Blockchain-enabled Decentralized Identity Management Leveraged by Self-Sovereign Identity in Bangladesh Public Transportation

By
Md Asif Mahmud Sabuj
211-15-4020

FINAL YEAR DESIGN PROJECT REPORT

This Report Presented in Partial Fulfillment of the Requirements for the **Degree of Bachelor of Science in Computer Science and Engineering**

Supervised by
Mr. Afjal Hossan Sarower
Lecturer (Senior Scale)
Department of Computer Science and Engineering
Daffodil International University

Co-Supervised by
Mr. Md. Monarul Islam
Lecturer
Department of Computer Science and Engineering
Daffodil International University

DAFFODIL INTERNATIONAL UNIVERSITY
Dhaka, Bangladesh

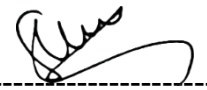
May 14, 2025

APPROVAL

This Project titled **"Blockchain-enabled Decentralized Identity Management Leveraged by Self-Sovereign Identity in Bangladesh Public Transportation"**, submitted by **Md Asif Mahmud Sabuj**, ID No: **211-15-4020** to the Department of Computer Science and Engineering, Daffodil International University has been accepted as satisfactory for the partial fulfillment of the requirements for the degree of B.Sc. in Computer Science and Engineering and approved as to its style and contents. The presentation has been held on **14 May, 2025**.

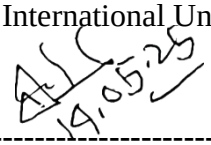
BOARD OF EXAMINERS

Dr. S.M Aminul Haque — **Chairman**
Professor and Associate Head
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Sharmin Akter — **Internal Examiner**
Assistant Professor
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University

Ms. Syada Tasmia Alvi — **Internal Examiner**
Sr. Lecturer
Department of Computer Science and Engineering
Faculty of Science & Information Technology
Daffodil International University



Dr. Md. Arshad Ali — **External Examiner**
Professor
Department of Computer Science and Engineering
Hajee Mohammad Danesh Science & Technology University

DECLARATION

We hereby declare that this project has been done by me under the supervision of **Mr. Afjal Hossan Sarower**, **Lecturer (Senior Scale)**, Department of Computer Science and Engineering, Daffodil International University. We also declare that neither this project nor any part of this project has been submitted elsewhere for the award of any degree or diploma.

Supervised by:

13.05.25

Mr. Afjal Hossan Sarower
Lecturer (Senior Scale)
Department of Computer Science and Engineering
Daffodil International University

Co-Supervised by:

13.05.25

Mr. Md. Monarul Islam
Lecturer
Department of Computer Science and Engineering
Daffodil International University

Submitted by:

14.05.25

Md Asif Mahmud Sabuj
Student ID: 211-15-4020
Department of Computer Science and Engineering
Daffodil International University

ACKNOWLEDGEMENTS

This work would not have been possible without the support and contributions of many individuals over the past two semesters. We are deeply grateful to everyone who has assisted us in one way or another.

First, we express our heartfelt thanks and gratefulness to the almighty for His divine blessing making it possible for us to complete the **Final Year Design Project (FYDP)** successfully.

We are grateful and wish our profound indebtedness to **Mr. Afjal Hossan Sarower**, **Lecturer (Senior Scale)**, Department of Computer Science and Engineering, Daffodil International University, Dhaka, Bangladesh. Deep knowledge and keen interest of our supervisor in the field of **Blockchain** carry out this project. His endless patience, scholarly guidance, continual encouragement, constant and energetic supervision, constructive criticism, valuable advice, reading many inferior drafts, and correcting themat all stages have made it possible to complete this project.

We would like to express our heartfelt gratitude to the Head of the Department of Computer Science and Engineering, for his kind help in finishing our project and also to other faculty members and the staff of the Department of Computer Science and Engineering, Daffodil International University.

We would like to thank our entire course-mates at Daffodil International University, who took part in this discussion while completing the coursework.

Finally, we must acknowledge with due respect the constant support and patience of our parents.

ABSTRACT

Bangladesh's public transportation system is continually plagued by fragmentation, repetition of identification and ticketing and outdated fare collection methods. These shortcomings result in ineffective operation, poor multimodal transport integration and a high risk of identity data breach due to central storage. To overcome these problems, this paper proposed a system that is based on blockchain and built upon the SSI concept. The targeted service is realized through Hyperledger Fabric, Verifiable Credentials and Zero-Knowledge Proof to provide secure and trustworthy identity verification which could prevent the leakage of personal information. After successfully authenticating the user credentials by the approved organizations; the DTID is issued by the Bangladesh Road Transport Authority (BRTA) which serves as a verified universal travel credential for all service providers in transport. Ticketing and fare collection is powered by smart contracts, no more haggles or inflated pricing, chips are deposited into escrow and fares are released to the beneficiary upon trip conclusion. The system even allows for offline verification via QR codes and NFC, so it's usable in areas with no internet connection. This decentralized system aims to modernize and standardize Bangladesh's fragmented public transportation structure by driving privacy, transparency, and interoperability toward an overall safer, more efficient, and user-friendly public transportation experience.

Keywords: Blockchain, Self-Sovereign Identity (SSI), Decentralized Identity Management, Digital Transport ID (DTID), Hyperledger Fabric, Public Transportation, Verifiable Credentials, Zero-Knowledge Proof

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

1.1 Introduction

Identity management will, therefore, be required to provide a secure, seamless, and trustful access to the services on the public transit network. ITS with electronic identity Most developed countries have implemented electronic identity systems within their transportation infrastructure to handle ticketing automaton, pass discounts and authorize safe passage. [1] Even in advanced systems, there are processes related to the identity verification which apply centralized databases, paper documents or biometrics, which are major drawbacks. These systems are vulnerable to security compromises, single points of failure, and a lack of user control over personal data. [2] Moreover, the lack of interoperability among different transport providers leads to fragmented user experiences, duplicate registrations, and little cross-platform ticketing. [3] In Bangladesh, the public transport system is even more fragmented and mostly reliant on manual, paper-based identity verification processes. The regular travelers who utilize buses, trains, metros, and ferries have themselves exposed to delays, re-presentation of identities, and inefficient service integration. There is typically the separate ticketing and verification framework for each transportation form, but no unified system or central database. This non-unified makeup causes inefficiency not only to commuters but even to operators and regulating agencies, making the application of real-time verification, secure fare collection, and price-based entitlement more difficult to implement on a large scale. One of the most significant issues with the current setup is that centralized identity management systems are utilized to hold sensitive user data in isolated silos controlled by transport operators or retained in government databases. These systems are extremely concerning because a breach into any of these systems has the potential to compromise thousands if not millions of individual identities. [4] Furthermore, privacy is even more eroded when individuals are not in charge of how their information is held, accessed, or transmitted. From an operational perspective, centralized methods also hinder automation and real-time updates, which keeps the system inefficient, prone to human errors, and vulnerable to fraud or ticket duplication. To avoid such limitations, more and more the world is shifting towards Decentralized Identity Management, with an emphasis on Self-Sovereign Identity (SSI) platforms. SSI permits users to possess and control their own online identity, separate from any central organization. Using DIDs, VCs, and cryptographic proofs, users can safely prove their identity and only reveal the necessary information. [2] The system is particularly advantageous for use with public transportation where relatively frequent, rapid and reliable verification is desired without unduly violating the user's privacy. [3]

