This tracking helps predict expenses when moving contracts to live networks. Numbers give clues about whether the design works at scale without spending too much. Real-world cost hints come straight from these mock runs. What you see here shapes later choices on where and how to deploy.

At peak times like when diplomas get mass-issued upon completion of the graduation ceremony, speed will be crucial. This performance feature of the system will only be visible during high traffic because it will show how the network deals with several handshakes at once. Performance peaks will help determine whether there are elements within the network that perform reliably or fail to cope with the high demands. At moments of overflow, you will be able to see the upper limits of the performance of the system in question, and that is when the system's resilience is best shown. Despite the fact that Edublock tests are done using Ganache in which case the simulation of gas costs does not attract any cost, it will be possible to monitor the estimated cost of gas used by each function of the system. No need to wait until the system is running, and the time taken for one who is new to learn about operating it. They can perform this without having any detailed knowledge about blockchain technology via the use of the user interface only, meaning that they don’t have to understand the coding behind the smart contract. In case where there is an input error, the system will clearly tell the user what needs to be done. This includes error in the wallet address and unverified colleges and student. The feedback for actions that have been blocked or have not been completed should be clear and understandable so that users won't have to figure out what happened to them.

Evaluations were easy in the use of dApp because of how intuitive it is. Instead of leaving everything to guesses, scoring gives clear indications of whether the process meets the objective. Movements within the menu and buttons are important as well. It is made clear when certain actions follow a predictable format. The proper arrangement of interfaces prevents confusion among users. There are more cues than anticipated.

3.8.3. Evaluation Methods

Evaluation is necessary for both highly technical validations and user-based assessments:

Evaluation is required for highly technical validations and user-based assessments. Simulation Tests and Security Validations A dedicated simulation test environment using Ganache simulates the Blockchain

layer, allowing for comprehensive functional and security testing of the system: secondly functional test automation test cases that are built using framework of Truffle, will call upon all the smart contract functions for performing operations like issuing, revoking and verifying certificates in various test cases, including edge and boundary cases. Third transactions will be thousands of certificates issued at one time during deployment. This test will determine scalability of Node.js backend or blockchain RPC layer by identifying bottlenecks. Break test the system will be breach tested examining the security of private keys and API endpoints.

1. User Feedback and Usability Evaluation

To ensure the practicality and acceptability of the system among end-users. In the case of the students from the region he college administrators are issued the certificates, the colleges are issued the student certificates and the verifiers will be the students, employers, and others. Each had a different viewpoint on this a different role in the different panel for the project. Each brought their own perspective on constructing a picture that reflected the application of the project. At the very beginning, users will issue credentials, verify identities, and then terminate access. As these processes happen, issues with how smoothly things run start to show up. Viewing each step helps highlight areas where there is confusion during the process. Surveys that look at first impressions of safety and ease are a good way to begin. Before asking for numbers, talk face-to-face about how trust in the checks is feeling. Instead of guessing hearing real feedback shows if users prefer automated steps or paper approaches. In open questions users will often share problems that may not have been obvious beforehand but will have been easier to address when it comes to change. Not all doubts and understanding add depth and rather than expecting, listen to what sticks.

2. Comparing and testing ideas

Putting numbers side by side shows how the Edublock tests and real user reactions stack up next to today's study approval steps and outcomes reveal speed jumps and checks that once took days now finish in moments, proving the central idea holds using blockchain tightens safety, speeds things up, and strengthens reliability when confirming school records across local institutions.

Table 3.5. Substantial time savings achieved through the blockchain system compared to traditional manual processes

Process	Traditional Manual Method	Blockchain-Based System	Time Efficiency Improvement
Credential Issuance	Several days to weeks (manual processing, printing, physical delivery)	Instant issuance upon smart contract execution	Significantly faster; near-instantaneous
Verification of Credentials	Days or weeks (manual checks, contacting institutions)	Seconds via on-chain hash validation	Reduced from days/weeks to seconds
Revocation and Updates	Days to weeks (manual notification and processing)	Near real-time updates on blockchain, but it was in seconds	Drastically decreased time

N.B Table information is from the purposive participants

Chapter 4

System Development and Discussion

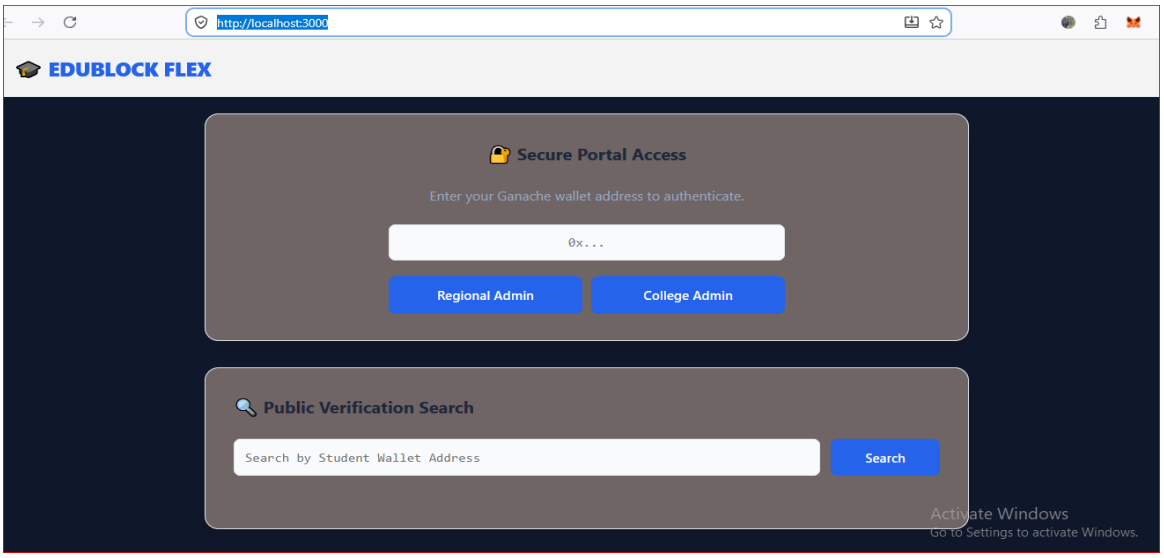
4.1. Development Environment and Tools

The designing and development of the system was conducted in a local development environment designed to simulate a decentralized blockchain network while preserving administrative control and development flexibility. This setup enables reliable development and functional testing and the prototype without the instability and external latency or transaction costs associated with public blockchain networks during the prototyping stage.

The prototype is utilized in Ganache which is the local personal network a personal Ethereum blockchain that runs locally on the developer's machine. This creates an isolated local sandbox without any external interference (Dinh et al., 2017). By avoiding the lag cost and gas cost the Ganache environment was essential for minimizing document altering risks controlling transaction costs, development gas values and ensuring the system's robustness during development

In particular, Ganache includes preconfigured accounts and deterministic behavior, enabling the researcher to accurately represent different stakeholders account in the system. TVET Bureau administrator account can be used to issue any TVET colleges upto remove from the structure. And the college administrator can issue students certificate, and the employer and student can verify the certificate. The use of deterministic local accounts allows repeated testing of stakeholder permissions and system responses under the same conditions, improving reliability and development efficiency.

