Self Sovereign Identity and Blockchain For University Certificate Verification

PHASE II REPORT

Submitted by

Deshna Ramani	**22011103011**
Aravind S	**22011103051**
Shriyadithya Nair	**22011103054**

in partial fulfilment for the award of the degree of

BACHELOR OF TECHNOLOGY
IN COMPUTER SCIENCE AND ENGINEERING
(CYBERSECURITY)

DEPARTMENT OF COMPUTER SCIENCE AND ENGINEERING
SCHOOL OF ENGINEERING
SHIV NADAR UNIVERSITY CHENNAI

APRIL 2026

SHIV NADAR UNIVERSITY CHENNAI

BONAFIDE CERTIFICATE

Certified that this report titled "**Self Sovereign Identity and Blockchain For University Certificate Verification**" is the bonafide work of **Deshna Ramani** (Reg. No: **22011103011**), **Aravind S** (Reg. No: **22011103051**), **Shriyadithya Nair** (Reg. No: **22011103054**) who carried out the work under my supervision. Certified further that to the best of my knowledge, the work reported herein does not form part of any other thesis or dissertation on the basis of which a degree or award was conferred on an earlier occasion on this or any other candidate.

SIGNATURE

Dr. T. Nagarajan

Professor

Head of the Department

Department of Computer Science & Engineering

School of Engineering

Shiv Nadar University Chennai,

Kalavakkam -603110.

SIGNATURE

Dr. Rourab Paul

Assistant Professor

Supervisor

Department of Computer Science & Engineering

School of Engineering

Shiv Nadar University Chennai,

Kalavakkam -603110.

ABSTRACT

The credibility of academic credentials is increasingly threatened by certificate forgery, slow manual verification procedures, and the lack of a unified trusted validation mechanism. To address these challenges, this project proposes a decentralized academic credential verification platform based on blockchain and Self-Sovereign Identity (SSI) principles. Through the use of Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), the system enables secure issuance, storage, sharing, and validation of academic records while ensuring integrity, transparency, and resistance to tampering.

The proposed architecture identifies the Government as the trust anchor, Universities as credential issuers, Students as credential holders, and Employers as credential verifiers. The implemented workflow includes DID registration, schema publication, credential issuance, student wallet-based proof generation, and employer-side verification. Conceptually aligned with Hyperledger Indy and Aries-based SSI architecture, and demonstrated through an integrated role-based web application, the platform presents a practical, privacy-aware, and scalable solution for modern academic certificate verification.

Keywords- Self-Sovereign Identity, Blockchain, Academic Credential Verification, Verifiable Credentials, Digital Wallet, Decentralized Identifiers, Trust Framework

ACKNOWLEDGEMENT

We would like to express our sincere gratitude to all those who have provided invaluable guidance, support, and encouragement throughout the course of this project.

First and foremost, We are deeply grateful to Dr. T. Nagarajan, Professor and Head, Department of Computer Science and Engineering, School of Engineering, Shiv Nadar University Chennai, for his steadfast guidance and unwavering encouragement. His insights into the field of artificial intelligence and cognitive science have been instrumental in shaping the direction of this research.

We would also like to extend our heartfelt thanks to our supervisor, **Dr. Rourab Paul**, Assistant Professor, Department of Computer Science and Engineering, School of Engineering, Shiv Nadar University Chennai, for his mentorship and commitment to the success of this project. His expertise in Cybersecurity and Blockchain has been invaluable, providing us with clarity and focus to tackle complex challenges and refine the methodology of this work.

We also acknowledge the support of our family, whose understanding and encouragement have been crucial to this project's implementation. Their unwavering belief in us has been a constant source of motivation and strength.

Deshna Ramani	**Aravind S**	**Shriyadithya Nair**
(22011103011)	(22011103051)	(22011103054)

TABLE OF CONTENTS

LIST OF FIGURES

Chapter 1: Introduction

1.1 Background and Motivation

University degree verification is a critical step in admissions, recruitment, and professional background checks. In practice, however, most verification still depends on manual processes, paper records, and institution-specific workflows. These methods are slow, labor-intensive, and often inconsistent across organizations, especially when verification is needed across states or countries.

At the same time, credential fraud continues to grow. Fake universities and forged certificates reduce trust in academic records and create risk for both institutions and employers. Because of this, there is a clear need for a system that can verify credentials quickly and reliably.

As education and employment become more digital and global, credentials must be secure, portable, and easy to validate. Blockchain and Self-Sovereign Identity (SSI) provide a strong foundation for this. Blockchain offers tamper-resistant recordkeeping, while SSI gives users control over their own identity data. With Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), students can share only the information required for verification without exposing unnecessary personal details.

This project addresses the limitations of traditional verification by combining blockchain and SSI to build a decentralized, trusted, and scalable framework for academic credential validation.

1.2 Gap Analysis of Existing University Certificate Verification Systems

Current university certificate verification systems do not fully meet the needs of a secure, efficient, and globally usable verification model. The major gaps are summarized below.

- **Verification Efficiency Gap**

Current state: Verification is mostly manual and depends on document checks and institution-to-institution communication.
Expected state: Verification should be automated and near-instant, with minimal human effort.
Identified gap: Manual workflows cause delays, increase administrative workload, and introduce avoidable human errors.