The identity verification by the existing system of public transport in Bangladesh is not sufficient for the purpose of the present time. But it cannot provide the seamless experience for the user, would expose the user to security risk and it would not enable interoperability or offline verification. [1] All these security, privacy, and operational inefficiencies significantly hinder the development of a smart, user-centric transport environment. Due to this, this study supports a blockchain-based decentralized identity management system via SSI a solution that has the potential to unify public transport services under a secure, privacy-protecting, and interoperable digital identity platform. [3]

1.2 Motivation

Digital technologies are transforming the way societies interact with critical services, and there is an increasing demand for secure, interoperable, and privacy-preserving identity systems particularly in high-impact sectors such as public transportation. Bangladesh's transport ecosystem is still heavily reliant on manual identity verification and unconnected service providers, resulting in inefficiencies, user frustration, and high risks of fraud. From a computer science standpoint, it's an attractive problem: how do we create an identity management protocol that removes dependencies on centralized data repositories while preserving assurances on the identities mapped within? Not only did this problem garner interest from me because of its national significance, but it also had technical complexity and room to iterate. By combining SSI with the benefits of blockchain technology, smart contracts, and modern cryptographic mechanisms such as Zero-Knowledge Proofs (ZKPs), it is possible to design a scalable privacy-first solution that allows users to take back control of their identities. It also needs to perform consistently well in low-connectivity environments an engineering challenge that pushes the envelope of decentralized application design. At the same time personally, this project allows me to bring my expertise in blockchain, cryptography, decentralized systems, and secure identity management to good use in a meaningful and socially impactful manner. It also maintains my growth as a developer and researcher and sets me up for future work in fields like digital governance, fintech, and urban technology. By addressing this problem, I hope to pave the way for a smarter, safer, and more user-centric public infrastructure in-Bangladesh- while deepening my own exploration into real-world decentralized systems.

On a personal level, working on this project allows me to apply my knowledge of blockchain, cryptography, decentralized systems, and secure identity management in a meaningful and socially impactful way. It also helps me grow as a developer and researcher, preparing me for future work in fields such as digital governance, fintech, and urban technology. By solving this problem, I aim to contribute to a smarter, safer, and more user-centered public infrastructure in Bangladesh, while deepening my own understanding of real-world decentralized systems.

1.3 Objectives

The key objectives of this project are:

- To design and implement a blockchain-based digital identity management system for public transportation in Bangladesh.
- To apply the Self-Sovereign Identity (SSI) model for privacy-preserving, user-controlled identity verification.
- To develop a secure ticketing mechanism using Digital Transport IDs (DTIDs) and Verifiable Credentials.
- To integrate smart contracts for automated fare locking, distribution, and fraud prevention.
- To enable offline verification using NFC for improved accessibility in low-connectivity areas.
- To ensure interoperability across various transport modes including buses, trains, metros, cars and ferries.

1.4 Methodology

The proposed project is developed on a permissioned Hyperledger Fabric-based blockchain network due to its performance, scalability, and mid-level privacy policies. The passengers register via a decentralized wallet app and submit the credentials (e.g., NID, student ID, bank info). These are then verified by universities, banks, and each jurisdictions government who issue Verifiable Credentials. After validation, the BRTA supplies the user with a Digital Transport ID (DTID), which the user keeps in the wallet. They then book trips after which the fares are guaranteed by smart contracts which escrow funds and automate payments according to the consumption pattern. Identity and ticket validation is done using QR or NFC, and you're even able to make use of the app offline, automatically syncing when available. It employs ZKPs and digital signatures to authenticate credentials without revealing any sensitive data.

1.5 Project Outcome

The proposed system will results in a decentralized digital identity and ticketing system for public transportation of Bangladesh. Demonstration of how citizens can Identify themselves, obtain their own DTID, and book tickets and affirm their identity across modes of transportation – bus, train, metro, ferry – with one single and interoperable digital identity. Leveraging SSI principles and blockchain technology, the platform is secure, private and does not store personal information; it rather relies on cryptographic proofs to validate the data and not preserve it on a centralized server. The prototype will also demonstrate automatic fare locking, billing, and revenue sharing through smart contracts, along with secure identity management. That provides an avenue for easy, seamless transactions without having to rely on middlemen and third parties. One of the key features of the system is its support for offline verification using NFC, which allows even those in low-connectivity or rural areas to access and benefit from the platform. Ultimately, this project lays the groundwork for a nationwide, scalable solution that not only enhances the public transport experience but also sets a precedent for broader digital identity initiatives within e-governance and other service sectors in Bangladesh.

1.6 Organization of the Report

This report is organized into six chapters, each contributing to the overall understanding, design, and validation of the proposed system:

- **Chapter 1: Introduction** introduces the problem domain, outlines motivations, defines objectives, describes the methodology, and summarizes the expected outcomes.
- **Chapter 2: Background** explores the existing identity management landscape in public transport, reviews related literature and applications, and highlights gaps that justify this research.
- **Chapter 3: Research Methodology** presents the system architecture, component design, identity lifecycle, and technical workflow, including detailed cryptographic models and verification processes.
- **Chapter 4: Implementation and Results** discusses the environment setup, performance metrics, comparative analysis of blockchain platforms, and results observed through prototype testing.
- **Chapter 5: Engineering Standards and Design Challenges** outlines the technical, ethical, and sustainability aspects of the system and maps the design decisions to national engineering competencies.

- **Chapter 6: Conclusion and Future Work** summarizes key findings, acknowledges limitations, and proposes directions for expanding the system's impact and scalability.

Chapter 2

Background

2.1 Introduction

This chapter presents the background and foundational knowledge that underpin the proposed blockchain-enabled Self-Sovereign Identity (SSI) system for Bangladesh's public transportation network. It starts by reviewing the current state of identity management in public transport and highlights the shortcomings of centralised methods. The paper proceeds with a comprehensive literature review that covers relevant academic works and actual deployments of digital identity systems, in particular those based on blockchain and SSI solutions.