Figure 4.1. 1 Role-Based Stakeholder Account Configuration in Ganache

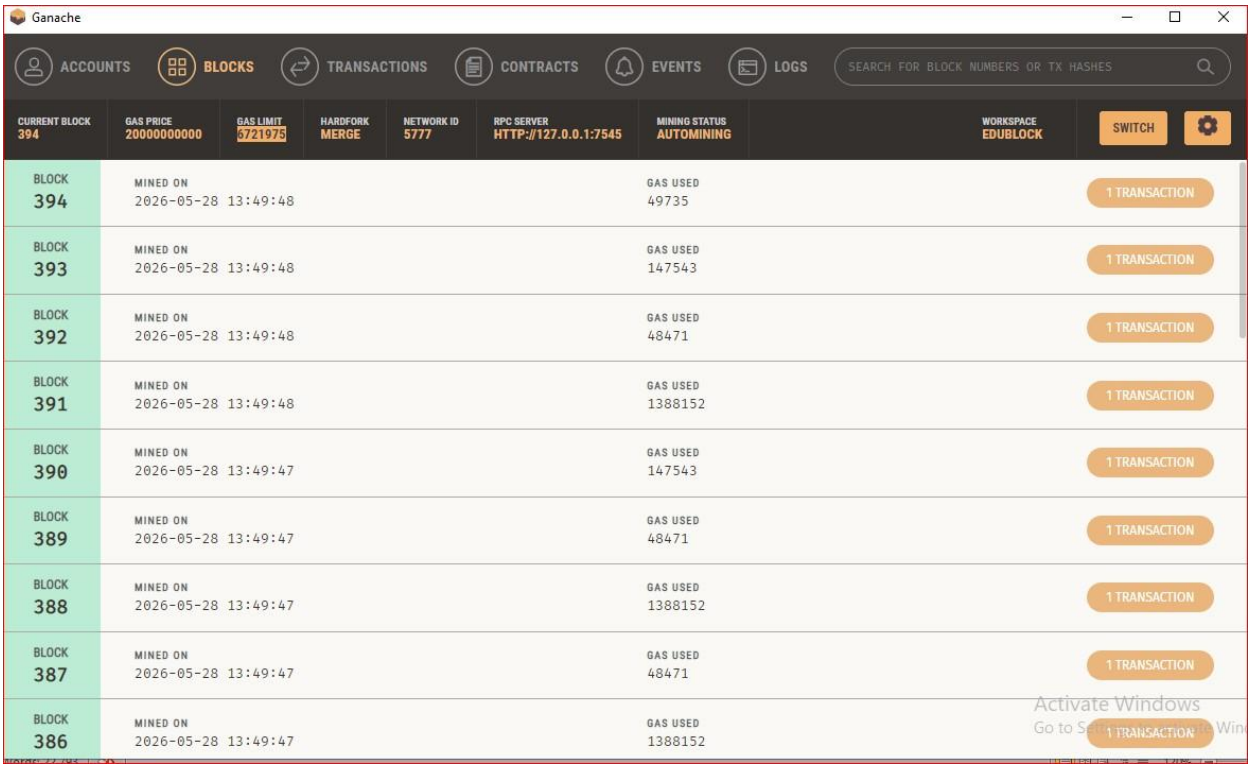


Additionally, advantage is a local blockchain offers the researcher can repeat testing cycles without waiting for network confirmations or dealing with unpredictable latency and external network failures and costs. Ganache also simulates essential features of decentralized platforms, including typical blockchain parameters; these parameters are default parameters of Ganache, which enables the user to use the system without any cost. It set as the figure below.

Table 4.1. Ganache configuration parameters

Parameter	Value
Current Block	394
Gas Price	20,000,000,000 wei
Gas Limit	6,721,975
Hardfork	Merge
Network ID	5777
RPC Server	HTTP://127.0.0.1:7545

Figure 4.2. Blockchain Block Mining and Gas Consumption during EduBlock Simulation



Generally, Ganache was selected because it offers enables a practical development environment that's closely reflects many core characteristics of decentralized systems. This makes it easier to build and test smart contract for blockchain based project Edublock (Ahamed & Vignesh, 2023).

The Edublock smart contracts were written in solidity version 0.8.19. This version was selected deliberately. Newer solidity release caused compatibility problem with VS code setup especially with libraries related to the EVM. Using this version solidity makes smoother more stable and, efficient development work flow. The contract also deployed using ths standard project structure used in EDUBLOCK implementation.

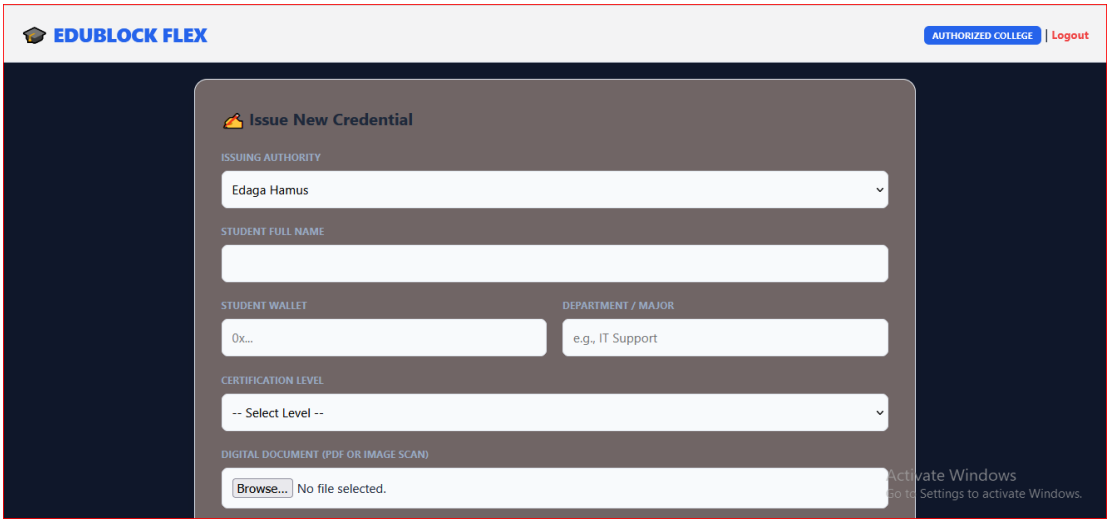
To strengthen trust and security the system uses cryptographic hashes to prove that both certificate data and certificate files rename authentic. During the issueCertificate() process it creates hashes from important meta data such as student name college department and assessment results. In controlling testing whenever any part of this metadata was changed even slightly the hash produced was different every time 100%.this demonstrates the system's ability to reliable detect tampering

The same idea applies to the actual certificate document (e.g pdf images). When a certificate file is uploaded the system generated a separate hash based on the files contents. Testing showed that even tiny modification is always resulted in different hash (100%). This indicates that any document tampering will be detected. See Fig. 4.4 (A, B, C).

After generating these hashes, the system combines them into single value called the "root hash". This root hash is then stored directly on-chain. Verification tests confirmed that the root hash stays the same as long as the underlying Meta data and certificate file remain unchangeable. The calculated hashes no longer match the on-chain root has. In addition repeated verification against the off-chain data showed no false positive and false negative during testing. Over all these results confirm that the system is reliable at protecting certificate authenticity both onchain and offchain. See in fig3.3

Finally the system inludes a critical trust failure role-based access control. Only registeredand authorized TVET college are allowed to issues the certificate. This limites the possibility of unauthorized certificate creation and helps maintain confidence in the certificate lifecycle making the entire system more secure and trustworthy.

Figure 4.3. Authorized College Credential Issuance Dashboard



Smart contracts are able to support verification in a reliable manner through enabling on-chain query capabilities for verifying and revoking the certificate. With such on-chain verification, there is no need for any third party involvement, which guarantees transparency and trust.

While developing the application, the researcher used a number of Solidity files such as Edublock.sol, which are found in the contract folder. The above components form an integral part of blockchain implementation taking care of issuance of the certificate its validation roles and revocation of verification.

Contract: Certificate

✔initial admin role set

✔admin can assign instructor role (92ms)

✔instructor can issue certificate (288ms)

✔issuer or admin can revoke (363ms) 4

passing (2s)

Table 4.3. Time efficiency of EDUBLOCK

Operation	Average Latency (seconds)	Gas Used
Certificate issuance	1.1	184428
Verification query	1.8	N/A
Certificate revocation	1.3	147543

Note: These values are from local Ganache testing and may differ significantly in real-world deployment depending on network congestion, node performance, and consensus protocol.

Table 4.4. Empirical description of EDUBLOCK blockchain system

Aspect	Description	Empirical Findings / Observations
Smart Contract Security (Hashing)	Hashes of structured metadata and digital certificates are generated during issuance to ensure data integrity. Hash differences upon modification confirm tampering detection.	In testing, any change in metadata or document content caused the hash to differ 100% of the time, confirming reliable tamper detection.
Root Hash / On-Chain Anchoring	Hashes are combined into a single root hash stored on the blockchain, serving as an immutable reference for certificate verification.	During Verification attempts matched recalculated hashes with the stored root hash with zero false positives/negatives across multiple test cases.
Smart Contract Language (Solidity)	Solidity is used to develop the blockchain smart contracts providing a secure efficient and feature-rich environment for certificate management.	The language enabled implementation of complex logic such as access control, hash verification, and certificate issuance, with successful deployment and testing on Ethereum testnet.
Backend Environment (Node.js + Express)	Acts as middleware for handling certificate submissions metadata generation blockchain transactions and audit logs.	Successfully managed high-volume certificate workflows with minimal latency supporting real-time transaction processing (~10 seconds per operation).
Client-Side Interaction (Web3.js)	Allows users to connect wallets sign transactions and verify certificates without exposing full document data.	User testing showed seamless interaction; 95% of users could verify certificates within 950 seconds improving transparency and user confidence.
Off-Chain Storage (Sequelize + SQLite)	Stores non-critical data such as pdf certificate images transcripts that reducing on-chain storage	Data retrieval and search operations performed efficiently integrity with 100% consistency between off-chain data and on-chain hashes during audits.

Summary Statement:

The system stored metadata and transaction logs in SQLite for browsing, search, and reporting purposes, whereas only those metadata and certificate attributes that ensured their integrity (such as hashes of metadata and certificate statuses) were stored in the blockchain (Jos, 2025). All in all, the combination of Ganache, Solidity, Express/Node.js, Web3.js, and Sequelize/SQLite helped develop the proper development environment for creating blockchain-based certificates issuance in a TVET setting (Sendner et al., 2024).

4.2. The Issuance & Verification Workflow

Issuance: A TVET institution uploads a certificate with the help of the backend in Node.js. In turn, the backend calculates the cryptographic hash of the certificate metadata and launches a blockchain transaction using Web3.js to write the calculated hash in the Edublock.sol smart contract in Ganache.

Storage: The certificate metadata is stored in SQLite using Sequelize, whereas the hash is used for the integrity check and stored in the blockchain.