- **Security and Authenticity Gap**

Current state: Credentials are commonly shared as paper copies or unsecured digital documents.
Expected state: Credentials should be tamper-proof, cryptographically protected, and easy to validate.
Identified gap: Existing formats are vulnerable to forgery and manipulation, which lowers trust.

- **Portability and Accessibility Gap**

Current state: Credentials are often tied to individual institutions and are difficult to verify across regions.
Expected state: Credentials should be portable and verifiable across institutions and geographies.
Identified gap: Lack of a common framework leads to repetitive checks and slows student

and workforce mobility.

- **System Architecture Gap**

Current state: Most systems are centralized and controlled by single institutions.

Expected state: Systems should be decentralized to reduce single points of failure and improve resilience.

Identified gap: Centralized systems are more exposed to outages, breaches, and access bottlenecks.

- **Interoperability Gap**

Current state: Institutions use isolated databases and non-uniform data formats.

Expected state: Standardized formats should support seamless cross-platform verification.

Identified gap: Poor interoperability increases verification time, cost, and complexity.

- **Identity Ownership Gap (SSI Perspective)**

Current state: Institutions maintain end-to-end control over issuance, storage, and validation.

Expected state: Individuals should own and manage their credentials through SSI mechanisms.

Identified gap: Limited user control weakens privacy and creates dependency on centralized authorities.

1.3 Key Objectives

1. Build a tamper-resistant blockchain-based credentialing framework that preserves authenticity and integrity.

2. Enable students to own and manage their credentials through SSI-based digital identity and wallet support.

3. Provide a trusted verification pipeline using DIDs and cryptographic proofs for fast and secure certificate validation.

1.4 Scope Definition

1. **System Architecture and Technology Framework:** The project designs a credential verification system on a permissioned blockchain using Hyperledger Indy. SSI components are used for decentralized identity through digital wallets and DIDs, with a focus on secure and tamper-resistant credential handling.

2. **Credential Lifecycle and User Roles:** The workflow covers credential issuance, storage, sharing, and verification. Universities act as issuers, students as holders, and employers as verifiers. A governing authority is included to maintain trust relationships.

3. **Privacy, Security, and System Efficiency:** The design applies cryptographic verification and supports selective disclosure so users can share only required fields while maintaining privacy.

Chapter 2: Related Work

2.1 Review of Existing Blockchain-Based Credential Verification Approaches

Recent work in decentralized credential verification proposes several blockchain-based methods to improve trust and authenticity. One approach uses Ethereum smart contracts to issue and verify academic credentials, offering transparency and immutability [2]. However, public-chain dependence introduces practical constraints such as transaction fees and scalability limits under heavy usage.

Another line of work uses Hyperledger Indy and Aries for decentralized identity and access control [1]. This design applies Identity-Based Encryption (IBE) for key management instead of a full SSI model. While IBE supports authentication and delegation without prior key exchange, it adds computational overhead and does not fully enable user-controlled identity ownership.

Based on these observations, our system combines Hyperledger Indy for SSI-compatible credential records and Hyperledger Aries for secure peer-to-peer agent communication. We also integrate encrypted storage and API-based interactions with wallets and verifiers. This results in a privacy-preserving and user-centric framework that is better suited to low-cost, scalable academic credential verification.

2.2 Decentralized Permissioned Blockchain

A decentralized permissioned blockchain is maintained by a set of trusted participants rather than a single central authority. In this model, hashing protects data integrity by making unauthorized changes detectable, and digital signatures verify the issuer identity and

message authenticity. Together, these mechanisms create a secure and auditable foundation for credential storage and verification.

2.2.1 Blockchain for University Certificate Verification

In university certificate verification, blockchain helps store and validate digital records in a tamper-resistant way. This improves authenticity checks and reduces dependency on manual intermediary verification [2].

2.2.2 Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) is a digital identity approach in which individuals control their own identity data. By reducing dependence on central intermediaries, SSI supports secure authentication and authorization while improving privacy and user autonomy [3].

2.2.3 Decentralized Identifiers (DIDs)

Decentralized Identifiers (DIDs) are unique identifiers that can be created and controlled by users without a central issuing authority. They support secure and verifiable credential exchange across decentralized systems [1].

2.2.4 Verifiable Credentials (VCs)

Verifiable Credentials (VCs) are digitally signed claims issued by trusted entities. They allow verifiers to confirm authenticity cryptographically, often without contacting the issuer each time [1].

2.2.5 SSI in University Certificate Verification

Applying SSI to university certificate verification allows students to hold and share credentials directly from their wallets. Employers can verify proofs quickly while students retain control over what data is disclosed [2].