2.2 Literature Review

Table 1: Literature Review

Title	Authors	Year	Methodology	Limitation
Leveraging self-sovereign identity & distributed ledger technology in renewable energy certificate ecosystems [1]	Md Sadek Ferdous et al.	2023	Proposed threat model, requirement analysis, use case demo with DIDs, VCs, and smart contracts.	No real deployment, interoperability and legal uncertainty, scalability issues
A Blockchain-Based System for Healthcare Digital Twin [2]	Sadman Sakib Akash et al	2022	Develop a mathematical data model, system architecture design, and a blockchain based protocol flow analysis	No real-world testing, No evaluation in different healthcare infrastructure.
Blockchain-enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation [3]	Lukas Stockburger et al	2021	Case study and prototype of SSI transport ID; compared 4 blockchain systems	High cost, interoperability issues, poor connectivity
On the Integration of Self-Sovereign Identity with TLS 1.3 Handshake to Build Trust in IoT Systems [4]	Leonardo Perugini et al	2024	OpenSSL implementation of the modified TLS 1.3 handshake and performance analysis through real-world IoT experiments.	High computational cost for DID resolution; additional overhead in mutual authentication scenarios.

Blockchain-Aware Decentralized Identity Management and Access Control System [5]	Aarti Amod Agarkar et al	2024	Ethereum-based SSI system with ZKP, smart contracts, SSO	Requires cryptocurrency (GAS) for transactions; blockchain consensus mechanisms introduce latency.
Self-Sovereign Identity Empowered Non-Fungible Patient Tokenization for Health Information Exchange Using Blockchain Technology [6]	Yan Zhuang et al	2023	Case study with 3M transactions, NFT-based patient IDs, ZKP	High cost, requires in-person verification, limited control
Enforcing Security Policies on Interacting Authentication Systems [7]	Francesco Buccafurri et al	2024	Theoretical framework with formalization of authentication policies, dependency verification algorithm, and an SSI-based implementation	High computational cost, regulatory compliance issue
A Blockchain-Empowered and Privacy-Preserving Digital Contact Tracing Platform [8]	Eranga Bandara et al	2021	SSI proofs + Mystiko blockchain, performance tested	High cost, private key management risk, adoption barrier
Digital Identity Using Blockchain [9]	Alexandru-Cristian Careja et al	2023	Blockchain-based ID model with APIs and ECDSA	High storage demand, scalability, complexity
Edge Computing: Smart Identity Wallet Based Architecture and User Centric [10]	Syrine Sahmimaet al	2019	Smart wallet on public blockchain, multi-signature	Scalability, privacy, key management risk
Integrating an Academic Management System with Blockchain [11]	Sérgio Guerreiro et al	2022	Case study using FenixEdu and Ethereum blockchain	High learning curve, adoption issues
BRON: A Blockchained Framework for Privacy Information Retrieval in Human Resource Management [12]	Gulshan Kumar et al	2024	Hyperledger-based HRM, performance tested	Scalability, post-quantum risk, dataset limitations
Trust Framework for Self-Sovereign ID in	Alan Ling et al	2024	Design Science Methodology, 6-	Regulatory inconsistency,

Metaverse Health Care Applications [13]			step framework	emergency use challenge
Blockchain-based Governance Models Supporting Corruption-Transparency [14]	M.M. Ibrahimy et al	2024	Systematic Literature Review of 45 studies	No practical implementation, scalability issues
A Multi-Layer Trust Framework for Self-Sovereign Identity on Blockchain [15]	A. De Salve et al	2023	Experimental evaluation on Ethereum blockchain using the Extended Epinions dataset	High gas cost, scalability (graph complexity)
How Modeling Helps in Developing Self-Sovereign Identity Governance Framework [16]	M. Sroor et al	2022	Case study using EGC tool, model creation	Tool license limits, complexity
A Systematic Literature Review of Blockchain-Based e-KYC Systems [17]	Md. Abdul Hannan et al	2023	Systematic Literature Review (SLR) using PRISMA methodology, analyzing 19 studies	Lack of standards, privacy, adoption gap
Self-Sovereign Identity in University Context [18]	Araceli Queiruga-Dios et al	2023	Blockchain-based academic ID model with VCs	No real use, adoption and regulation issues
Self-Sovereign User Scenarios in the Educational Domain [19]	Gerd Kortemeyer	2023	SSI conceptual framework for education	Governance, integration, student access issues
SSI4Web: A Self-Sovereign Identity (SSI) Framework for the Web [20]	Md Sadek Ferdous et al	2022	Hyperledger Indy & Aries-based SSI web auth	Usability & backup issues, no real use
Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education [21]	Alex Grech, Ira Sood et al	2021	European case studies, governance review	Global adoption, GDPR, interoperability
Blockchain-Based Voting System [22]	Jiayang Yao et al	2020	Ethereum-based e-voting with smart contracts	Complex auth process, low usability
A Study of Blockchain Adoption in the Rail Sector [23]	Alessio Tardivo et al	2023	Semi-SLR & gap analysis in rail	High cost, regulatory barriers, low adoption

2.2.1 Similar Applications

Identity Identification management is an important function in PT, it is required in public transport to ensure that passengers are identified securely and transparently, and to avoid fraud, and making an unbalancing of transport operations performance. [1] Nowadays infrastructures around the globe use central databases of IDs, physical IDs or verification with biometrics which works, but have their own cyber threats such as identity theft, privacy disclosure or slow authentication.[2][1] In Bangladesh, the public transport remains divided, and its operators have their respective identity check and ticketing. This stranded this community, and resulted in a lack of interoperability and redundant registrations and more hassle for the end-user. Other countries, too, have trialed various digital identity systems in attempts to tackle similar issues. For example, the Estonians have a national eID system for securely accessing different public services (such as transportation) with cryptographic authentication. [1] China has already started using facial recognition in rail stations to automate the process of identifying passengers and checking tickets. [3] However, these systems are still based on centralized identity models and are vulnerable to cyberattacks and single points of failure. [2] [4] Moreover privacy of user is not guaranteed as people have little control over storage and dissemination of their personal data. [4] These challenges underscore the importance of a defusing to a more decentralized model (e.g., SSI) where users gain the majority of control over their own identities without sacrificing security or privacy. [1] [5] [6]

2.2.2 Related Research

Recent research has concentrated more and more on the use of Self-Sovereign Identity (SSI) and blockchain technologies to revolutionize digital identity management, especially for sectors such as transportation. SSI provides a decentralized paradigm that allows individuals to have full control over their identity attributes while validating the identity in a cryptographically proven manner, without having to trust the centralized authorities.

Enabling security, privacy and user autonomy Several studies have shown the potential of SSI. For instance, Stockburger et al. (2021) have studied SSI-based identity systems for public transportation and conclude that these systems can enhance data protection and standardisation. They contrasted blockchain platforms such as Sovrin, uPort, Civic and Namecoin, highlighting the advantages and challenges of integration cost, interoperability, and responsiveness being some of those concerns. [1] Further research on the use of blockchain for identity verification in areas of finance, healthcare, education are also of interest. These researches highlight the potential advantages of DIDs and VCs for creating trustless and tamper-evident systems. But one common issue associated with these implementations is the requirement of constant internet connection which is not feasible in the low bandwidth scenarios, a likely case in a country like Bangladesh. In order to solve that problem, lately some proposals are considering the integration of offline-enabled technologies, such as Near Field Communication (NFC), so that the verification of credentials can be performed in locations with no or poor Internet connectivity. Furthermore, by relying on Zero-Knowledge Proofs (ZKPs), the privacy of users is additionally enforced, as users are able to demonstrate the validity of their certificates, without the necessity to disclose any personal information. Overall, although existing studies confirm the viability and advantages of blockchain-integrated SSI in the public transportation domain, the real-world deployment especially in developing nations is rarely progressed. Costs of implementation, regulatory ambiguity, and the lack of standardized models are a few of the challenges

yet to be addressed. These observations motivate the solution we propose in this paper, that aims to design a scalable privacy-preserving identity system for the contextual socio-economic infrastructure environment of Bangladesh.