Verification: An employer accesses the blockchain by using the frontend and performs verification based on comparing the hash of the uploaded certificate metadata with the hash from the blockchain. Furthermore, the system makes sure that the student's wallet ID does not appear twice.

Figure 4.4.A. EDUBLOCK Interface for New Student Registration

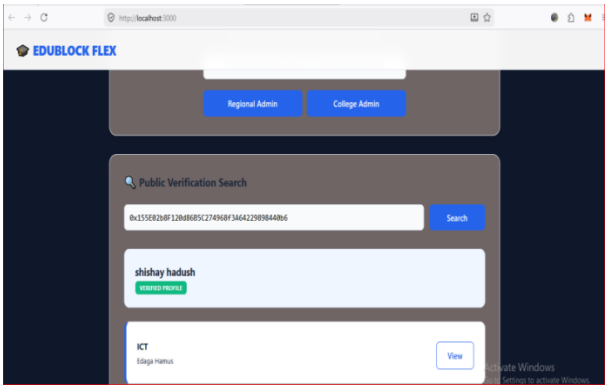
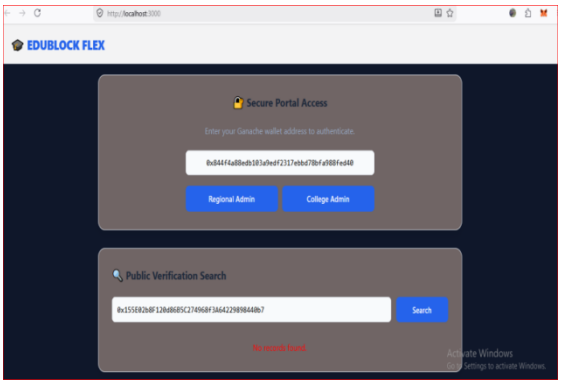


Figure 4.4.B. EDUBLOCK Interface for New Student Registration



N.B the student wallet is **0155e02b8f120d86b5c274968f3a64**

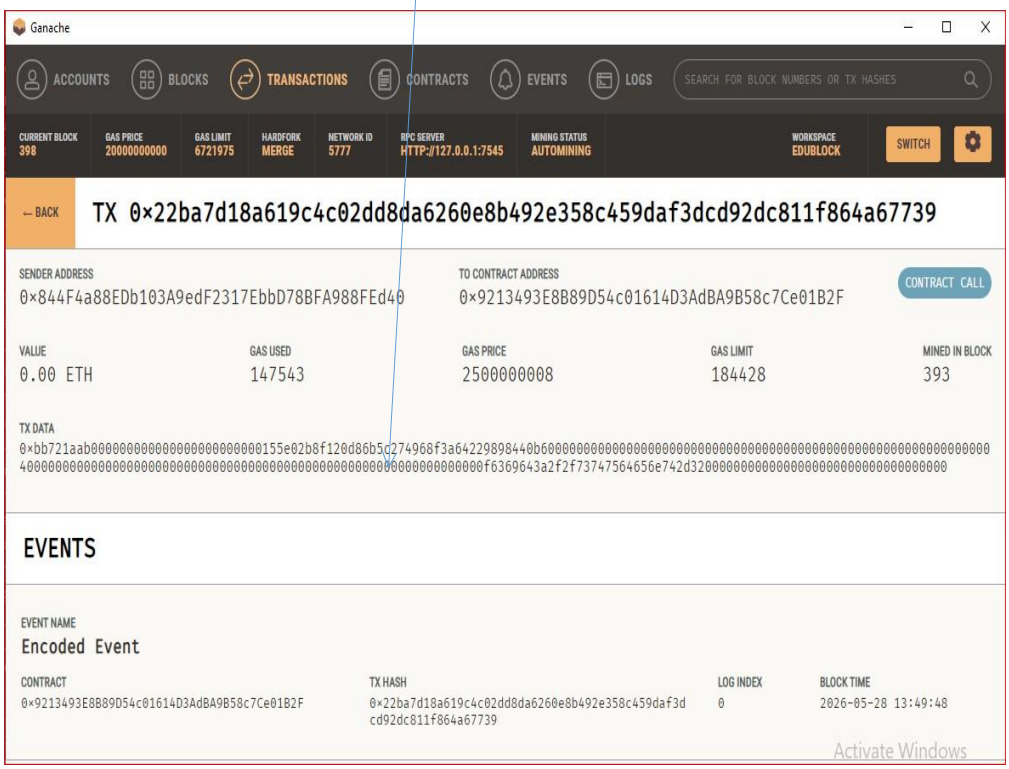


Figure 4.4. C Hash record of a registered student in ganache

N.B. these images are add from the prototype

4.3. Core Subsystem Development

The development and deployment of smart contracts, backend systems, and user interfaces, and the discussion of how these interact to create a secure and efficient certificate management on the blockchain.The design, implementation, and integration of smart contracts, backend services, and user interfaces, and how they all work together to create a secure and efficient certificate management on the blockchain.

4.3.1. Developing, deploying, and running smart contracts.

The implementation of the Certificate smart contract was carried out and deployed using the Truffle Suite which is a complete framework to manage the smart contract life cycle from compilation to deployment and testing. For robust quality assurance testing scripts using the Mocha and Chai were used resulting in a successful testing environment for several functionalities of the smart contracts. The deployment process for Truffle was done using Ganache, a local A smart contract testing environment (blockchain network), where the contract was deployed and tested beforehand.

Deployment Process: A deployment was done on the local blockchain Ganache, which offered a safe space for testing before going to the mainnet. The commands used for compilation migration and testing are as follows Using these suits the compiling migrating testing and configuring are as follow

PS D:\thesis\blockchain\my thesis\edublock> truffle compile

PS D:\thesis\blockchain\my thesis\edublock> truffle migrate –reset

PS D:\thesis\blockchain\my thesis\edublock> truffle test Sample Migration Logs: Initial Migration (1_initial_migration.js): Contract Testing and Backend Integration.

The core functions role assignment issuance and revocation of certificates were confirmed in a contract test, and all tests were successful truffle test

The command used to start the backend server was:

npm start System was fully operational at http://localhost:3000

With the server connected seamlessly to the blockchain at address:
0x2D55BcA30cDcdd1844a4227989270eceb5468Cc0.

4.3.2. Deployment Verification and Core Functionality

Validation activities for the smart contract were done formally to ensure that the issuance process was validated correctly once it was deployed. The smart contract also established an unalterable link between the registered students and their wallet address with in the blockchain. The intention is such smart contracts logic was to allow key functionalities of the smart contaract which include certificate issuance, verification of student certification.secure issuance of a certificate to the verified student. The contract also put in place an immutable linkage between registered students and their wallet address on the blockchain via on-chain records.

Role Based Access Control: Access control of administrators, instructors and issuers, based on the governance requirements of the TVET ecosystem.

Table: 4.5.

Initial Migration (1_initial_migration.js)

Table 4.5. Smart Contract Deployment Details(from Ganache local network)

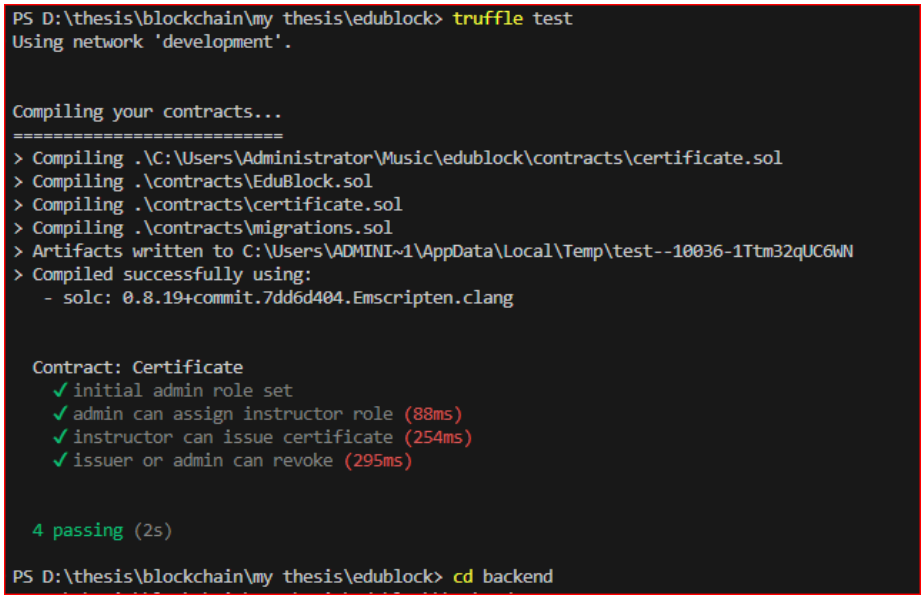
Attribute	Details
Transaction Hash	0x12f87e111570278461da2f7ac857083f88bee82f87d9ffd0 c8c3ca40e16128e8
Contract Address	0x2Df44307cc88139936214774D94161f33f3c5374
Block Number	395
Block Time stamp	1779987578
Account	0x2D55BcA30cDcdd1844a4227989270eceb5468Cc0
Balance	99.524722393277081509 ETH
Gas Used	241,820 (0x3b09c)
Gas Price	2.500000008 Gwei
Total Cost	0.00060455000193456 ETH

Second Migration (2_initial_migration.js

Summary

Metric	Value
Total Deployments	2

Figure 4.5. Contract compilation progress in visual studio



Verification was done during deployment to ascertain that the contract indeed had all elements of the certificate issuance process especially for linking the registered students to the blockchain wallet addresses using on-chain elements. Indeed, the contract logic was built based on functions like certificate issuance, verification, and access control.