2.3 Existing SSI based Decentralised blockchain platforms

Feature	Trinsic	uPort	TruScholar
Infrastructure Type	Cloud-hosted, vendor-managed	Public Ethereum blockchain-based	Blockchain-based certificate platform
Cost Model	Pay-per-credential issuance and verification	High gas fees (transaction-based)	Not clearly defined; depends on platform usage
Scalability	Limited by API rate limits and throttling	Poor scalability due to public blockchain congestion	Cannot process multiple batches in parallel
Performance	Affected by API throttling	Non-deterministic due to network congestion	Limited due to lack of batch parallelism
Vendor Dependency	High (vendor lock-in for wallets, agents, hosting)	Moderate (depends on Ethereum network)	High (platform-controlled environment)
SSI Flexibility	Moderate	Limited (requires custom logic)	Limited SSI flexibility
Selective Disclosure	Limited, vendor-controlled	Requires custom implementation	Not supported
Role of Institutions	Limited control over infrastructure	Independent users on network	Universities act as clients

Chapter 3: Proposed Methodology

3.1 Operational Workflow

The proposed university certificate verification model combines blockchain with Self-Sovereign Identity (SSI). The system is organized around four core entities:

- **Governing Authority (Trust Anchor):** Establishes trust by authorizing universities as valid credential issuers.
- **Universities (Issuers):** Publish schemas and credential definitions, then issue Verifiable Credentials (VCs) to students.
- **Students (Holders):** Receive credentials in digital wallets and control how and when they are shared.
- **Employers (Verifiers):** Request proof from students and verify it against ledger-backed records.

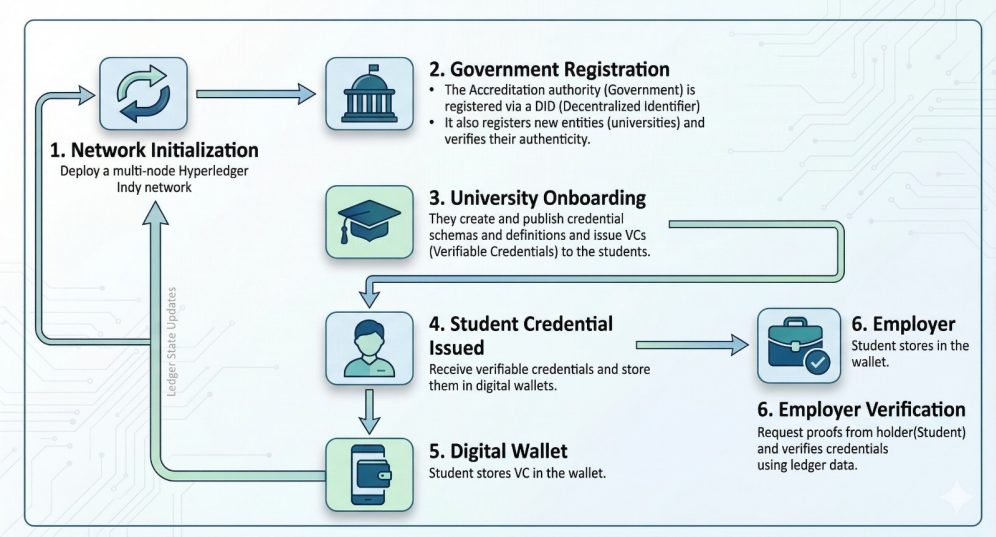

Figure 3.1: Overall Workflow of the Proposed System

3.2 Ledger Deployment

This project implements an SSI framework using **Hyperledger Indy** and **Hyperledger Aries**. Indy acts as the distributed ledger for decentralized identity data, while Aries provides the agent communication layer needed for credential exchange.

The network is deployed with Docker through a local Verifiable Organizations Network (VON) setup. Multiple validator nodes run as independent services, each maintaining a replicated ledger copy. Consensus is handled by the Plenum Byzantine Fault Tolerant (BFT) protocol to preserve consistency and fault tolerance.

On top of the ledger, Aries agents manage identity operations such as DID creation, secure peer-to-peer messaging, and VC issuance and verification. Because Aries follows standard protocols, the implementation remains modular and practical for real-world SSI deployments.

The ledger stores essential identity artifacts, including:

- Decentralized Identifiers (DIDs) and their associated public keys
- Credential schemas defining the structure of credentials
- Credential definitions used for issuing verifiable credentials
- Revocation registries to support credential revocation

This architecture clearly separates responsibilities: Indy secures the ledger layer, Aries handles interaction between entities, and Docker-based deployment makes the setup portable across environments.

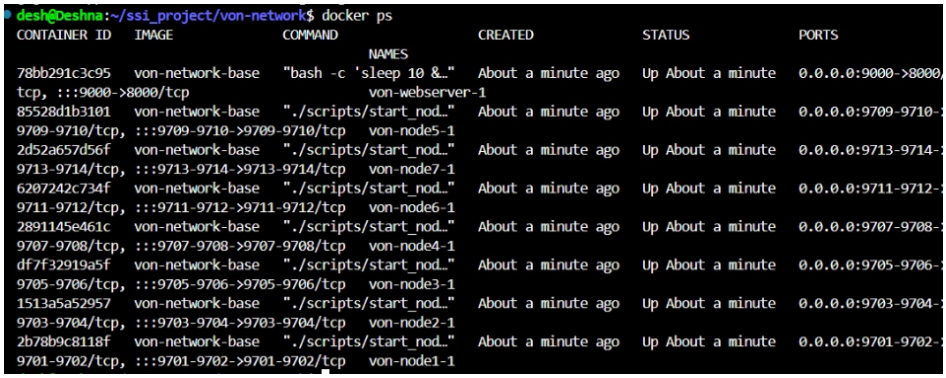

Figure 3.2: Ledger Initialisation

3.3 Schema and Credential Definition

Once universities are verified, they define the credential schema and its definition for issuance.