2.3 Gap Analysis

Despite advancements in blockchain and SSI-based identity management, several research gaps exist in their application to public transportation, particularly in developing countries like Bangladesh. Existing studies primarily focus on theoretical models or pilot implementations in developed countries, lacking real-world deployment in large-scale transit networks. One critical gap is the lack of interoperability between different transportation providers. Ticket and identity control systems are generally isolated from one another which makes their easy integration difficult over different means of transport. There's also the issue of offline verification as many blockchain and SSI authentication models are dependent on internet access and useless in low-network conditions. There are also regulatory obstacles to blockchain-based identity solutions. Most governments do not have detailed legal structures that provide for decentralized identity systems and concerns over compliance, data protection, and liability exist for them. There are also costs in the high implementation and technical complexity - a barrier for transport operators, especially in emerging economies which can't afford extensive digital infrastructure. Our work fills these gaps A Blockchain-Based Self-Sovereign Identity (SSI) system for Bangladesh's public transport. This system will:

- Facilitate decentralization and tamper-proof identity verification to allow frictionless travel in various transport modes.
- Verify verifiable credentials and cryptographic signatures to authenticate securely without revealing personal data.
- On-device verification, can verify the credentials offline using NFC SSI authentication, making it more accessible.
- Automatically distribute fares through smart contracts, killing financial middlemen and reducing fraud.

Blockchain, SSI, and smart contracts are combined in this system to disrupt transportation in Bangladesh with a secure, efficient and privacy-friendly identity.

2.4 Summary

This section presented a comparative study of existing IdM proposals suitable for PT, emphasizing on the fact that most proposals are based on centralized databases, use manual confirmation, and have low levels of systems of systems interoperability. Literature review examined identity solutions based on blockchain especially Self-Sovereign Identity (SSI) that has advantage in privacy, security, and decentralization. The gap analysis revealed main problems to be data security, no offline verification of the data and inefficient isolation of fare. We proposed a SSI-based framework to solve them by secure decentralized ID verification process, automatic fare distribution and trans-modality travel.

Chapter 3

Research Methodology

3.1 Methodology

This chapter discusses the methodological aspect of the proposed design and simulation of blockchain technology inspired Self-Sovereign Identity (SSI) scenario of the public transportation of Bangladesh to meet that specific requirement. The content encompasses not only concept-research strategy and system design methodology, but also explains how decentralized identity, smart contracts and how privacy-preserving mechanism are used to overcome the shortcomings of current centralized mechanisms. The methodology consists of two main parts:
Theoretical Research Methodology: Which concentrates on the design paradigm, models and enabling technologies employed to provide a proving solution.
Technical System Implementation: A detailed overview of the system architecture, components and the logic of our prototype, described more in Depth in section (3.2 Detailed Methodology and Design)

3.1.1 Overview

The proposed system follow a problem-solving approach to design privacy-preserving, and decentralized identity management system for Bangladesh's FPT infrastructure. Current systems are heavily rely on centralized databases, which have various limitation such as:

- Limited privacy of user
- Repetitive document verification
- Inefficient ticketing across modes
- Inability to interoperate between services

To address these issues, the proposed system integrates the principles of Self-Sovereign Identity (SSI) with Hyperledger Fabric, a permissioned blockchain framework. In this architecture, users interact with the system through a decentralized wallet, where they submit Verifiable Credentials (VCs) such as National ID, student ID, or bank account proof. These credentials aren't centralized; rather, authorized verifying authorities (like government agencies, businesses, and universities) confirm them through the form of cryptographic attestations. Once verified, user receives a Digital Transport ID (DTID) that users then can use for identity verification when he/she purchases ticket or is availing the transport services. Tickets are issued through smart contracts, allowing escrow fare lockup and fair transport provider payouts. To ensure the privacy of the users, ZKPs are being used for the identity proofs, and for the offline verification the code based on QR/NFC and still the access is kept in the low/no network areas.

This approach represents a synthesis between decentralized identity architecture with cryptographic security and blockchain enabling automation, and delivers a scalable, user-centric solution for transportation that can do away with duplicate verification, central

supervision, and connecting with third parties.

3.1.2 Proposed Methodology

The The proposed framework is a decentralized, privacy-preserving, and interoperable digital identity framework created tailored for the public transport sector of Bangladesh. Leveraging Hyperledger Fabric distributed permissioned ledgers, the framework enables trusted parties (i.e. government, education and financial institutions) to issue cryptographically-signed Verifiable Credentials that do not require end user data localization. Those credentials are then stored in a decentralized digital wallet app, which acts as a user's gateway to managing their identities, purchasing tickets and paying through a secure channel. If the verification is successful, Bangladesh Road Transport Authority (BRTA) will issue a Digital Transport ID (DTID) which acts as unified digital ID of the user across the modes of transport. The solution uses smart contracts to automatically calculate transport fare, escrow payments and enable revenue piece-meal to transport vendors after a travel has been concluded. For inclusivity, we enable online and offline verification mechanisms with QR codes and NFC tags, such that no private information is released for ticket validation thanks to the Zero-Knowledge Proofs (ZKPs). During the procedure, only legitimate blockchain nodes are allowed to visit corresponding data in their functional areas to be the confidential, auditable and regulatory. As illustrated in Figure 1, the user initiates the flow by submitting credentials through the wallet, which are then verified by authorized entities operating as blockchain nodes. Verified data is cryptographically validated, leading to DTID issuance by BRTA and enabling the user to securely purchase tickets and access transport services - all within a decentralized and trustless ecosystem.

