

Dr.FANS: A Decentralized Micro-credential Verification System Towards Higher Qualifications

by

Abrar Mahbub Tanim (201014073)
Md. Foysal Hossain (181014105)
Humira Saria (201014013)

*Project report (CSE499) submitted in partial fulfillment of the
requirements for the degree of*

Bachelor of Science in Computer Science and Engineering

Under the supervision of

Dr. Nafees Mansoor



DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
UNIVERSITY OF LIBERAL ARTS BANGLADESH

FALL 2024

© *Abrar Mahbub Tanim*

© *Md. Foysal Hossain*

© *Humira Saria*

All rights reserved

DECLARATION

Project Title Dr.FANS: A Decentralized Micro-credential Verification System
Towards Higher Qualifications
Authors Abrar Mahbub Tanim, Md. Foysal Hossain, Humira Saria
Student IDs 201014073, 181014105, 201014013
Supervisor Dr. Nafees Mansoor

We declare that this project report entitled *Dr.FANS: A Decentralized Micro-credential Verification System Towards Higher Qualifications* is the result of our own work except as cited in the references. The project report has not been accepted for any degree and is not concurrently submitted in candidature of any other degree.

Abrar Mahbub Tanim
201014073

Department of Computer Science and Engineering
University of Liberal Arts Bangladesh

Md. Foysal Hossain
181014105

Department of Computer Science and Engineering
University of Liberal Arts Bangladesh

Humira Saria
201014013

Department of Computer Science and Engineering
University of Liberal Arts Bangladesh

Date: January 30, 2025

CERTIFICATE

This is to certify that the project report entitled **Dr.FANS: A Decentralized Micro-credential Verification System Towards Higher Qualifications**, submitted by **Abrar Mahbub Tanim, Md. Foysal Hossain, Humira Saria** (Student ID: 201014073, 181014105, 201014013) are undergraduate students of the **Department of Computer Science and Engineering** has been examined. Upon recommendation by the examination committee, we hereby accord our approval of it as the presented work and submitted report fulfill the requirements for its acceptance in partial fulfillment for the degree of *Bachelor of Science in Computer Science and Engineering*.

Dr. Nafees Mansoor, Associate Professor

Dept. of CSE, University of Liberal Arts Bangladesh

**Prof. Muhammad Golam Kibria, PhD, SMIEEE,
Professor & Head (Acting)**

Dept. of CSE, University of Liberal Arts Bangladesh

Raihan Kibria, Senior Lecturer

Dept. of CSE, University of Liberal Arts Bangladesh

Ms. Rubaiya Hafiz, Senior Lecturer

Dept. of CSE, University of Liberal Arts Bangladesh

Place: Dhaka

Date: January 30, 2025

ACKNOWLEDGEMENTS

We would like to express our deep and sincere gratitude to our research supervisor, *Dr. Nafees Mansoor*, for giving us the opportunity to conduct research and providing invaluable guidance throughout this work. His dynamism, vision, sincerity and motivation have deeply inspired us. He has taught us the methodology to carry out the work and to present the works as clearly as possible. It was a great privilege and honor to work and study under his guidance.

We are greatly indebted to our honorable teachers of the Department of Computer Science and Engineering at the University of Liberal Arts Bangladesh who taught us during the course of our study. Without any doubt, their teaching and guidance have completely transformed us to the persons that we are today.

We are extremely thankful to our parents for their unconditional love, endless prayers and caring, and immense sacrifices for educating and preparing us for our future. We would like to say thanks to our friends and relatives for their kind support and care.

Finally, we would like to thank all the people who have supported us to complete the project work directly or indirectly.

Abrar Mahbub Tanim

Md. Foysal Hossain

Humira Saria

University of Liberal Arts Bangladesh

Date: January 30, 2025

Dedicated to
*my Mother and Father for
their continuous efforts in my
betterment. And to my
teammates for their
continuous support in this
project and in my life.*

– Abrar Mahbub Tanim

Dedicated to
*my parents, younger brother,
and my friends (Abrar and
Saria), who were there for me
when I needed support during
this long journey.*

– Md. Foysal Hossain

To Dr.FANS
The Team.

– Humira Saria

ABSTRACT

Micro-credentials are transparent, competency-based qualifications that allow individuals to demonstrate specific knowledge and skills in a focused domain. They address the need for flexible, personalized education by offering shorter, verifiable credentials that enhance employability and support lifelong learning, making them especially valuable in today's rapidly evolving workforce. The project focuses on developing a system for the inclusion of credit-bearing micro-credentials into traditional higher education programs while focusing on important issues like flexibility, personalized learning, and credential verification. The growing need for flexible, skill-based certifications from students and employers has highlighted the importance of educational models offering concise, targeted credentials. Credit-bearing micro-credentials allow students to demonstrate validated skills while earning official degrees. However, the existing system has recognition, portability, security, and trust issues. This paper proposes using Hyperledger Besu, a blockchain platform, to manage and verify micro-credentials securely. Furthermore, this paper reviews existing literature related to micro-credential and academic certification, presents various models for credentialing, and discusses the benefits and challenges of approaching those models. Additionally, it introduces three algorithms for smart contract implementation. In terms of performance, the evaluation of the proposed system shows an average block creation time of 2.3 seconds while having a block retrieval time of 3.30 milliseconds, demonstrating reliable functionality. Overall, the study demonstrates how integrating blockchain can enhance the credibility, portability, and acceptance of micro-credentials in the workforce and educational institutions.

Keywords: Credit-bearing Micro-credential, Education, Blockchain, Smart Contract, Hyper-ledger Besu

Contents

1	Introduction	1
1.1	Problem statement	2
1.2	Aims, objectives and Motivation	2
1.2.1	Aims	2
1.2.2	Objective	2
1.2.3	Motivation	2
1.3	Project Specification	3
1.3.1	Secure Credential Verification and Management	3
1.3.2	Decentralized Credential Issuance and Verification	4
1.3.3	Off-Chain Storage with IPFS	4
1.3.4	Course Exemption Requests and Review	5
1.3.5	Functional Requirements	5
1.3.6	Non-Functional Requirements	6
1.4	Outcome	6
1.5	Report Layout	7
1.6	Summary	8
2	Literature Review	9
2.1	Preliminaries	9
2.1.1	Blockchain	9
2.1.2	Consortium Blockchain	10
2.1.3	IPFS	10
2.1.4	Smart Contract	10
2.1.5	Micro-Credential	11
2.2	Related Works	11
2.2.1	Micro-credential and Academic Certification	11
2.2.2	Micro-credetial with Blockchain	13
2.2.3	Blockchain with Academic Certification	16

2.3	Performance Metrics	19
2.3.1	System Design Attributes	20
2.3.1.1	System Complexity	20
2.3.1.2	Off-Chain	20
2.3.1.3	Light Weight Solution	20
2.3.1.4	Scalability	20
2.3.1.5	Interoperability	21
2.3.2	Security & Privacy	21
2.3.2.1	Pseudonymity	21
2.3.2.2	Authenticity	21
2.3.2.3	Confidentiality and Privacy	21
2.3.2.4	Immutability	22
2.3.2.5	Non-Repudiation	22
2.3.3	System Efficiency	22
2.3.3.1	Availability	22
2.3.3.2	Transaction Latency	22
2.3.3.3	Transaction Throughput	23
2.3.3.4	Data Storage Efficiency	23
2.3.4	Blockchain Specific Features	23
2.3.4.1	Smart Contract	23
2.3.4.2	Consensus Base	23
2.3.5	User-centric & Governance Aspects	23
2.3.5.1	Transparency	24
2.3.5.2	User-centric	24
2.3.5.3	Regulatory Compliance	24
2.3.6	Application Specific Parameters	24
2.3.6.1	AI	25
2.3.7	Micro-credential Specific Parameters	25
2.3.7.1	Standardized Metadata	25
2.3.7.2	Granularity	25
2.3.7.3	Stackability	25
2.3.7.4	Digital Badge Image	26
2.3.7.5	Revocation Capability	26
2.3.7.6	Interoperability	26
2.3.7.7	Level-Up	26
2.4	Performance Analysis	26

2.4.1	Performance Analysis of Existing works with Blockchain	27
2.4.2	Performance Analysis of Existing works without blockchain	35
3	Methodology	38
3.1	Introduction	38
3.2	System Development Model	39
3.2.1	Agile Model	39
3.3	System Analysis	40
3.3.1	System Design	41
3.3.2	Implementation	41
3.4	Requirement Engineering	42
3.5	Requirement Engineering Process	42
3.5.1	Feasibility Study	42
3.5.2	Requirement Gathering	43
3.5.3	Software Requirement Specification	43
3.5.4	Software Requirement Validation	44
3.6	Software Requirement for Development	44
3.6.1	Microsoft Visual Studio	44
3.6.2	Remix IDE	45
3.6.3	Truffle	45
3.6.4	NodeJS	46
3.6.5	Metamask	46
3.6.6	Hyperledger Besu	47
3.6.7	Docker	47
3.6.8	Web3.py	47
3.6.9	Prometheus	48
3.6.10	Grafanna	48
3.6.11	MongoDB	48
3.6.12	EtherJS	49
3.6.13	Lucid Chart	49
3.6.14	Mendeley	49
3.6.15	LaTex	50
3.7	Required Programming Language	50
3.7.1	Solidity	50
3.7.2	Python	51
3.7.3	React	51

3.7.4	JavaScript	51
4	Design and Development	53
4.1	Project Management and Financial Activities	53
4.1.1	Work Breakdown Structure	53
4.1.2	Estimate Costs	54
4.1.2.1	Project Planning and Initiation	54
4.1.2.2	Requirements Analysis	55
4.1.2.3	System Design	55
4.1.2.4	Implementation or Coding	55
4.1.2.5	Testing	55
4.1.2.6	Deployment	56
4.1.2.7	Maintenance	56
4.1.3	Budget Plan	56
4.1.4	Funding Plan	57
4.1.4.1	Government Grants	57
4.1.4.2	Investor	57
4.1.4.3	Crowdfunding	57
4.2	System Design and Description	58
4.3	Implementation	60
4.3.1	Smart Contract	60
4.3.2	Deployment of Smart Contract in Hyperledger Besu	62
4.3.3	QBFT Test Accounts	65
4.3.4	Interplanetary Filing System (IPFS)	66
4.4	Web User Interface	67
4.5	Proposed System's Strengths and Limitations	70
5	Business Model	72
5.1	Value Proposition	72
5.2	Customer Segments	72
5.2.1	Higher Education Institutions (HEIs)	72
5.2.2	Employers and Recruiters	72
5.2.3	Micro-Credential Providers (Issuing Bodies)	73
5.2.4	Government and Accreditation Bodies	73
5.3	Channels	73
5.3.1	Direct Engagement with Institutions	73
5.3.2	Online Platform	73

5.3.3	Digital Marketing and Outreach	73
5.3.4	Strategic Partnerships	73
5.4	Customer Relationships	73
5.4.1	Self-Service and Support	74
5.4.2	Training and Onboarding	74
5.4.3	Community Engagement	74
5.5	Revenue Streams	74
5.5.1	Licensing Fees	74
5.5.2	Subscription-Based Model	74
5.5.3	Consulting and Integration Services	74
5.6	Key Resources	74
5.6.1	Technology Infrastructure	75
5.6.2	Human Resources	75
5.6.3	Intellectual Property	75
5.7	Key Activities	75
5.7.1	Research and Development	75
5.7.2	System Deployment and Maintenance	75
5.7.3	User Training and Adoption	75
5.8	Key Partnerships	75
5.8.1	Educational Institutions	76
5.8.2	Micro-Credential Providers	76
5.8.3	Blockchain Networks and Developers	76
5.8.4	Government and Accreditation Bodies	76
5.9	Cost Structure	76
5.9.1	Development and Maintenance	76
5.9.2	Infrastructure Costs	76
5.9.3	Customer Support and Marketing	76
6	Result Analysis	77
6.0.1	Configuration	77
6.0.2	Metric	78
6.0.3	Prometheus and Grafana for Blockchain Metrics	78
6.0.3.1	Using Prometheus and Grafana for Blockchain Metrics . . .	79
6.1	Proposed System's Performance Result	79

7	Conclusions	83
7.1	Social, Legal, Ethical, and Environmental Aspects	83
7.1.1	Social	83
7.1.2	Legal	84
7.1.3	Ethical	85
7.1.4	Environmental	85
7.2	Brief Summary	86
7.3	Future works	87
	References	89
7.4	Addressing Complex Engineering Problems	97
7.4.1	Depth of Knowledge Required	97
7.4.2	Range of Conflicting Requirements	98
7.4.3	Depth of Analysis Required	98
7.4.4	Familiarity of Issues	98
7.4.5	Extent of Applicable Codes	98
7.4.6	Extent of Stakeholder Involvement	99
7.4.7	Interdependence and Conflicting Needs	99

List of Figures

1.1	Workflow of the System	3
2.1	Performance Evaluation Metrics	19
2.2	Performance Analysis of Blockchain Based Solutions	34
2.3	Performance Analysis of Non-blockchain Based Solutions	37
3.1	Agile model	39
4.1	Work Breakdown Structure	54
4.2	Use case diagram of the proposed system	58
4.3	Activity diagram of the proposed system	59
4.4	QBFT Network Structure	63
4.5	ABI File Structure	63
4.6	Smart Contract Deployer	63
4.7	Successful Deployment of the developed Smart Contract	64
4.8	issueToken() Receipt	64
4.9	getToken() Receipt	65
4.10	Allocated accounts for QBFT	65
4.11	IPFS Dashboard	66
4.12	Login Page	68
4.13	Profile Section	68
4.14	Admin Dashboard Page	69
4.15	Issue Token Page	69
4.16	Institution Profile	70
4.17	Database	70
6.1	Block Creation Time with 50 Transactions	79
6.2	Block Creation Time with 100 Transactions	80
6.3	Block Creation Time with 200 Transactions	80
6.4	Block Retrieval Time	81

6.5	Prometheus Dashboard	81
6.6	Grafana Dashboard 1	82
6.7	Grafana Dashboard 2	82

List of Tables

4.1	Cost Breakdown	56
-----	--------------------------	----

Chapter 1

Introduction

With the rapid pace of technological advancements and the evolving nature of work, there is a growing demand for continuous learning and skill development. Following this, the traditional educational models are being supplemented with alternative credential mechanisms. An example of this alternative is micro-credentials. Micro-credentials are defined as bite-sized learning experiences that are competency-based, on-demand, shareable, and personalized [Hunt et al. \(2020\)](#). Micro-credentials offer a more flexible way of recognizing knowledge, skills, and competencies. It allows learners to combine smaller units of learning according to their specific needs and can facilitate lifelong learning [Romasanta & Diloy \(2024\)](#). Another critical factor of micro-credential is the recognition of prior learning, where one can showcase their learnings for further study or to any employers [Wang \(2023\)](#). There is no general definition for micro-credentials, however, according to [Selvaratnam & Sankey \(2021\)](#), micro-credentials can be defined in four ways. Firstly, there are postgraduate short programs that focus on demonstrating outcomes or recognizing prior base learning. Secondly, there are postgraduate programs that involve completing multiple short courses to combine credit in a way that can be accumulated to earn a recognized award like a graduate certificate. Thirdly, undergraduate options exist where short accredited courses can supplement a full program, potentially replacing a few courses within a larger program. Finally, Undergraduate non-accredited or co-curricular courses are designed to enhance a student's job prospects by building their portfolio.

Blockchain is a decentralized and distributed digital ledger that securely records transactions across a network of computers. In the education sector, blockchain provides a tamper-proof and transparent method to store and verify academic records and credentials. Educational institutions can securely store and issue digital certificates with this technology. This eliminates the risk of any intermediaries and also reduces the risk of fraud and falsification of credentials. Moreover, this allows individuals to have more control

over their educational records while focusing on the verification process for different stakeholders involved.

1.1 Problem statement

A significant gap exists in the literature and practice regarding the integration of blockchain technology with credit-bearing micro credentials. With micro credentials being incorporated into formal learning there is a possibility for the credentials be easily replicated, leading to fraudulent proof of learning.

1.2 Aims, objectives and Motivation

1.2.1 Aims

The paper aims to develop a system incorporating credit-bearing micro-credential with traditional learning using blockchain technology. The proposed system uses blockchain technology to securely manage and verify student credentials. It allows educational institutions to set rules and guidelines based on their learning objectives, which can later be used for course exemption. The system also provides students with tokens, enabling them to access their credentials anytime and anywhere.

1.2.2 Objective

- Develop a secure micro credential verification system using blockchain technology.
- Create a network that will help HEI to easily acknowledge the credentials and give exemption of courses based on their policies.

1.2.3 Motivation

Following the financial fallout of COVID-19, both public and private sectors face evolving workforce demands. Students and businesses now seek flexible, cost-effective ways to verify skills [Pirkkalainen et al. \(2023\)](#). Credit-bearing micro-credentials provide a solution by offering transparent, competency-based qualifications that enhance employability and support lifelong learning [McGreal & Olcott Jr \(2022\)](#). These credentials allow students to showcase verified expertise in specific domains, offering greater control over their educational and career paths. Unlike traditional degree-based models, micro-credentials provide short-term, verifiable certifications, but institutions must adapt validation criteria

for employer recognition [Carnevale et al. \(2020\)](#) [Abreu et al. \(2020\)](#). While many focus on non-credit micro-credentials, this system highlights credit-bearing options, which offer immediate value, support degree completion, and create a structured learning pathway [Kishore et al. \(2021a\)](#). Credential management poses challenges as lost printed certificates require lengthy administrative validation. Digital certificates, though convenient, are vulnerable to forgery. Blockchain provides a secure, tamper-resistant system for credit-bearing micro-credentials, ensuring authenticity, reducing fraud, and streamlining verification. By integrating blockchain, this paper proposes a secure, transparent framework to enhance trust and recognition in academic credentialing [Ali & Bhaya \(2021a\)](#) [Jaramillo & Piedra \(2020a\)](#).

1.3 Project Specification

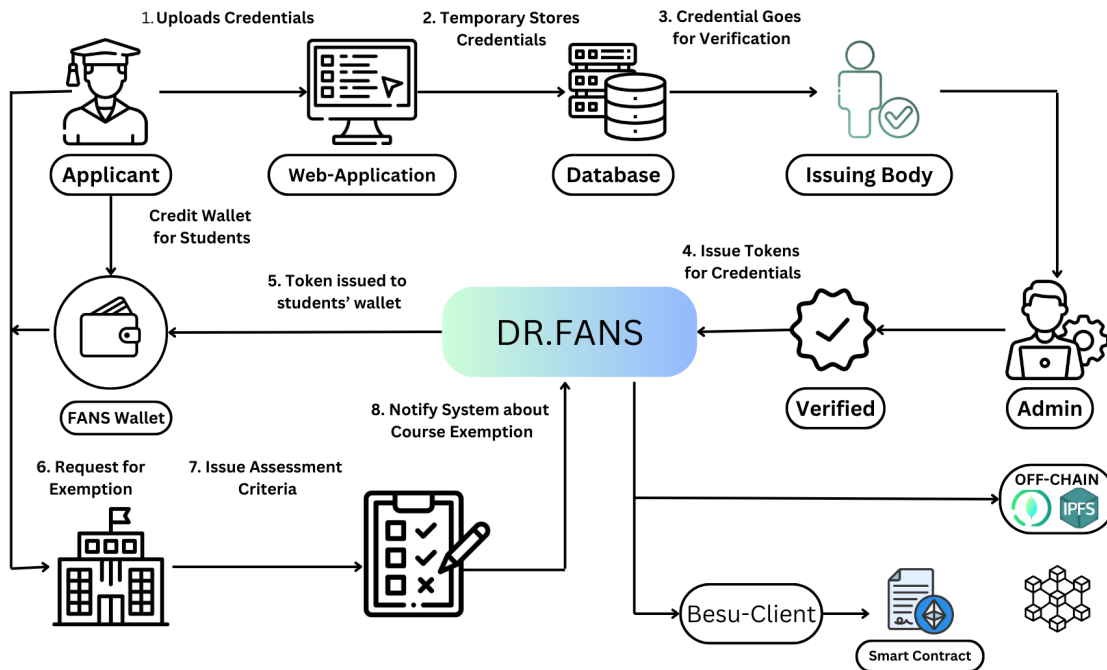


Figure 1.1: Workflow of the System

1.3.1 Secure Credential Verification and Management

The proposed system leverages blockchain technology to provide a secure and decentralized approach for verifying and managing academic credentials. The system ensures

that only authorized institutions can issue and validate credentials while maintaining transparency and tamper-proof security.

- A **trusted authority (TA)** will oversee institutional registration and credential validation within the network.
- Institutions will be onboarded through a verification process where the TA assigns unique identifiers and generates cryptographic keys for credential management.
- Each institution will receive a private-public key pair, which will be used to digitally sign and verify issued credentials.
- Students and issuers will use the public key of the issuing institution to authenticate credential validity without relying on intermediaries.

1.3.2 Decentralized Credential Issuance and Verification

Micro-credential providers will issue credentials in the form of blockchain tokens, ensuring immutability and authenticity. These tokens will contain key details such as student information, course completion, institutional identity, and a reference to off-chain storage for detailed credential records.

- **Smart contracts** deployed on Hyperledger Besu will govern credential issuance, ensuring that only verified institutions can generate tokens.
- Issuing body can revoke credentials if they are found to be fraudulent or invalid.
- Institutions and other verifying entities can retrieve credential details and validate authenticity through blockchain queries.
- The **consortium blockchain model** ensures a permissioned environment where only authorized participants can interact with the system.

1.3.3 Off-Chain Storage with IPFS

To optimize blockchain efficiency, large credential files will be stored using the **Inter Planetary File System (IPFS)**. Only the cryptographic hash (CID) of the stored document will be recorded on the blockchain to ensure data integrity.

- When an institution issues a credential, the document is uploaded to IPFS, and the resulting CID is stored on the blockchain.

- Educational Institutions and verifiers can retrieve the document using the IPFS hash, ensuring that the data remains tamper-proof and accessible.
- This hybrid approach ensures scalability while maintaining a decentralized trust model.

1.3.4 Course Exemption Requests and Review

Once tokens are issued, students can request course exemptions through the system. Institutions can review the verified tokens and, based on their policies, decide whether to grant exemptions.

- Students submit exemption requests linked to their issued tokens.
- Institutions access and verify the student's tokens using the blockchain.
- Policies set by each institution guide the exemption approval process.
- Approved exemptions are recorded in the system and reflected in the student's academic profile.

1.3.5 Functional Requirements

- **User Registration:** The system should allow users (students, institutions, and verifiers) to register securely.
- **Credential Issuance:** Institutions should be able to issue blockchain-based tokens representing academic credentials.
- **Credential Verification:** Employers and institutions should be able to verify issued credentials using blockchain records.
- **Course Exemption Requests:** Students should be able to request course exemptions based on issued credentials.
- **Course Exemption Review:** Institutions should be able to review course exemptions based on students' requests.
- **Smart Contract Execution:** The system should facilitate automated transactions for credential issuance and verification.

- **IPFS Integration:** Large academic records should be stored off-chain using IPFS with a cryptographic reference on the blockchain.
- **Database:** The system should be optimized to allow on-chain and off-chain storage to efficiently manage credential data.

1.3.6 Non-Functional Requirements

- **Security:** The system should ensure data integrity and prevent credential fraud through blockchain immutability.
- **Privacy:** Sensitive user data should remain protected, with access restricted to authorized entities.
- **Scalability:** The platform should support an increasing number of users without performance degradation.
- **Reliability:** The system should provide consistent uptime, ensuring credentials are always accessible. .
- **Auditability:** Credential issuance and verification logs should be transparent and traceable for verification.
- **Efficiency:** Transaction processing should be optimized for quick credential verification.
- **User-Friendliness:** The system should offer an intuitive interface for students, institutions, and verifiers.

1.4 Outcome

The deployment of the blockchain-based micro-credential verification system has demonstrated significant improvements in credential management, security, and transparency. The key outcomes are outlined below:

- **Secure and Transparent Credential Verification:** By leveraging blockchain, issued micro-credentials are securely recorded on an immutable ledger, preventing fraud and ensuring trust in the verification process. Institutions and employers can verify credentials instantly without relying on intermediaries.

- **Decentralized and Tamper-Proof Storage:** The system eliminates the risk of certificate forgery by storing credentials in a decentralized manner using Hyperledger Besu. Each credential is securely hashed and linked to the blockchain, ensuring authenticity and preventing unauthorized modifications.
- **Seamless Integration and Accessibility:** Using smart contracts, credential issuance, verification, and revocation are automated, reducing administrative overhead. Students and employers can access verified credentials anytime, improving efficiency in academic and professional validation.
- **Flexible Policy Management:** Educational institutions can define credentialing policies within smart contracts, allowing for automated course exemptions based on verified micro-credentials. Blockchain ensures all credential-related actions are transparently recorded, simplifying auditing and compliance.
- **Efficient and Scalable System:** The integration of MongoDB for off-chain storage ensures fast retrieval of credential metadata while blockchain secures the core verification process. The system supports large-scale issuance and verification without performance bottlenecks.
- **Reliable and Trustworthy Digital Identity:** The decentralized nature of blockchain enables students to maintain control over their credentials, securely sharing them with employers and institutions without dependence on centralized authorities.