Schema: Specifies the credential structure (e.g., Name, Degree, Year, Grade).

Credential Definition: Links the schema with the issuer's public key material and metadata required for cryptographic proof checks.

Both artifacts are stored on the Indy ledger and signed by the university's private key, making them tamper-evident and publicly verifiable.

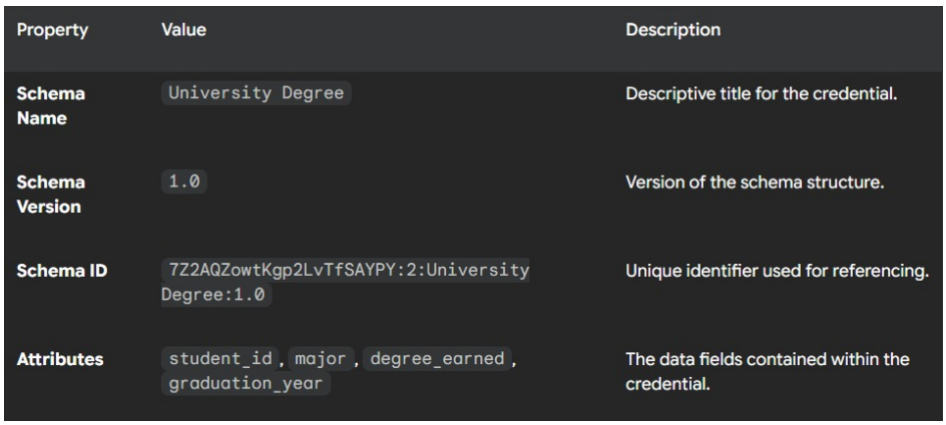

Figure 3.3: Schema

Property	Value	Description
Cred Def ID	`7Z2AQZowtKgp2LvTfSAYPY:3:CL:11:degree_tag`	Unique identifier linking the Schema ID and Issuer DID.
Schema ID Used	`7Z2AQZowtKgp2LvTfSAYPY:2:UniversityDegree:1.0`	Confirms which schema this definition is based on.
Tag	`degree_tag`	A simple tag used for searching/filtering.
Revocation Support	`false`	This credential is not configured for runtime revocation.

Figure 3.4: Credential Definition

3.4 Application Interface and User Interaction Flow

The application is built as a role-based web system. Each user type logs in through a dedicated portal and receives a role-specific dashboard, which keeps interaction clear and straightforward.

When a university publishes a schema, it is stored in the backend and immediately available in the university dashboard. After issuance, each credential is linked to the corresponding student identity.

When a student logs in, the wallet fetches only that student's credentials, preserving data isolation and privacy. The student can then generate a proof token and share it with an employer.

The employer uses the token to validate the credential through the platform, without needing direct manual confirmation from the issuing university.