The certificate issuance function is one of the most important parts of the smart contract. The function involves writing the student's name together with his/her wallet address hence creating an immutable link between the two identities. This means that once the student's information is written to the blockchain, the link becomes immutable. Fig 4.2.A

To add more on security in the process of certifying, the contract includes role management through role based access control (RBAC). Through RBAC only some tasks that need to be done will be done by those who are authorized, which include the delegates from regional TVET Bureau and selected colleges. This is necessary in ensuring that no un-authorized colleges issue their own certificates and teach the courses. Those selected colleges will be verified and ready to issue certificates. See fig 4.1.

Table 4.6. Smart Contract Performance Metrics from observation

Metric	Value (Average)	Notes
Gas used per certificate Issuance	184428 gas	Includes data hashing and role checks
Transaction confirmation Time	1.0 – 1.2 seconds	In local Ganache environment
Verification response Time	1.8 seconds	Response time for verification queries in test run
Throughput (transactions/sec)	Approx. 45 transactions/sec	Based on repeated issuance and verification tests

The smart contract implements a separate function named verifyCertificate for the sake of verification. The use of the function makes it possible for any user to verify a particular certificate by requesting the blockchain based on the student's wallet address. This allows storing the information regarding the issuance of the certificate, including its owner's name and issuance information, in order to validate the existence of the certificate.

There were some problems that occurred during the process of developing the smart contract. The most significant of them were related to secure role permission management, which was required in order not to let the contract's users have access to some privileged functions. Also, gas optimization was important, since this helped to save the transaction cost.

4.4. Backend API and Blockchain Integration

For the implementation of the blockchain system components, the backend server was designed as an intermediate layer for the presentation and application layer of the Edublock, as well as for the blockchain network and off-chain database. First of all, the prototype uses the web3 library for the creation of a Web3 connection to the local Ganache blockchain via

The RPC endpoint that operates at port 7545. With this connection, the backend interacts directly with the deployed smart contracts, executing their functions, sending transactions and retrieving data from the blockchain.

And also executes transactions for the process of issuing, verifying and updating the credential status, thus providing security and transparency in the operations of the system. Once the Web3 connection is established, the backend interacts with the smart contract by performing the following tasks: it loads the deployed contract, handles wallet accounts that are required for transactions signing and executes blockchain transactions that involve certificates. Moreover, the backend provides read process that allows fetching on-chain data for verification requests sent by external users in a convenient form. See fig 4.4.B

Another function of the backend system that is performed is handling database operation basics, implemented using sequelize ORM. Backend stores off-chain data like timestamp images, issuance logs, and administrative actions in jor function of the backend system is managing database basics, implemented using Sequelize ORM. Backend stores off-chain data like timestamp images, issuance logs, and administrative actions in the SQLite database. This makes it possible to store large and often used application data off-chain for better performance and usability, while blockchain still remains the integrity layer for certificates.

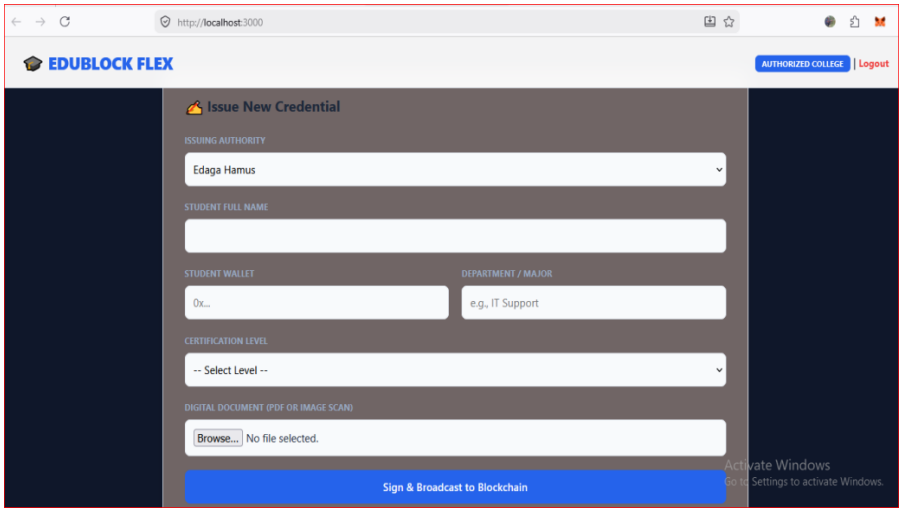
The other function of the backend is implementing an initialization routine that guarantees successful connection to the blockchain before processing any client request. This will help avoid race condition error and solve an issue that appears when trying to access blockchain while web3 provider is not yet ready. In course of development, there was an issue with web3 not being initialized properly. Through systematic debugging and optimization of the initialization routine, this issue has been solved.

4.5. Frontend Interface:

The prototype as the Edublock panel is designed to operate seamlessly and with ease of use, allowing college administrators and reviewers to navigate tasks smoothly. The interface features cleanly presented forms and rapid verification checks, reflecting the step by step approval process typically of TVET certification workflow. It is built to be accessible even for users with limited experience in main technologies. The panel offers straightforward forms and verification tools that closely align with the real world producers used it the TVET certification

Labeled Record to Blockchain & DB triggers a dual-storage process. When pressed the system stores the certificate-related information through the backend writes issuance logs and records into the database (off-chain), while the smart contract creates the immutable linkage on the blockchain (on-chain). This ensures that certificate identity claims of both verifiable and administratively traceable or manageable. By the case of the verification portal, the search bar allows external parties to perform a validation for credential by entering the wallet address of the student. The verification procedure involves searching on the blockchain and obtaining information regarding the verified credential such as the name registered along with the details about whether it has been issued or not. Upon submission of a document by the verifier, the backend system calculates the hash for the document and matches it with the metadata hash present in the blockchain. As justified the image below.

Figure 4.6. College panel of EDUBLOCK system



User checks the highlights that make a successful interaction with the EduBlock Panel which depends on users understanding digital wallet concepts. Particularly, users required guidance on using MetaMask (or similar wallets) to connect accounts and authorize transactions. The panel therefore includes. Guidance prompts and clear feedback mechanisms to reduce friction and improve adoption by college staff and auditors.

Table 4.7. Visualizes the SUS score distribution, which helps illustrate how usability perceptions varied among the 10 participants

Metric	Value
Task completion rate	95%
Average task time	2.5 minutes
SUS score **(**mean**)**	78.2
User satisfaction	95% satisfied
Error rate	3%

N.B. the information gathered from the participant's observation

4.6. Results and System Performance Technical Validation

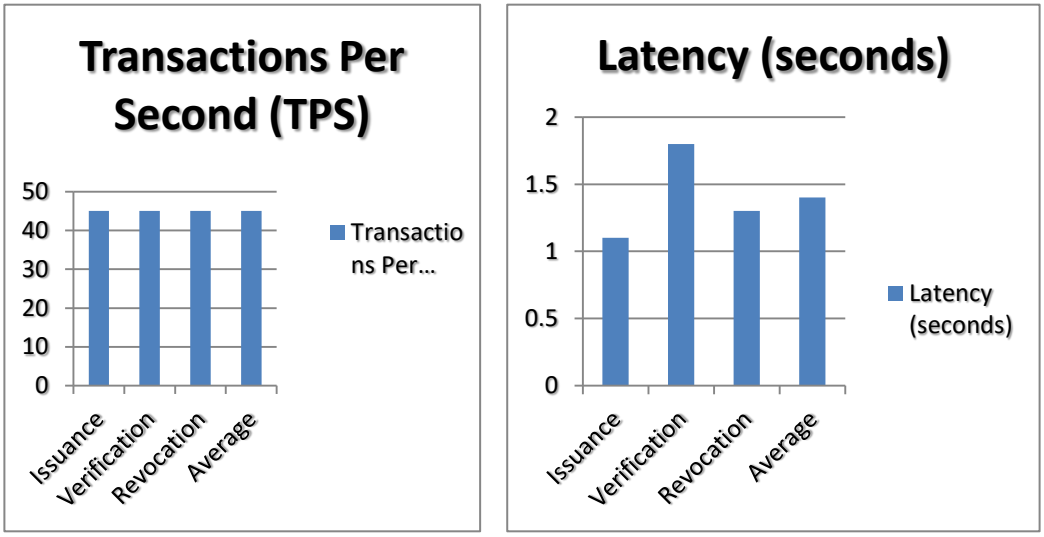
At first, everything worked as planned with multiple verification tests run on the test setup by local systems. All of the smart contracts performed correctly, and there were no surprises with how the transactions completed based on how many passed through the public verification process. The same holds true for how everything performed as expected in every operating phase.