The proposed blockchain-based micro-credential verification system provides a comprehensive solution to enhance security, authenticity, and accessibility in academic credentialing. By combining blockchain with smart contracts, the system ensures verifiable, tamper-proof, and universally accessible credentials, transforming the traditional approach to education and employment verification.

1.5 Report Layout

Chapter 1 outlines the problem statement, aims, objectives, motivation, project specification, functional- nonfunctional requirement, outcome and summary of the report.

Chapter 2 focuses on the preliminaries, related works, comparative analysis, performance analysis and comparative analysis table of the proposed system. Basically it presents literature reviews.

Chapter 3 explores the specifics of requirements analysis, use case modeling, and implementation requirements. It specifies the actions and factors that must be taken into account for the project to be implemented properly.

Chapter 4 analyzes the project's interface design, user experience, and front-end and back-end design specs. This chapter offers details on the system's intended aesthetic and functional layout.

Chapter 5 covers the project's budget phase. It reviews the findings and discusses their importance of creating a budget. It describes every phase of the budget broadly with proper justification.

Chapter 6 shows the result and analysis of the proposed system. It compares the results with both public and private blockchain and which one performs better.

Chapter 7 investigates the project's larger effects on the community and the environment. It discusses moral questions, environmental concerns, and the project's long-term viability. At the chapter's conclusion, the project's overall activities are summarized, along with future plans and prospective advancements.

1.6 Summary

In this chapter, the problem statement, aim, motivation, functional and non-functional requirements, importance, and short overview of the proposed system are described.

Chapter 2

Literature Review

In this section, the following topics have been covered in relation to developing Blockchain-based Micro-credential verification system.

2.1 Preliminaries

2.1.1 Blockchain

Blockchain technology acts as a distributed ledger, providing a secure, decentralized, and transparent platform for managing data [Kumutha & Jayalakshmi \(2022\)](#). Due to its immutable and tamper-proof nature, blockchain provides an excellent solution for managing controller recovery and flow rule migration in SDN for UAVs. This system is able to store the flow rules records in the blockchain, from which the controller can verify and compare the authenticity of the rules during the recovery process and if a forwarding device fails, blockchain technology can enable the seamless migration of its flow rules to another device, ensuring network resilience and integrity. Blockchain technology provides a reliable and efficient method for managing SDN controller recovery and flow rule migration for SDN forwarding devices. Because of blockchain's decentralized architecture, data security and integrity are maintained since no single entity can alter the data [Angelis & Da Silva \(2019\)](#). Furthermore, a secure and trustworthy method of maintaining UAV network configurations is guaranteed by the intrinsic resistance of blockchain technology to malicious attacks. This robust security framework prevents unauthorized access and modifications, making it an optimal choice for critical applications in UAV networks.

2.1.2 Consortium Blockchain

A blockchain includes a consensus mechanism. The consensus mechanism plays a role for nodes to agree on the blockchains' current state. Through a consensus mechanism, a single, reliable, and unchangeable record is maintained without the need for any central authority. Thus guaranteeing all nodes have the same perspective on the blockchain [Hussein et al. \(2023a\)](#). The system that has been proposed, uses a Quorum Byzantine Fault Tolerance (QBFT) consensus mechanism. The QBFT network operates by guaranteeing consensus through a series of actions. Every round a block proposal is made which is then distributed to validators who upon receiving it, send a prepared message. The prepared message is followed by a commit message. When two-thirds of validators offer a commit message, a consensus is attained which is then added to the block. Despite any faulty nodes, this consensus assures that the networks are robust and safe [Gerrits et al. \(2021a\)](#).

2.1.3 IPFS

The InterPlanetary File System (IPFS) is a decentralized, peer-to-peer protocol designed to make the web faster, safer, and more open by fundamentally changing how data is distributed across the internet. Unlike traditional HTTP-based systems that rely on centralized servers, IPFS uses a distributed network of nodes to store and share data. Each file or piece of content is given a unique cryptographic hash, ensuring data integrity and enabling efficient content addressing [Tschorsch & Scheuermann \(2016\)](#). This decentralized approach not only reduces reliance on single points of failure but also enhances data availability and resilience. IPFS is increasingly being adopted for applications ranging from decentralized web hosting to blockchain-based storage solutions, making it a cornerstone of the Web3 ecosystem [Khalid et al. \(2023\)](#).

2.1.4 Smart Contract

Smart contracts are executable codes on the blockchain that automate and enforce agreements between parties without a trusted third party. They manage the storage, retrieval, and validation of flow rules on the blockchain, ensuring that only valid and authorized updates are applied to the network [Alharby & Van Moorsel \(2017\)](#). The risk of fraudulent activity is decreased when smart contracts are used since they do not require intermediaries or central authorities. Smart contracts can automate the recovery procedure in the event of a controller failure by reapplying the last known good state to a repaired or replacement controller after collecting flow rules from the blockchain. For flow rule migration, smart contracts facilitate the transfer of rules between forwarding devices, ensuring that these

updates are securely and accurately reflected on the blockchain. UAV communication and network performance are guaranteed by this automation, which also improves fault tolerance and security [Pourbahrami et al. \(2020\)](#).

2.1.5 Micro-Credential

Micro-credentials have emerged as a transformative educational trend, offering targeted, competency-based certifications that address specific skill gaps in various industries. These credentials are particularly valued for their flexibility, enabling learners to pursue education tailored to their career goals without committing to traditional degree programs [Patterson \(2024\)](#). The integration of micro-credentials into global higher education systems has enhanced opportunities for lifelong learning, often supported by digital platforms that ensure accessibility and scalability. Recent studies highlight their role in empowering underrepresented groups and advancing specialized fields like gerontology and global health [Komeiha \(2025\)](#). Furthermore, institutional frameworks, such as Australia's National Micro-Credential Framework, underscore the importance of standardization and quality assurance to enhance their credibility and adoption. These developments suggest that micro-credentials are not only a tool for personal and professional growth but also a mechanism for institutions to adapt to rapidly changing labor market demands.

2.2 Related Works

This section is discussed from three perspectives. The initial part is related to existing works of Micro-credential with the implementation of Academic Certificate Validation, the following part is about Micro-credential with the implementation of Blockchain, and the latter part is about the involvement of Blockchain in Academic Certification.

2.2.1 Micro-credential and Academic Certification

This subsection examines existing works on micro-credentials within the context of academic certificate validation. It explores how micro-credentials have been utilized to certify specific skills and knowledge areas, thereby enhancing the traditional academic certification process.

The article [LaMagna \(2017\)](#) mentions the use of digital badges in the education program. Higher Educational Institutions (HEI) is facing various internal and external pressures on how they provide education. In the face of this, the primary focus of HEI has been student retention. It can no longer be assumed that students achieve learning objectives

that are specified by courses or programs. Thus it has become essential for accreditation that students' progress towards learning objectives is measured in a quantifiable way. The article aims to provide an understanding within the educational landscape of how micro-credentials can be used to address such pressures. The article [LaMagna \(2017\)](#) offers to use digital badges for micro-credentials. These are condensed forms of educational programs that enable learners to meet more manageable learning objectives while pursuing a college degree. The digital badges will be used to convey the type of skills that the learner has acquired through the micro-credentials. It has to be visually representable and also contains metadata of what was achieved through the micro-credentials. The metadata will show information on what evidence was required to complete the course and how much time was devoted to completing the course. The metadata will also include learning goals and all learning activities in a manner that the outside audience can easily understand. The article [LaMagna \(2017\)](#) also talks about the digital badge program. The maturity of digital badges and making them stackable showcases the level of knowledge achieved by a learner. These stackable digital badges that stack will show off increased proficiency, expertise, or abilities attained.

This paper [Clements et al. \(2020\)](#) provides practical guidelines for organizations on the design and implementation of an open badging system. Open badges are digital micro-credentials that acknowledge a variety of skills and experiences acquired both within and beyond traditional educational contexts. The paper also presents a comprehensive framework for designing and implementing an open badging system. Initially, organizations should undertake broad system planning, taking into account the scope, workflow, participants, and resources. Subsequently, they should focus on the design of the badges, paying particular attention to badge scope, metadata, images, and associated learning resources. The third stage involves the publication of badges using an appropriate issuing platform. Finally, the framework underscores the importance of change management, recommending the appointment of a badge champion and emphasizing the engagement of both earners and consumers to ensure smooth implementation and widespread acceptance.

The COVID-19 pandemic has led to significant job losses and creation globally. A talent gap exists between job seekers' skills and employer needs, presenting challenges for companies in transforming business models. Closing this gap is a priority, but many companies struggle with curriculum design. Malaysia faces a high youth unemployment rate due to skill mismatches, highlighting the need for innovative approaches like micro-credentials. This study explores the potential of micro-credentials as a solution for the talent gap, focusing on a new model at Wawasan Open University. The study [Tan et al. \(2024\)](#) aims to address institutional readiness, resources, and industry recognition

while providing guidelines for effective implementation. The proposed micro-credential model works by facilitating a clear progression from micro-credentials to formal academic qualifications, offering flexible learning options, multiple exit points, and ensuring industry recognition. These features support learners in acquiring specialized skills, addressing the talent gap, and enhancing employability.

2.2.2 Micro-credential with Blockchain

This part focuses on integrating blockchain technology with micro-credential systems. It reviews various studies and implementations where blockchain has been used to enhance the security, transparency, and efficiency of micro-credentialing processes.

The article introduces a novel web-based system aimed at enhancing skill acquisition among learners. The system integrates quizzes and digital badges, leveraging the Ethereum blockchain for secure transactions and IPFS(Inter Planetary Filing System) for badge image storage. Additionally, Firebase serves as the platform for examination management, registration, and course storage. By addressing the inherent limitations of traditional Learning Content Management Systems (LCMS), the proposed system offers substantial benefits to both learners and educators [Chukowry et al. \(2021\)](#).

The objective of this research [Kishore et al. \(2021b\)](#) is to design, implement, evaluate, and promote the adoption of a blockchain-based micro-credential system within a business school. The study aims to understand the value blockchain technology adds to both the issuers and recipients of micro-credentials and the challenges that need to be addressed for widespread adoption. The authors also aim to address the challenges of distributing and verifying micro-credentials. The research adopts a Design Science Research Methodology (DSRM) to carry out the study. DSRM involves six key steps: Problem identification, Objective definition, design and development, demonstration, evaluation, and communication. The paper provides an implementation based on MIT's Blockcerts, where certificate generation happens through command lines. Which authors believe is not suitable for long-term adoption. For user interaction and long-term adoption, the authors developed a web application called cert-manager, which simplifies the credential generation process [Kishore et al. \(2021b\)](#).

The research [Güneş & Fırat \(2022\)](#) introduces DALE (Decentralized Autonomous Learning Ecosystem) as a system designed for Open and Distance Learning (ODL). DALE comprises four layers around the Core, analogous to a cell nucleus, which hosts DAO and blockchain technologies. Level 1 of DALE is dedicated to Nodes (Education Providers) such as Universities, Schools, labs, or individuals. Level 2 contains micro-credits generated

by providers following DALE Accreditation Standards. Level 3 consists of Learning Objects (LOs), transferable learning units connected with credits. Level 4 is the front end of DALE, housing Smart content integrated with LOs. DALE aims to create a flexible, scalable, and transferable ODL system. It fosters a decentralized approach to learning, accessible beyond formal institutions. The integration of blockchain and DAO technologies enhances DALE's functionality and transfer ability.

The study [Ghonim & Corpuz \(2021\)](#) introduces a digital system integrating Blockchain and badge technologies to enhance competency-based learning in applied programs. The system aims to improve practical class quality and promote digitization through students' e-portfolios. Blockchain technology tracks and analyzes assessment outcomes, generating comprehensive results for students' Learning Evidence Outcomes (LEO) per skill and competency. Micro-credentials are awarded based on demonstrated skills, stored in an e-portfolio, and represented through digital badges. Employers can use competency-based transcripts, validated by third parties, to design personalized development plans for employees and strategically invest in workforce enhancement. Digital Competency-Based Education (CBE) and micro-credentials strengthen industry relationships and provide updated insights to employers about potential employees' skills and weaknesses.

This paper [Mardisentosa et al. \(2021\)](#) aims to propose an evaluation and management strategy to safeguard the confidentiality of student documents with Blockchain technology. It seeks to examine the application of blockchain micro-credentials in university student achievement records and establish a basis for secure and effectively managed student credentials. The research methodology employed in this work is the Literature Review Study (LRS) method, which they believe is superior because it provides a subjective summary that helps interpret the study more effectively. This qualitative approach examines prior studies on blockchain-enabled student accomplishment records and offers a synthesis. The examination of the literature review also aids in comprehending the prospective influence of blockchain micro-credentials on student success records at institutions. This paper also has suggestions for future research combining blockchain and AI technology [Mardisentosa et al. \(2021\)](#).

The objective of the research [McGreal \(2023\)](#) is to emphasize the advantages of using blockchain for the preservation and dissemination of credentials, guaranteeing authenticity, and enabling credit transfer for students enrolled in various institutions. The paper's design methodology extensively examines the current literature regarding blockchain technology and its educational uses. The study examines the characteristics and advantages of

blockchain technology concerning micro-credentials. The research examines the implications of blockchain's immutability, which guarantees that once data is stored, it remains unalterable and irretrievable, providing a trustworthy record of student achievements. It also addresses students' need to manage their credentials and the limitations of traditional paper-based systems in handling and transferring credentials across different universities. The study also references other blockchain applications in education, including MIT's Digital Credentials Consortium and University College London's degree registration and verification utilizing blockchain technology.

The objective of this research [McGreal \(2024\)](#) is to investigate the possibilities of using blockchain and artificial intelligence (AI) to enhance the effectiveness of micro-credentials in the education sector. The paper emphasizes acknowledging and transferring academic credits for students in diverse educational institutions and locations. The text highlights the significance of micro-credentials in offering convenient and visible proof of abilities or expertise. Furthermore, it showcases the ability of blockchain technology to securely store and distribute micro-credentials, with the assistance of AI in managing and delivering them. This paper also discusses several applications of blockchain technology in education, including examples like Holberton School and Blockstack. These implementations empower students by allowing them full ownership of their data. It also highlights the importance of researching the technical and administrative integration of various technologies, which includes creating standards for how they might work together and be accepted by institutions and employers.

The article [Choi et al. \(2019\)](#) proposes a system compatible with OpenBadges by IMS Global Learning Consortium. OpenBadges sets up the badges, while IMS Global certifies them. The system can be used for certificate issuance and management in both online and offline education. Students receive digital badges upon completing micro-learning units. For the system a blockchain-based approach was taken, creating a badge issuance and management system. IMS Global sets the standards for digital credentials through the OpenBadge Specification platform. Mozilla OpenBadges framework issues badges to students, with metadata defined by OpenBadge. Badgr is used for creating, issuing, and managing digital badges, though it doesn't originally support blockchain. The article suggests using blockchain with the Blockcert platform to manage these badges. When a badge is issued, the transaction is recorded on the blockchain. The badge repository, or "backpack," serves as a centralized location for managing these badges. The system uses both Bitcoin and Ethereum networks, with the Ropsten test network for Bitcoin and a regression test mode for Ethereum. The REST API server handles OpenBadge operations, while the Blockcert server manages blockchain transactions.

2.2.3 Blockchain with Academic Certification

This subsection explores the application of blockchain technology specifically for academic certification. It highlights existing research and practical implementations that leverage blockchain to ensure the authenticity, integrity, and reliability of academic credentials.

The article [Saleh et al. \(2020a\)](#) discusses the use of blockchain technology to enhance the verification process of educational certificates. The article [Saleh et al. \(2020a\)](#) identifies some key security features including authorization, confidentiality, ownership, and privacy. It mentions the use of hyper ledger fabric blockchain. The research proposes an architecture that uses an off-chain database to store user certificates. Moreover, it proposes various key features to ensure certificate verification, mainly transparent network, permissioned access, uniquely identifiable digital certificate, and grievance redressal.

The objective of this research [Siddiqui et al. \(2022\)](#) is to combine blockchain with IoT and create the framework for creating and securing academic and other credentials. The framework establishes authentication, authorization, confidentiality privacy, and ownership through the use of such technologies. The research [Siddiqui et al. \(2022\)](#) proposes to use an IoT device in the certificate validation to not compromise, confidentiality, integrity, or privacy. The device will be used to exchange credentials with 3rd parties. In the research [Siddiqui et al. \(2022\)](#) each certificate will be represented as a token. And with an exchange of each token certification can be transferred from one person to another. The certificates are directly issued on the blockchain. Blockchain and IoT are combined in this research to cut transportation i.e. to eliminate third-party logistics providers or centralized systems. Moreover, because blockchains are tamper-proof records of transactions, their inherent transparency and immutability increase the trust between devices. And most of all By leveraging blockchain technology in IoT applications, transactions can be executed and verified in near real-time without the need for any centralized systems.

The article [Rahman et al. \(2023a\)](#) focuses on utilizing blockchain and IPFS technology to address the challenge of fake certification which is a very pressing issue in South Asia. With blockchain and IPFS, the system aims to securely store and verify academic credentials. The proposed system recognizes multiple stakeholders for this operation which are applicants, companies, admins, and general users. Here applicants will upload their credentials which will be then verified by admins through contacting the HEI. After the credentials are verified they will be uploaded to IPFS where their hash will be encrypted and securely stored in the blockchain. After they are secured companies can easily search for the credentials and verify their authenticity. With frameworks like ganache metamask, truffle, react, and node js, the blockchain platform is created. the proposed solution offered in

article [Rahman et al. \(2023a\)](#) offers a transparent, efficient, and secure method for verifying academic credentials.

The research [Leka & Selimi \(2020\)](#) proposes a blockchain-based solution that deals with the inefficiencies that come with maintaining and certifying academic credentials through traditional methods. The research [Leka & Selimi \(2020\)](#) highlights the potential of blockchain to provide a decentralized, secure, and efficient solution. The author identifies 4 different stakeholders for the system which are the accreditation body, the university, students, and employers. The system research utilizes the Ethereum blockchain to implement smart contracts and uses IPFS to store the certificates. Moreover, it uses the AES encryption method to store the certificates in the public blockchain. There are 3 main users of this system. First comes the issuer who is responsible for issuing the certificates and it can be universities or training centers. Secondly, the user comes which can be students or employers. The user will be able to share their information through a public key. And finally comes the accreditation body which validated the certificates.

The research [Manoj et al. \(2021\)](#) proposes a method to verify educational credentials and facilitate credit transfer which has been obtained locally or from any online educational portal. The research aims to enhance the data accuracy and reliability of such credentials. The research proposes a token-based framework to transfer credits using blockchain. The credit value is transferred as a token to the student's wallet after the completion of each course. The research presents a proof of work consensus mechanism to verify the tokens and uses the Ethereum blockchain to deploy smart contracts. The stakeholders in this system are the students and the universities. Through public key encryption and hashing techniques, the security of the system is enhanced and the scalability of the system is tested through load testing with multiple universities.

The research [Delgado-von Eitzen et al. \(2021\)](#) presents an innovative comprehensive framework for the application of blockchain technology in education, focusing on the secure, GDPR-compliant, and scalable certification and verification of academic information. The proposed model focuses on leveraging blockchain technology, specifically Hyperledger Fabric, to establish a secure and decentralized system for storing, verifying, and sharing different types of academic information, both formal and informal. The framework incorporates private and consortium blockchains, smart contracts, off-chain storage using IPFS, and access control mechanisms to achieve scalability and privacy. It allows reliable storage and verification by a third party of any type of academic record without compromising the privacy of personal data and complying with the requirements of the

GDPR. On the other hand, the framework, based on a set of blockchains, enhances the performance and scalability of the system.

This research's [Jaramillo & Piedra \(2020b\)](#) objective is to examine the application of blockchain technology for academic certification in higher education institutions and highlight its advantages and obstacles. The research identified key stakeholders in the certification process and presented a framework for blockchain deployment in educational institutions. It also evaluates the educational applications of blockchain technology, concentrating on academic certification, sovereign identity, and passport learning. The research also examined the distinctions among physical, digital, and blockchain certificates. It also outlines the procedures for developing a decentralized application. The study also explores the potential for creating a global blockchain network, allowing each institution to manage its private blockchain to protect student data and enable the efficient verification of academic credentials worldwide [Jaramillo & Piedra \(2020b\)](#).

The objective of this paper [Bahrami et al. \(2020\)](#) is to provide a dependable and tamper-resistant system for the issue and verification of academic certificates. Moreover, to address the widespread problems of forgery and manipulation linked to conventional certificate verification methods. The suggested method automates the verification process with blockchain-based smart contracts, which inherently guarantees security and durability, thus diminishing dependence on individual entities for trust and validation. The proposed architecture entails the implementation of a blockchain-based platform that employs smart contracts to manage academic certificates. The authors suggest a completely decentralized system that includes all essential processes, such as user registration, certificate issue, and verification, conducted on the Hyperledger Fabric blockchain. This method guarantees that the certificates are maintained on a permissioned and immutable ledger, substantially diminishing the probability of fraudulent operations [Bahrami et al. \(2020\)](#).

The paper [Ali & Bhaya \(2021b\)](#) examines the features and attributes of blockchain technology. Additionally, it provides insight into the possible advantages and challenges of implementing blockchain technology in higher education. The authors suggested a methodology that utilizes blockchain technology to create, protect, and verify academic certificates in higher education to address the problem of counterfeit certificates. The proposed methodology comprises three essential stages: certificate issuance, certification creation request, and verification of certification authenticity. The system verifies the identity and eligibility of students who request a certificate. Subsequently, the registration and student affairs offices conduct additional verifications. Once all the necessary details have been verified, the model employs hash functions to generate encrypted and compressed

versions of student certificates. Subsequently, these items are added to the blockchain network. The model additionally provides a website or application that enables other organizations to verify the authenticity of supplied certificates. They can achieve this by inputting the certificate information and cross-referencing it with the hashes contained in the blockchain.

2.3 Performance Metrics

Blockchain technology brings together a variety of complex techniques, including consensus algorithms, cryptographic methods, and mathematical principles. To ensure the effective integration of micro-credentials within a blockchain network, specific requirements must be fulfilled. These parameters are divided into 7 categories which include the evaluation of security, scalability, and interoperability within the credentialing system, while also detailing the requirements for non-blockchain micro-credential systems. The evaluation matrix will consider aspects such as:

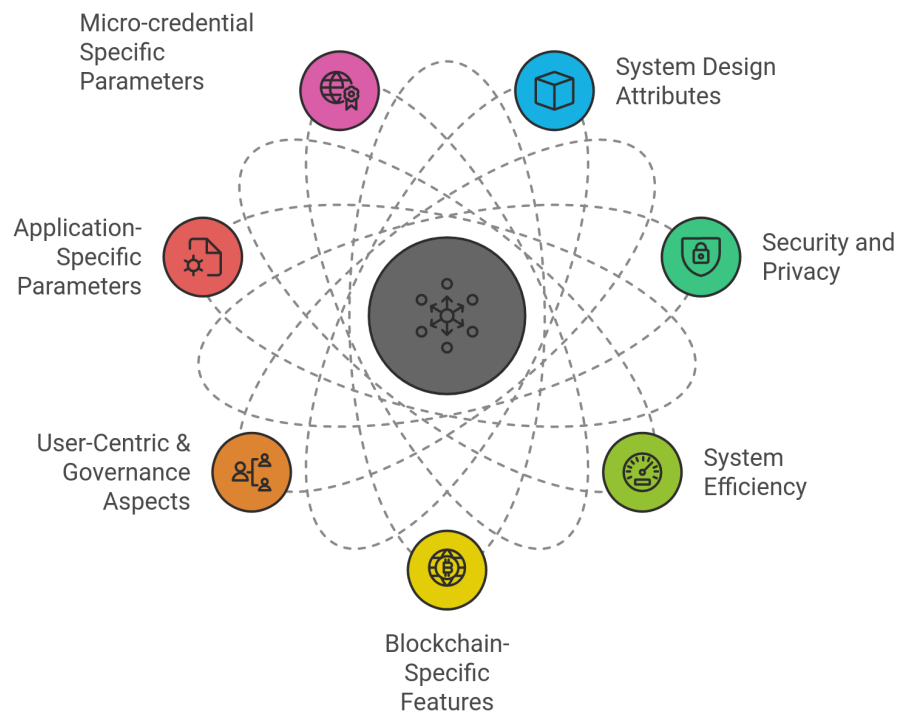


Figure 2.1: Performance Evaluation Metrics

2.3.1 System Design Attributes

Understanding the various characteristics of a blockchain system is crucial for evaluating its effectiveness and applicability in different contexts. This section delves into key attributes such as system complexity, off-chain storage, lightweight solutions, scalability, and interoperability.