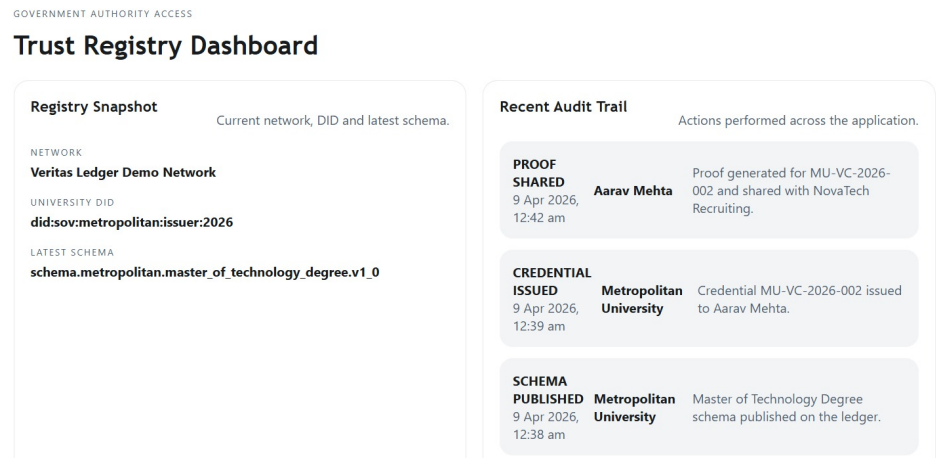

Figure 3.5: Government Dashboard

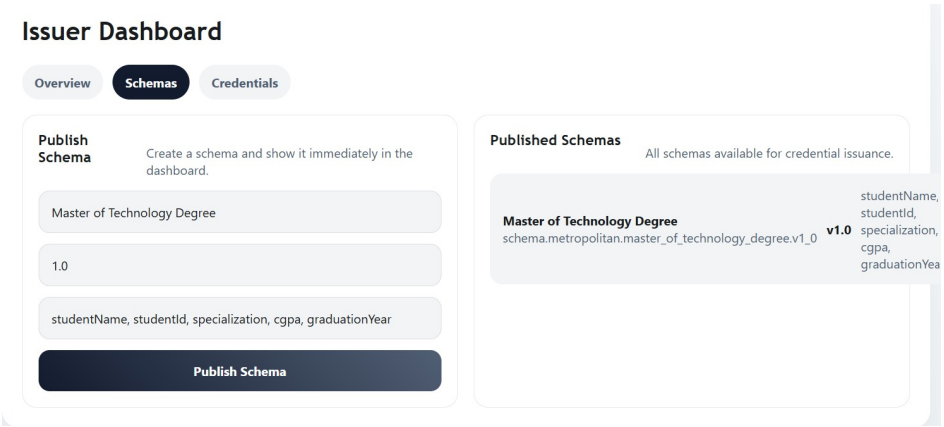

Figure 3.6: University Dashboard

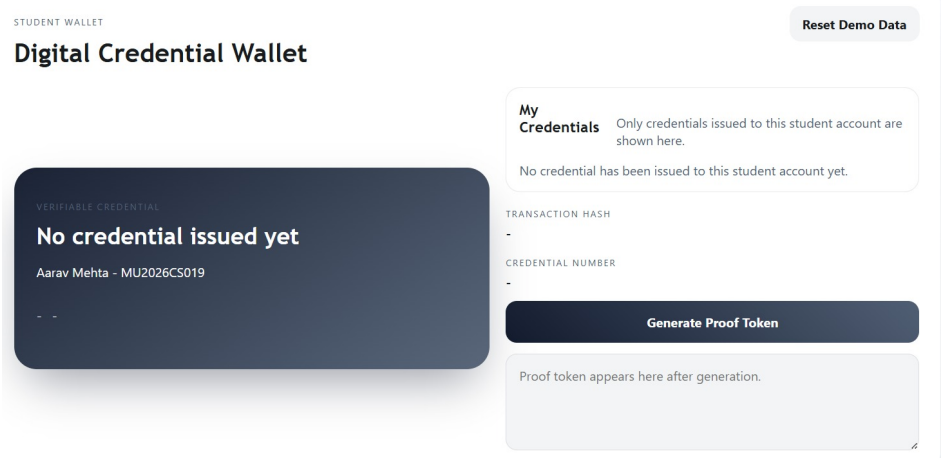

Figure 3.7: Student Dashboard

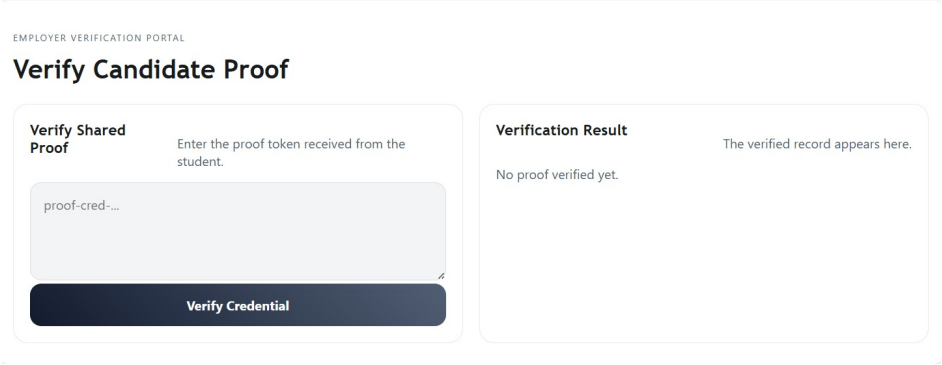

Figure 3.8: Employer Dashboard

3.5 Functional Workflow

This section describes the key transactions performed in the application:

3.5.1 Transaction 1: University DID Registration

This transaction establishes a university as a trusted issuer. The government, acting as trust anchor, validates and registers the university's DID on the ledger. After registration, the university can publish schemas and issue credentials.

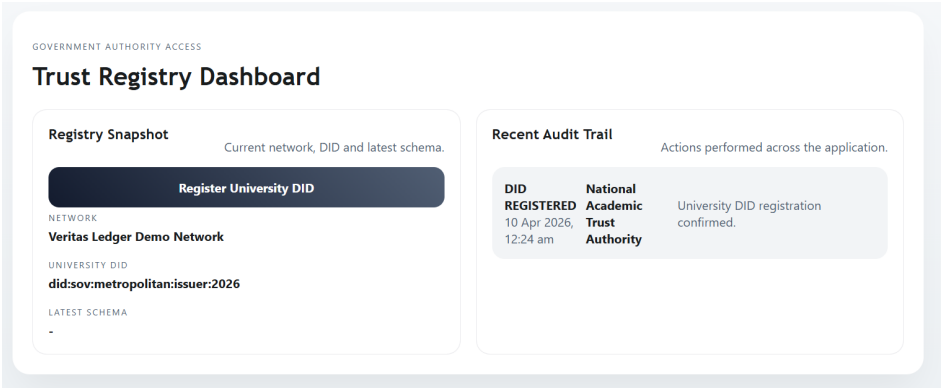

Figure 3.9: University DID Registration

3.5.2 Transaction 2: Schema Publication

The university publishes a credential schema that defines certificate fields such as student name, student ID, program, CGPA, graduation year, and honors. Once published, it can be

used for standardized issuance.