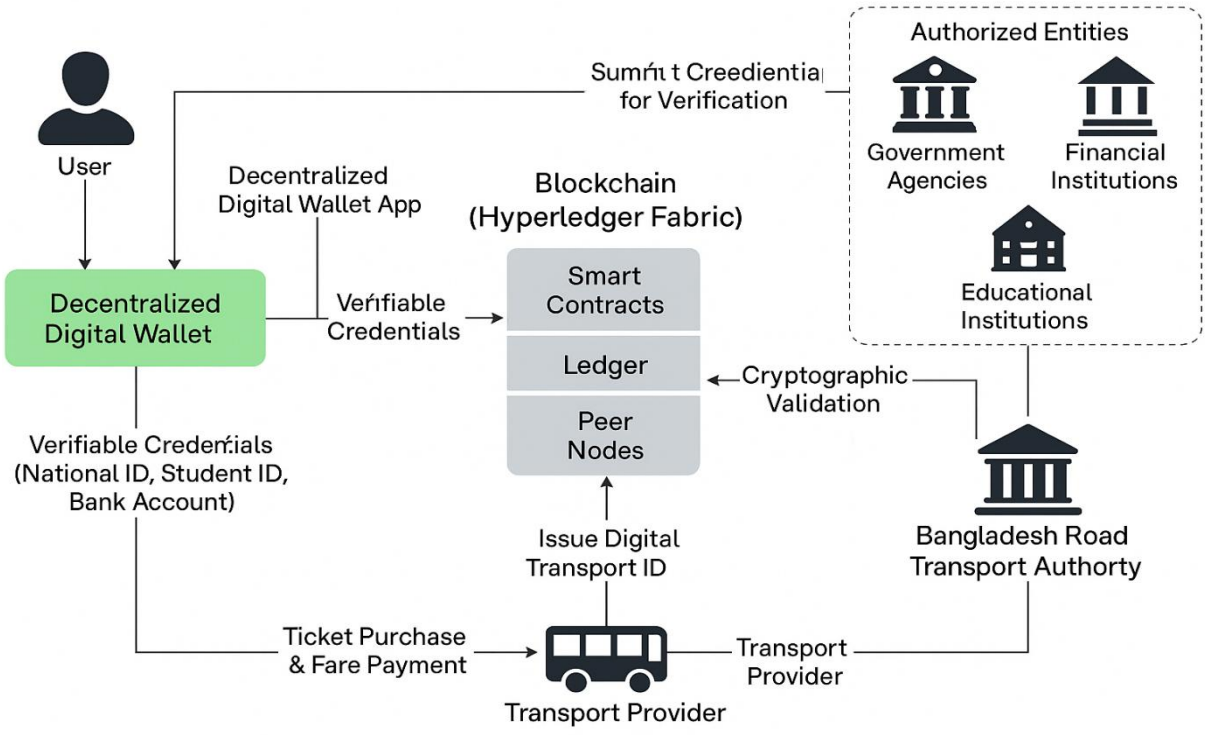


Fig 1: Proposed Methodology

3.1.3 Functional and Nonfunctional Requirements

Functional Requirements

F1: In the proposed system is smart contract enabled platform. Its automate user identity verification, DTID issueance, ticket booking and fare payment settlement in a seamless tamperproof way.

F2: Implemented a self-sovereign identity (SSI) framework that will allow user's to control their information & ensure their privacy and compliance with specific decentralized identity principles.

F3: The adaptation of functions within the transport ecosystem allows for GN, BN, and E to act as verification entities by showcasing that proof of identity occurs before the issuance of a DTID.

F4: Transport providers such as Green Line Paribahan, Shohagh Paribahan, Hanif Enterprise need to register with the BRTA and be issued Transport Provider ID (TPID), which is mandatory for regulatory compliance.

F5: The escrow payment mechanism holds ticket fares in the smart contract. As soon as the journey is completed, the smart contract releases payments to the hired transport providers automatically.

F6: The system allows also to validate offline tickets through last-synced blockchain information, allowing travellers to reach any area even in regions with low network access.

Transactions Are Recorded Using Unique Digital Signatures and Cryptographic Hashing To Authenticate Transactions. All travel records and ticket verifications are immutable.

Non-functional Requirements

S1: No unauthorized actor can issue fraudulent DTIDs or manipulate records in the system, as only registered users, verified transport providers, and approved entities have access to system functionalities.

S2: Strong Cryptographic Security - Each of the key transactions, such as issuance of DTID, verification of tickets and payments should be digitally signed with the help of digital signatures at the beginning when it is created to guard against any identity theft or unauthorized transaction modifications.

S3: Interoperability - The system should be able to work with already implemented transit networks supporting integration across different transport modes (buses, metro, ferries), and let third-party digital wallet services handle DTIDs and payment solutions.

S4: Data Privacy and Compliance – The architecture should adhere to policies to protect user data that are defined as per data protection laws like GDPR and Bangladesh's Digital Security Act, ensuring that user data cannot be accessed without user consent.

S5: Scalability - Handle thousands of transactions per second for large metropolitan transport demand, using a blockchain(Hyperledger fabric) optimized for maximum

efficiency to minimize gas fees and transaction latency.

S6: Offline Operation - The protocol should be operable in a network-starved environment where transport providers could validate tickets against a stored version of the blockchain and synchronize where required.

S7: Auditability Efficiency – Regulators and transport providers must have access to transaction logs on a permissioned basis through public, tamper-proof blockchain records, while retaining adequate privacy protections for users.

S8: Low Transaction Overhead - Execution of smart contracts should be optimized to minimize computational overhead and transaction fees (gas fee), making it cost-effective and fast for users and providers.

S9: High Availability and Fault Tolerance - The system shall deploy redundancy mechanisms to provide always-on availability even with infrastructure failure or blockchain node outage.

S10: Usability and Accessibility - The system should be user-centered with mobile and web interfaces that are intuitive and accessible, support multiple languages, and accommodate a range of populations, including those who don't have experience with blockchain technology.