2.3.1.1 System Complexity

When a system interacts with a user, the complexity of the system becomes noticeable. This complexity is not a natural characteristic of the system by itself, it shows up through its interaction with another system, usually during the processes of measuring and controlling [Casti \(1986\)](#).

2.3.1.2 Off-Chain

Off-chain transactions are verified external to the main blockchain network, usually saving the user money and speeding up the transaction process. IPFS is an off-chain example. The costs associated with directly storing large amounts of data on the blockchain are reduced by using IPFS as a middleman storage platform [Rahman et al. \(2023b\)](#). Off-chain refers to storing data outside the blockchain to reduce the load and improve efficiency. While the core credential verification data is recorded on the blockchain, detailed or sensitive information can be stored off-chain, with a reference or hash on the blockchain ensuring its integrity and linkage.

2.3.1.3 Light Weight Solution

A lightweight approach preserves user privacy while utilizing a simplified technique to minimize data size and store it within the blockchain network [Mansoor et al. \(2023\)](#). A lightweight solution involves minimizing the computational and storage requirements while maintaining security and efficiency. This can be achieved by utilizing protocols like IPFS for off-chain storage, employing compact data structures for on-chain records, and optimizing consensus mechanisms for faster processing.

2.3.1.4 Scalability

If a network can grow to accommodate increased user demand, it demonstrates scalability [Shi et al. \(2020a\)](#), [Yadav & Shevkar \(2021\)](#). This means that if there's a sudden surge in activity, a scalable network can handle it by expanding its capacity. Scalability ensures the

network can support more users and transactions without losing performance or efficiency. It involves optimizing resources and adapting to changing workloads.

2.3.1.5 Interoperability

Generic communication between blockchains, or the transfer of any kind of data in a decentralized and trustless manner, is the main focus of general interoperability [Schulte et al. \(2019\)](#). Improving collaboration and information sharing between diverse educational institutions is a key component of interoperability in educational environments. Reaching interoperability facilitates integration within the education ecosystem, cooperation between various D-Apps, and application portability [Any et al. \(2024\)](#).

2.3.2 Security & Privacy

Security and privacy are crucial in the context of blockchain-based systems, particularly in micro-credentialing. This section explores the crucial elements that ensure robust security and privacy, such as pseudonymity, authenticity, confidentiality, and immutability. These components are vital to maintaining the integrity and trustworthiness of the credentialing process, protecting sensitive data, and preventing unauthorized access and tampering.

2.3.2.1 Pseudonymity

During a transaction, a user's identity is unknown, yet it is still possible to identify and follow the person responsible for each action they do [Chen \(2018\)](#).

2.3.2.2 Authenticity

Blockchain authentication is defined as a verification procedure that validates users before allowing them to interact with data. This allows a separate layer of security where the identity of the requester is confirmed before allowing access to vital data. [Saleh et al. \(2020b\)](#)

2.3.2.3 Confidentiality and Privacy

The private information of the student, which is preserved by the academic institution and the student, is one of the conditions for secrecy [Saleh et al. \(2020c\)](#). Only individuals with consent may access the necessary information since personal details will be utilized in confidentially [Shi et al. \(2020b\)](#). By using encryption and permissioned access controls, the system safeguards personal and credential data, ensuring that only those with the right credentials can view or verify specific information.

2.3.2.4 Immutability

Decentralized systems ensure that the information about digital resources remains trustworthy and reliable. With this, since multiple parties are accessing and storing data, having immutable metadata statements helps maintain the integrity and authenticity of the information [Rahardja et al. \(2021\)](#).

2.3.2.5 Non-Repudiation

Due to non-repudiation, participants in a blockchain cannot contest the transaction and conduct it within a transaction [Mansoor et al. \(2023\)](#). In a blockchain-based credential verification, the system ensures that once credentials are recorded and verified on the blockchain, the issuer cannot deny having issued them.

2.3.3 System Efficiency

Evaluating the performance of a blockchain system is essential to ensure its effectiveness and reliability. This section covers critical performance metrics such as availability, transaction latency, transaction throughput, and data storage efficiency. Each of these metrics provides valuable insights into the system's capacity to handle transactions, maintain data accessibility, and optimize storage, ultimately reflecting the overall performance and scalability of the blockchain network.

2.3.3.1 Availability

In a blockchain network, the data contained in the block must be valid and accessible. This mechanism allows nodes to check whether the data for the block is available without downloading the entire block. It is an assurance that transaction data for a block is open and accessible to other network participants [Zhang et al. \(2019\)](#).

2.3.3.2 Transaction Latency

A blockchain performance statistic, expressed in milliseconds (ms) or microseconds (μ s), assesses how long it takes to complete a transaction in a blockchain network. The entire time it takes for mining to add a transaction to a block and blockchain is Latency in Transactions [Wan et al. \(2019\)](#).

2.3.3.3 Transaction Throughput

A crucial blockchain performance statistic that is measured in transactions per second (TPS) or transactions per minute (TPM) units is the total number of successful transactions over a given period [Li et al. \(2020\)](#).

2.3.3.4 Data Storage Efficiency

Optimizing storage to minimize overhead and redundancy while preserving scalability and sustainability is necessary for blockchain data storage efficiency [Mansoor et al. \(2023\)](#). Reducing overhead and redundancy while preserving scalability and sustainability is the goal of blockchain data storage efficiency [Mansoor et al. \(2023\)](#).

2.3.4 Blockchain Specific Features

Blockchain-specific features are critical parameters, used to evaluate the effectiveness and reliability of a blockchain system. This section focuses on key attributes of smart contracts and consensus mechanisms, which are fundamental to the operation and security of decentralized applications.

2.3.4.1 Smart Contract

Smart contracts are self-executing programs on a blockchain that automatically enforce agreements when specific conditions are met. They are essential for decentralized applications (dApps), allowing these applications to operate without intermediaries, ensuring transactions are fast, transparent, and secure [Ethereum \(2014\)](#). This infrastructure allow dApps by facilitating reliable and autonomous operations within the blockchain ecosystem.

2.3.4.2 Consensus Base

All nodes can securely transfer and update data, giving the system a consensus base. Because nodes on the blockchain are publicly connected changes can only occur when the majority of nodes accept the change [Saleh et al. \(2020c\)](#). This mechanism ensures that all participants agree on the validity and authenticity of the credentials.

2.3.5 User-centric & Governance Aspects

The user-centric and governance aspects are critical parameters used to review and evaluate the effectiveness of blockchain systems. This section discusses key elements such as transparency, user-centric design, and regulatory compliance. These features ensure that

the system is accessible, meets user needs, adheres to educational standards, and maintains trust through transparent and accountable processes.

2.3.5.1 Transparency

Through the use of a shared and decentralized ledger, one can determine the completion of a transaction. This ensures that the record is open and visible to all participants [Nugent et al. \(2016\)](#). One can determine the ownership status of an asset or the completion of a transaction, through a shared and decentralized ledger. This ledger provides a transparent and immutable record of all relevant information [Nugent et al. \(2016\)](#). This ensures that the transaction is open and visible to all participants.

2.3.5.2 User-centric

The user-centric parameter focuses on designing educational systems and resources that prioritize the needs, preferences, and experiences of the student. This approach involves understanding user feedback, enhancing accessibility, and ensuring the intuitive use of these systems to improve the learning experience. In an educational context, user-centric design ensures that learning tools and resources are tailored to the unique needs and goals of each student, making education more personalized and effective [Shneiderman & Plaisant \(2010\)](#).

2.3.5.3 Regulatory Compliance

Regulatory compliance in the context of this research involves ensuring that these short, specialized learning units adhere to established educational standards and policies. This means that micro-credentials must be recognized and accredited by relevant authorities to ensure they meet quality and competency benchmarks [Ahsan et al. \(2023\)](#).

2.3.6 Application Specific Parameters

Application-specific parameters are essential for evaluating how specialized features can enhance educational systems. In this context, Artificial Intelligence (AI) stands out as a transformative technology. AI in education personalizes learning experiences by analyzing data on student's habits, performance, and preferences, thereby tailoring educational content to meet individual needs.

2.3.6.1 AI

Artificial Intelligence (AI) is revolutionizing education by creating personalized learning paths for students based on their interests and previous work. By analyzing data on students' learning habits, performance, and preferences, AI systems can tailor educational content and recommend resources that best suit each individual's needs [Chander \(2024\)](#). This approach enhances the learning experience, making it more engaging and effective.

2.3.7 Micro-credential Specific Parameters

Micro-credential specific parameters help us evaluate how effective and reliable micro-credential systems are. This section focuses on important features like standardized metadata, granularity, stackability, digital badge images, revocation capability, interoperability, and level-up mechanisms. These features ensure that micro-credentials are clear, consistent, modular, and can work well across different platforms, making them more credible and useful in education.

2.3.7.1 Standardized Metadata

Micro-credential issues include standardized meta-data. This meta-data ensures transparency and consistency among the credentials. It also guarantees the badge's validity and authenticity which is specified by the awarding institutions. This makes it simpler to validate and understand the accomplishment as a result [Vordenberg et al. \(2024\)](#).

2.3.7.2 Granularity

Micro-credentials are mostly smaller than traditional degrees. They cover specific skills or knowledge areas which makes them highly relevant. Students can be motivated and their accomplishments are shown more effectively using digital badges that are more particular and detailed [Fanfarelli & McDaniel \(2017\)](#).

2.3.7.3 Stackability

Stackability offers a more modular approach to micro-credentials as they can be frequently stacked or accumulated over time to work towards a larger qualification. With the primary concept of stackability, higher education can bundle its learning offerings and cause a shift in practice. This will help learners to accumulate badges over time and in turn create a comprehensive picture of skill, knowledge, and competencies [Fanfarelli & McDaniel \(2017\)](#).

2.3.7.4 Digital Badge Image

Micro-credentials are represented by digital images which can be easily displayed on a digital platform. These badges are typically clickable, allowing viewers to access more detailed information about the specific credentials or achievements they represent [Pitt et al. \(2019a\)](#). These images are visual representations of achievements, skills, or competencies that are earned through micro-credentials [Pitt et al. \(2019b\)](#).

2.3.7.5 Revocation Capability

Micro-credential issuers have the authority to cancel credentials if it is discovered that they were granted based on incorrect information or if the credentials require updating or correction. This feature ensures ongoing trust and integrity in the credentialing process [Varadarajan et al. \(2023\)](#).

2.3.7.6 Interoperability

Micro-credentials are intended to be designed in such a way that they work seamlessly across various platforms and systems. Interoperability ensures that the badges are shared, recognized, and verified across different platforms, systems, and institutions [Rieder \(2022\)](#).

2.3.7.7 Level-Up

Level-up mechanism in digital badges is a process of advancing to a higher level within a badge system which is based on specified criteria or achievements. These badges are designed to increase student engagement and motivation in micro-credential courses [Rigole et al. \(2017\)](#).

2.4 Performance Analysis

This paper has two subsections for performance analysis, such as existing works with blockchain and existing works without blockchain, to provide a clear and systematic comparison. The study of this section provides a clear sense of the advantages and disadvantages of existing work having specific parameters, as defined in Section 5, for both subsections. This approach allows us to analyze how blockchain-based solutions address problems like immutability, transparency, and security. At the same time, it analyzes the benefits and challenges of non-blockchain-based solutions, providing a comprehensive understanding of performance.

2.4.1 Performance Analysis of Existing works with Blockchain

The performance analysis of existing blockchain-based systems provides valuable insights into their effectiveness and applicability in various contexts, particularly in areas such as micro-credentials. This section evaluates the key metrics and characteristics of these systems, highlighting strengths, limitations, and areas for improvement. Figure 5 presents a detailed comparison of the performance of different blockchain systems, offering a visual representation of their performance metrics

The proposed system in research [Chukowry et al. \(2021\)](#) integrates the Ethereum blockchain with other modern tools such as Firebase, IPFS, and Metamask, to create a comprehensive platform. By using smart contracts, academics can securely create examinations and allocate digital badges, while learners can access courses, take examinations, and earn digital badges to showcase their skills and achievements. The system ensures accountability through transparent and immutable records of transactions, while also offering pseudonymity for user privacy. Digital badges serve as authentic representations of learners' accomplishments, encouraging them to engage in life-long learning. While the system may lack strong confidentiality features, it offers compatibility with modern web technologies. However, it can be assumed that the system is not scalable because the system is centered around e-assessment. The proposed system does not mention any efficient solution on how it will handle such a huge amount of transactions as a lot of students will be participating in it. It can be assumed that the transaction latency and transaction throughput will have problems over time. Moreover, digital badges will be used in this process, there is no mention of data storage efficiency. The system also does not integrate with other blockchains making it non-interoperable. Other than that, with its user-centric design and focus on pedagogy, the system aims to facilitate credit transfer and enable learners to pursue continuous skill development in a rapidly evolving educational landscape.

In this research paper [Kishore et al. \(2021b\)](#), they discuss the use of blockchain technology in education that supports storing and sharing worldwide micro-credentials. Further, they also mentioned that beyond offering an efficient means to secure personal data and privacy, credentials maintenance and distribution can be made more accessible using blockchain while ensuring that such control remains within the student's sphere, which introduces complexities into existing systems. Smart contracts are also described in the paper as an approach to secure and automated transactions. The research also looks into the ability of blockchain technology to verify students' achievements and maintain official credentials sustainability as well as availability, thus enhancing their confidentiality.

Moreover, blockchain technology provides privacy by allowing students to control who can access their information and it emphasizes the transparency aspect through which students can attest to what they know, and employees can validate their skills. However, this article does not mention how the data is stored anywhere. The system does not discuss any capabilities designed outside blockchain or suggest how one might create such a thing in a lightweight manner. Almost all the information gets saved within the blockchain. After such circumstances, it will appear that this on-chain could not scale over time because it becomes heavier yearly. Consequently, it may also affect transaction latency and throughput in the system. Finally, there is reference made to the significance of academic integration, particularly for credit transfer purposes, when considering how blockchain may be used as an archival system, making it easier for anyone to monitor progress among individual students.

The combination of micro certifications and blockchain technology represents a shift in education towards decentralization and innovation [Güneş & Fırat \(2022\)](#). Blockchain distributed ledger system supported by contracts guarantees transparency and accountability, in integrating micro certifications. The DALE model demonstrates this merging by creating a learning environment that goes beyond conventional educational limits. DALE promotes a user-focused strategy using blockchain ledger and decentralized management to empower students and educational institutions. Nevertheless, challenges like scalability and following regulations are still present. Despite these challenges, the merging of micro certifications and the use of blockchain technology offer a glimpse into a future where learning never ends, embracing flexibility, authenticity, and ease of access. As studies advance DALE emerges as a symbol of creativity and progress in education ushering in an age where conventional learning barriers fade away making room, for a diverse and lively educational environment.

This paper [Ghonim & Corpuz \(2021\)](#) narrates the design and development of a Blockchain-integrated digital CBE system for the improved verification and presentation of skills and competencies acquired by learners. The complication of the system is clear by the inclusion of advanced technological solutions, including Blockchain itself. However, in-depth specific features such as smart contracts and off-chain solutions are not considered. Moreover, the immutability and transparency provided by Blockchain ensure accountability and authenticity. Also, the system focuses on making credentials available to employers for immediate verification, allowing for an easy transition from the corridors of learning to the working world. While the aspect of making credentials transparent and verifiable has been aimed at, scalability, pseudonymity, and privacy are yet to be fully explored. Nonetheless, the potential for the system to further academic integration and

lifelong learning is cemented through the inclusion of competency-based education in academic curricula. Digital badges are mentioned regarding micro-credentials. However, the challenge of regulatory compliance, interoperability, and efficient data storage is not discussed.

The article [Choi et al. \(2019\)](#) has a certain level of system complexity as it involves the use of digital badges and blockchain technology. Moreover, two blockchains are used in this process which are bitcoin and ethereum. The system proposed in the article does not have a direct mention of smart contracts, however, it suggests a potential use based on a digital badge platform. The system primarily focuses on digital badge issuance and its management on-chain. While the system provides an efficient management of digital badges, it does not provide any lightweight solution for blockchain. The system also seems to be scalable as only digital badge information is being stored in the blockchain and as such it will be able to handle heavy loads and a huge userbase. Users can decide whether to receive and disclose digital badges and thus the system supports pseudonymity and privacy. Moreover, the use of digital signatures and public key encryption ensures authenticity in the system. Another important feature of this system is that it is designed to support badge management systems. With the integration of blockchain technology, the system ensures, immutability, and non-repudiation. Two systems were demonstrated in this paper. However, both of them lack the discussion on scalability and potential limitations of the system. Moreover, there is also a limited exploration of potential vulnerabilities in the blockchain-based platform. However, one performance measure is mentioned in the system which is the badge award time in which the Bitcoin-based system scored 24.53s while the Ethereum-based based scored 3.86s. However, the two systems do not explicitly mention the use of a consensus base. However, it can be assumed it played a crucial role in determining the transaction throughput and transaction latency. The system is centered around the creation, issuance, and management of digital badges and also the system ensures the support of lifelong learning by enabling the share of digital badges.

The system proposed in research [Saleh et al. \(2020a\)](#) utilizes smart contracts in the network with the combination of hyperledger fabric. Smart contracts in hyperledger fabric are known as chain codes. Document storage in this system is done off-chain to make the blockchain network more efficient. The system does not explicitly mention any use use light weight solutions for the encryption method. Although there is no mention of how scalable the system is, it is generally assumed to be scalable given Hyperledger Fabric's reputation for robust scalability features. As blockchain technology is used in this framework, the system proposes to have key features such as pseudonymity availability, accountability, and authenticity. These features are ensured in this system. Moreover, the

system also ensures privacy, immutability, and non-repudiation. However, the system does not explicitly mention the use of any consensus base. The system is also not mentioned to be compatible with third-party organizations issuing credentials or micro-credentials, since permissioned blockchain is used here. The system is not user-centric as the certificates are maintained by the issuer only. Even though the transaction latency and transaction throughput are not explicitly mentioned in the research, Hyperledger fabric is designed to have low latency and high transaction throughput. The platform is optimized for performance, allowing for quick transaction processing which supports a high volume of transactions per second.

The framework outlined in [Siddiqui et al. \(2022\)](#) identifies three primary stakeholders: educational institutions, learners, and teachers. Additionally, it includes organizations that will be able to verify certificates. The system utilizes smart contracts to issue certificate transactions. With the use of blockchain technology authenticity of certificates is ensured. Moreover, the system also ensures immutability and non-repudiation of data. However, since the system is not user-centric only educational institutions are used for managing the server. Due to this privacy is not ensured in the system as organizations can look up the data through the distributed ledger. Pseudonymity is ensured through the use of the local ID of the student. There is no explicit mention of a consensus base in the system and there is no mention of how the certificates are being stored in the system. Due to this, it is not possible to assume that the system is scalable or that the transaction latency and transaction throughput of the system. Since the network is maintained by educational institutions, the network is not interoperable with third-party organizations and not compatible with other forms of credentials. Moreover, the system does not use any digital badges, and all the data is stored on a chain.

The research outlined in [Rahman et al. \(2023a\)](#) employs multiple components such as blockchain, IPFS, and smart contracts. It also incorporates various tools including Ganache, MetaMask, Truffle, React, and Node.js, indicating a notable level of complexity in the system. The system ensures the use of smart contracts with the Ethereum blockchain. The system also utilizes smart contracts and the certificates are stored in off-chain storage for data storage efficiency. Even though the paper does not explicitly mention the use of any lightweight solutions, the use of IPFS potentially suggests a lightweight solution. Moreover, it also makes the system scalable. Through the use of cryptography keys, the system ensures pseudonymity, privacy, immutability, and non-repudiation ensuring a tamper-proof record. However, the system is not transparent as users cannot easily look up the data stored on the blockchain. The system does not explicitly mention the use of any consensus base. However, with the use of both on-chain and off-chain data in the system,

it can be assumed that the system has an optimized transaction latency and throughput. With that, it can be said that the system is scalable. Since the system is user-centric, it is assumed that the system's focus on academic credentials implies support for lifelong learning verification.

The system proposed in research [Leka & Selimi \(2020\)](#) indicates a level of complexity as it has the use of various technologies. The system is based on the Ethereum blockchain and utilizes smart contracts to facilitate the distribution and verification of academic certificates. The system also uses IPFS to store the credentials off-chain. It also uses AES encryption which is a lightweight encryption. These features indicate the use of lightweight solutions here. Moreover, the system also indicates the feature of pseudonymity and privacy through the use of public keys. The system ensures immutability and non-repudiation through the use of the Ethereum blockchain. The research does not mention what consensus mechanism was used. Moreover, the system lacks comparison with existing certification systems and also there is an absence of detailed analysis and cost implications. However, keeping the cost implication aside, the use of data storage efficiency can be used to assume that the system is scalable. The system is indicated to not be transparent as one cannot easily look for information in the blockchain. There is no explicit mention of transaction latency and throughput in the research, however, since the system is using lightweight solutions it can be assumed to have low transactional latency and high throughput. The system also indicates that there is regulatory compliance as there is an accreditation body present to verify the stakeholders. Moreover, due to the accreditation body, it is assumed that it would verify third-party credentials which ensures compatibility with other forms of credentials. This also ensures life-long learning for the system. However, there is no mention of the use of digital badges in the system or integration with other types of blockchain, thus making it not interoperable.

The research outlined in [Manoj et al. \(2021\)](#) describes a system with a straightforward architecture, involving only two stakeholders. It is built on the Ethereum blockchain and uses a smart contract written in Solidity for transferring tokens between universities and students. The system is not meant to be user-centric as the teachers transfer credits completed to the students' wallets as tokens. Even though the system is load-tested by having multiple universities registered on the account, however, it does not test for the number of students registered on the platform. The system ensures a consensus mechanism that uses a distributed consensus protocol which ensures that all nodes in the network agree on the validity of the transaction. The system proposes an off-chain solution where metadata are stored, however, the data storage efficiency cannot be assumed as it is stored in CSV files. The use of CSV files also does not mention any use of encryption which raises

concern for privacy security. With the use of blockchain technology, the system ensures the immutability and non-repudiation features of the tokens. Since the tokens directly come from the university or teachers, it is assumed that the system is not compatible with other forms of credentials. Moreover, the system cannot be integrated with other forms of blockchain which makes it not interoperable. The paper mentions transaction throughput by load testing of different universities in the system and given the results it can be assumed that the transaction latency is at an optimized state. The system has no use of digital badges and is assumed to be regulatory compliant as the tokens are directly served by the university.

Considering the multi-layered architecture involving private and consortium blockchains, the System complexity of the proposed framework [Delgado-von Eitzen et al. \(2021\)](#) is moderate. Smart contracts play a pivotal role in managing access permissions and ensuring transaction integrity. Off-chain storage, especially IPFS-distributed file systems, improves data scalability and confidentiality. The framework's lightweight solution status may be limited because of the blockchain technology's computational cost, even while it encourages accountability through transparent transaction recording. Pseudonymity protects user identities, aligning with privacy regulations like GDPR (General Data Protection Regulation). Distributed ledger technology and redundant infrastructure maintain availability, while tamper-proof transaction records guarantee accountability. The proven authenticity of academic data is amplified by the immutability of blockchain records. Encryption and controlled permissions help maintain confidentiality. Standardized protocols may be necessary for interoperability with external systems, even while compatibility with blockchain frameworks is prioritized. Regulatory compliance, particularly with GDPR, is a key element for ensuring data privacy. Academic integration facilitates seamless interaction with existing educational systems. While transaction latency and throughput may vary, the framework demonstrates efficiency in data storage, especially with off-chain solutions like IPFS. Flexibility in managing access permissions and sharing data accommodates diverse academic needs. Finally, support for lifelong learning initiatives and the potential for issuing digital badges underscore the framework's adaptability to evolving educational paradigms.

This research [Jaramillo & Piedra \(2020b\)](#) discusses the benefits of blockchain technology, highlighting its decentralized and distributed model, which reduces system complexity and enhances information security and transparency. This paper also suggested collaboration between institutions where institutions can interact, which can increase scalability and interoperability. It highlights the use of Solidity language for smart contracts, ensuring document authenticity through instant verification and immutability using hash keys;

immutability ensures that data cannot be altered or deleted . Although it is not directly mentioned, if a user alters data, non-repudiation can ensure that the user cannot deny the transaction. The paper suggested that blockchain operates through consensus mechanisms, eliminating the need for intermediaries in certificate validation, which can reduce transaction latency. Although it did not directly address transaction throughput, it can be assumed that when consensus-based mechanisms are used, and transaction latency is reduced, transaction throughput can also be affected. It also emphasizes transparency through decentralization and traceability, ensuring secure data recording. The paper proposes integrating blockchain technology in academic certification in higher education institutions, highlighting its data storage efficiency through a protocol called IPFS, which can reduce the load of the blockchain and ensure a lightweight solution. It also highlights that User-centric features can allow students to store their evidence of learning securely and efficiently. It also discusses confidentiality and privacy, with three actors identified: students receiving validated certificates, students sharing their certificates with employers, and individuals owning and sharing their data without consent. However, it did not mention pseudonymity, where users can use unique identities rather than real-world identities. It also didn't mention anything about availability or compatibility. Although this paper discussed digital certificates, it did not mention digital badges.