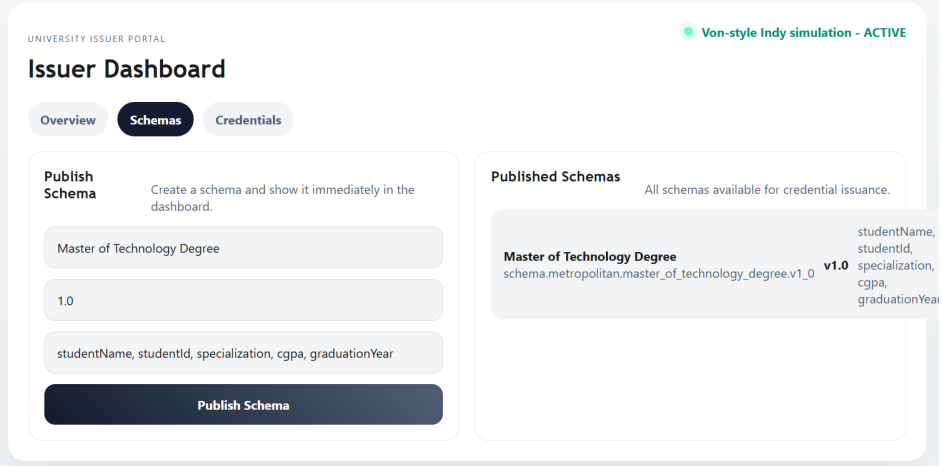

Figure 3.10: Schema Publication

3.5.3 Transaction 3: Credential Issuance

Using a selected schema, the university enters student academic details and issues a VC. The credential is securely recorded and linked to the student holder.

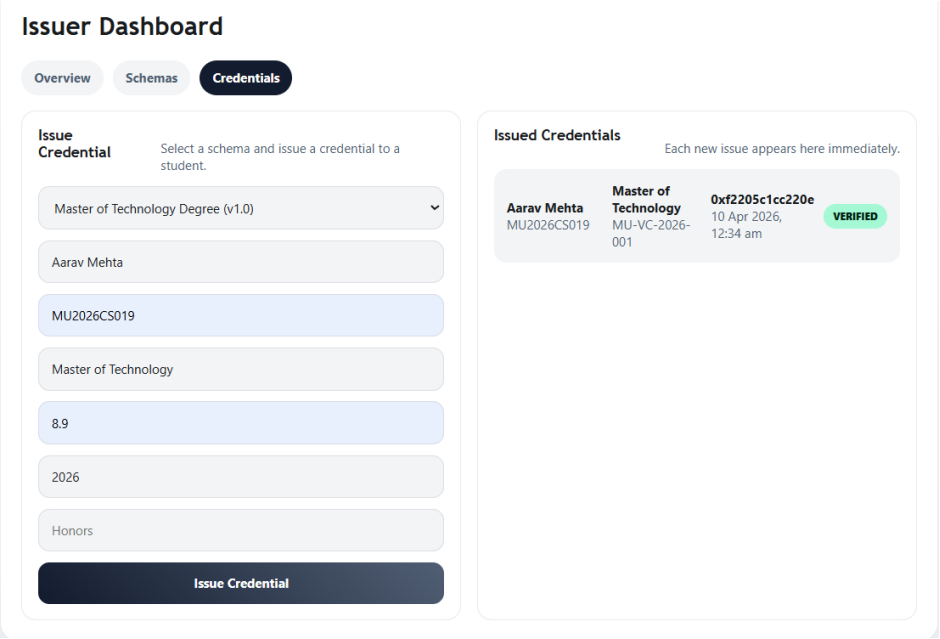

Figure 3.11: Credential Issuance

3.5.4 Transaction 4: Credential Availability in Student Wallet

After issuance, the credential appears in the student's wallet. The student can access only credentials mapped to their identity, demonstrating holder-level ownership and controlled access.

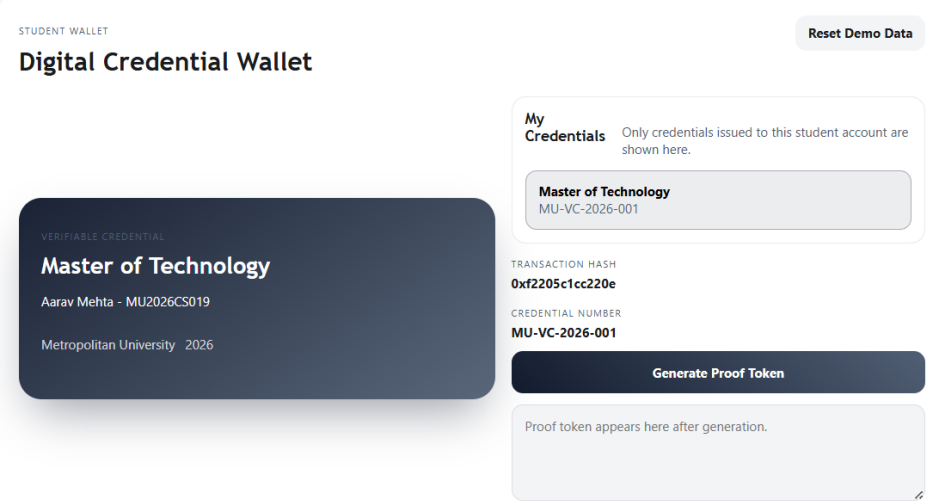

Figure 3.12: Credential Availability in Student Wallet

3.5.5 Transaction 5: Proof Generation and Sharing

The student selects a credential and generates a proof token for sharing. This enables controlled disclosure and avoids exposing unnecessary credential details during verification.