3.1.4 Context Diagram

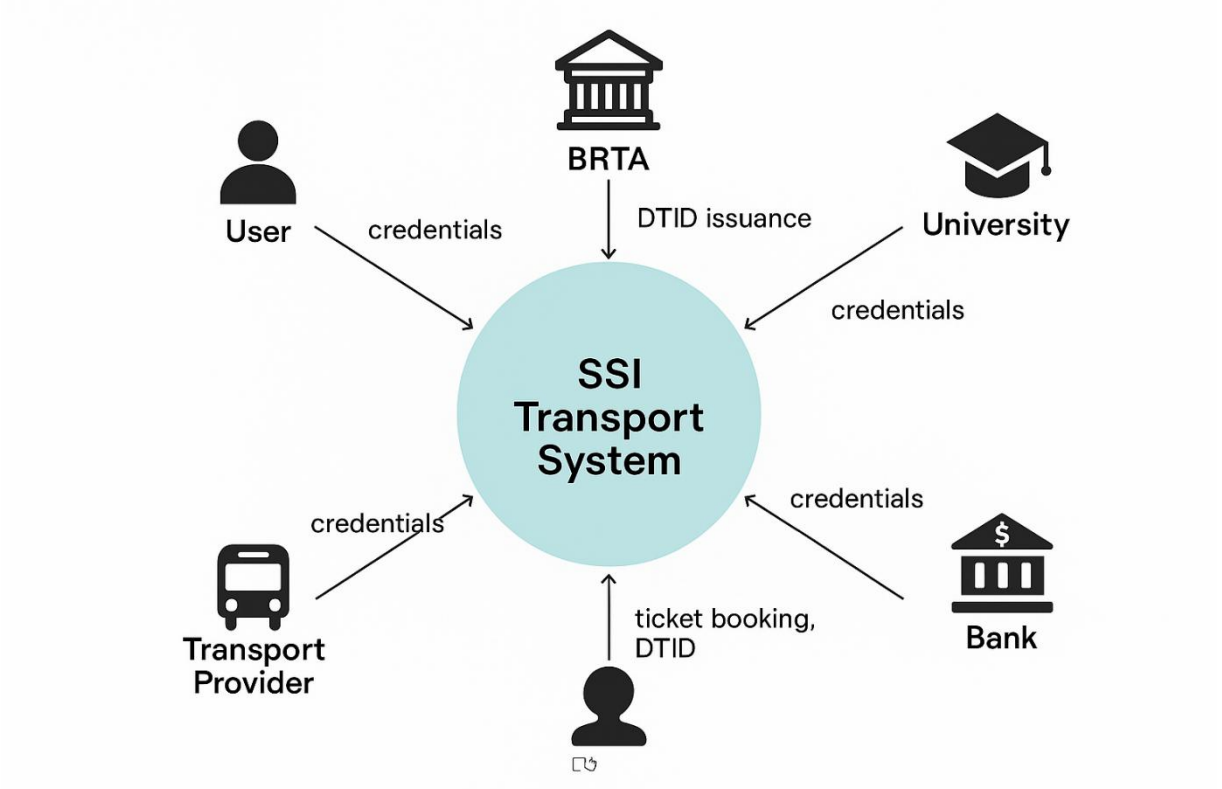


Fig 2: High Level interaction

Fig 2 illustrates the high-level interaction between users, the BRTA, and associated verification bodies. The user submits credentials, which are verified by institutions

through the blockchain. Upon verification, the BRTA issues a Digital Transport ID (DTID), enabling users to book transport services.

3.1.5 Data Flow Diagram Level 1

Fig 2 shows the breakdown of core system processes, including credential validation, DTID

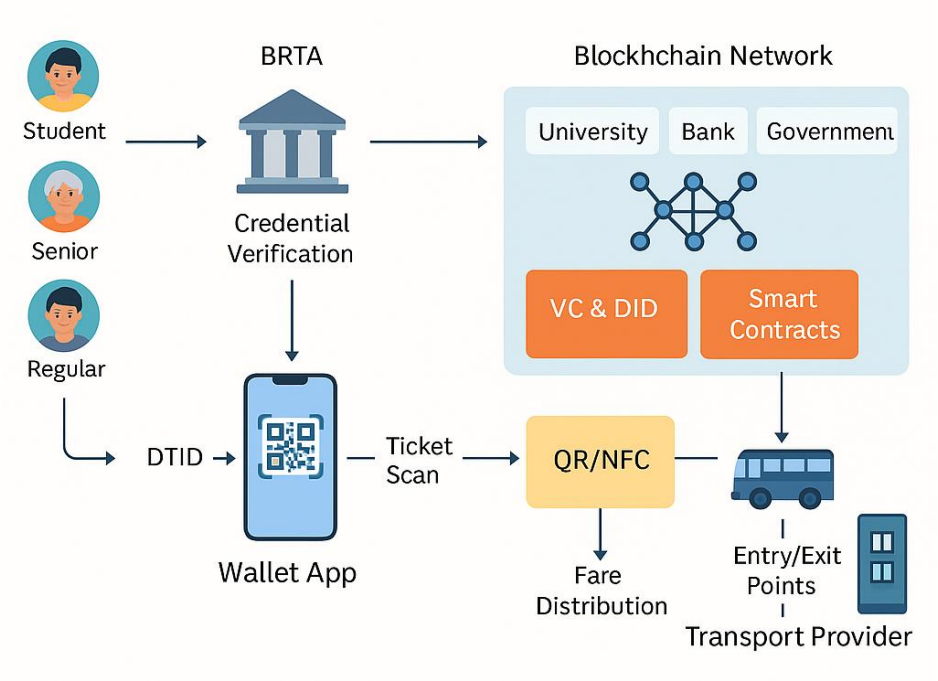


Fig 4: High Level Diagram

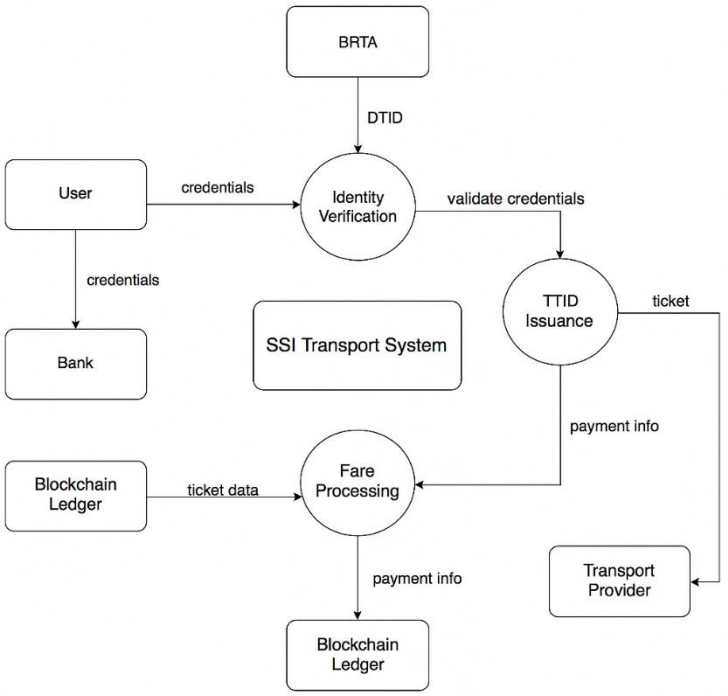


Fig 3: L1 DFD

issuance, ticket booking, and fare settlement. Data is securely exchanged between users, the blockchain verification layer, and transport providers using smart contracts and cryptographic protocols.

3.1.6 UI Design

The user interface (UI) for the blockchain-enabled Self-Sovereign Identity (SSI) transport system was developed using React for the frontend and Firebase for backend services including authentication, data storage, and role-based access control. The UI was designed to simulate a complete digital experience for all stakeholders passengers, verification authorities (e.g., BRTA), and transport providers reflecting the core principles of decentralization, usability, and privacy.