The research [Bahrami et al. \(2020\)](#) proposed a system designed to streamline the certificate verification process by utilizing blockchain technology and smart contracts, hence decreasing system complexity. The suggested system is entirely centered around the management of academic certificates. The solution employs blockchain-based smart contracts to automate the process of verification and improve security. However, it failed to address off-chain or lightweight solutions. Additionally, there is a lack of discussion regarding the effectiveness of data storage. However, it discusses improving scalability by decentralizing essential services in the certification process enhancing speed and reliability in private networks. The solution guarantees authenticity by utilizing blockchain technology to achieve tamper-proof verification. Furthermore, it improves confidentiality by employing public key encryption to safeguard academic records, which are then securely stored on the blockchain [Bahrami et al. \(2020\)](#).

Moreover, the system guarantees pseudonymity by anonymizing the user's signatures during verification, enhancing privacy. The suggested approach guarantees interoperability by distributing certificates among various institutions on a unified and unchangeable ledger. However, it failed to address the issue of availability. Nevertheless, it mentioned immutability by securely keeping academic records and access history on the blockchain, prohibiting unauthorized data modification. It also emphasizes transparency through

	System Complexity	Smart Contract	Off-Chain	Light Weight Solution	Scalability	Pseudonymity	Availability	Authenticity	Confidentiality and Privacy	Interoperability	Immutability	Non-Repudiation	Consensus Base	Transparency	User Centric	Transaction Latency	Transaction Throughput	Regulatory Compliance	Data Storage Efficiency	AI	Digital Badge
[17]	X	✓	✓	X	X	✓	✓	✓	✓	X	✓	✓	✓	X	✓	X	X	X	✓	X	✓
[18]	X	✓	X	X	X	✓	✓	✓	✓	X	✓	✓	✓	✓	✓	X	X	X	X	X	X
[19]	✓	✓	X	X	X	X	✓	✓	✓	X	✓	✓	X	✓	✓	X	X	X	X	✓	✓
[20]	✓	X	X	X	X	✓	✓	✓	✓	X	✓	✓	✓	X	X	X	X	X	X	X	✓
[24]	✓	X	✓	X	X	✓	✓	✓	✓	X	✓	✓	X	✓	✓	✓	✓	X	X	X	✓
[25]	X	✓	✓	✓	✓	✓	✓	✓	✓	X	X	✓	X	X	X	✓	✓	X	✓	X	X
[27]	✓	✓	X	X	X	✓	X	✓	X	X	✓	✓	X	X	X	X	X	X	X	X	X
[28]	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓	X	X	X	✓	✓	X	✓	X	X
[29]	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	✓	✓	X	✓	X	✓	✓	✓	✓	X	X
[30]	X	✓	✓	X	✓	✓	✓	✓	X	X	✓	✓	✓	✓	✓	✓	✓	✓	X	X	X
[32]	✓	✓	✓	X	✓	✓	✓	✓	✓	X	✓	✓	✓	✓	✓	✓	✓	✓	✓	X	✓
[37]	X	✓	✓	X	X	X	✓	✓	X	X	✓	✓	X	✓	X	X	X	X	X	✓	X

Figure 2.2: Performance Analysis of Blockchain Based Solutions

decentralization in the certification process. The system works with PoW consensus mechanism, however, they also discussed another consensus mechanism named PoA . However, Non-repudiation and lifelong learning are not mentioned. Furthermore, it failed to address the digital badge, transaction latency, and transaction throughput [Bahrami et al. \(2020\)](#).

The features of blockchain technology are examined in this study [Ali & Bhaya \(2021b\)](#). Additionally, it offered a blockchain-based approach to higher education. System Complexity is a significant factor in the proposed model, which operates on a permissioned blockchain. This complexity arises from the need for consensus mechanisms and secure data management, making it a robust solution for certificate verification. Nevertheless, Smart Contracts—frequently used in blockchain applications to automate procedures—are absent from the model. In the same way, Off-Chain solutions—which could improve efficiency by lightening the load on the blockchain network—are not mentioned. The

model's complicated data management and verification procedures disqualify it as a Lightweight Solution. However, it notes scalability issues, recognizing the system's need to manage increasing transactions efficiently, even though the suggested architecture does not address them [Ali & Bhaya \(2021b\)](#). Regarding pseudonymity, the model does not offer any safeguards to ensure users stay anonymous when using the system. Although there is no direct mention of availability, it mentions allowing users to verify certificates anytime and anywhere, increasing availability. It increases authenticity by using a safe verification technique to guarantee that academic credentials are valid. Nevertheless, privacy and confidentiality—two crucial aspects of safeguarding sensitive student data—are not addressed. Furthermore, compatibility was not addressed. However, it offers immutability, a key feature of blockchain technology that guarantees data integrity. The paper does not cover non-repudiation, which ensures that parties cannot withdraw from participating in transactions. To improve participant trust, the model includes a consensus base, which is essential for validating and updating student certifications. Transparency is mentioned in the study because the model makes it possible to see the procedures for issuing and verifying academic certificates. Interoperability is mentioned in the study as an issue, although it is not addressed [Ali & Bhaya \(2021b\)](#). Furthermore, the paper does not discuss data storage efficiency—essential for handling massive amounts of data. The approach does not seem user-centric since features that improve user experience are not highlighted. Furthermore, it ignores lifelong learning, which is becoming increasingly important in the current educational environment. Lastly, neither transaction throughput nor transaction latency are covered in this article [Ali & Bhaya \(2021b\)](#).

2.4.2 Performance Analysis of Existing works without blockchain

The performance analysis of existing systems that do not rely on blockchain technology offers a comparative perspective on traditional solutions and their capabilities. Figure 6 provides a visual comparison of the performance metrics of non-blockchain systems, illustrating their effectiveness in addressing similar challenges without the use of decentralized technologies.

The article [Bell et al. \(2022\)](#) designed digital badges with standardized metadata, including comprehensive details such as the issuer, the criteria required for earning the badge, and the supporting evidence. This approach facilitates the creation of stackable credentials in a modular fashion, enabling the issuance of badges that are aligned with specific skills and competencies, thereby addressing the needs of both faculty and students. The system permits individuals to earn multiple badges and combine them to showcase

comprehensive skills and achievements. The capability for badge revocation is assured by implementing mechanisms for the verification of badges upon interaction. Furthermore, the framework acknowledges the concept of open badging, which allows for the sharing of verifiable badges across various organizations.

The framework presented in [Clements et al. \(2020\)](#) incorporates metadata into digital badges, thus offering an explicit description of the skills or knowledge necessary for badge acquisition. These badges serve as representations of personal achievements, providing a comprehensive summary of the student's competencies. Furthermore, the framework allows students to amalgamate various badges to demonstrate a wider range of skills. The article suggests utilizing tools like Makebadges for the creation of digital badge images. It pertains to the crucial attribute of revocation ability, which allows badge issuers to retract badges under conditions of misconduct or when credentials held are invalid. The framework further maintains the importance of conformance to standard, for instance, Open Badges Infrastructure (OBI), to ensure that there is interoperability between diverse platforms and systems. Finally, the framework supports the creation of competencies and knowledge whereby students move into the higher-order badges as they show improved competencies.

In the research [Ahmat et al. \(2021\)](#) the framework ensures granularity in that it allows enrolled students to engage in various micro-credentials of their choice, even if those are outside of their area of study. It supports capability for students to gain digital badges via micro-credential modules that can be collected along with the academic record. Moreover, the framework insists on the standards to be maintained relating to digital badges, focusing on the quality and integrity of the micro-credential certification scheme. Further, it supports the collaboration between higher education institutions and micro-credential providers in the development of a program on micro-credentials responding to the needs of the industry; hence, it would be easier to transfer credits across stackable micro-credentials programs from different educational providers. Also, the framework encourages students to take modules related to their career goals across several institutions in a network and increase their competency. The Common Micro-credentials Framework (CMF) discussed in [Antonaci et al. \(2021\)](#) ensures that courses are designed according to its standardized metadata, which includes learning outcomes, hours of study required, European Qualifications Framework (EQF) level, and the number of credit points earned. Courses aligned with this framework offer a specific level of granularity by stipulating a workload of 100-150 hours. This structure allows learners to accumulate credentials for each 4-6 ECTS, which can contribute to a larger degree program. The framework employs

Reference Paper	Standardized Metadata	Granularity	Stackability	Digital Badge Image	Revocation Capability	Interoperability	Level-Up
[64]	✓	✓	✓	X	X	✓	✓
[65]	✓	✓	✓	X	X	X	✓
[60]	✓	✓	✓	✓	✓	✓	✓
[61]	✓	✓	✓	✓	✓	✓	✓
[71]	✓	✓	✓	✓	✓	X	X

Figure 2.3: Performance Analysis of Non-blockchain Based Solutions

Bologna tools such as the European Qualification Framework (EQF), the European Credit Transfer and Accumulation System (ECTS), and the Diploma Supplement (DS) to enhance interoperability between institutions. Additionally, it provides learners with opportunities to progress and elevate their qualifications within the European Qualification Framework.

The analysis of the proposed model in article [Tan et al. \(2024\)](#) highlights its potential in addressing the talent gap while identifying areas for improvement. Key strengths of the model include standardized metadata, which ensures transparency and consistency; granularity, which allows for a tailored educational experience; and stackability, which facilitates the accumulation of skills towards larger qualifications. Additionally, the use of digital badges enhances the visibility of achievements, and the revocation capability maintains the integrity of the credentialing process. However, the model's lack of interoperability may hamper the seamless recognition of credentials across various platforms, and the absence of a level-up mechanism may affect learner engagement and motivation. Addressing these weaknesses is essential to fully realize the model's benefits.

Chapter 3

Methodology

Blockchain-Based Micro-Credentials verification system for higher education is developed using Agile methodology, ensuring iterative progress and adaptability. This approach emphasizes continuous stakeholder collaboration to improve features and meet evolving requirements. Continuous improvement through stakeholder feedback and incremental improvements guarantees secure credential verification and seamless institutional integration. Given that educational institutions have different policies, course exemption criteria, and security requirements, Agile provides a structured yet flexible approach. This approach ensures that the system evolves based on real-time feedback and new technological advancements.

3.1 Introduction

The proposed system utilizes blockchain technology to address key challenges in credential management, such as fraud, inefficiency, and lack of transparency. It integrates blockchain-based micro-credential verification with traditional education system, enabling students to manage and securely share their academic credentials. At the same time, institutions retain control over course exemptions. By storing credit-bearing micro-credentials on the blockchain, the system ensures that credentials are tamper-proof and easily verifiable. These credentials are also accessible to students through a digital wallet. Unlike rigid development models, the Agile approach ensures that the system is continuously improved to meet institutional requirements, security standards, and evolving educational frameworks. Each development phase is conducted in iterative sprints, ensuring that new insights and stakeholder feedback influence future improvements.

3.2 System Development Model

3.2.1 Agile Model

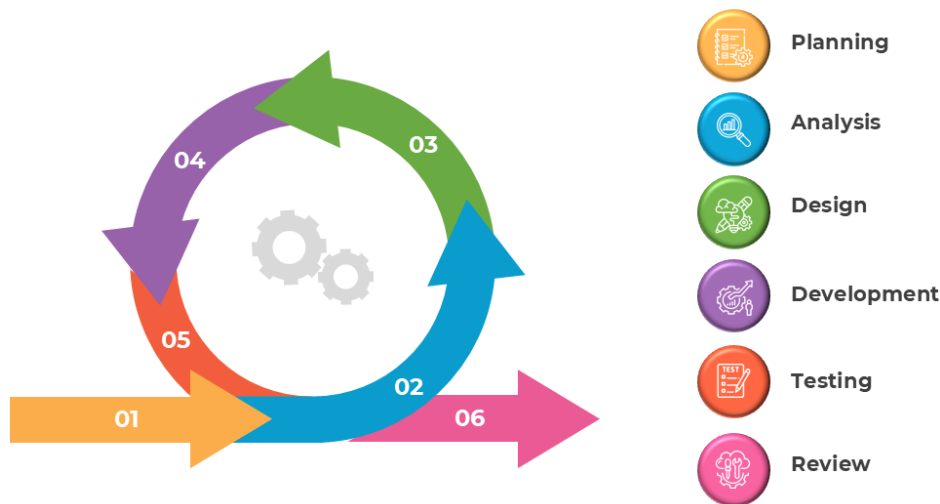


Figure 3.1: Agile model

The system is developed using the agile methodology, emphasizing iterative progress, collaboration, and adaptability. Unlike traditional linear approaches, agile allows the development team to break the project into smaller, manageable sprints. The Agile methodology divides the project into six interconnected phases. Each sprint focuses on delivering a specific feature or component, such as blockchain integration, digital wallet functionality, or credential verification mechanisms. Each sprint delivers a functional segment of the system, which is tested and improved before progressing to the next iteration. Regular feedback from stakeholders ensures that the system evolves to meet user needs and adapts to changing requirements. This approach accelerates development and minimizes risks by identifying and addressing issues early in the process. This ensures that the system is continuously optimized.

The system's goals are defined in the planning phase, including integrating blockchain technology for secure credential verification and institutional control over course exemption. During this phase, stakeholder needs (students and institutions) are gathered and documented, ensuring the system meets functional and non-functional requirements.

Based on these needs, a comprehensive system design is developed. This design includes the blockchain architecture and how credentials will be stored and verified securely. It also outlines how institutional rules will be integrated to manage course exemption processes. The system architecture is created during the design phase, ensuring it adapts to institutional requirements. The design also addresses how blockchain will be integrated for secure data storage and verification. UI/UX designs are developed to ensure a user-friendly interface for students and easy management for institutions. Based on the design, Agile sprints are planned to ensure features are developed iteratively and stakeholder feedback is incorporated immediately. In the development phase, the design is translated into code. Key features, such as credential storage on blockchain and the integration of smart contracts for secure credential verification, are implemented in this phase. Development includes setting up blockchain nodes, developing the digital wallet, and integrating data privacy and security measures. During this phase, testing mechanisms are also implemented to ensure the security and functionality of the blockchain system. Each feature is thoroughly tested in the testing phase to ensure it functions according to specifications. Security testing ensures that data integrity and credential verification processes are secure. User acceptance testing (UAT) is conducted to ensure that students and institutions can easily interact with the system. Blockchain nodes and smart contracts are tested for reliability and performance under real-world conditions. Any issues found are addressed promptly through continuous iterations and improvements, ensuring the system meets the defined functional and security requirements. Once the system passes testing, it enters the deployment phase. The system is deployed within pilot institutions, and the blockchain nodes are set up for secure credential verification. In this phase, institutions use the system to manage micro-credentials and process course exemption requests. The system is continuously monitored and updated in the review phase based on real-time feedback from students and institutions. Performance improvements and security patches are implemented regularly to ensure the system remains robust, reliable, and adaptable to changing educational policies and technological advancements. Continuous integration of new features ensures that the system evolves based on stakeholder feedback and emerging needs, maintaining its reliability and security over time.

3.3 System Analysis

System analysis is a critical phase that involves understanding the system's objectives, features, and operational requirements. It provides a comprehensive overview of how the system will function. The core objectives of the system are to provide students with

secure, verifiable credentials, including both academic and micro-credentials. It also allows institutions to customize exemption policies based on their specific criteria. Additionally, the system ensures blockchain-based security, fraud prevention, and transparency. The system defines clear user roles: Students can request, store, and share credentials (academic and micro-credentials) through the system, with control over who can access them. The verifying body ensures the authenticity of the micro-credentials. After that, Students can also request course exemptions based on their verified micro-credentials. Universities are notified of the verification and grant course exemptions according to their policy, using the blockchain system for secure validation. Security and performance considerations focus on ensuring data integrity and preventing credential tampering through the blockchain's tamper-proof nature.

3.3.1 System Design

The system design phase focuses on creating a blueprint for the micro-credential platform. This includes defining the architecture, data flow, and user interfaces. Key components of the design include:

- **Blockchain Integration:** A decentralized ledger to store and verify credentials securely.
- **Digital Wallet:** A user-friendly interface for students to access and share their credentials.
- **Smart Contracts:** Automated workflows for credential management.
- **Institutional Dashboard :** A dashboard for educational institutions to define course exemption criteria.

3.3.2 Implementation

The implementation phase brings the system design to life by translating requirements into functional code. Key activities during this phase include:

- **Smart Contract development:** Implementation of smart contracts for credential management.
- **Blockchain Development:** Distributed ledger network is established, ensuring decentralized credential storage and transparent validation across multiple nodes.

- **Digital Wallet Integration:** Responsive, easy-to-use interface has been built for students, with secure access controls and credential-sharing mechanisms implemented.
- **Institutional Dashboard Implementation:** Universities define the exemption rules of the courses within the system.
- **Security and Performance Optimization:** The system ensures tamper-proof credential storage through advanced encryption, safeguarding data integrity and preventing unauthorized modifications. A high-performance blockchain network is deployed to enable fast, secure, and efficient credential verification in real time.

3.4 Requirement Engineering

Requirement engineering is a systematic process of identifying, analyzing, documenting, and validating the functional and non-functional requirements of the Blockchain-Based Micro-Credentials verification system for higher education. This process is essential for aligning stakeholder expectations with system capabilities, preventing future design flaws, and ensuring seamless integration with existing educational frameworks. This phase ensures that the system is designed and implemented according to the needs of students, educational institutions, and accreditation bodies. It also guarantees that the system delivers high performance and reliability.

3.5 Requirement Engineering Process

The Requirement Engineering Process consists of four key phases: Feasibility Study, Requirement Gathering, Software Requirement Specification (SRS), and Software Requirement Validation. This structured approach ensures that the system is built on a solid foundation, minimizing risks and maximizing stakeholder value.

3.5.1 Feasibility Study

The feasibility study evaluates whether the proposed Blockchain-Based Micro-Credentials verification system for higher education is technically, operationally, and financially viable before proceeding with full-scale development.

Technical Feasibility:

- The system leverages blockchain technology to store verifiable, tamper-proof credentials securely.

- Smart contracts automate credential management, reducing manual workload.
- Cryptographic encryption ensures secure transactions and prevents credential fraud.

Operational Feasibility

- The system aligns with institutional needs, providing universities with a dashboard for credential issuance and exemption rules.
- Students can store, manage, and share credentials through a digital wallet, ensuring ease of use.
- The system supports real-time processing, ensuring seamless credential verification and exemption approvals.

Economic Feasibility

- It reduces administrative costs by eliminating manual verification processes and credential fraud risks.
- The long-term ROI (return on investment) is high as universities and businesses are adopting secure digital methods to verify credentials.

3.5.2 Requirement Gathering

Requirement gathering for the proposed system involve the participation of stakeholders such as students, educational institutions, accreditation bodies and employers. This helps to understand their needs and expectations while ensuring the system meets their requirements. Data collection techniques such as interviews, surveys, and workshops are used to collect functional requirements (e.g., credential issuance, verification mechanisms and digital wallet integration) and non-functional requirements (e.g., security, scalability and reliability). This process ensures that the system addresses real-world challenges and delivers tangible benefits while maintaining usability and security.

3.5.3 Software Requirement Specification

The Software Requirement Specification (SRS) defines the functional and non-functional requirements that guide system development. The system's behavior, including features like User Authentication, Role-based access control, Credential Issuance, verification and Storage, Course exemption, Smart contract and blockchain integration, is described in

depth by the functional requirements. Non-functional requirements include security, reliability, auditability, efficiency and user-friendliness. This article covers the usage of use case diagrams, activity diagrams and work breakdown structures, among other standard documentation techniques. These techniques are used to effectively document software requirements.

3.5.4 Software Requirement Validation

Software Requirement validation ensures that the documented specifications are accurate, consistent, comprehensive and complete. This involves reviewing the SRS with stakeholders and addressing any gaps or inconsistencies. Validating requirements early in the process reduces the risk of errors or misalignment with user expectations. Validation also improves communication between stakeholders and development teams, ensuring that everyone is aligned on the system's goals. Ultimately, it saves time and costs by preventing costly rework, improving the quality of the final product, and increasing customer satisfaction.

3.6 Software Requirement for Development

The software requirements listed below are necessary for developing the proposed Blockchain-Based Micro-Credentials verification system for higher education. First, a robust blockchain platform like Hyperledger Besu is essential for supporting smart contracts and providing a secure, decentralized ledger to manage credentials. The system must support a reliable consensus mechanism to ensure integrity and transparency in credential issuance and verification. It should include secure authentication and authorization components to protect user data and prevent unauthorized access. Off-chain storage solutions like MongoDB are required for managing additional metadata efficiently. Comprehensive testing tools and frameworks should be used to validate performance, security, and scalability under different conditions. Monitoring solutions like Prometheus and Grafana will help track blockchain operations, ensuring system reliability and uninterrupted service.

3.6.1 Microsoft Visual Studio

Microsoft Visual Studio Code (VSCode) is a versatile and feature-rich source code editor that has been utilized for developing the blockchain-based academic credential verification system. It offers extensive support for various programming languages and provides productivity-enhancing extensions, such as Solidity language support for smart contract

development. With cross-platform compatibility and a lightweight design, VSCode ensures accessibility and flexibility for developers working across different operating systems. The editor's debugging tools, integrated terminal, and version control support make it an ideal choice for efficiently writing, testing, and deploying smart contracts and other system components. For this project, Visual Studio Code has been instrumental in managing the complexity of developing a decentralized credential verification platform by streamlining the coding process and enhancing developer productivity [Kumar et al. \(2024\)](#).

3.6.2 Remix IDE

Remix IDE is a powerful and open-source integrated development environment (IDE) designed specifically for Ethereum smart contract development using the Solidity programming language. It is a vital tool for building the blockchain-based academic credential verification system, enabling efficient smart contract creation, testing, and deployment. Remix IDE is widely regarded as one of the most popular platforms for writing, analyzing, and debugging Ethereum-based smart contracts. The IDE features a robust code editor, a console for interacting with the Ethereum blockchain, and a rich set of plugins to enhance functionality. These include integrated testing environments and static analysis tools to identify potential issues in the smart contract code. With its user-friendly interface, Remix IDE supports both local and remote development, making it accessible for developers of all skill levels. For this project, Remix IDE has facilitated rapid prototyping and streamlined the development process, ensuring the system's smart contracts meet the required standards for security and efficiency [Fukuzawa et al. \(n.d.\)](#).

3.6.3 Truffle

Truffle is a widely-used Ethereum development framework that simplifies the development, deployment, and testing of decentralized applications (dApps). It has been instrumental in constructing the blockchain-based academic credential verification system, particularly for managing smart contract lifecycle processes. Truffle provides features such as automated compilation and deployment of smart contracts, as well as a built-in testing framework, which ensures comprehensive validation and debugging. With its JavaScript-based API, Truffle facilitates seamless interaction with deployed smart contracts, enabling developers to integrate smart contract functionality into dApps efficiently. Additionally, Truffle's extensive documentation and active developer community offer valuable resources and support for developers of all skill levels. These features make Truffle an essential tool for accelerating the development of secure and robust blockchain

applications, including systems designed for academic credential management [Vaidya et al. \(2024\)](#).

3.6.4 NodeJS

The proposed blockchain-based academic credential verification system relies on Node.js, an open-source server-side JavaScript runtime environment. Node.js offers high performance and scalability, making it capable of handling multiple tasks concurrently and processing significant amounts of data efficiently. Its non-blocking, event-driven architecture is particularly suited for applications requiring real-time interaction, such as decentralized systems. As Truffle and related tools used in this project are JavaScript-based applications, Node.js serves as the foundation for their operation. Its integration into the system underscores its critical role in supporting the development, testing, and deployment of smart contracts and decentralized applications (dApps). By leveraging JavaScript throughout the application stack, Node.js ensures a unified development environment. Additionally, its active community and abundant resources make it a stable and reliable platform for building innovative solutions like this blockchain-based credential management system [Panda & Satapathy \(2021\)](#).

3.6.5 Metamask

MetaMask is a browser-based digital wallet that enables secure cryptocurrency management and seamless interaction with decentralized applications (dApps) on blockchain networks such as Ethereum. It plays a vital role in the proposed blockchain-based academic credential verification system by providing secure authentication, transaction authorization, and smart contract interaction capabilities. Through its user-friendly interface, MetaMask simplifies Ethereum account management, allowing users to sign transactions and interact with deployed smart contracts efficiently. The integration of MetaMask into the system ensures that credential issuers and verifiers can securely access and execute blockchain transactions. Its JavaScript-based API allows for smooth interaction with web applications, making it an essential component for enhancing blockchain usability. Additionally, MetaMask benefits from extensive documentation and a strong developer community, further solidifying its role as a reliable tool for blockchain-based credential management [Jain et al. \(n.d.\)](#).