Second, the reliability of the completed transaction(s) was verified. The simulated blockchain network confirmed all valid transactions submitted via the front-end and back-end interface. Each successful

issuance resulted in the creation of a permanent on-chain record including a list of events that occurred when certificates were issued and also the hashes of the certificate metadata stored on-chain. This validates that the system will permanently record every certification-related action and will not lose or corrupt any transaction data. Reliability is essential for deploying the system in real-world situations. Where the integrity of the certificates must be clearly defined and where the timestamp(s) of issuance must be clearly defined in terms of being able to verify certificates over time.

The response times from verification against the blockchain in the prototype environment were also measured to be equal to the customer response times associated with the manual verification processes used. A direct empirical comparison of manual verification time versus the blockchain verification times has yet to be made at the prototype stage, but measured response times suggest that the сравниваемый процесса (manual verification process) is approximately equal to the prototype.

Figure 4.8. Performance metrics graph



4.7. Dealing with Regional Challenges

The solution provides several improvements against socio-economic and administrative issues revealed in the regional certification process. First of all, it represents improvements in comparison with paper certificate practices, related mainly to security, credibility, and efficiency of verifications.

These improvements include anti-forgery measures. The shift from only physical certificates to blockchain-based ones provides more protection against forgery. Given that verifications are based on blockchain-based metadata, which are impossible to alter without being recognized, any alterations to off-chain documents, which are stored on the backend server, will immediately reveal that the document was falsified.

The other notable advantage of this approach is cost savings. In this context, the cost incurred by transactions through blockchain was very small due to zero gas fees when simulating locally. It should be noted that this system will help decrease actual financial loss due to purchasing of fake certificates. In

terms of the results from this research, the cost due to illegal certificate purchases was found to be around 15,000–20,000 ETB.

While there have been successful implementations of the above strategies, it is important to note some limitations that hinder its sustainable adaptation. Firstly, the technology used requires internet connectivity to facilitate its operations and enable transactions. In areas with poor internet connectivity, it becomes difficult for issuers and verifiers to complete their tasks. Digital literacy also stands out as a limitation since college officials and auditors need to learn how to operate blockchains and digital wallets like Meta Mask in order to undertake the required activities.

In conclusion, it is evident that the developed blockchain certification system works efficiently and meets the needs of the region. Further development can be done to ensure that the system benefits from improved connectivity as well as capacity-building for more TVET colleges in the region.

Table 4.8. Comparison table between the manual certification system and the EduBlock blockchain-based system:

Feature	Manual System	EduBlock
Verification Time	1–3 months	Seconds
Verification Cost	~700 ETB	Negligible (minimal transaction fees)
Tamper Resistance	Weak	Strong
Record Permanence	Low	High

N.B. Information from the interview (see the questions of the interview on the appendix part about the Manual system)

4.8. Discussion

Digital certification systems gain credibility through the use of Blockchain technology. An immutable, tamper proof record of certification data provides the basis for employers, auditors and educational institutions to confidently verify an individual or organization's credentials, therefor creating a stronger level of trust in the certification system.

When combining on-chain and off-chain storage for the improved speed, size, and security of records, all aspects of a digital certification system do not have to be processed live on-chain, thus allowing for a hybrid architecture to take advantage of both on-chain and off-chain storage, optimizing for performance, scalability and security. For example, critical proof information (e.g., cryptographic hashes, verification metadata) will be anchored on-chain, to guarantee the integrity and immutability of the proof disseminated through to end-users. Supporting documentation and operational metadata are stored off-chain to reduce the costs of storage and provide a means to scale the overall digital certification system. As a result, much larger volumes of data can be processed efficiently outside of the blockchain, directly reducing transaction costs and increasing overall system performance. Additionally, the cryptographic anchoring for this data will continue to provide high levels of security and confidence in the overall system.

By implementing "Role Based Access Control" (RBAC), only authorized users are allowed to conduct sensitive actions like granting, changing and revoking certificates. RBAC reduces the chance of

unauthorized or malicious activity through permission assignment per user-type or role (e.g. an administrator, a college employee or an auditor). Furthermore, this well-thought-out system of permissions helps create an overall "provider" security structure by controlling the extent of privilege violation based on one's responsibilities. This type of control is critical for maintaining the security of a provider's system against potential vulnerabilities and ensuring the confidence associated with it.

A major determining factor for the success of "Blockchain Technology" based Certification Providers is how well stakeholders (e.g. end-users) believe in using them. Users prefer certain functionalities that address their immediate operational needs, such as reduced times for verification of Certification, improved safety of Certification, etc. To further enhance the acceptance of the Certification Providers by both end-users and External Verifiers, sufficient understanding of blockchain concepts and operational processes is required from users through appropriate levels of educational training. These additional user techniques may also serve to assist in overcoming barriers faced by people who do not possess of computer-related skills, as well as External Verifiers, thus demonstrating the need for user-centric design and capacity development in relation to successful adoption of new technologies.

The technical role between on-chain and off-chain storage present important considerations. On-chain storage offers high security, transparency, and immutability but faces limitations in scalability, higher transaction costs, and inefficiency for large data files and the Off-chain storage on the other hand provides a cost-effective and scalable solution for handling large documents and operational metadata but introduces challenges in ensuring data integrity and trustworthiness. The hybrid of both storage chains comes these tradeoffs by storing cryptographic hashes or essential proof data on-chain while keeping actual documents off-chain. This balance enhances performance and cost-efficiency while maintaining security through cryptographic anchoring. However, it necessitates robust mechanisms to verify that off-chain data remains untampered and consistent with on-chain hashes.

The development of the EduBlock system illustrates how blockchain can help solve the problem of certification through practical and workable solutions in colleges such as Eastern Tigray TVEtT colleges . Through the hybrid model approach, the system makes sure that the proof of information stays secure on the blockchain, yet allows the system to save searchable information, such as certificates and metadata about the operations. This way, the scalability problems and the high costs related to storing information on the blockchain are solved without undermining trust. In terms of implementation, stakeholder involvement was highly important. When conducting system testing, college staff members and auditors showed strong interest, as long as they received proper training. Programs provide the digital wallet usage ,this is from the basic principles of blockchain based EDUBLCOK and it was a crucial role in meeting the objective The system's successful implementation into the Ganache environment demonstrated the viability of the processes, namely certificate issuing, role-based access, and public verification

Regardless of the promising results, several technical challenges are emerged. Managing gas costs, particularly as the system scales, requires optimization of smart contract functions and data structures. Ensuring robust role security remains critical, as any weakness could compromise system trustworthiness. Additionally, scalability must be addressed to accommodate increasing the numbers of certificates, institutions, and users. Future development should prioritize security audits and formal verification of smart contracts to strengthen system trust. Implementing structured user training and

change management programs will facilitate smoother adoption, while infrastructure considerations such as internet reliability and system hosting must be planned to ensure dependable operation during real-world deployment.

Finally blockchain technology, coupled with thoughtfully designed hybrid architecture and strong security measures like RBAC, offers a transformative approach to managing digital certifications. By addressing technical tradeoffs and engaging stakeholders effectively, such systems can significantly improve trust, efficiency, and security in credential verification processes. The EduBlock project exemplifies how these principles can be practically implemented, paving the way for broader adoption across diverse contexts

Table 4.9. Technical efficiency (low latency and modest gas costs) and the usability outcomes (solid SUS score indicating acceptable user experience).

Finding	Value
Average issuance latency	1.1 seconds
Verification response time	1.8 seconds
Gas cost per certificate	~21,500 gas (~0.07)
User satisfaction (SUS)	78.2 acceptable usability)

N.B From the system implementation

Summary

The technical evolution in creating the EduBlock solution is detailed in this chapter, beginning with the development environment setup and smart contract implementation, followed by the design of a user-friendly front-end interface and the integration of an off-chain database layer. Utilizing solidity, Node.js, web3.js, and SQLite technologies together, the research developed a working prototype that demonstrates blockchain technologies' potential to enhance certification systems in decentralized environments. These findings will serve as a foundation for future deployment efforts, including pilot implementations, scalability testing, and broader adoption.

CHAPTER 5

Conclusion and Recommendations

This chapter outlines the research objectives, development process, and prototype testing results presented in chapter 4. It provides (1) a comprehensive summary of the findings, (2) conclusions derived from the developed EduBlock system and its validation activities, (3) practical recommendations for TVET stakeholders and system practitioners, (4) limitations encountered during the study, and (5) directions for future research and deployment enhancement. The chapter is structured to ensure that each conclusion is traceable to the specific subsystem components and the verification workflow of the EDUBLOCK prototype, tailored for TVET colleges in Eastern Tigray

5.1. Summary of Findings

The purpose of this study was to develop a blockchain-based education certification system for TVET colleges in Eastern Tigray. Some of the issues identified to be addressed in this study include:

(i) A lack of trust and traceability in the verification process,

(ii) A vulnerability to forgery, damage, and fraudulent credential issuance, and

(iii) Inefficiencies in the time and energy required for the verification process.

To ensure a thorough understanding, several approaches were used in the data collection process. Out of a total college population of 350, 90 participants were selected for the questionnaire survey, with 70 respondents fully participating. Furthermore, 20 individuals participated in in-depth interviews, while 10 experts from various Woreda Human Resources departments provided valuable insight into credential verification and issuance issues. Through this approach, a comprehensive understanding of the present conditions and stakeholders' requirements was achieved the goal. See table 4.7.