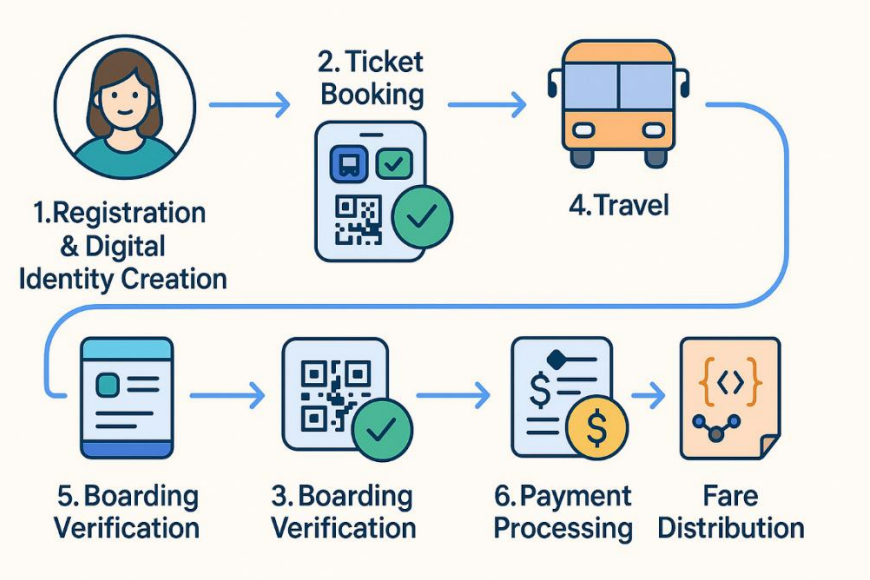


Fig 5: User Flow

Design Goals

The primary goal of the UI design was to make blockchain-based identity and ticketing workflows accessible and intuitive, even for non-technical users. Special focus was placed on:

- Simplicity – Clean layout and form inputs for ease of registration and interaction.
- Clarity – Clear user prompts, error messages, and status indicators (e.g., successful credential verification or DTID issuance).
- Responsiveness – Optimized for both desktop and mobile screens using responsive layout principles.
- Accessibility – UI components are easily navigable, including offline support simulation for low-connectivity areas using Firebase's local caching.

Core UI Components

The prototype includes multiple interactive screens to simulate the real-world system behavior. Key interfaces are as follows:

- User Registration Page: Allows users to create an account and upload document (e.g., NID, student verification, bank proof). React form validation ensures all fields are completed before submission.

- Credential Verification Dashboard: After registration, credentials are sent for verification. Simulated institutions (universities, banks, government) respond asynchronously, and verified credentials are shown in the BRTA dashboard UI.
- Digital Transport ID (DTID) Display: Once verified, users receive a DTID, visible within the dashboard as a digitally signed credential. This DTID is the key to seamless ticket booking.
- Ticket Booking Interface: Users can choose transport mode (bus, metro, ferry), route, and fare category (e.g., student discount). Upon confirmation, a QR code/NFC-enabled digital ticket is generated and stored in the wallet.
- QR Code & NFC Scan Simulation: This module simulates both entry and exit point verification. Users scan their DTID or ticket, and the system validates credentials using Firebase's role-based logic, mimicking blockchain validation.
- Admin/BRTA Panel: Designed for regulatory authorities to manage transport provider registrations, approve credential verifications, and issue DTIDs. This interface mimics the issuer role in the SSI architecture.

Some of the UI screenshot given below –

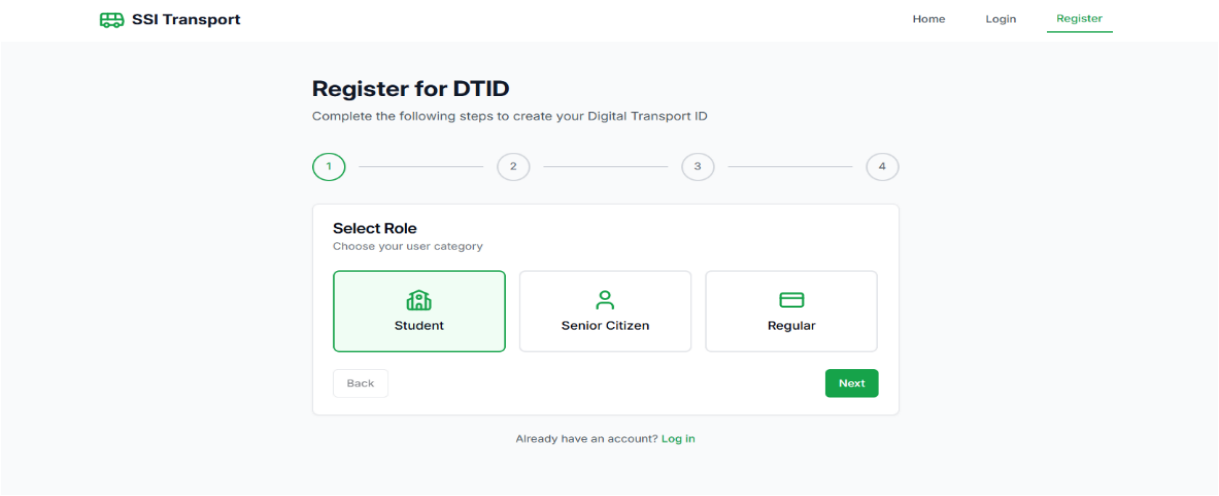


Fig 6: Role Select

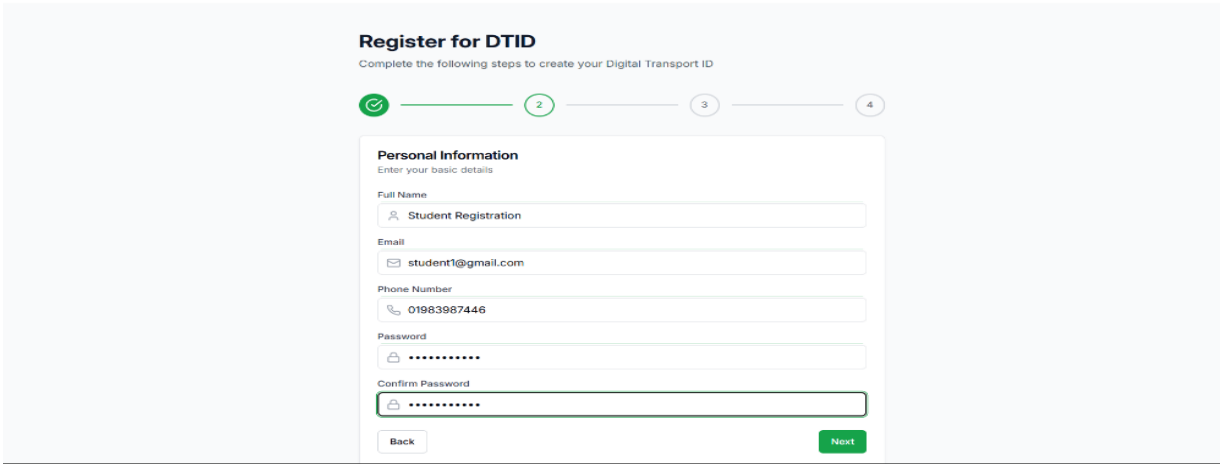


Fig 7: Registration Page (Form FIll Up)