3.6.6 Hyperledger Besu

Hyperledger Besu is crucial for the proposed blockchain-based academic credential verification system as it provides a secure and permissioned blockchain environment, ensuring that only authorized entities participate in credential issuance and verification. By leveraging smart contracts, Hyperledger Besu automates credential validation processes, reducing errors and enhancing operational efficiency. One of its key advantages is its support for privacy and confidentiality, ensuring that sensitive credential data remains protected while maintaining transparency where necessary. Additionally, Hyperledger Besu offers customizable consensus mechanisms, such as Quorum Byzantine Fault Tolerance (QBFT), which enhances security and reliability. Its integration capabilities with public blockchains like Ethereum also provide flexibility in implementing secure and scalable blockchain applications. Enterprises increasingly adopt Hyperledger Besu for its ability to facilitate private transaction processing while maintaining high transaction throughput. These features make it an optimal choice for building a decentralized and verifiable academic credential management system, ensuring both security and efficiency in the credentialing process [Nair et al. \(2024\)](#).

3.6.7 Docker

Docker is a platform that allows developers to develop, distribute, and run applications in lightweight, portable containers. In our Blockchain-Based Micro-Credentials verification system for higher education, Docker plays a key role in simplifying deployment and maintaining consistency across different environments. We use Docker to run Hyperledger Besu, ensuring that our blockchain infrastructure remains stable and easily replicable. By containerizing Besu nodes, we eliminate configuration discrepancies and make the network deployment process efficient. Additionally, Docker enables seamless testing and production deployment, allowing our team to focus on development rather than infrastructure management. With Docker, our system benefits from faster deployment, improved scalability, and reduced dependency conflicts, making it an ideal solution for our decentralized micro-credential verification framework [Wu et al. \(2024\)](#).

3.6.8 Web3.py

Web3.py is essential to this system as it provides the necessary tools for interacting with the Ethereum blockchain, which serves as the foundation for implementing the proposed solutions. It is a Python library that allows developers to integrate blockchain functionality into their applications, enabling users to interact with smart contracts, read and write

data to the blockchain, and manage digital assets securely. In our system, Web3.py facilitates interaction with smart contracts deployed on Hyperledger Besu by providing programmatic access through the given ABI. It enables seamless blockchain integration, making transaction handling, contract deployment, and querying efficient. With its well-documented APIs and active community support, Web3.py ensures reliable and scalable development for decentralized applications [Sara \(n.d.\)](#).

3.6.9 Prometheus

Prometheus is essential for monitoring and analyzing our blockchain-based micro-credential verification system. It is an open-source monitoring solution designed for collecting, storing, and querying time-series data, making it ideal for tracking blockchain network performance and smart contract interactions. In our system, Prometheus helps monitor Hyperledger Besu nodes, capturing metrics such as transaction processing time, block creation rates, and network activity. It integrates with Grafana for real-time visualization, providing insights into system performance and potential issues. With its powerful querying language (PromQL) and efficient alerting system, Prometheus ensures reliability, scalability, and proactive maintenance of our decentralized application [Misal \(2024\)](#).

3.6.10 Grafana

Grafana is essential for visualizing and analyzing the performance of our blockchain-based micro-credential verification system. It is an open-source analytics platform that enables real-time monitoring of Hyperledger Besu nodes and smart contract activities. In our system, Grafana integrates with Prometheus to display blockchain metrics such as transaction throughput, block creation time, and node performance. Its customizable dashboards provide clear insights into system health, helping identify bottlenecks and optimize performance. With its interactive graphs, alerting system, and support for multiple data sources, Grafana ensures efficient monitoring, making our decentralized application more reliable and scalable [Eichhorn et al. \(n.d.\)](#).

3.6.11 MongoDB

MongoDB is essential for managing off-chain data in our blockchain-based micro-credential verification system. It is a NoSQL database that provides flexibility, scalability, and efficient storage for handling credential metadata, user profiles, and transaction logs. In our system, MongoDB stores off-chain information such as user details, issued credentials, and verification history while ensuring fast retrieval and seamless integration with Hyperledger

Besu. Its document-based structure allows dynamic schema updates, making it adaptable to evolving system requirements. With features like indexing, aggregation, and horizontal scaling, MongoDB ensures efficient data management, enhancing the performance and reliability of our decentralized application [Kheng et al. \(n.d.\)](#).

3.6.12 EtherJS

Ethers.js is essential for integrating blockchain functionality into our blockchain-based micro-credential verification system. It is a lightweight and efficient JavaScript library designed for interacting with Ethereum-based networks, including Hyperledger Besu. In our system, Ethers.js facilitates seamless communication with smart contracts, enabling credential issuance, verification, and retrieval. It provides robust wallet management, secure transaction signing, and efficient contract interactions. With its modular architecture, Ethers.js simplifies blockchain queries, event listening, and data fetching, ensuring a smooth user experience. Its strong community support and built-in utilities make it an ideal choice for building a reliable and scalable decentralized application [Naik & Naik \(n.d.\)](#).

3.6.13 Lucid Chart

Lucidchart is a web-based diagramming tool that is used in the development of our blockchain-based micro-credential verification system. It enables users to create, share, and collaborate on various visual representations, including system architectures, smart contract workflows, and blockchain network diagrams. With its customizable templates and drag-and-drop functionality, Lucidchart simplifies the creation of technical diagrams. Being cloud-based, it allows access from any device, ensuring seamless collaboration. Its multiple export options make it easy to integrate diagrams into project documentation, aiding in clear communication and efficient system design [Alasaly & Grando \(2021\)](#).

3.6.14 Mendeley

Mendeley is a comprehensive reference management and academic networking tool that supports the research and development process of our blockchain-based micro-credential verification system. It helps in finding, sharing, and organizing research papers efficiently, making access to academic resources and collaboration easier. Mendeley simplifies reference management by accurately incorporating citations and bibliographies. Its cross-platform interface provides an intuitive user experience, allowing users to build a personal library accessible from any device. With robust search and labeling features, Mendeley

streamlines the research workflow, ensuring efficient organization and retrieval of relevant materials [Shilpa & India \(n.d.\)](#).

3.6.15 LaTeX

LaTeX is a document preparation tool widely used for technical and scientific writing, making it beneficial for our blockchain-based micro-credential verification system. It ensures a consistent and polished output by allowing users to focus on content while automatically managing the layout. LaTeX enhances the uniformity and professionalism of project documentation, particularly in handling mathematical formulas with its advanced typesetting capabilities. It supports citations, references, and bibliographies through various packages, ensuring well-structured documents. Integration with version control systems facilitates collaboration, while its cross-referencing features help maintain clarity and organization in research papers and reports [Bahrani et al. \(n.d.\)](#).

3.7 Required Programming Language

Developing the blockchain-based micro-credential verification system requires expertise in Solidity, JavaScript, and Python. Solidity is used to implement smart contracts on the Hyperledger Besu blockchain, ensuring secure and transparent credential management. JavaScript plays a key role in deploying smart contracts using Truffle, writing scripts to compile, migrate, and interact with contracts. It also helps integrate blockchain functionality into the front-end application. Python is essential for backend automation and data processing, supporting tasks such as querying blockchain data, managing transactions, and ensuring efficient system operations. These languages collectively enable a seamless and functional decentralized system.

3.7.1 Solidity

Solidity is essential for developing the blockchain-based micro-credential verification system. It is a high-level, statically typed programming language that supports inheritance, polymorphism, libraries, and complex user-defined types, making it ideal for building secure and efficient smart contracts. Solidity enables the creation of self-executing contracts where the rules are directly encoded, ensuring transparency and automation in credential issuance and verification. It helps securely manage the storage and validation of credentials on the blockchain, making the system tamper-proof. With features like inheritance and

interfaces, Solidity ensures that smart contracts remain modular, maintainable, and secure for decentralized applications [Vaccargiu et al. \(n.d.\)](#).

3.7.2 Python

Python is a dynamic and versatile programming language essential for the blockchain-based micro-credential verification system. It plays a key role in backend development, enabling efficient data processing, automation, and integration with blockchain networks. Python simplifies interaction with Hyperledger Besu using Web3.py, allowing seamless smart contract deployment and blockchain queries. Its readability and simplicity make it accessible to both beginners and experienced developers. With a strong community constantly adding new features, Python remains a reliable tool for handling complex tasks, ensuring smooth system operations, and enhancing the overall efficiency of decentralized applications [Mwape et al. \(2025\)](#).

3.7.3 React

React is essential for our blockchain-based micro-credential verification system. It is a modern JavaScript library used for building interactive and efficient user interfaces. In our system, React powers the front-end, enabling seamless interaction with the blockchain and smart contracts deployed on Hyperledger Besu. With its component-based architecture, React ensures a modular and scalable UI, making it easier to manage state and render real-time blockchain data. It integrates smoothly with Web3.js and Ethers.js, allowing users to connect wallets, verify credentials, and interact with smart contracts effortlessly. React's extensive ecosystem, fast rendering through the virtual DOM, and strong community support make it an ideal choice for building responsive and dynamic decentralized applications [Brett et al. \(2024\)](#).

3.7.4 JavaScript

JavaScript is crucial for our blockchain-based micro-credential verification system. It is a high-level, interpreted language known for its dynamic and versatile capabilities. In our system, JavaScript is used to write scripts for compiling Solidity contracts, deploying them on Hyperledger Besu, and interacting with deployed contracts. It plays a key role in smart contract deployment using Truffle, ensuring smooth blockchain integration. JavaScript enables efficient backend communication through asynchronous programming, making transactions and data retrieval seamless. Its extensive ecosystem provides access to

powerful libraries and tools, offering flexibility, scalability, and strong community support for decentralized application development [Cherukuri \(n.d.\)](#).

Chapter 4

Design and Development

4.1 Project Management and Financial Activities

Project management play a vital role in overseeing the development, deployment, and maintenance of the blockchain-based management system for credit-bearing micro-credentials. Their responsibilities include ensuring efficient resource allocation, stakeholder coordination, and strict adherence to project timelines. Concurrently, financial activities such as budgeting, securing funding, and financial monitoring are essential to ensure the system's long-term sustainability and operational success.

This section explores the intersection of project management and financial strategies within the proposed blockchain-based management system. It emphasizes the significance of effectively addressing challenges related to resource management, cost control, and scalability. By implementing robust project management practices and sustainable financial planning, the system can successfully facilitate the verification and management of credit-bearing micro-credentials while ensuring its long-term viability and impact.

4.1.1 Work Breakdown Structure

A Work Breakdown Structure (WBS) is a project management technique that divides a project into smaller, more manageable parts. The overall scope of the project is organized and defined by these parts, which are usually represented in a hierarchical form. An increasingly detailed definition of the project work is given at each sub level of the WBS. By using WBS, project managers can effectively plan, organize and manage projects by determining the necessary activities, dependencies and resources required at each level of this structure. Figure 4.1 presents the WBS of our proposed scheme. It plays an important role to provide a roadmap for project implementation, management and enabling effective coordination of activities.

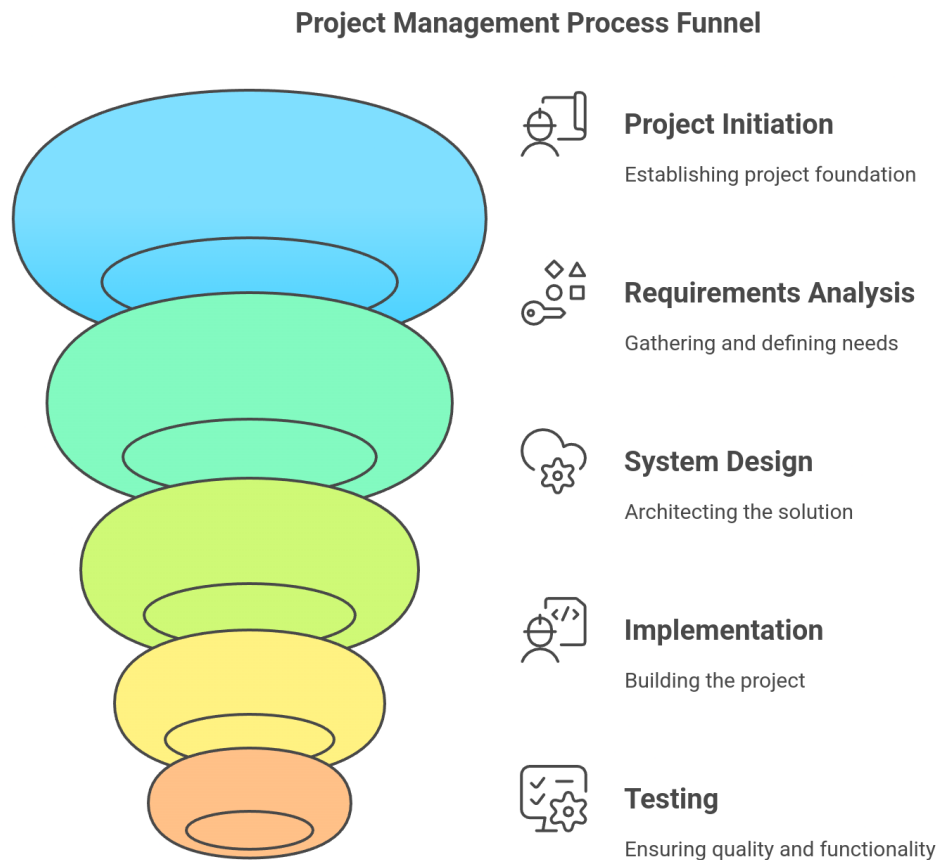


Figure 4.1: Work Breakdown Structure

4.1.2 Estimate Costs

To calculate the costs related to each of the work packages within the WBS, both direct and indirect costs need to be considered. An example of estimated costs for each work package taking into account different cost factors is given below:

4.1.2.1 Project Planning and Initiation

- **Define Project Scope:** No direct costs.
- **Identify Stakeholders:** No direct costs.
- **Create Project Charter:** No direct costs.

4.1.2.2 Requirements Analysis

- **Identify Requirements:** No direct costs.
- **Requirements Documentation:** No direct costs.
- **Conduct Market Research:** Cost of market research reports or consulting fees.
- **Review Requirements with Stakeholders:** Consulting fees.
- **Requirements Specification:** No direct costs.

4.1.2.3 System Design

- **Develop System Architecture:** Cost of design tools and UI/UX resources.
- **Create Detailed Design Specifications:** Cost of design tools.
- **Review Design with Stakeholders:** Consulting fees.
- **Finalize Design Documents:** No direct cost.

4.1.2.4 Implementation or Coding

- **Set Up Development Environment:** Cost of hardware, software licenses, and cloud services.
- **Develop Smart Contract:** Developer salaries or consulting fees.
- **Conduct Code Reviews:** No direct cost.

4.1.2.5 Testing

- **Prepare Test Plan:** No direct cost.
- **Unit Testing:** Testing resources' salaries or consulting fees.
- **Integration Testing:** Testing resources' salaries or consulting fees.
- **System Testing:** Testing resources' salaries or consulting fees.
- **User Acceptance Testing:** Testing resources' salaries or consulting fees.

4.1.2.6 Deployment

- **Create Deployment Plan:** No direct cost.
- **Deploy System to Production:** Deployment resources' salaries or consulting fees.
- **Conduct Post-Deployment Verification:** Deployment resources' salaries or consulting fees.

4.1.2.7 Maintenance

- **Monitor System Performance:** Maintenance resources' salaries or consulting fees.
- **Provide Technical Support:** Support resources' salaries or consulting fees.
- **Implement Bug Fixes and Patches:** Development resources' salaries or consulting fees.
- **Perform System Enhancements:** Development resources' salaries or consulting fees.

4.1.3 Budget Plan

It is essential to create a project budget that includes all necessary costs and materials for the execution of projects, together with contingency funding. Any organization can improve the management of their financial resources, plan for additional needs, and achieve more effectively their objectives through the development of an integrated budget.

Table 4.1: Cost Breakdown

Cost Type	Description	Cost (in taka.)
Hardware	Networking devices	5,000
	High-performance Computer 1	1,00,000
	High-performance Computer 2	1,20,000
	Server Setup	80,000
	Total cost	3,05,000
Developer	Salary of 2 developers in 6 months	4,00,000
Software	Blockchain tools and licenses	50,000
Maintenance	Maintenance cost (per month)	10,000
	Internet bill (per month)	2,000
Field Testing	Credential validation testing	60,000
Logistic Supports	Documentation and stationary	30,000
Total Project Budget		8,55,000

Based on our analysis, Table 4.1 provides an estimate of the costs for making this proposed system. The cost of making the project may vary depending on other factors.

4.1.4 Funding Plan

A funding plan, ensuring that the project has the necessary resources to achieve its objectives while maintaining financial health and sustainability, is essential for the effective management of the financial aspects of the project. The funds will be raised through a combination of government grants, angel investing, and crowdfunding.

4.1.4.1 Government Grants

The availability of government grants or funding sources to support technology firms may vary depending on the nation in which the firm is located. The group would have to fulfill certain requirements, such as having a solid business plan and a clear route to revenue, in order to be eligible for government grant.

4.1.4.2 Investor

Securing funding from micro-credential providers and organizations in the education sector could play a pivotal role in the success of the proposed system. Providers of credit-bearing micro-credentials, who recognize the potential for streamlined and transparent credential verification processes, may see long-term benefits in adopting a blockchain-based solution and choose to invest.

Additionally, forming partnerships with institutions and companies specializing in education technology, blockchain, and credential management can provide valuable financial support. These entities may view the project as an opportunity for future returns by enabling a secure, decentralized system that enhances trust, transparency, and efficiency in issuing and managing academic credentials. This approach not only ensures project funding but also aligns stakeholders with the system's success.

4.1.4.3 Crowdfunding

Funding can be increased through the launch of a crowdfunding campaign targeted at educators, students, and technology enthusiasts who are interested in supporting innovative solutions in academic credential verification. The team would need to create an engaging video and presentation showcasing the benefits of a blockchain-based micro-credential system. Setting clear financial targets and offering meaningful rewards, such as early access to the platform or exclusive features, can help attract backers and ensure the success of the crowdfunding campaign.

4.2 System Design and Description

The proposed system offers a secure and efficient approach for verifying and managing academic and micro-credentials. By leveraging blockchain technology, the system ensures tamper-proof credential storage, real-time verification, and a seamless process for course exemption management.

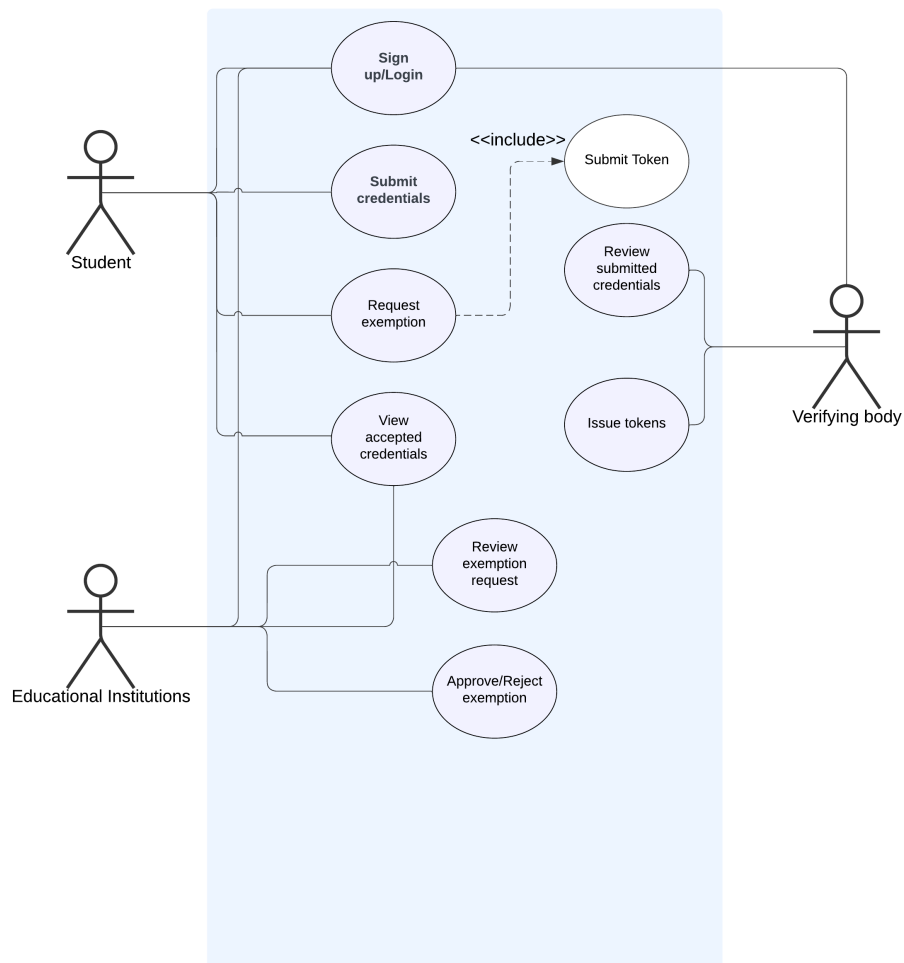


Figure 4.2: Use case diagram of the proposed system

Figure 4.2 shows a use-case representation of the proposed system. The diagram illustrates how each actor interacts with the system to perform various actions, ensuring a comprehensive understanding of the system's functionalities. It visually represents the interactions between the primary actors, such as students, educational institutions, and the verifying body and the key use cases involved in the system. The diagram illustrates how

each actor interacts with the system to perform various actions, ensuring a comprehensive understanding of the system’s functionalities.

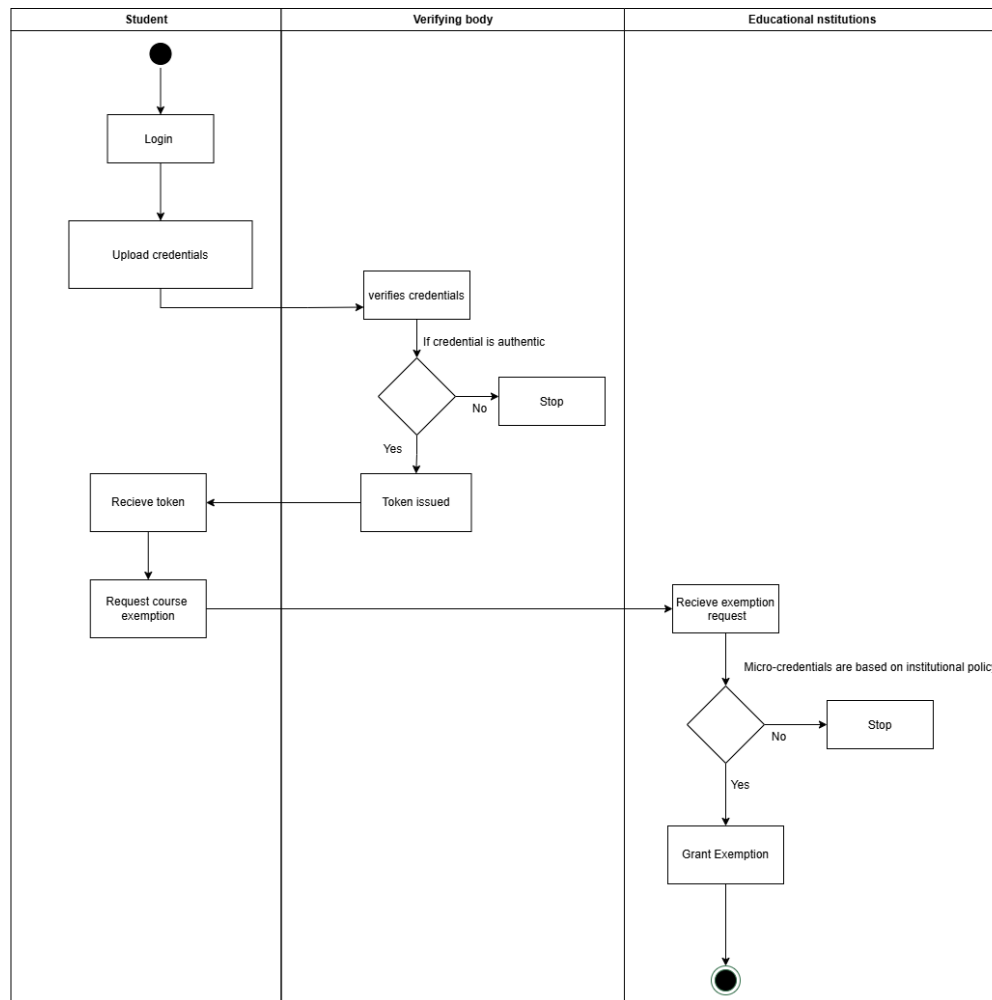


Figure 4.3: Activity diagram of the proposed system

Figure 4.3 shows workflow of the proposed system. It highlights the key interactions between students, the verifying body, and educational institutions. The process begins when the student logs in and uploads the necessary credentials. Once the credentials are submitted, the student waits for the verifying body to authenticate the credentials. The verifying body is responsible for verifying the submitted credentials. If the credentials are authentic, a token is issued to the student and credentials are stored on blockchain. Then, if a student wants, they can request for exemption with their authenticated token. Upon receiving the exemption request, the institution evaluates it based on its internal policies. The exemption is granted if the request is valid and the micro-credentials meet institutional criteria.