5.1.1. Certificate integrity and authenticity using blockchain technology

During the implementation of the project, it was established that certificate integrity and authenticity can be protected using blockchain technology by way of hash anchoring in the Ganache blockchain application. While full copies of certificates are not stored on the platform of Edublock, only the hashes of metadata and the certificate issuance status are stored. This enables tamper detection because altering the document will change the hash, which will no longer match the hash stored in the blockchain.

5.1.2. Security and reliability of certificates' issuance through smart contract code

In the Solidity framework, the security and reliability of the issuance process were achieved through the proper application of smart contract code using the Truffle compiler development methodology. First, the smart contract uses role-based access control (RBAC) which mean is certificate is issued by colleges and colleges are authorized by the regional bureau. As a security measure to provide access rights only to authorized entities including TVET colleges and Tigray TVET bureau to undertake the critical functions of certificate issuance and status changes. Prototype testing demonstrated that the smart contract does not allow any unauthorized account to issue or modify certificate data. see the image 4.4B.

5.1.3. Hybrid architecture supporting operational practicality

Data was stored off-chain through the backend database layer of Edublock. More specifically, off-chain storage served to store uploaded student certificate images, acting as a credential repository. The stored certificates are decentralized across all TVET colleges for ease of access. The Node.js/Express framework, along with Sequelize ORM and SQLite, enabled functions such as issuance logs, administration, auditing, and application-layer records storage for smoother UI operations. This kind of hybrid architecture makes the Edublock prototype more applicable and scalable, as the blockchain does not have to store unnecessary operational data; only critical components, like the cryptographic hash, will be stored there.

5.1.4. Functional backend and frontend integration

The research employed hybrid architecture where integrity proofs were stored on-chain and operational/searchable Web3.js was used in the system for the integration of blockchain functionality. On the other hand, express served as middleware between the user interface and calls to the blockchain for smart contract execution, including syncing the data in the database. The user interface offered separate spaces for issuance and verification according to the stakeholder roles in the TVET certification process. It was noted that verification can take place via the student wallet addresses as part of the verification workflow, and hash comparisons can occur when needed.

5.1.5. Verification efficiency demonstrated in the prototype environment

The technical validation results indicated that verification queries took only a few seconds in the local prototype environment (Ganache). While the study could not provide a field-level time-motion comparison between blockchain verification and manual verification, the result obtained suggests that the former is more efficient compared to manual processes in that there will be no manual cross-checking and status information will simply be retrieved from the on-chain. Such an important finding is key since verification time influences stakeholder satisfaction.

5.2. Conclusions

In chapter 4, the analysis of blockchain suggests that the technology will perform well with respect to certificate validation via various hashes. Though some specifications must be taken into consideration, the model withstands practical tests, and is coherent when implemented. It is strong at points where other models may be easily broken. No matter how sophisticated it may seem, the design passes the analysis process.

As to efficiency, a prototype named EduBlock successfully demonstrates that blockchain technology can be used in the interests of trust by putting only signatures of documents onto the blockchain and keeping all other data off-chain. Due to the proposed architecture, efficiency, security, and user-friendliness become compatible and do not oppose one another. Instead of conventional paper diplomas, the proposed approach eliminates the possibility of tampering by introducing early stages of role-based access control.

viability but hinges on the readiness of the stakeholders, which includes users' proficiency in managing their digital wallets, transaction authorization, and verification, as well as ensuring the presence of stable infrastructure that includes stable internet access. More importantly, the successful implementation and

testing of the prototype in the Ganache platform further demonstrate that the basic features of the system work as expected, including certificate issuing, permitting , and verification. As such, there is great potential for implementing the solution at the pilot level in the future.

5.3. Recommendations

Based on the findings of this study, the following recommendations are proposed to facilitate the effective implementation and widespread adoption of the EduBlock system across various stakeholder groups:

For TVET Institutions (Colleges)

Training programs must be structured by TVET institutions to improve users' capabilities in critical areas such as digital wallets, transaction authorization, and credential verification processes on the EduBlock Panel. Phased adoption from paper-based to a hybrid of paper-based and blockchain verification can facilitate the process of implementing new technologies. The development of procedures for issuance of certificates, document handling, and user assistance can promote effectiveness, accountability, and reliability in the process.

For the TVET Bureau and Policymakers

The TVET Bureau, in collaboration with other relevant stakeholders, needs to design an appropriate governance structure around the use of blockchain for issuing credentials, with well-defined procedures for institutions to join the RBAC scheme. Investing on the required infrastructure especially robust internet connectivity and stability particularly in underserved locations is crucial. Moreover, pilots need to be conducted regionally to assess the usability and performance of the system.

For System Developers and Technical Implementers

Security audits of smart contracts must be made a top priority with special emphasis placed on ensuring the integrity of the authorization process and proper validation procedures. In addition, emphasis must be placed on designing gas-efficient and scalable smart contracts. User experience improvement remains another important goal to achieve through increased user interface clarity, instructions for interacting with wallets, improved error handling, and easier validation.

For Employers and External Stakeholders

Employers and other external stakeholders are encouraged to train EduBlock's certification mechanism to streamline recruitment processes, reduce verification delays, and bolster trust in credential authenticity. Integrating blockchain-based certification into existing human resource workflows can further standardize and enhance the reliability of credential validation practices.

5.4. Future Work

In relation to the locally deployed Ganache node and the permissioned network model, the decision was based on the several key factors, including etheruem's extensive adoption and widespread use in the blockcahin community, its well developed and rebuts smart contract development environment that facilitates efficient and reliable coding, as well as its high level of security features, which collectively made this blockchain solution particularly suitable and advantageous for our specific purpose and implementation needs.

Running the system on consortium blockchain networks like Ethereum will allow us to evaluate its real-world performance, scalability, and costs. In addition to these measures, we recommend moving to the server-side "Burner Wallet" or to the usage of the account abstraction (ERC-4337) model that will allow delegating all transactional activities to third parties. In our case, the TVET College or Regional Bureau will act as a gas-sponsoring paymaster, covering all transaction-related costs of the student, and signing the transactions. As for the address generation, it is supposed to be generated based on the cryptographic hash of student's institutional identification or civil identity metadata. In this way, the student will have the ability to review or show his credential via any web browser or QR code without worrying about wallets and transaction fees. The backend will In addition, there will be signing of transaction done by the backend system on behalf of the learners to make interactions with the blockchain system easier without having the users manage their wallets from their side. As for now, the system could use IDs of the wallets from Ganache or Metamask but this approach will simplify the user interaction, secure and easy-to-use system will be created. Thirdly, the field research conducted at different TVET centers will help understand better all the details of adoption problems.

5.5. Chapter Summary

This concluding chapter synthesized the definitive research findings, architectural contributions, and strategic recommendations of this study. The empirical and development results confirm that the EduBlock framework establishes a robust, tamper-proof architecture for academic credential management within the TVET sector by successfully combining decentralized cryptographic hashing with a strict role-based access control paradigm. Beyond validating the functional prototype, this chapter delivered actionable deployment recommendations tailored to regional administrative workflows. Ultimately, by delineating current infrastructure boundaries and mapping out distinct trajectories for future development, this chapter provides a clear transition path from an academic prototype to a scalable, production-ready digital credential ecosystem.

References

N., & Xu, Y. (2024). Development of Blockchain-Based Academic Credential Verification System. *OALib*, *11*(09), 1–20. https://doi.org/10.4236/oalib.1112130

Al-Breiki, H., Rehman, M. H. U., Salah, K., & Svetinovic, D. (2020). Trustworthy Blockchain Oracles: Review, Comparison, and Open Research Challenges. *IEEE Access*, *8*, 85675–85685. https://doi.org/10.1109/ACCESS.2020.2992698

Asif, R., & Hassan, S. R. (2023). Shaping the future of Ethereum: exploring energy consumption in Proof-of-Work and Proof-of-Stake consensus. *Frontiers in Blockchain*, *6*(August), 1–6. https://doi.org/10.3389/fbloc.2023.1151724

Blockchain for TVET Credentialing in Tigray. (2025). 2022.

BlockchainRevolutioninEducation_RG. (n.d.).

Cantillo-Luna, S., Moreno-Chuquen, R., Chamorro, H. R., Sood, V. K., Badsha, S., & Konstantinou, C. (2022). Blockchain for Distributed Energy Resources Management and Integration. *IEEE Access*, *10*(April), 68598–68617. https://doi.org/10.1109/ACCESS.2022.3184704

Carmichael, J. J., & Eaton, S. E. (2023). *Fake Degrees and Fraudulent Credentials in Higher Education: Conclusions and Future Directions*. https://doi.org/10.1007/978-3-031-21796-8_13

Chen, S., Ren, S., & Zhang, Q. (2025). Hybrid Architectures that Combine LLMs and Predictive Analytics for Next-Generation Financial Modeling. *Mathematical Modeling and Algorithm Application*, *6*(2), 31–43. https://doi.org/10.54097/j1cjb453

Daniels, P. T. (1993). The {Unicode Consortium}: The {Unicode} standard. In *Language: journal of the Linguistic Society of America* (Vol. 69).