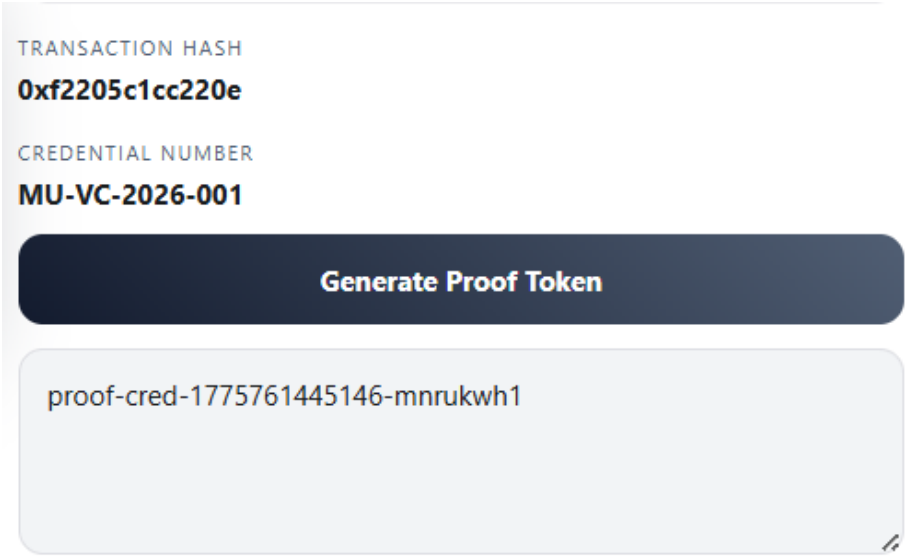

Figure 3.13: Proof Generation and Sharing

3.5.6 Transaction 6: Employer Verification

The employer submits the received token, and the system validates it against issued credential records and ledger-backed metadata. On success, confirmed credential details are displayed.

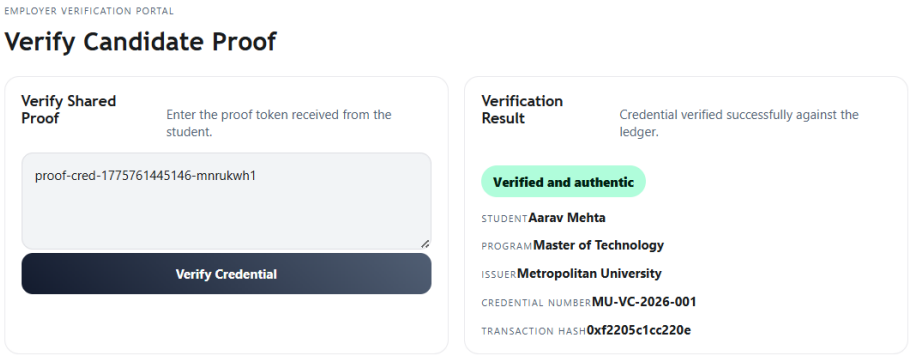

Figure 3.14: Employer Verification

3.6 Audit Trail and Monitoring

The audit layer records major operations such as DID registration, schema publication, credential issuance, proof generation, and verification. Each event is securely logged to

support transparency, traceability, and accountability. These logs also help the governing authority monitor trust relationships and maintain network integrity.

3.7 Computational Cost and Network Efficiency

Hyperledger Indy's consensus mechanism (**Plenum**) provides Byzantine fault tolerance up to $(n-1)/3$ faulty nodes.

- **No Mining or Gas Fees:** Validation handled by trusted validator nodes.
- **Cost Model:** Infrastructure-based, dependent on node capacity.
- **Throughput:** Typically 100–200 transactions per second.

This offers a practical balance of cost, privacy, and performance for academic verification networks.

3.8 Results and Performance

The implementation demonstrates that an SSI-enabled credential workflow can be executed in a decentralized and practical way. In the deployed setup, the university issues VCs, students hold and control them, and employers verify proofs through secure DID-based communication.

Key strengths of the solution:

- Smooth API interoperability for fast issuance and verification across agents.
- Low latency during typical credential and proof operations.
- Stable ledger behavior under repeated transactions, with room to scale.

Overall, the results support the feasibility of combining SSI and blockchain for academic credential verification. The system improves tamper resistance, preserves privacy, and remains usable through a role-based interface suitable for practical deployment.