4.3 Implementation

This section details the implementation process of the proposed system, focusing on deploying the smart contract across two distinct blockchain environments. Hyperledger Besu was chosen to serve as the private, permissioned network, ensuring robust security and controlled access. Additionally, a public blockchain environment was also simulated to demonstrate seamless integration and interaction between the private network and external decentralized systems.

4.3.1 Smart Contract

Solidity was selected as the smart contract programming language to ensure that the code remains the same in both public and private blockchain after deployment. The smart contract uses Solidity version 0.8.0. SDN controllers and the trusted authority can use the deployed smart contract to interact and change the state of the blockchain.

Algorithm 1: Issue Token

- 1: **Data:** Token Structure
 - 2: **Input:** Credential Information
 - 3: **Output:** new tokenId
 - 4: Generate a unique tokenId of 5 characters
 - 5: Create a new token using Token(tokenId, Credential Information)
 - 6: Store the token details in tokens[tokenId] mapping
 - 7: Emit the TokenIssued event with tokenId, name, credentialTitle, credentialID
 - 8: Return tokenId
-

Algorithm 1 shows the function responsible for issuing a new token (credential) within the system. Only the trusted authority (contract owner) has the access and rights to execute this function. Whenever a new credential needs to be issued, the trusted authority will call the issueToken function and pass the required credential details, including the issuer and recipient public keys, name, credential ID, title, type, grade, institution, and IPFS hash, as arguments. The smart contract will then increment the tokenCount to generate a unique token ID. It will create a new token object with the provided details and store it in the tokens mapping. Finally, the contract emits a TokenIssued event, which logs key details such as the token ID, name, credential title, and credential ID. The function ensures that all tokens are securely stored and uniquely identified.

Algorithm 2 shows the function responsible for revoking a previously issued token. This function can only be executed by the trusted authority. When revocation is necessary,

Algorithm 2: Revoke Token

- 1: **Data:** Token Structure
 - 2: **Input:** tokenId
 - 3: Verify that `tokens[tokenId]` exists
 - 4: Check that the token is not already revoked using `isRevoked`
 - 5: Set `tokens[tokenId].isRevoked = true`
 - 6: Emit the `TokenRevoked` event with `tokenId`
-

the trusted authority calls the `revokeToken` function and passes the corresponding token ID as an argument. The smart contract verifies the existence of the token in the `tokens` mapping and checks that it has not already been revoked. If the checks pass, the `isRevoked` property of the token is set to `true`, marking it as invalid. The function then emits a `TokenRevoked` event to log the revocation action with the token ID. This ensures that any revoked tokens can no longer be considered valid, maintaining the integrity of the credential system.

Algorithm 3: Validate Token

- 1: **Data:** Token Structure
 - 2: **Input:** tokenId
 - 3: **Output:** Boolean (`true` if valid, `false` if revoked)
 - 4: Verify that `tokens[tokenId]` exists
 - 5: Return `!tokens[tokenId].isRevoked`
-

Algorithm 3 shows the function for validating the status of a token. It takes a token ID as input and checks its existence in the `tokens` mapping. If the token exists and its `isRevoked` property is `false`, the function returns `true`, indicating the token is valid. Otherwise, it returns `false`, signifying the token has been revoked.

Algorithm 4: Retrieve Token Details

- 1: **Data:** Token Structure
 - 2: **Input:** tokenId
 - 3: **Output:** All token details
 - 4: Verify that `tokens[tokenId]` exists
 - 5: Retrieve and return all details from `tokens[tokenId]`
-

Algorithm 4 shows the function for retrieving token details. The `getToken` function takes a token ID as input, verifies its existence, and retrieves the corresponding token object from the `tokens` mapping. It then returns all metadata, including the issuer, recipient, credential details, and revocation status.

4.3.2 Deployment of Smart Contract in Hyperledger Besu

Hyperledger Besu is an enterprise-focused Ethereum client, which is a part of the Hyperledger project. As per the functionality of the system, it is necessary for the blockchain network to be private or permissioned for more secure transactions. Besu is designed to accommodate the requirements of both public and private blockchains [Fan et al. \(2022\)](#)[Boggio Viola \(2024\)](#). Combined with Besu's compatibility with the Ethereum client, it makes it the ideal ecosystem to implement our system. Fundamentally, Hyperledger Besu is an Ethereum Virtual Machine (EVM) built on the Java platform. Thus, in order to run it, a version of Java 17 or higher is required. This allows Besu to communicate with decentralized applications (dApps) and execute smart contracts.

A blockchain includes a consensus mechanism. The consensus mechanism plays a role in enabling nodes to agree on the blockchain's current state. Through a consensus mechanism, a single, reliable, and unchangeable record is maintained without the need for any central authority, thus guaranteeing that all nodes have the same perspective on the blockchain [Hussein et al. \(2023b\)](#).

The system proposed here uses a Quorum Byzantine Fault Tolerance (QBFT) consensus mechanism. Figure 4.4 showcases the network structure. The QBFT network operates by guaranteeing consensus through a series of actions. Every round, a block proposal is made, which is then distributed to validators. Upon receiving it, the validators send a prepare message. The prepare message is followed by a commit message. When two-thirds of validators offer a commit message, a consensus is attained, and the block is added. Despite any faulty nodes, this consensus assures that the networks are robust and safe [Gerrits et al. \(2021b\)](#).

After setting up the private network, a truffle project containing the smart contract is placed in the root folder. The solidity compiler compiles the code into bytecode and generates ABI, which will be deployed to the blockchain network. Figure 4.5 shows the generated ABI for the smart contract.

Figure 4.6 shows the migration script. It takes the smart contract artifacts as input. A function is exported, accepting the truffle 'deployer' object as its argument. This function defines the deployment steps, typically utilizing the 'deployer.deploy()' method to deploy contracts along with any required constructor arguments or initialization parameters. Additionally, the migration script can manage contract dependencies, ensuring that dependencies are deployed prior to dependent contracts.

After compiling the smart contract, the truffle-config.js file is set accordingly to connect to the Besu network. It takes network specifications for Besu, such as network ID, host,

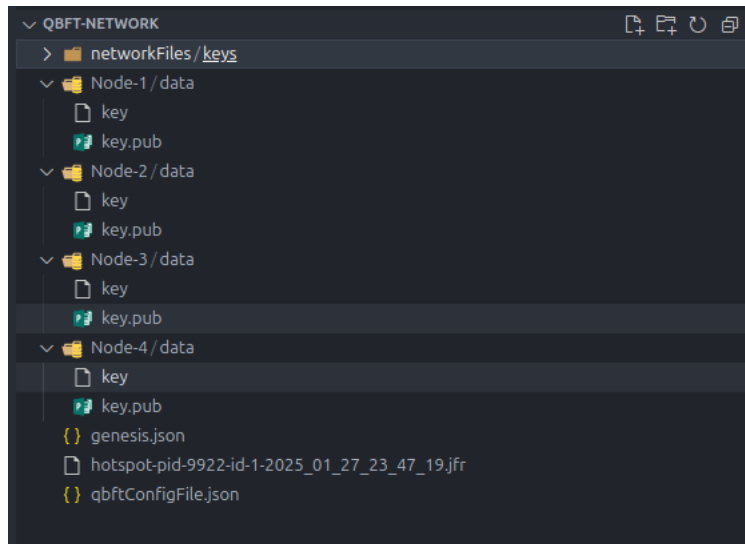


Figure 4.4: QBFT Network Structure

```

1  {
2    "contractName": "Token",
3    "abi": [
4      {
5        "inputs": [],
6        "stateMutability": "nonpayable",
7        "type": "constructor"
8      },
9      {
10       "anonymous": false,
11       "inputs": [
12         {
13           "indexed": false,
14           "internalType": "uint256",
15           "name": "tokenId",
16           "type": "uint256"
17         },
18         {
19           "indexed": false,
20           "internalType": "string",
21           "name": "name",
22           "type": "string"
23         },
24         {
25           "indexed": false,
26           "internalType": "string",
27           "name": "credentialTitle",
28           "type": "string"
29         },
30         {
31           "indexed": false,

```

Figure 4.5: ABI File Structure

```

1  const Token = artifacts.require("Token");
2
3  module.exports = function (deployer) {
4    deployer.deploy(Token);
5  };

```

Figure 4.6: Smart Contract Deployer

port etc. The contract is then deployed to the Besu network. Figure shows the successful deployment of the smart contract.

Figure 4.8 shows a successful transaction while adding a new credential using the


```
Result {
  '0': BN {
    negatives: 0,
    words: [ 1, <1 empty item> ],
    length: 1,
    red: null
  },
  '1': '0x1234567890AbcdEF1234567890AbcdEf12345678',
  '2': '0xABcdEFABcdEFabCdEFabCdEFABcdEFabCD',
  '3': 'Alice Smith',
  '4': 'CRED001',
  '5': 'Advanced Solidity Programming',
  '6': 'Certificate',
  '7': 'A',
  '8': 'Solidity Academy',
  '9': 'QmTzQ1Zt4ZNQCj2hA7CpSFF1oACZ39fQvGpRQ72vGsX5Wx',
  '10': false,
  token id: BN {
    negatives: 0,
    words: [ 1, <1 empty item> ],
    length: 1,
    red: null
  },
  issuerPublicKey: '0x1234567890AbcdEF1234567890AbcdEf12345678',
  recipientPublicKey: '0xABcdEFABcdEFabCdEFABcdEFabCdEFabCD',
  name: 'Alice Smith',
  credentialID: 'CRED001',
  credentialTitle: 'Advanced Solidity Programming',
  credentialType: 'Certificate',
  grade: 'A',
  institution: 'Solidity Academy',
  ipfsHash: 'QmTzQ1Zt4ZNQCj2hA7CpSFF1oACZ39fQvGpRQ72vGsX5Wx',
  isRevoked: false
}
```

Figure 4.9: getToken() Receipt

4.3.3 QBFT Test Accounts

The QBFT consensus environment in the Besu-based setup is specifically designed to simulate a consortium blockchain network using the Quorum Byzantine Fault Tolerance (QBFT) consensus algorithm. It is particularly suitable for testing scenarios that mimic real-world production consortium environments, offering a robust framework for private and permissioned networks. [Lopes \(2023\)](#).

```

"config": {
  "chainId": 1337,
  "berlinBlock": 0,
  "qbft": {
    "blockperiodseconds": 2,
    "epochlength": 30000,
    "requesttimeoutseconds": 4
  }
},
"nonce": "0x0",
"timestamp": "0x58ee40ba",
"gasLimit": "0x47b760",
"difficulty": "0x1",
"mixHash": "0x63746963616c2062797a616e74696e65206661756c7420746f6c6572616e6365",
"coinbase": "0x0000000000000000000000000000000000000000000000000000000000000000",
"extraData": "0xf87aa0000000000000000000000000000000000000000000000000000000000000f85494d713fed0d452eb4dc777ed0aeb46e5dca83bcca94f2e1d78",
"alloc": {
  "fe3b55788fb62b89f4916b721be55ceb828dbd73": {
    "balance": "0xad78ebc5ac620000"
  },
  "627306090aba3A6e1400e9345bc60c78a8BEf57": {
    "balance": "9000000000000000000000000"
  },
  "f17f52151EbEF6C7334FAD080c5704D77216b732": {
    "balance": "900000000000000000000000"
  }
}
}

```

Figure 4.10: Allocated accounts for QBFT

The environment uses accounts and private keys configured in the Besu genesis file to control the participating nodes. These nodes are pre-configured to act as actual participants (validators) within the network, ensuring strict permissioning and governance. These accounts are pre-allocated with test currency for testing. Figure shows the allocated code

in the genesis.json file. The setup supports realistic network behaviors, including multi-node configurations, while providing production-ready features such as block gas limits, gas prices, and RPC APIs. This environment is ideal for testing private decentralized applications (DApps) or consortium-based applications that require specific governance rules. It provides a controlled yet realistic platform for evaluating application behavior and network dynamics under production-like conditions

4.3.4 Interplanetary Filing System (IPFS)

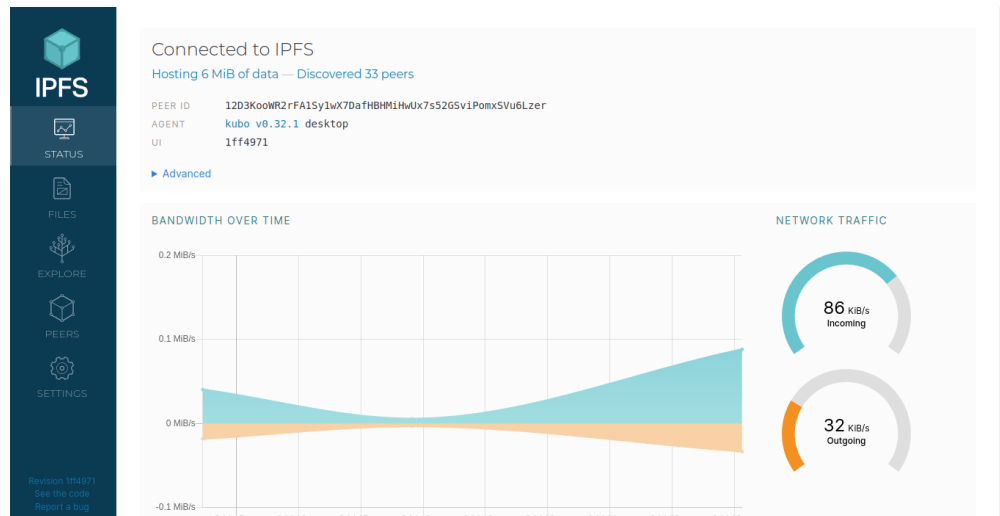


Figure 4.11: IPFS Dashboard

The InterPlanetary File System (IPFS) is a decentralized storage protocol designed to store and share data in a distributed manner. Unlike traditional centralized storage systems, IPFS uses a peer-to-peer (P2P) network to store files, making them accessible globally without relying on a central server. Files in IPFS are split into smaller chunks, each assigned a unique cryptographic hash. These hashes serve as content identifiers (CIDs), ensuring data immutability and integrity [Reddy et al. \(2024\)](#).

When a file is uploaded to IPFS, its hash is returned as the reference for future access. This hash acts as a permanent address, ensuring that even if a file is moved or replicated, its integrity remains verifiable. IPFS uses a distributed hash table (DHT) to locate and retrieve files efficiently across the network. Since files are accessed based on their content hash rather than location, IPFS is highly resistant to failures and censorship.

In this project, IPFS serves as the off-chain storage solution for academic credentials. Credential details, such as certificates and supporting metadata, are stored on IPFS to reduce the on-chain storage burden. The IPFS hash (CID) of each credential is stored on

the blockchain, ensuring immutability and authenticity. This allows the system to leverage blockchain's security while maintaining scalability and cost-effectiveness. By combining IPFS and blockchain, the system ensures secure, decentralized, and tamper-proof credential management.

Algorithm 5: Upload Document to IPFS

```
1: Input: Document ID
2: Output: IPFS CID (Content Identifier)
3: Fetch the document from the database using the provided ID.
4: if Document does not exist then
5:   Return 404: Document not found.
6: end if
7: if The file does not exist on the server then
8:   Return 404: File not found on the server.
9: end if
10: Read the file from the server using its filepath.
11: Upload the file to IPFS using the ipfsClient.add() function.
12: Retrieve the CID (Content Identifier) from IPFS.
13: Update the document's ipfsCID field in the database with the retrieved CID.
14: Save the updated document to the database.
15: Return 200: File uploaded to IPFS with the CID.
16: Error Handling: If any error occurs, log the error and return 500: Failed to
    upload to IPFS.
```

Algorithm 5 describes the process of uploading a document to IPFS and updating its record in the database. It begins by fetching the document using its unique ID. If the document or its file is not found on the server, appropriate error responses are returned. The file is read from the server and uploaded to IPFS, generating a unique Content Identifier (CID). This CID is then stored in the document's database record, ensuring its reference is securely maintained. Finally, the updated document is saved, and a success response, including the CID, is returned. Error handling is also done in the process to ensure easy debugging.

4.4 Web User Interface

Figure 4.12 demonstrates the login page for the Dr. FANS system. This page serves as the gateway for users to access the platform's credential management features. It provides fields for entering the user's email and password, ensuring a secure login process.

If a user does not already have an account, they are provided with a clear option to redirect to the sign-up page, enabling new users to create an account and join the

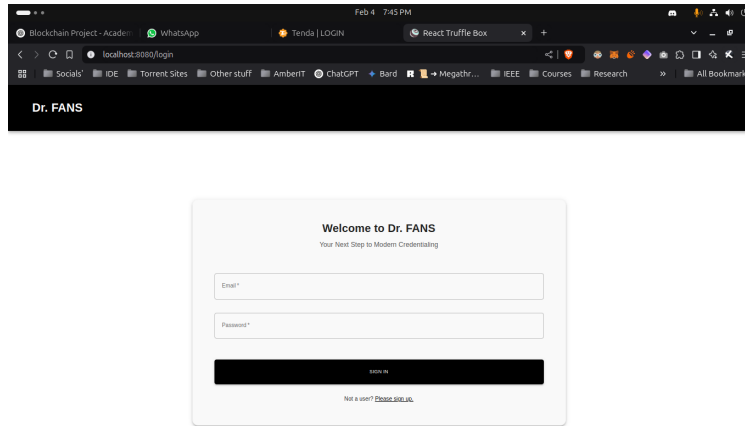


Figure 4.12: Login Page

platform. The design of the page is simple and user-friendly, with minimal distractions, focusing solely on authentication. The tagline, “Your Next Step to Modern Credentialing,” highlights the platform’s commitment to delivering innovative credential verification services.

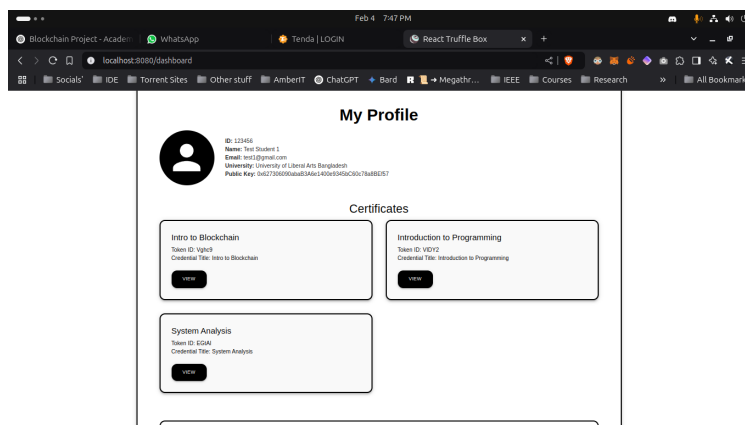


Figure 4.13: Profile Section

Figure 4.13 shows the “My Profile” page, displaying user information such as ID, name, email, university, and public key. The “Certificates” section lists issued tokens with details like token ID and credential title, along with a “View” option for more information. Users can also submit acquired credentials, enabling seamless token management and blockchain-based verification.

Figure 4.14 illustrates the admin section of the system, where administrators can view the list of submitted credentials from students. Each credential entry displays key details such as the student’s name, course title, institution, and additional identifiers. The “View Details” button allows the admin to access further information about the specific credential

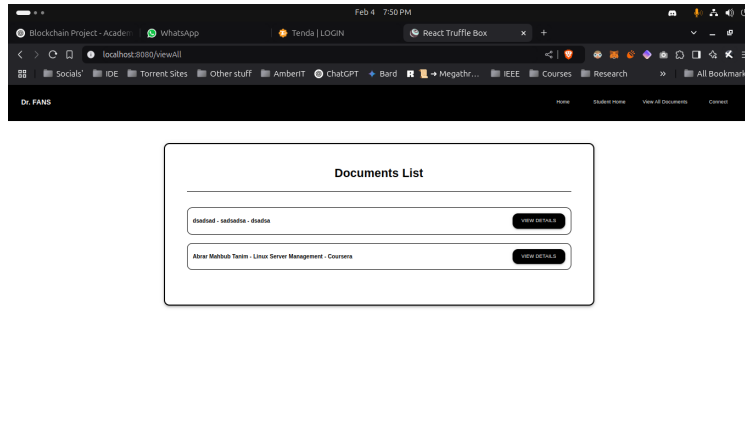


Figure 4.14: Admin Dashboard Page

for verification or review purposes. This interface streamlines the credential review process for administrators.

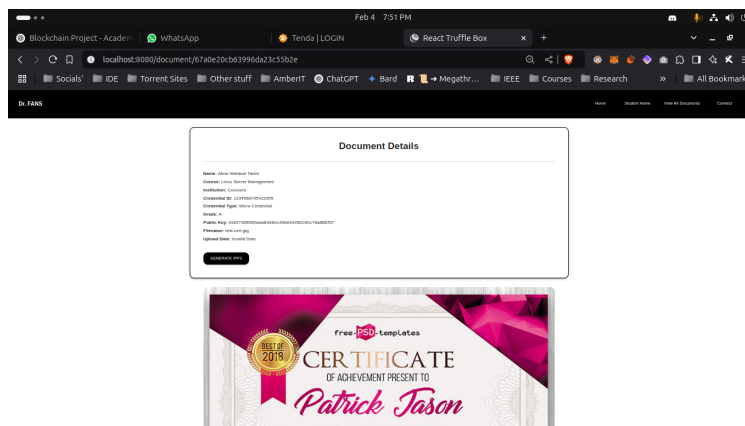


Figure 4.15: Issue Token Page

Figure 4.15 shows the document details page, where admins can view credential information, verify the document, upload it to IPFS using the "Generate IPFS" button, and issue a blockchain token to securely record the credential.

Figure 4.16 displays the Institution Profile page, where institutions can manage their profile details and review course exemption requests. The page provides options to review submissions and access token information, streamlining the credential verification process.

Figure 4.17 shows the MongoDB Compass interface, highlighting database connections and collections. It provides a clear overview of stored data, aiding in efficient database management and monitoring.

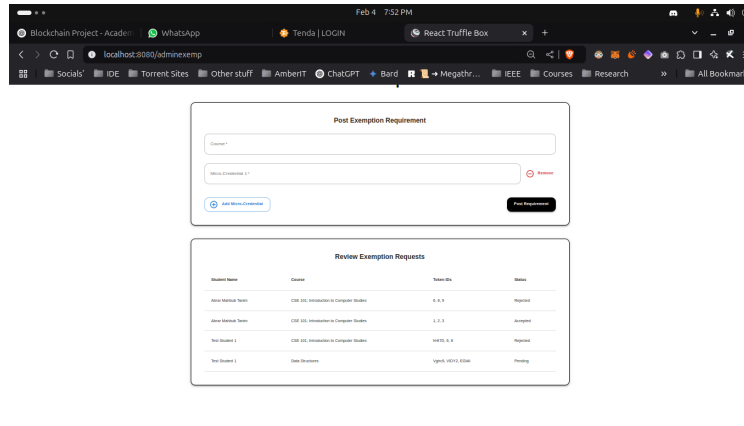


Figure 4.16: Institution Profile

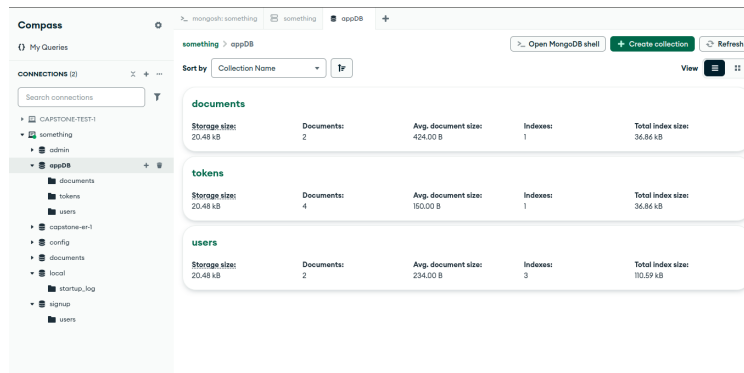


Figure 4.17: Database

4.5 Proposed System's Strengths and Limitations

The proposed system introduces a secure and transparent credential verification mechanism by leveraging blockchain technology. By deploying smart contracts on Hyperledger Besu, the system ensures that all credential transactions and updates are immutably recorded on the blockchain, guaranteeing auditability and accountability. The use of Hyperledger Besu's private and permissioned network configuration enhances security by restricting data access to authenticated participants, thereby preserving data integrity and confidentiality. The system also employs the Quorum Byzantine Fault Tolerance (QBFT) consensus algorithm, which ensures block finality and network resilience, making it highly suitable for secure and controlled environments such as academic credential verification.

The deterministic nature of smart contracts ensures consistent adherence to predefined terms, minimizing risks and providing a tamper-proof mechanism for credential issuance and revocation. Furthermore, the use of IPFS for storing credential data enhances scalability and reduces on-chain storage requirements while maintaining the integrity and availability

of the data.