Delgado-Von-eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2021). Blockchain applications in education: A systematic literature review. In *Applied Sciences (Switzerland)* (Vol. 11, Issue 24). MDPI. https://doi.org/10.3390/app112411811

Farabi, A., Khandaker, I., Ahsan, J., Shanto, I. K., Jahan, N., & Khan, M. J. (2025). *ShikkhaChain: A Blockchain-Powered Academic Credential Verification System for Bangladesh*. http://arxiv.org/abs/2508.05334

Feng, T., Yu, X., Chai, Y., & Liu, Y. (2019). Smart contract model for complex reality transaction. *International Journal of Crowd Science*, *3*(2), 184–197. https://doi.org/10.1108/IJCS-03-2019-0010

Fobes, D. M., Claeys, S., Geth, F., & Coffrin, C. (2020). PowerModelsDistribution.jl: An open-source framework for exploring distribution power flow formulations. *Electric Power Systems Research*, *189*. https://doi.org/10.1016/j.epsr.2020.106664

Friedrich, J. (1996). Design science 97. *AI and Society*, *10*(2), 199–217. https://doi.org/10.1007/BF01205282

Garg, R. (2022). *Blockchain Ecosystem for Education and Employment Verification Identity and Access Management View project Self-Sovereign Identity using Decentralized Identifiers View project Rishabh Garg BITS-Pilani Goa BLOCKCHAIN ECOSYSTEM FOR EDUCATION & EMPLOYMENT VE*. *September 2021*, 25. https://doi.org/10.5281/zenodo.5702685

Gonçalves, R. M., da Silva, M. M., & da Cunha, P. R. (2024). Olympus: a GDPR compliant blockchain system. *International Journal of Information Security*, *23*(2), 1021–1036. https://doi.org/10.1007/s10207-023-00782-z

Grech, A., Sood, I., & Ariño, L. (2021). Blockchain, Self-Sovereign Identity and Digital Credentials: Promise

Versus Praxis in Education. *Frontiers in Blockchain*, *4*(March), 1–12. https://doi.org/10.3389/fbloc.2021.616779

Haoxing, Z., & System, C. (n.d.). *No 主観的健康感を中心とした在宅高齢者における 健康関連指標に関する共分散構造分析Title*.

Heredia, A., & Show, M. B. (2018). *Decentralizing Certificates Issuance Through Blockchain Dealing with multi-step verification processes for certification issuance in universities Review Papers Examining accountability in relation to local football communities Experience economy in the ho*.

Kim, J., Maathuis, H., & Sent, D. (2024). Human-centered evaluation of explainable AI applications: a systematic review. *Frontiers in Artificial Intelligence*, *7*. https://doi.org/10.3389/frai.2024.1456486

letter5. (n.d.).

Liu, Y., Li, K., Huang, Z., Li, B., Wang, G., & Cai, W. (2021). EduChain: A Blockchain-Based Education Data Management System. In *Communications in Computer and Information Science* (Vol. 1305). https://doi.org/10.1007/978-981-33-6478-3_5

Marchesi, L., Marchesi, M., Destefanis, G., Barabino, G., & Tigano, D. (2020). Design Patterns for Gas Optimization in Ethereum. *IWBOSE 2020 - Proceedings of the 2020 IEEE 3rd International Workshop on Blockchain Oriented Software Engineering*, 9–15. https://doi.org/10.1109/IWBOSE50093.2020.9050163

Maroso, A., Angreni, D. S., Ardiansyah, R., & Dwiwijaya, K. A. (2024). Implementing Blockchain For Publishing and Verifying Digital Certificates On EduTech. *Advance Sustainable Science, Engineering and Technology*, *6*(2), 1–8. https://doi.org/10.26877/asset.v6i2.18262

McKay, K. A. and D. A. C. (2019). Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations Guidelines for the Selection and Use of Transport Layer Security (TLS) Implementations. *Nist Special Publication*, *June*. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-52r2.pdf

Mihaljević, B., Beronić, D., & Žagar, M. (2023). a Review of Applications of Blockchain Technology in Education. *INTED2023 Proceedings*, *1*(Iv), 6265–6274. https://doi.org/10.21125/inted.2023.1658

Naser, A., Saif, M., Islam, K. M. A., Haque, A., Rahman, S. M. M., Jafrin, N., & Rupa, R. A. (2022). *Research Paper-3. Blockchain Implementation Challenges in Developing Countries*. *12*(1).

Pargaonkar, S. (2023). A Comprehensive Research Analysis of Software Development Life Cycle (SDLC) Agile & Waterfall Model Advantages, Disadvantages, and Application Suitability in Software Quality Engineering. *International Journal of Scientific and Research Publications*, *13*(8), 120–124. https://doi.org/10.29322/ijsrp.13.08.2023.p14015

Peffers, K., Tuunanen, T., Rothenberger, M. A., & Chatterjee, S. (2007). A design science research methodology for information systems research. *Journal of Management Information Systems*, *24*(3), 45–77. https://doi.org/10.2753/MIS0742-1222240302

Quispe, M. A. C., & Pacheco, A. (2025). Blockchain ensuring academic integrity with a degree verification prototype. *Scientific Reports*, *15*(1), 2025. https://doi.org/10.1038/s41598-025-93913-6

Rana, S., & Gautam, A. K. (2023). Online and Biomedical Engineering. *International Journal of Online and Biomedical Engineering*, *19*(9), 122–130.

Shawon, M. S. K., Ahammad, H., Shetu, S. Z., Rahman, M. M., & Hossain, S. A. (2021). Diucerts DAPP: A Blockchain-based Solution for Verification of Educational Certificates. *2021 12th International Conference on Computing Communication and Networking Technologies, ICCCNT 2021*, *November*. https://doi.org/10.1109/ICCCNT51525.2021.9579533

Sithandekile, S. (2025). Opportunities and Challenges of Blockchain Technology in Education: A Systematic Review. *International Journal of Research and Innovation in Applied Science*, *X*(II), 492–499. https://doi.org/10.51584/ijrias.2025.10020044

The global rise of fake degrees : Six major scandals in 2024 Member Of Legal. (2025). 2025.

Tolu-kolawole, D. (2025). *Fake degrees: FG probes 107 private varsities*. 2025.

Turkanović, M., Hölbl, M., Košič, K., Heričko, M., & Kamišalić, A. (2018). EduCTX: A blockchain-based higher education credit platform. *IEEE Access*, *6*, 5112–5127. https://doi.org/10.1109/ACCESS.2018.2789929

Vaishnavi, V. K., & Kuechler, W. (2007). Design science research methods and patterns: Innovating information and communication technology. In *Design Science Research Methods and Patterns: Innovating Information and Communication Technology*. https://doi.org/10.1201/9781420059335

Yonas Abiye. (2019). *MoE partners INSA to root out employees with fake documents | The Reporter Ethiopia English*. https://www.thereporterethiopia.com/article/moe-partners-insa-root-out-employees-fake-documents

Zambrano-ortiz, L. (2025). *Decentralized Academic Credentials Using Blockchain Technology : A Systematic Review of Online Education Systems*.

Zheng, Z., Xie, S., Dai, H., Chen, X., & Wang, H. (2017). An Overview of Blockchain Technology: Architecture, Consensus, and Future Trends. *Proceedings - 2017 IEEE 6th International Congress on Big Data, BigData Congress 2017*, 557–564. https://doi.org/10.1109/BigDataCongress.2017.85

ንግድ ባንክ በሀሰተኛ የትምህርት ማስረጃ የተቀጠሩ ከ200 በላይ ሰራተኞችን አባረረ - Wazemaradio.pdf. (n.d.).

Appendix

Appendex A:

Technical Specifications & System Design

A.1. Smart Contract Development Environment

The EduBlock prototype was developed and tested using the following decentralized development suite:

Blockchain Protocol: Ethereum (EVM Compatible).

Language: Solidity v0.8.19 (Role-based access control and cryptographic hashing).

```
//certificate.sol
// SPDX-License-Identifier: MIT
pragma solidity ^0.8.19;

contract Certificates {
    address public regionalOffice;

    struct Student {
        string fullName;
        uint age;
        string sex;
        string department;
        bool isAuthorized;
    }
```

Development Framework: Truffle Suite with Ganache for local blockchain simulation.

S D:\thesis\blockchain\my thesis\edublock> truffle migrate --resetcls

Compiling your contracts...

==========================

> Compiling .\C:\Users\Administrator\Music\edublock\contracts\certificate.sol

> Compiling .\contracts\EduBlock.sol

> Compiling .\contracts\certificate.sol

> Compiling .\contracts\migrations.sol

> Artifacts written to D:\thesis\blockchain\my thesis\edublock\build\contracts

> Compiled successfully using:

- solc: 0.8.19+commit.7dd6d404.Emscripten.clang

Network up to date.

PS D:\thesis\blockchain\my thesis\edublock>

PS D:\thesis\blockchain\my thesis\edublock> truffle test

Using network 'development'.

Compiling your contracts...