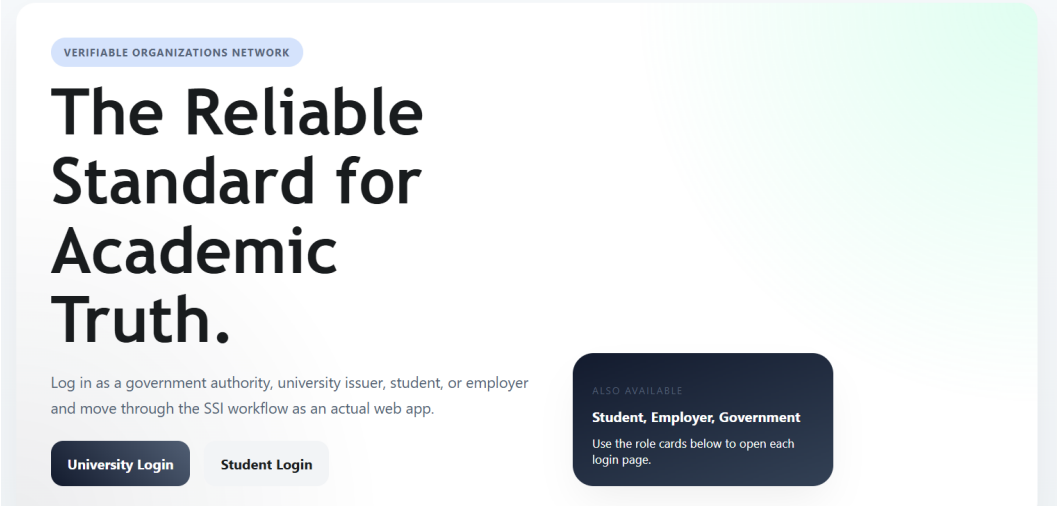

Figure 3.15: Main Application Landing Page

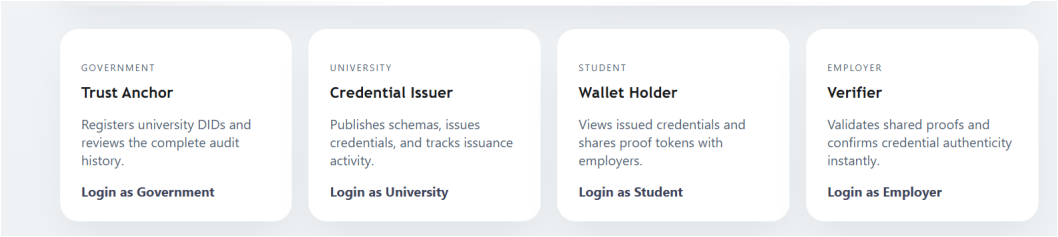

Figure 3.16: Login Portals for each Entity

Chapter 4: Conclusion

4.1 Summary and Conclusions

This project presents an SSI-based framework for issuing and verifying academic credentials using Hyperledger Indy and Hyperledger Aries. Decentralized Identifiers (DIDs) are used to establish verifiable identities, while Verifiable Credentials (VCs) are used to represent academic records in a secure digital form.

In the proposed model, authorized institutions issue digitally signed credentials to students. These credentials are stored in student wallets and can be shared with employers or other verifiers when required. Verification is completed through cryptographic proofs, so authenticity can be confirmed without depending on a centralized validation authority.

Along with the backend implementation, we developed a role-based interface to make the system easy to use for government authorities, universities, students, and employers. This improves usability and reduces technical barriers during credential issuance and verification.

Overall, the project meets its objective of building a functional decentralized credential verification system. The implementation demonstrates that SSI concepts can be applied effectively in a practical academic setting.

REFERENCES

[1] P.-J. Vrielynck, T. Van Hamme, R. Ghostin, B. Lagaisse, D. Preuveneers, and W. Joosen, **"A Self-Sovereign Identity Approach to Decentralized Access Control with Transitive Delegations,"** *Proceedings of the 29th ACM Symposium on Access Control Models and Technologies (SACMAT 2024)*, San Antonio, TX, USA, 29(3649158):1–9, 2024.

[2] S. Cheikhrouhou, M. Turki, S. Kallel, A. Abid, and M. Jmaiel, **"Blockchain-Powered Certificate Verification Enhanced by Self-Sovereign Identity and Off-Chain Caching,"** *International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, 10(11059603):1-2025.

[3] R. N. Zaeem, K. C. Chang, T.-C. Huang, D. Liau, W. Song, A. Tyagi, M. M. Khalil, M. R. Lamison, S. Pandey, and K. S. Barber, **"Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study,"** *IEEE/WIC/ACM International Conference on Web Intelligence (WI-IAT '21)*, Essendon, VIC, Australia, 21(3493917):1–8, 2021.

[4] N. Naik and P. Jenkins, **"Self-Sovereign Identity Specifications: Govern Your Identity Through Your Digital Wallet using Blockchain Technology,"** *IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 8(00021):1–7, 2020.

[5] C. Dong, A. Yao, Z. Xu, M. Lu, F. Jiang, S. Chen, and X. Liu, **"A Blockchain-Based Self-Sovereign Identity System for KYC Processes,"** *ACM International Symposium on Blockchain, Security, and Cryptography (BSCI '24)*, Singapore, 24(3660026):1–8, 2024.

[6] A. De Salve, A. Lisi, P. Mori, L. Ricci, and C. Turco, **"Self-Sovereign Identity for**

Privacy-Preserving Shipping Verification System," *International Conference on Blockchain Technology and Applications (ICBTA 2022)*, Xi'an, China, 5(3581992):1–11, 2022.

[7] Y. Ding, J. Yu, S. Li, H. Sato, and M. G. Machizawa, **"Data Aggregation Management With Self-Sovereign Identity in Decentralized Networks,"** *IEEE Transactions on Network and Service Management*, 21(3451995):6174–6188, 2024.

[8] X. Sun, J. Yang, F. Yang, and C. Li, **"A Self-Sovereign Identity Authentication Scheme for Multi-level Supply Chain Finance,"** *International Conference on Artificial Intelligence and Pattern Recognition (AIPR 2024)*, Xiamen, China, 7(3703974):1–7, 2024.