Despite its advantages, the system has certain limitations. The reliance on a permissioned blockchain network, as facilitated by Hyperledger Besu, may limit scalability and the ability to integrate with larger, open ecosystems. Additionally, while the QBFT consensus algorithm ensures security and fault tolerance, it may introduce latency in transaction validations during high transaction volumes, potentially impacting the system's performance under heavy workloads. Another challenge lies in the immutable nature of blockchain, which makes error rectification in smart contracts complex and resource-intensive. Any defect in the smart contract logic could lead to significant issues, requiring sophisticated solutions to address these challenges.

In summary, the proposed system demonstrates substantial improvements in security, transparency, and accountability for credential verification processes. However, addressing limitations such as scalability, transaction latency, and error rectification will be critical for achieving broader adoption and ensuring effective implementation. These efforts will determine the system's potential for becoming a robust solution for decentralized credential verification.

Chapter 5

Business Model

5.1 Value Proposition

A project's value proposition highlights the unique benefits it provides to its users. The proposed system aims to revolutionize academic credential verification by integrating blockchain technology with credit-bearing micro-credentials. This ensures a secure, immutable, and tamper-proof system where institutions can issue verifiable credentials, students can maintain lifelong records, and employers can instantly validate academic achievements. By leveraging blockchain's decentralized nature, this system eliminates credential fraud, reduces administrative burden, and enhances trust between stakeholders in the education sector.

5.2 Customer Segments

The system serves various stakeholders in academia, industry, and professional certification. The key customer segments include:

5.2.1 Higher Education Institutions (HEIs)

Universities and colleges seeking a secure and efficient method for issuing, storing, and verifying student credentials. Institutions will only be able to see verified tokens and, based on that, can provide course exemptions upon students' requests.

5.2.2 Employers and Recruiters

Companies looking to verify job candidates' academic credentials and certifications without intermediaries, ensuring trust and reducing hiring risks.

5.2.3 Micro-Credential Providers (Issuing Bodies)

Platforms such as Coursera, edX, Udacity, and other micro-credential providers will serve as the issuing body. They will verify students' achievements and issue blockchain-based tokens, ensuring authenticity and recognition of their certifications.

5.2.4 Government and Accreditation Bodies

Regulatory institutions responsible for credential validation and policy enforcement in education. The system provides transparent and traceable credential verification.

5.3 Channels

To maximize market reach, the system utilizes multiple channels for delivery and adoption:

5.3.1 Direct Engagement with Institutions

Working directly with universities, colleges, and micro-credential providers to integrate the system into their credentialing processes.

5.3.2 Online Platform

A dedicated web portal where institutions can review verified tokens, students can request course exemptions, and employers can validate academic qualifications.

5.3.3 Digital Marketing and Outreach

Leveraging SEO, content marketing, webinars, and online advertising to engage educational institutions, policymakers, and employers.

5.3.4 Strategic Partnerships

Collaborating with government agencies, ed-tech companies, and blockchain networks to promote system adoption.

5.4 Customer Relationships

Building strong relationships with users is key to system adoption and long-term success.

5.4.1 Self-Service and Support

Providing user-friendly interfaces, documentation, and FAQs for institutions, students, and employers.

5.4.2 Training and Onboarding

Offering training sessions and onboarding support for institutions adopting blockchain-based credentialing.

5.4.3 Community Engagement

Creating **forums and discussion groups** where institutions and employers can discuss best practices and improvements.

5.5 Revenue Streams

The project will generate revenue through the following models:

5.5.1 Licensing Fees

Institutions pay an annual or one-time licensing fee to use the blockchain-based credential issuance system.

5.5.2 Subscription-Based Model

Employers and verifiers pay monthly or annual fees to access credential verification services.

5.5.3 Consulting and Integration Services

Providing custom blockchain integrations for institutions seeking tailored solutions.

5.6 Key Resources

To successfully deliver its value proposition, the system relies on:

5.6.1 Technology Infrastructure

Utilizing Hyperledger Besu for blockchain, IPFS for off-chain storage, and smart contracts for credential management.

5.6.2 Human Resources

A team of blockchain developers, smart contract engineers, and education specialists ensures system functionality and user adoption.

5.6.3 Intellectual Property

Securing innovative blockchain-based credentialing models and smart contract frameworks.

5.7 Key Activities

To maintain operational efficiency, the project involves:

5.7.1 Research and Development

Continuous enhancement of smart contract security, system scalability, and interoperability with existing educational platforms.

5.7.2 System Deployment and Maintenance

Ensuring seamless integration with institutional workflows and providing ongoing system updates.

5.7.3 User Training and Adoption

Developing training modules, webinars, and documentation for institutions and employers.

5.8 Key Partnerships

The project benefits from collaborations with:

5.8.1 Educational Institutions

Universities and training organizations adopting blockchain-based credentialing.

5.8.2 Micro-Credential Providers

Partnerships with Coursera, edX, Udacity, and similar providers for credential issuance and verification.

5.8.3 Blockchain Networks and Developers

Partnering with Hyperledger and Ethereum communities for system scalability and improvements.

5.8.4 Government and Accreditation Bodies

Ensuring compliance with educational standards and regulatory frameworks.

5.9 Cost Structure

The major cost components include:

5.9.1 Development and Maintenance

Salaries for developers, blockchain architects, and system administrators.

5.9.2 Infrastructure Costs

Expenses related to hosting blockchain nodes, cloud storage, and security measures.

5.9.3 Customer Support and Marketing

Funds allocated for user assistance, promotional campaigns, and outreach initiatives. This business model ensures the sustainability and scalability of the blockchain-based credential verification system, providing a trusted, decentralized, and efficient approach to academic credentialing.

Chapter 6

Result Analysis

The performance evaluation benchmarks the efficiency and responsiveness of the deployed smart contract on the Hyperledger Besu blockchain. Hyperledger Besu was chosen due to its compatibility with Ethereum transactions and support for both public and private blockchain frameworks. To assess the model, a test environment was established, utilizing the QBFT consensus mechanism, a Proof of Authority (PoA) algorithm suitable for enterprise-grade applications. The evaluation focuses on block creation and retrieval times to analyze the performance, as no comparable systems with a similar framework exist.

A blockchain network with four nodes was created to simulate a multi-node environment. One node acted as the host, while the remaining three acted as validators. Transactions were executed from three separate terminals, simulating individual users issuing credentials. A total of 200 transactions were performed consecutively across the terminals. A script was used to automate the transactions and log block creation and retrieval times for analysis.

6.0.1 Configuration

The performance evaluation was conducted on a machine with the following specifications:

- Processor: Intel Core i5-8300H
- RAM: 8GB DDR4
- Operating System: Ubuntu 20.04

The blockchain network consisted of four nodes, each configured as an independent terminal instance. Testing was performed on a single computer, utilizing scripts designed for continuous transactions. These scripts captured block creation and retrieval times, providing a comprehensive analysis of the smart contract's efficiency under varying transaction loads.

6.0.2 Metric

- **Block Creation Time (ms):** Block creation time refers to the average time required for the blockchain network to gather, validate, and include a new block of transactions into the ledger. This metric is critical for assessing the efficiency of the network under varying transaction loads. The `issueToken()` function was tested with different batch sizes, including 50, 100, and 200 transactions, to measure the time required for block creation. A final test was conducted with 200 transactions executed simultaneously from three accounts, and the block creation time was recorded in milliseconds.
- **Information Retrieval Time (ms):** This metric measures the latency in accessing stored data from the blockchain. The `getToken()` function was tested to retrieve token information, and the time taken to fetch specific credential details from the blockchain was recorded. This metric is essential for understanding the system's responsiveness, particularly for applications requiring real-time access to tokenized credentials.
- **Transaction Rate (tx/s):** The transaction rate represents the frequency at which transactions are submitted to the blockchain. For the `issueToken()` function, the send rate was calculated for different batch sizes, evaluating the system's throughput under varying loads. This metric highlights the scalability of the blockchain and its ability to process a high volume of transactions efficiently.

6.0.3 Prometheus and Grafana for Blockchain Metrics

Prometheus is an open-source systems monitoring and alerting toolkit designed for collecting and querying metrics from various services. It uses a time-series database to store metrics data and provides a flexible query language called PromQL for extracting and analyzing performance metrics. Prometheus is highly efficient for monitoring blockchain networks, as it can gather real-time data such as transaction throughput, block creation times, and resource usage (CPU, memory) of nodes.

Grafana is a data visualization and monitoring tool that works seamlessly with Prometheus and other data sources. It enables users to create dynamic, real-time dashboards to visualize collected metrics through graphs, charts, and other formats. Grafana is particularly useful for blockchain metrics as it provides an intuitive way to track network performance, detect anomalies, and analyze trends over time.

6.0.3.1 Using Prometheus and Grafana for Blockchain Metrics

Prometheus and Grafana were utilized to monitor the blockchain network deployed on Hyperledger Besu. Prometheus was configured to collect real-time data from the blockchain nodes, capturing key metrics such as:

- **Block creation time:** The time required to validate and add a block to the blockchain.
- **Transaction throughput:** The number of transactions processed per second, crucial for understanding the system's scalability.
- **Node performance:** CPU and memory usage of individual nodes to ensure optimal resource utilization.

Grafana dashboards were set up to visualize these metrics, providing an intuitive interface for administrators to monitor the performance of the system. For example, the block creation time was displayed as a time-series graph, making it easy to observe patterns and anomalies under varying transaction loads. Similarly, transaction throughput was charted to measure the network's capacity under different stress conditions.

6.1 Proposed System's Performance Result

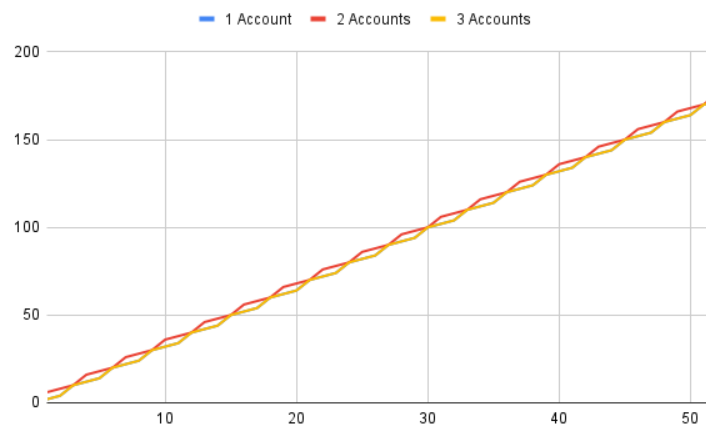


Figure 6.1: Block Creation Time with 50 Transactions

The chart for figure 6.1, 50 transactions demonstrates negligible differences in block creation time across tests conducted with 1 account, 2 accounts, and 3 accounts simultaneously. This indicates that the network maintains consistent performance under low transaction loads, regardless of the number of accounts submitting transactions.

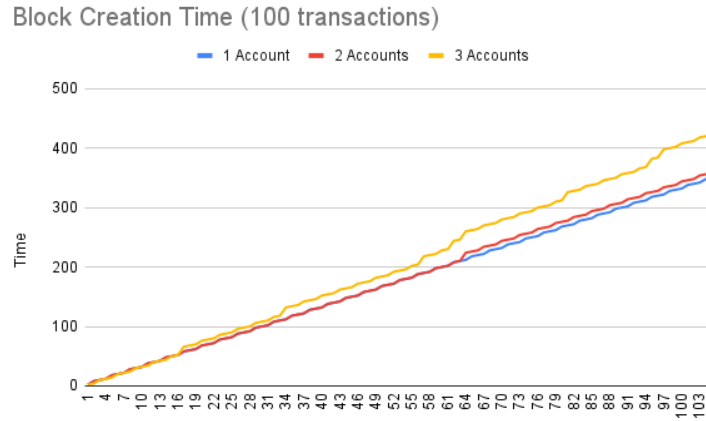


Figure 6.2: Block Creation Time with 100 Transactions

The chart for figure 6.2, 100 transactions begins to show slight variations in block creation time as the number of accounts increases. While the performance remains relatively consistent with 1 and 2 accounts, the test with 3 accounts exhibits a noticeable increase in block creation time. This suggests that higher simultaneous submission rates start to introduce minor delays as the transaction load increases.

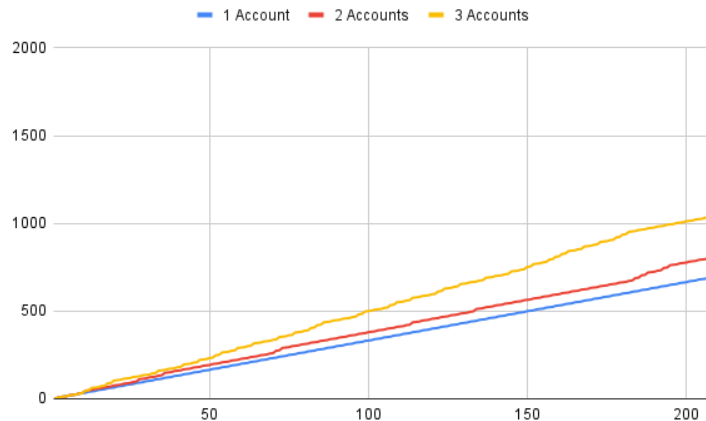


Figure 6.3: Block Creation Time with 200 Transactions

The chart in figure 6.3 for 200 transactions clearly shows significant differences in block creation time based on the number of accounts submitting transactions simultaneously. With 1 account, the block creation time remains relatively low and linear. However, with 2 accounts, there is a moderate increase in block creation time, while 3 accounts show the most pronounced delay. This demonstrates that the network begins to experience scalability challenges under high transaction loads, with block creation time increasing

significantly as the number of simultaneous transactions rises.

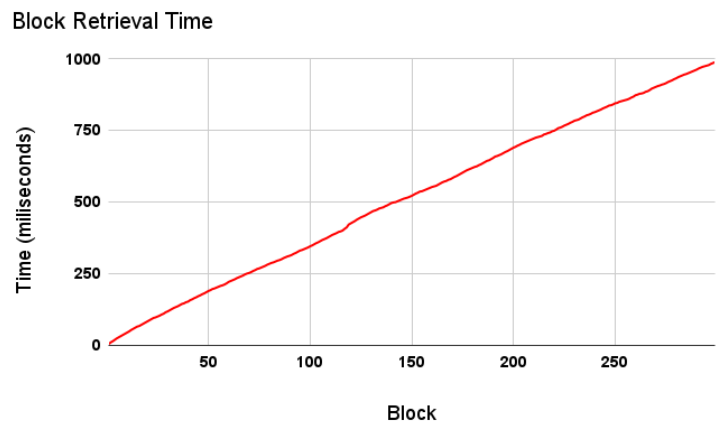


Figure 6.4: Block Retrieval Time

The block retrieval time was measured in milliseconds under the same test environment. Figure 6.4 indicates the average block retrieval time. The system showed consistent performance with retrieval times remaining in a narrow range. From the data, the retrieval time ranged from 1 millisecond to maximum of 10 milliseconds with the average retrieval time being 3.30 milliseconds. These highlight the efficiency of the system in accessing stored blocks even under varying loads. The minimal fluctuations in retrieval times suggest the system’s robustness for real world use cases.

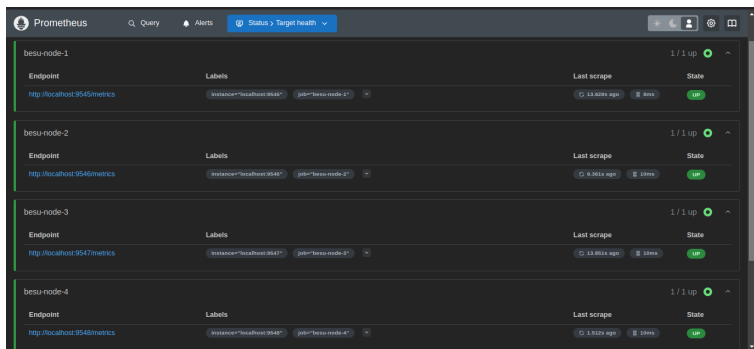


Figure 6.5: Prometheus Dashboard

Figure 6.5 shows the integration of Prometheus and Grafana for monitoring blockchain performance metrics. Prometheus is a powerful open-source monitoring system designed for collecting and storing time-series data, such as block creation times, transaction throughput, and resource utilization of nodes. It uses a pull-based mechanism to retrieve metrics from blockchain nodes and stores them in a time-series database for analysis.

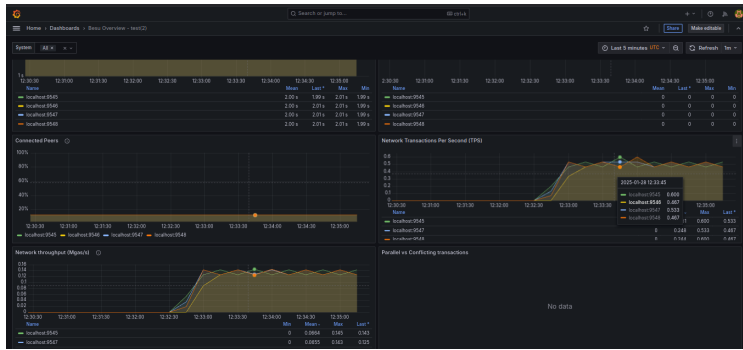


Figure 6.6: Grafana Dashboard 1

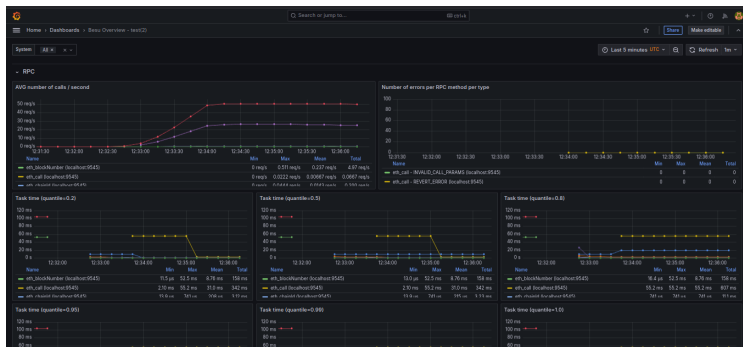


Figure 6.7: Grafana Dashboard 2

Figure 6.6 and 6.7 also highlights Grafana, a data visualization and monitoring tool that works seamlessly with Prometheus. Grafana provides an intuitive dashboard interface to visualize metrics in real-time through graphs, charts, and alerts. By using Grafana, administrators can track blockchain network performance, monitor node activity, and identify potential bottlenecks. Together, Prometheus and Grafana offer a robust solution for analyzing the efficiency, scalability, and reliability of the blockchain system.

Chapter 7

Conclusions

This chapter discusses the impact of the capstone project (Blockchain-Based Micro-Credentials verification system for higher education). It also discusses the social, legal, ethical, and environmental aspects to provide a comprehensive understanding. Additionally, this section briefly summarizes the project's expected outcomes. Furthermore, it explores open research areas that could contribute to further advancements in the field.

7.1 Social, Legal, Ethical, and Environmental Aspects

The proposed system incorporates credit-bearing micro-credentials with traditional learning using blockchain technology. However, its implementation will have an impact on society, legal contexts, the environment and ethics that need to be resolved. These are described below.

7.1.1 Social

The use of blockchain for credentialing requires reliable internet access and modern technology. Students from rural areas, lower-income backgrounds, or less-developed regions may not have access to the Internet or modern technology. It can create unfair differences. Some people might find it harder to access or share credentials than others. Institutions and governments could partner to provide subsidies, internet access, or technological devices to disadvantaged communities to mitigate the digital divide. Additionally, the system can be optimized for low-bandwidth and low-cost devices to make it accessible to a broader audience.

Students with disabilities may face challenges accessing or using the blockchain system if it lacks inclusivity. For example, accessibility features for visually or hearing-impaired users are essential to ensure equal access. The system should comply with WCAG (Web

Content Accessibility Guidelines). WCAG provides features like screen readers, high-contrast designs, and multilingual support. Educational institutions can provide training to ensure equal access for all students.

The blockchain system empowers students to manage and control their credentials. However, this also places an additional responsibility on them to safeguard and maintain those credentials. Some students may not be fully prepared to manage their records. This could lead to complications if access is lost or compromised. Universities and educational institutions should provide adequate training on using digital wallets. They should also offer resources to help students manage blockchain credentials securely. The system can include customer support to assist students. Additionally, easy-to-use interfaces can help reduce complexity and make the system more accessible.

7.1.2 Legal

The system will store sensitive personal and academic data. According to Bangladesh's Data Protection Act (draft) and global privacy laws like GDPR, data handling, storage, and sharing must meet legal standards. These measures are essential to safeguard students' privacy. Data should be encrypted to ensure security. Additionally, students' consent must be obtained for data storage and sharing. The system must comply with national data protection regulations to protect students' rights. It should ensure that students can manage their data and have complete control over its sharing. Moreover, students must be able to decline or restrict the use of their data when necessary.

The system will likely operate across borders, which could introduce challenges with jurisdictional conflicts. These conflicts may arise regarding how credentials are verified and shared between regions. Bangladesh's data protection laws may conflict with international practices or standards. The system must ensure compliance with Bangladesh's legal frameworks and international data transfer laws. The system should be flexible to comply with diverse legal requirements across different regions. This will facilitate cross-border credential verification while maintaining privacy and legal protections.

Blockchain-based credentials may not yet have legal recognition from all educational authorities in Bangladesh. Similarly, not all employers in the country may accept them as valid credentials. The system may not be widely adopted without formal recognition by regulatory bodies such as the University Grants Commission (UGC). Collaboration with UGC and other educational bodies in Bangladesh is essential to ensure the recognition

of blockchain-based credentials. Educational authorities can issue guidelines for using blockchain-based credentials within the country's accreditation system.

7.1.3 Ethical

Blockchain technology is designed to promote transparency. However, this could conflict with students' privacy rights. Making academic records publicly accessible, even on a permissioned blockchain, carries risks. It may inadvertently expose more personal data than initially intended. The system should include privacy-preserving features, such as zero-knowledge proofs and selective disclosure. These tools allow students to control what information is shared publicly. Personal and academic data access should be granted only with the student's consent.

If the algorithms used for credential verification or course exemptions are not fair, the system could unintentionally create biases. It's important to ensure the design is inclusive for everyone. For example, if an institution's guidelines for granting exemptions are based on factors that favor certain groups, it could lead to discrimination. Transparent rules should be established for how credentials are evaluated for exemptions. Institutions should ensure their policies do not result in unintended discrimination. They should also regularly review and update these policies to maintain fairness.

Although blockchain is secure, the system's trustworthiness relies on its implementation and how well it is maintained over time. Students and institutions must have confidence that the credentials stored on the blockchain are accurate and protected. Regular audits and transparent operations are essential to maintaining trust in the system. Using widely accepted blockchain standards can further enhance its reliability.

Students may lose access to their digital wallets or credentials due to technical failures or cyberattacks. This poses ethical concerns around accountability and responsibility for securing student data. The system should have robust backup and recovery procedures in place. Institutions should educate students about data security practices and provide recovery options for lost credentials. They must also ensure students' data is never permanently lost due to system errors.

7.1.4 Environmental

Blockchain networks consume large amounts of energy, especially those using proof-of-work mechanisms. This contributes to environmental degradation. This could be an issue, especially if educational institutions are committed to sustainability. The system should

adopt energy-efficient consensus mechanisms. These consume significantly less energy compared to traditional proof-of-work systems.

Running and maintaining blockchain nodes requires significant hardware and energy resources. This is especially true in decentralized systems with numerous nodes. As a result, it can create a considerable carbon footprint due to the demands of data centers. The system should minimize its carbon footprint using green data centers powered by renewable energy sources. Blockchain networks that focus on sustainability should be prioritized. Using eco-friendly protocols can help reduce the environmental impact.

7.2 Brief Summary

This project proposes a secure and reliable blockchain-based system integrating credit-bearing micro-credentials with traditional education. It addresses four key challenges: securely managing credentials (academic and micro-credentials), verifying credentials (academic and micro-credentials), giving institutions control over credit recognition, and streamlining the course exemption process. The system leverages blockchain's immutability, transparency, and traceability to enhance trust and efficiency in credential management.

This system guarantees that students and institutions can easily access and verify credentials at any time. Educational institutions can set specific rules and guidelines for earning and recognizing micro-credentials. This allows them to align these credentials with their learning objectives and course requirements. Students can use their verified credentials to request course exemptions. Students can use their verified credentials to request course exemptions. The blockchain system allows institutions to verify these credentials seamlessly and efficiently. This ensures the process is streamlined and decisions are based on trusted accurate data. Each student will have a digital wallet to store, manage, and share credentials. This feature enhances the accessibility and portability of their academic records. Blockchain technology will simplify and secure the credential verification process for institutions and organizations. This reduces the risk of fraud and lowers administrative burdens. The system will make it easier to integrate micro-credentials with traditional education. It will help institutions recognize and accredit prior learning. Overall, this system will improve the efficiency and security of credential management. It will also enhance the credibility of course exemption processes in education.