==========================

> Compiling .\C:\Users\Administrator\Music\edublock\contracts\certificate.sol

> Compiling .\contracts\EduBlock.sol

> Compiling .\contracts\certificate.sol

> Compiling .\contracts\migrations.sol

> Artifacts written to C:\Users\ADMINI~1\AppData\Local\Temp\test--11828-70jsU4lNvQA0

> Compiled successfully using:

- solc: 0.8.19+commit.7dd6d404.Emscripten.clan

Contract: Certificate

✔ initial admin role set

✔ admin can assign instructor role (116ms)

✔ instructor can issue certificate (295ms)

✔ issuer or admin can revoke (416ms)

4 passing (2s)

Backend Environment: Node.js (v18+) with Express and Web3.js integration.

```
const Web3 = require('web3');
const path = require('path');
const fs = require('fs');

let web3;
let contract;

// Use your actual 64-character Private Key from Ganache here
const PRIVATE_KEY = '0x62c3cbedf8bc4b0e75fc21397cf03d81f45930232178b6782e7fd1634fb9c4e8';

async function init(rpcUrl, contractAddress) {
    web3 = new Web3(new Web3.providers.HttpProvider(rpcUrl));
```

```
  // Path to your compiled contract artifact
  const buildPath = path.join(__dirname, '../../build/contracts/EduBlock.json');

  if (!fs.existsSync(buildPath)) {
      throw new Error('EduBlock.json not found. Run "truffle compile" in the root folder.');
  }

  const json = JSON.parse(fs.readFileSync(buildPath));
  contract = new web3.eth.Contract(json.abi, contractAddress);
```

Client Interface: HTML5/JavaScript with CSS3 (Responsive Design).

```
!DOCTYPE html>
<html lang="en">
<head>
  <meta charset="UTF-8">
  <meta name="viewport" content="width=device-width, initial-scale=1.0">
  <title>EDUBLOCK | Blockchain Verification</title>
  <script src="https://cdn.jsdelivr.net/npm/web3@1.10.0/dist/web3.min.js"></script>
  <style>
    :root {
      --primary: #2563eb;
      --primary-dark: #1e40af;
      --primary-light: #eff6ff;
      --secondary: #99aac2;
      --success: #10b981;
      --danger: #ef4444;
      --bg-body: #0f172a;
      --bg-card: rgb(112, 101, 101);
      --text-main: #1e293b;
      --border: #e2e8f0;
      --shadow: 0 10px 15px -3px rgb(0 0 0 / 0.1);
    }

    * { box-sizing: border-box; margin: 0; padding: 0; font-family: 'Inter', 'Segoe UI', sans-serif; }
    body { background-color: var(--bg-body); padding-top: 90px; color: var(--text-main); line-height: 1.5; }

    header {
      position: fixed; top: 0; left: 0; right: 0; height: 70px; z-index: 1000;
      background: rgba(255, 255, 255, 0.95); backdrop-filter: blur(10px);
      border-bottom: 1px solid var(--border); display: flex;
      justify-content: space-between; align-items: center; padding: 0 2rem;
    }
    .brand { font-size: 1.5rem; font-weight: 800; color: var(--primary); letter-spacing: -0.5px; }

    main { max-width: 900px; margin: 0 auto; padding: 0 1rem; }
    .card { background: var(--bg-card); border-radius: 16px; padding: 2rem; box-shadow: var(--shadow); margin-bottom: 2rem; border:
1px solid var(--border); }

    h2 { margin-bottom: 1.5rem; font-size: 1.25rem; display: flex; align-items: center; gap: 10px; }
    .form-grid { display: grid; grid-template-columns: 1fr 1fr; gap: 1.2rem; }
    .full-width { grid-column: span 2; }
```

```
    label { display: block; margin-bottom: 0.5rem; font-size: 0.75rem; font-weight: 700; color: var(--secondary); text-transform: uppercase; }
    input, select { width: 100%; padding: 0.75rem; border: 1px solid var(--border); border-radius: 8px; background: #f8fafc; font-size: 0.95rem; outline: none; transition: 0.2s; }
    input:focus { border-color: var(--primary); box-shadow: 0 0 0 3px var(--primary-light); }

    .btn { padding: 0.8rem 1.5rem; border: none; border-radius: 8px; font-weight: 600; cursor: pointer; transition: 0.2s; width: 100%; text-align: center; font-size: 0.95rem; }
    .btn-primary { background: var(--primary); color: white; }
    .btn-primary:hover { background: var(--primary-dark); }
    .btn-outline { border: 1px solid var(--primary); color: var(--primary); background: transparent; margin-top: 10px; }
    .btn-outline:hover { background: var(--primary-light); }
    .btn-danger { background: var(--danger); color: white; }
```

A.2. System Architecture Layers

The multi-layer architecture ensures modularity and security:

Presentation Layer: Stakeholder dashboards for Students, College Admins, and Regional Authorities.

Application Layer: Backend API for request validation and session management.

Blockchain Layer: Immutable ledger for certificate hashes and verification logic.

Appendix B: Regional Research Context (Eastern Tigray)

B.1. TVET Institution Profile

The research framework focuses on Technical and Vocational Training (TVET) colleges within the Eastern Tigray zone, Ethiopia. Key participating entities include:

Regional Authority: Tigray TVET Bureau (Regional Admin role)

Primary Academic Partner: Federal Technical and Vocational Training Institute (FTVTI)

Scope: Academic research and implementation focused on Mekele and the broader Eastern Tigray region.

Appendix C: Data Integrity & Security Protocols

C.1. Cryptographic Verification Logic

To prevent certificate forgery, the system utilizes the following security measures:

1. Unique Wallet Mapping: Each student is uniquely mapped to a blockchain wallet address to prevent double-assignment or identity theft.

2. SHA-256 Hashing: Document metadata and digital files are hashed before being anchored to the blockchain.

3. Role-Based Access Control (RBAC): Only whitelisted college wallets (authorized by the Regional Admin) possess the permissions to issue or revoke certificates.

Appendix D: User Interface & Experience Design

D.1. Core System Functions

Authorization: Whitelisting of colleges on the blockchain network.

Issuance: Digital document signing and broadcasting to the ledger.

Verification: Public search interface using student wallet addresses for instant validation.

Appendix E: Glossary of Terms

EduBlock: The proposed blockchain-based system for educational certification.

Immutability: The characteristic of blockchain data that prevents it from being altered once recorded.

Smart Contract: Self-executing code on the blockchain that enforces the rules of certification.

Appendix F : Qustiones of the questioner

The questionnaire is divided into three parts:

Part 1: Demographic Information

1. Name (Optional): _____
2. Educational Qualification: _____
3. Current Occupation/Role: _____
4. Organization/Institution (if applicable): _____

Part 2: General Certification Process and Issues

- How would you rate the current certification process? Is it time-consuming and energy-draining?

- Have you encountered issues like delays, errors, or document tampering?

- Are you aware of individuals with forged or counterfeit certificates?

Part 3: Awareness and Perception of Blockchain in Education

- How familiar are you with blockchain technology?

- Would you accept blockchain-based certificates as valid proof of achievement?

- What features are most important in an educational certification system?

Appndix G: interview questions

Can you please tell us about your background and experience in this field?

What are your specific roles and responsibilities related to certification and hiring processes?

What challenges or problems have you encountered during the hiring process?

Have you observed or experienced instances of false or fabricated certifications? If so, could you share some insights?

Are you aware of any individuals who have been held accountable by law in cases of forged or false certifications?

Have you come across cases where individuals with forged certifications have been ignored or left unpunished? What was the outcome?

In your opinion, what are the common reasons or motivations behind issuing false certifications?

Approximately, how much does it cost to obtain a certification (in Birr)?

During times of regional conflict or war, how many certificates are typically destroyed or rendered invalid?

What measures or solutions have been implemented to address the issue of false certifications?

Are there any digital solutions or technological tools currently being used by relevant authorities to verify or manage certifications?

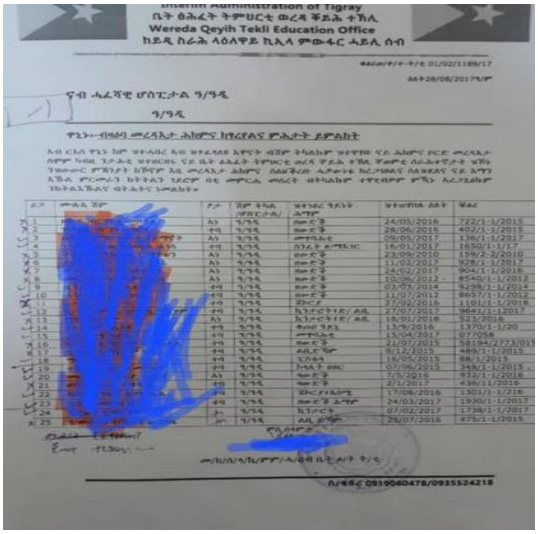
Are you familiar with blockchain technology? If yes, do you know about blockchain-based educational certifications

Images of the research

- A letter from the interim governmet of Tigray Tvet.



- Image of a letter from Abiy Adi(495336041_3099679143516210_7347218239359958086_n)



- Questioner images