7.3 Future works

This blockchain-based system for integrating micro-credentials with traditional education creates many opportunities for future research and improvement. Moreover, blockchain technology's growing need and popularity opens more paths for future progress. Blockchain integration into micro-credentials can be complex, but it offers notable advantages. Blockchain's decentralized features allow it to address issues with trust between strangers. Information manipulation or alteration is impossible due to its immutability. Since it operates without a central authority (decentralization), it ensures security and trust. Therefore, this section aims to identify and discuss open research areas related to Blockchain in micro-credentials.

Interoperability is crucial to ensure the smooth integration of Blockchain-Based Micro-Credentials verification system for higher education with existing education infrastructure. Future research will focus on developing standardized protocols to facilitate seamless communication between blockchain platforms. It will make data exchange smoother and improve the system's ability to work together. Additionally, frameworks will be developed to enable efficient data sharing between the blockchain-based system and third-party systems like government agencies, employers, and educational institutions. This will ensure that credentials can be transferred smoothly for validation, course exemptions, or job applications. These frameworks will improve the system's ability to connect with other organizations efficiently.

As the number of users (students, institutions) increases, scalability becomes a critical consideration for the system. Future research will use scalable blockchain technologies like Layer-2 solutions (e.g., sidechains) to help the system handle more transactions. These improvements will allow the system to support growing user demands without slowing down.

Widespread user adoption is essential for the system's success. Future work will aim to enhance the system's usability and increase adoption among students and institutions.

Ensuring the security and privacy of student credentials is paramount. Future research will explore using advanced cryptographic methods, like zero-knowledge proofs, to help protect sensitive data. These methods will keep credentials secure while allowing them to be verified. This ensures data privacy without compromising the system's transparency.

As blockchain-based credentials become more mainstream, regulatory compliance will be essential for their acceptance in academic and professional sectors. Future work will

explore the legal requirements for Blockchain-Based Micro-Credentials verification system for higher education to ensure they follow educational and data protection laws. This includes studying how these credentials can meet global standards and regulations. Clear policies will be developed to guide the acceptance and use of blockchain credentials across different regions and industries. These efforts will help make blockchain credentials more trustworthy and widely recognized.

References

- Abreu, A. W. S., Coutinho, E. F., & Bezerra, C. I. (2020). A blockchain-based architecture for query and registration of student degree certificates. In *Proceedings of the 14th brazilian symposium on software components, architectures, and reuse* (pp. 151–160).
- Ahmat, N. H. C., Bashir, M. A. A., Razali, A. R., & Kasolang, S. (2021). Micro-credentials in higher education institutions: Challenges and opportunities. *Asian Journal of University Education*, 17(3), 281–290.
- Ahsan, K., Akbar, S., Kam, B., & Abdulrahman, M. D.-A. (2023). Implementation of micro-credentials in higher education: A systematic literature review. *Education and Information Technologies*, 28(10), 13505–13540.
- Alasaly, B., & Grando, A. (2021). Development of a novel blockchain medical device supply chain tracking application.
- Alharby, M., & Van Moorsel, A. (2017). Blockchain-based smart contracts: A systematic mapping study. *arXiv preprint arXiv:1710.06372*.
- Ali, M. A., & Bhaya, W. S. (2021a). Higher education's certificates model based on blockchain technology. In *Journal of physics: Conference series* (Vol. 1879, p. 022091).
- Ali, M. A., & Bhaya, W. S. (2021b). Higher education's certificates model based on blockchain technology. In *Journal of physics: Conference series* (Vol. 1879, p. 022091).
- Angelis, J., & Da Silva, E. R. (2019). Blockchain adoption: A value driver perspective. *Business Horizons*, 62(3), 307–314.
- Antonaci, A., Henderikx, P., & Ubachs, G. (2021). The common microcredentials framework for moocs and short learning programmes. *Journal of innovation in polytechnic education*, 3(1), 5–9.
- Any, B., Ramadhan, T., Nabila, E. A., et al. (2024). Decentralized academic platforms: The future of education in the age of blockchain. *Blockchain Frontier Technology*, 3(2), 112–124.
- Bahrami, M., Movahedian, A., & Deldari, A. (2020). A comprehensive blockchain-based solution for academic certificates management using smart contracts. In *2020 10th international conference on computer and knowledge engineering (iccke)* (pp. 573–578).

- Bahrani, N., Spellerberg, C., & Wilkinson, B. (n.d.). Guide to preparing camera-ready manuscripts for nels 54.
- Bell, N., Liu, M., & Murphy, D. (2022). A framework to implement academic digital badges when reskilling the it workforce. *Information Systems Education Journal*, 20(1), 36–46.
- Boggio Viola, A. (2024). *The tokenization of assets: Analysing the emergence of a new market trend*. (Unpublished doctoral dissertation). Politecnico di Torino.
- Brett, L., Zeigler, A., & Fazea, Y. (2024). Toronto cupcakes e-commerce powered by react js frameworks for user-centric design. *Journal of Digital System Development*, 2(2), 12–27.
- Carnevale, A. P., Fasules, M. L., & Peltier Campbell, K. (2020). Workplace basic: The competencies employers want.
- Casti, J. L. (1986). On system complexity: Identification, measurement, and management. In *Complexity, language, and life: Mathematical approaches* (pp. 146–173). Springer.
- Chander, A. (2024, February). *Personalized learning: How ai is changing education*. Retrieved from <https://blog.neuralminds.io/personalized-learning-how-ai-is-changing-education/>
- Chen, J. (2018). Hybrid blockchain and pseudonymous authentication for secure and trusted iot networks. *ACM SIGBED Review*, 15(5), 22–28.
- Cherukuri, B. R. (n.d.). Progressive web apps (pwes): Enhancing user experience through modern web development.
- Choi, M., Kiran, S. R., Oh, S.-C., & Kwon, O.-Y. (2019). Blockchain-based badge award with existence proof. *Applied Sciences*, 9(12), 2473.
- Chukowry, V., Nanuck, G., & Sungkur, R. K. (2021). The future of continuous learning—digital badge and microcredential system using blockchain. *Global Transitions Proceedings*, 2(2), 355–361.
- Clements, K., West, R. E., & Hunsaker, E. (2020). Getting started with open badges and open microcredentials. *International Review of Research in Open and Distributed Learning*, 21(1), 154–172.
- Delgado-von Eitzen, C., Anido-Rifón, L., & Fernández-Iglesias, M. J. (2021). Application of blockchain in education: Gdpr-compliant and scalable certification and verification of academic information. *Applied sciences*, 11(10), 4537.
- Eichhorn, T., Moreira, J. L. R., Pires, L. F., & Meertens, L. (n.d.). Enhancing observability: Real-time application health checks.
- Ethereum, W. (2014). Ethereum whitepaper. *Ethereum*. URL: <https://ethereum.org> [accessed 2020-07-07].

- Fan, C., Lin, C., Khazaei, H., & Musilek, P. (2022). Performance analysis of hyperledger besu in private blockchain. In *2022 ieee international conference on decentralized applications and infrastructures (dapps)* (pp. 64–73).
- Fanfarelli, J. R., & McDaniel, R. (2017). Exploring digital badges in university courses: Relationships between quantity, engagement, and performance. *Online Learning*, 21(2), n2.
- Fukuzawa, M., Kay, M., McConnell, B., Thoney-Barletta, K., & Warsing, D. (n.d.). Mechanisms for dealing with the unexpected in small-scale contracting using smart contracts.
- Gerrits, L., Samuel, C. N., Kromes, R., Verdier, F., Glock, S., & Guitton-Ouhamou, P. (2021a). Experimental scalability study of consortium blockchains with bft consensus for iot automotive use case. In *Proceedings of the 19th acm conference on embedded networked sensor systems* (pp. 492–498).
- Gerrits, L., Samuel, C. N., Kromes, R., Verdier, F., Glock, S., & Guitton-Ouhamou, P. (2021b). Experimental scalability study of consortium blockchains with bft consensus for iot automotive use case. In *Proceedings of the 19th acm conference on embedded networked sensor systems* (pp. 492–498).
- Ghonim, A., & Corpuz, I. (2021). Moving toward a digital competency-based approach in applied education: Developing a system supported by blockchain to enhance competency-based credentials. *International Journal of Higher Education*, 10(5), 33–45.
- Güneş, A., & Firat, M. (2022). Decentralized infrastructure of micro-credentials and blockchain technology. In *2nd international conference on educational technology and online learning–icetol 2022*.
- Hunt, T., Carter, R., Zhang, L., & Yang, S. (2020). Micro-credentials: The potential of personalized professional development. *Development and Learning in Organizations: An International Journal*, 34(2), 33–35.
- Hussein, Z., Salama, M. A., & El-Rahman, S. A. (2023a). Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity*, 6(1), 30.
- Hussein, Z., Salama, M. A., & El-Rahman, S. A. (2023b). Evolution of blockchain consensus algorithms: a review on the latest milestones of blockchain consensus algorithms. *Cybersecurity*, 6(1), 30.
- Jain, K., Vasesi, S., Mittal, H. K., & Kumar, J. (n.d.). Blockchain stationed managerial framework for logistics & oblige chain direction for reliable data control.
- Jaramillo, M. P., & Piedra, N. (2020a). Use of blockchain technology for academic certification in higher education institutions. In *2020 xv conferencia latinoamericana de tecnologias de aprendizaje (lacto)* (pp. 1–8).

- Jaramillo, M. P., & Piedra, N. (2020b). Use of blockchain technology for academic certification in higher education institutions. In *2020 xv conferencia latinoamericana de tecnologias de aprendizaje (lacto)* (pp. 1–8).
- Khalid, M. I., Ehsan, I., Al-Ani, A. K., Iqbal, J., Hussain, S., Ullah, S. S., et al. (2023). A comprehensive survey on blockchain-based decentralized storage networks. *IEEE Access*, 11, 10995–11015.
- Kheng, D. G. K., Qiang, L. Z., Poh, R., & Guan, C. T. (n.d.). Analysis of big data technologies for data asset management in transportation domain.
- Kishore, S., Chan, J., Muthupoltotage, U. P., Young, N., & Sundaram, D. (2021a). Blockchain-based micro-credentials: Design, implementation, evaluation and adoption. In *Hawaii international conference on system sciences*.
- Kishore, S., Chan, J., Muthupoltotage, U. P., Young, N., & Sundaram, D. (2021b). Blockchain-based micro-credentials: Design, implementation, evaluation and adoption. In *Hawaii international conference on system sciences*.
- Komeiha, M. (2025). Perceptions, feasibility, and acceptability of micro-credentials in global health graduate education. *McMaster University Repository*. Retrieved from <https://macsphere.mcmaster.ca/handle/11375/30647>
- Kumar, N. K., Honnunar, N. V., Prakash, M. S., & Lohith, J. (2024). Vulnerabilities in smart contracts: A detailed survey of detection and mitigation methodologies. In *2024 international conference on emerging technologies in computer science for interdisciplinary applications (icetcs)* (pp. 1–7).
- Kumutha, K., & Jayalakshmi, S. (2022). *Blockchain technology and academic certificate authenticity—a review. expert clouds and applications, vol. 209*. Springer, Singapore.
- LaMagna, M. (2017). Placing digital badges and micro-credentials in context. *Journal of Electronic Resources Librarianship*, 29(4), 206–210.
- Leka, E., & Selimi, B. (2020). Bcert—a decentralized academic certificate system distribution using blockchain technology. *International Journal on Information Technologies & Security*, 12(4), 103–118.
- Li, C., Li, P., Zhou, D., Yang, Z., Wu, M., Yang, G., ... Yao, A. C.-C. (2020). A decentralized blockchain with high throughput and fast confirmation. In *2020 {USENIX} annual technical conference ({USENIX} {ATC} 20)* (pp. 515–528).
- Lopes, J. (2023). Exploring consensus algorithms in quorum.
- Manoj, R., Joshi, S., Dabholkar, U., Prakash Panicker, G., Peter Kuriakose, K., Zaguia, A., & Monirujjaman Khan, M. (2021). Blockchain ecosystem for credit transfer in education. *Mathematical Problems in Engineering*, 2021(1), 8526456.

- Mansoor, N., Antora, K. F., Deb, P., Arman, T. A., Manaf, A. A., & Zareei, M. (2023). A review of blockchain approaches for kyc. *IEEE Access*.
- Mardisentosa, B., Rahardja, U., Zelina, K., Oganda, F. P., & Hardini, M. (2021). Sustainable learning micro-credential using blockchain for student achievement records. In *2021 sixth international conference on informatics and computing (icic)* (pp. 1–6).
- McGreal, R. (2023). Blockchain and micro-credentials in education. *International Journal of E-Learning & Distance Education*, 38(1), n1.
- McGreal, R. (2024). Empowering micro-credentials using blockchain and artificial intelligence. In *Global perspectives on micro-learning and micro-credentials in higher education* (pp. 75–90). IGI Global.
- McGreal, R., & Olcott Jr, D. (2022). A strategic reset: Micro-credentials for higher education leaders. *Smart Learning Environments*, 9(1), 9.
- Misal, J. (2024). Mastering automation tools for incident management and monitoring.
- Mwape, M. C., Kulig, B., Nurkhoeriyati, T., Roman, F., Parmar, A., Emmambux, N. M., & Hensel, O. (2025). Modeling and optimization of energy efficiency and product quality in staple food roasting using machine learning: A case study on cassava processing. *Thermal Science and Engineering Progress*, 103258.
- Naik, P., & Naik, G. (n.d.). Every stuff you need for development of decentralized app using blockchain technology, shashwat publication, july 2023.
- Nair, R. R., Rattan, D. P., & Thomas, K. (2024). Optimizing vaccine delivery: The role of smart contracts in building transparent supply chain management systems. *Available at SSRN 5014168*.
- Nugent, T., Upton, D., & Cimpoesu, M. (2016). Improving data transparency in clinical trials using blockchain smart contracts. *F1000Research*, 5.
- Panda, S. K., & Satapathy, S. C. (2021). An investigation into smart contract deployment on ethereum platform using web3. js and solidity using blockchain. In *Data engineering and intelligent computing: Proceedings of icicc 2020* (pp. 549–561).
- Patterson, G., L. Hepburn. (2024). Implementing a competency-based assessment approach to micro-credentials. *Distance Education*. Retrieved from <https://www.tandfonline.com/doi/abs/10.1080/01587919.2024.2441247>
- Pirkkalainen, H., Sood, I., Padron Napoles, C., Kukkonen, A., & Camilleri, A. (2023). How might micro-credentials influence institutions and empower learners in higher education? *Educational Research*, 65(1), 40–63.
- Pitt, C., Bell, A., Onofre, E., & Davis, K. (2019a). A badge, not a barrier: Designing for-and throughout-digital badge implementation. In *Proceedings of the 2019 chi conference on human factors in computing systems* (pp. 1–14).

- Pitt, C., Bell, A., Onofre, E., & Davis, K. (2019b). A badge, not a barrier: Designing for-and throughout-digital badge implementation. In *Proceedings of the 2019 chi conference on human factors in computing systems* (pp. 1–14).
- Pourbahrami, S., Balafar, M. A., Khanli, L. M., & Kakarash, Z. A. (2020). A survey of neighborhood construction algorithms for clustering and classifying data points. *Computer Science Review*, 38, 100315.
- Rahardja, U., Hidayanto, A. N., Putra, P. O. H., & Hardini, M. (2021). Immutable ubiquitous digital certificate authentication using blockchain protocol. *Journal of applied research and technology*, 19(4), 308–321.
- Rahman, T., Mouno, S. I., Raatul, A. M., Al Azad, A. K., & Mansoor, N. (2023a). Verifi-chain: a credentials verifier using blockchain and ipfs. In *International conference on information, communication and computing technology* (pp. 361–371).
- Rahman, T., Mouno, S. I., Raatul, A. M., Al Azad, A. K., & Mansoor, N. (2023b). Verifi-chain: a credentials verifier using blockchain and ipfs. In *International conference on information, communication and computing technology* (pp. 361–371).
- Reddy, N. J., Vamsi Krishna, K., Abhiram Varma, J., Hurtis, R., & Sheela Devi, M. (2024). Decentralized file storage system using ipfs and blockchain. In *International conference on smart data intelligence* (pp. 291–304).
- Rieder, A. T. (2022). Using micro-credentials and digital badges in education and training: a literature review. In *Society for information technology & teacher education international conference* (pp. 246–251).
- Rigole, N., Hollingsworth, L., & Ray, J. (2017). Badges and gamification in elearning: Effects on achievement and engagement.
- Romasanta, J. K. N., & Diloy, M. A. (2024). Micro-credentials: Educator’s perspective. In *2024 5th technology innovation management and engineering science international conference (times-icon)* (pp. 1–4).
- Saleh, O. S., Ghazali, O., & Rana, M. E. (2020a). Blockchain based framework for educational certificates verification. *Journal of critical reviews*.
- Saleh, O. S., Ghazali, O., & Rana, M. E. (2020b). Blockchain based framework for educational certificates verification. *Journal of critical reviews*.
- Saleh, O. S., Ghazali, O., & Rana, M. E. (2020c). Blockchain based framework for educational certificates verification. *Journal of critical reviews*.
- Sara, B. (n.d.). Unlocking smart contracts: A deep dive into mathematical foundations, applications, and design.

- Schulte, S., Sigwart, M., Frauenthaler, P., & Borkowski, M. (2019). Towards blockchain interoperability. In *Business process management: Blockchain and central and eastern europe forum: Bpm 2019 blockchain and cee forum, vienna, austria, september 1–6, 2019, proceedings* 17 (pp. 3–10).
- Selvaratnam, R. M., & Sankey, M. D. (2021). An integrative literature review of the implementation of micro-credentials in higher education: Implications for practice in australasia. *Journal of Teaching and Learning for Graduate Employability*, 12(1), 1–17.
- Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020a). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & security*, 97, 101966.
- Shi, S., He, D., Li, L., Kumar, N., Khan, M. K., & Choo, K.-K. R. (2020b). Applications of blockchain in ensuring the security and privacy of electronic health record systems: A survey. *Computers & security*, 97, 101966.
- Shilpa, S., & India, B. (n.d.). Enhancing research efficiency with mendeley: A comprehensive guide to referencing and collaboration.
- Shneiderman, B., & Plaisant, C. (2010). *Designing the user interface: strategies for effective human-computer interaction*. Pearson Education India.
- Siddiqui, S. T., Ahmad, M. O., Khamruddin, M., Gupta, A. K., & Singha, A. K. (2022). Blockchain and iot for educational certificates generation and verification. In *2022 2nd international conference on computing and information technology (iccit)* (pp. 298–303).
- Tan, K. T., Chan, J. I. L., Arumugam, P. V., & Lee, H. W. (2024). Closing the talent gap: A proposed micro-credential model in malaysian formal education. *Turkish Online Journal of Distance Education*, 25(4), 67–80.
- Tschorsch, F., & Scheuermann, B. (2016). Bitcoin and beyond: A technical survey on decentralized digital currencies. *IEEE Communications Surveys & Tutorials*, 18(3), 2084–2123.
- Vaccargiu, M., Neykova, R., Novielli, N., Ortu, M., & Destefanis, G. (n.d.). More than code: Technical and emotional dynamics in solidity's development.
- Vaidya, R., Tembhurnikar, A., Mohite, C., Puri, S., Kulkarni, S., & Buchade, A. (2024). Blockchain-powered certificate authentication: Enhancing trust and transparency. In *2024 ieee international conference on blockchain and distributed systems security (icbds)* (pp. 1–5).
- Varadarajan, S., Koh, J. H. L., & Daniel, B. K. (2023). A systematic review of the opportunities and challenges of micro-credentials for multiple stakeholders: learners, employers, higher education institutions and government. *International Journal of Educational Technology in Higher Education*, 20(1), 13.

- Vordenberg, S. E., Fusco, N. M., Ward, K. E., Darley, A., Brady, J. H., Culhane, N. S., ... others (2024). An integrative review of micro-credentials and digital badges for pharmacy educators. *American Journal of Pharmaceutical Education*, 88(3), 100660.
- Wan, L., Eyers, D., & Zhang, H. (2019). Evaluating the impact of network latency on the safety of blockchain transactions. In *2019 IEEE International Conference on Blockchain (Blockchain)* (pp. 194–201).
- Wang, L. (2023, October). *Micro-credentials: An important part of a bigger ecosystem*. Retrieved from <https://www.unesco.org/en/articles/micro-credentials-important-part-bigger-ecosystem>
- Wu, M., Xu, F., Subramaniam, G., Li, Z., Chen, L., & Zhu, W. (2024). Advancing hematopoietic stem cell transplantation typing: Harnessing hyperledger fabric's blockchain architecture. *IEEE Access*.
- Yadav, J., & Shevkar, R. (2021). Performance-based analysis of blockchain scalability metric. *Tehnički glasnik*, 15(1), 133–142.
- Zhang, R., Xue, R., & Liu, L. (2019). Security and privacy on blockchain. *ACM Computing Surveys (CSUR)*, 52(3), 1–34.

Appendices

7.4 Addressing Complex Engineering Problems

7.4.1 Depth of Knowledge Required

The proposed project involves integrating blockchain technology with micro-credentials to create a secure, tamper-proof system for credential issuance and verification. This requires interdisciplinary knowledge spanning technical, theoretical, and educational domains, aligned with the following knowledge profiles:

- **Engineering Fundamentals**

Advanced understanding of blockchain principles, decentralized storage (IPFS), and smart contract mechanisms is required to ensure system robustness and data security.

- **Specialized Knowledge**

Knowledge of blockchain frameworks (e.g., Hyperledger Besu) and the education sector's policies for micro-credentials is crucial to align the system with institutional requirements.

- **Engineering Design in Practice**

Designing course exemption logic and credential verification processes requires translating abstract institutional policies into functional, secure smart contract implementations.

- **Engineering Practice (Technology)**

Expertise in deploying blockchain nodes, integrating APIs, and cryptographic techniques ensures the system's scalability and operational efficiency.

- **Engagement with Research**

The project draws on the latest research in blockchain and micro-credentials to develop innovative solutions that address current challenges in educational credentialing systems.

This diverse depth of knowledge highlights the interdisciplinary complexity of the project, requiring both theoretical and applied expertise.

7.4.2 Range of Conflicting Requirements

The project navigated a range of conflicted requirements during its development. Firstly, The project uses IPFS for decentralized storage to enhance scalability and allowed secure storage of large credentials, however this added a dependency of IPFS node availability which added a layer of complexity to the project. Secondly, the project uses Hyperledger Besu which is a permissioned blockchain to ensure better control, privacy and also elimination of transaction fees but this vastly reduced global accessibility.

7.4.3 Depth of Analysis Required

The depth of analysis required for this project stems from the need to implement a transformative policy to integrate micro-credentials as credit-bearing micro-credentials. This project involves an abstract thinking to conceptualize a framework where micro-credentials can seamlessly align with traditional learning models. Abstract modeling plays a pivotal role in designing the course exemption logic which ensures that institutions can interpret and apply credential data accurately based on their unique policies.

7.4.4 Familiarity of Issues

The familiarity of issues within this project highlights the challenges posed by working outside the domain of education technology (EdTech). While the technological aspects, such as blockchain integration and credential management, are central to the system, the broader scope involves complexities in educational policies and frameworks.

7.4.5 Extent of Applicable Codes

The project must adhere to strict data protection regulations such as the General Data Protection Regulation (GDPR) and the Family Educational Rights and Privacy Act (FERPA). These laws set the standards for how academic and micro-credentials should be stored, processed, and verified, ensuring that student data remains secure and private. Compliance with these regulations is crucial to gaining institutional trust and user confidence in the system. Beyond regulatory requirements, the project's blockchain implementation must also follow industry best practices. Smart contracts need to be designed with security and immutability in mind. Adhering to established blockchain security protocols ensures the

system remains resilient against tampering, unauthorized modifications, and potential cyber threats.

7.4.6 Extent of Stakeholder Involvement

The success of this project relies on the involvement of multiple stakeholders, each bringing their own perspectives and needs. Micro-credential providers such as Coursera and edX play a vital role in issuing verifiable credentials, ensuring that students' achievements are accurately documented. Educational institutions must integrate these credentials into their existing academic frameworks to ensure they align with accreditation standards. This integration is essential for the validation process, allowing micro-credentials to hold academic value. A strong collaboration between credential issuers and universities is necessary to create a seamless verification process that enhances trust.

7.4.7 Interdependence and Conflicting Needs

The proposed system operates at the intersection of multiple technologies, including blockchain, the InterPlanetary File System (IPFS), and institutional databases. These components must work in harmony to ensure seamless credential storage and verification. Blockchain provides immutability and transparency, while IPFS offers decentralized storage for supporting documents. At the same time, universities and credential providers maintain their own databases, which must integrate smoothly with the system without compromising security or efficiency. However, this high level of interdependence also introduces challenges, particularly in balancing decentralization with institutional requirements. Blockchain-based credential verification aims to eliminate centralized control, enhancing transparency and trust. Yet, many universities and employers prefer permissioned or private network configurations to maintain oversight, ensure compliance with regulations, and protect sensitive data.