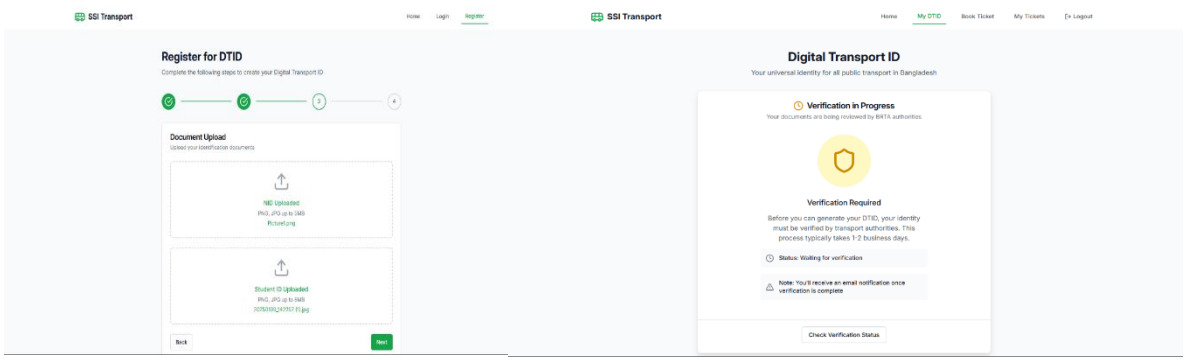


Fig 8: Registration Page (Doc Submit & Status pending)

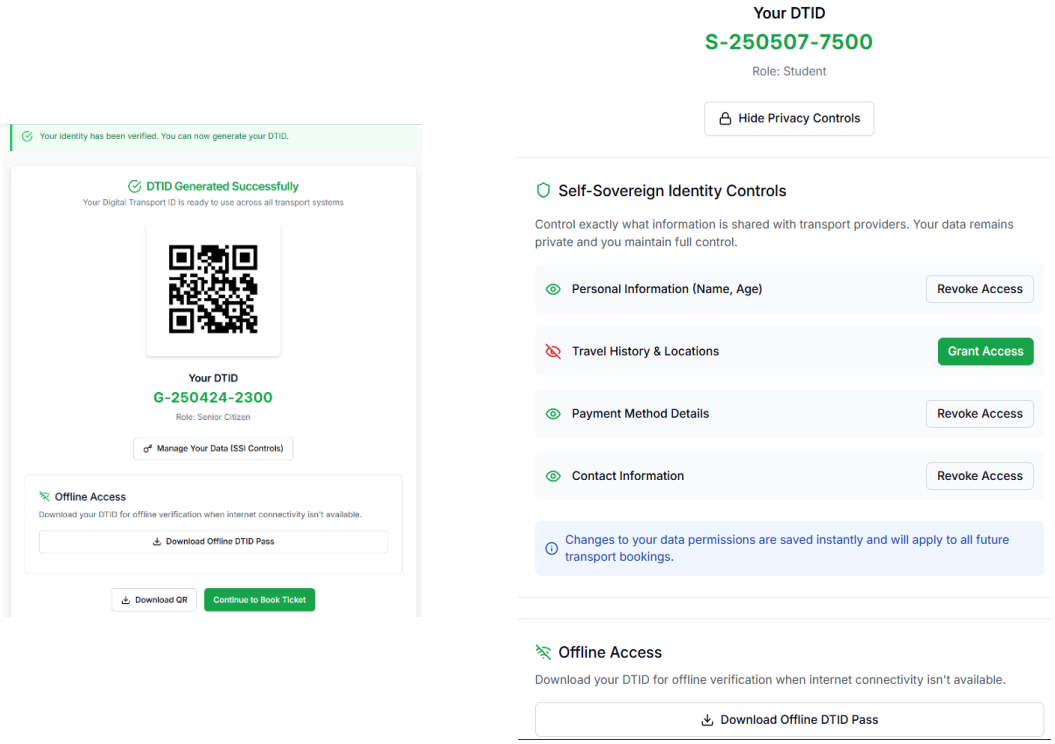


Fig 9: Offline Accessible DTID

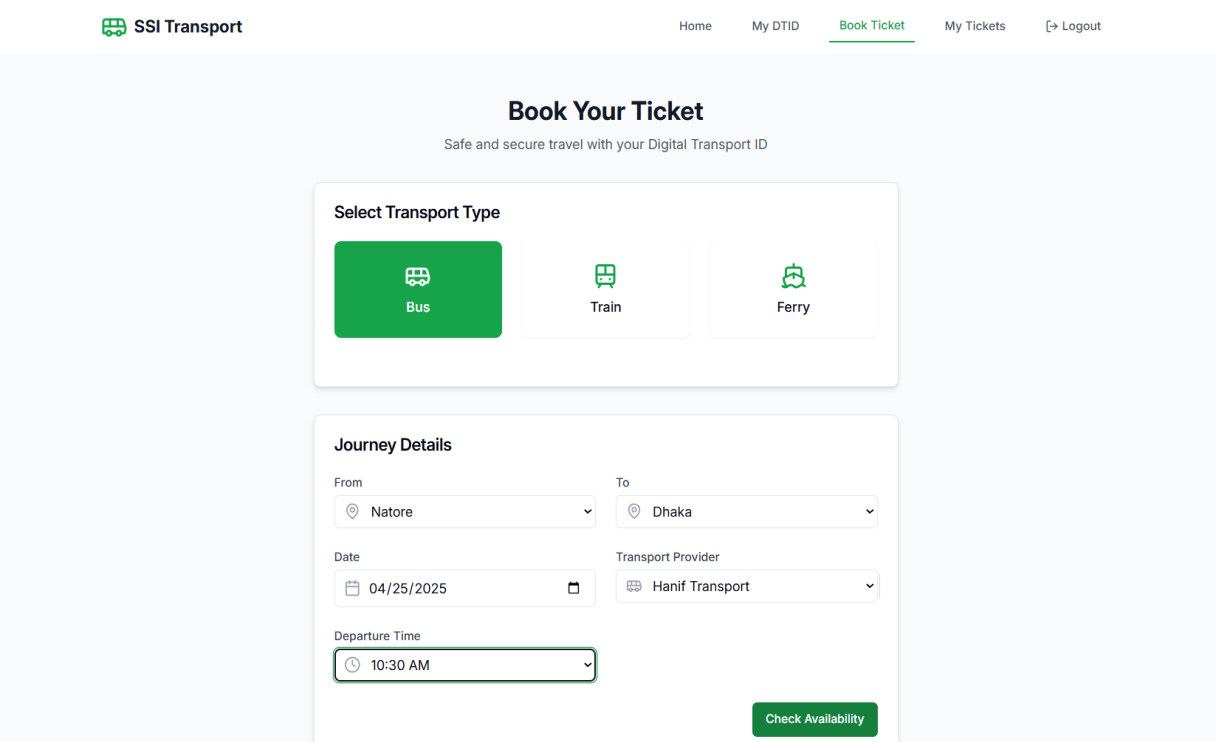


Fig 10: Ticket Booking Page

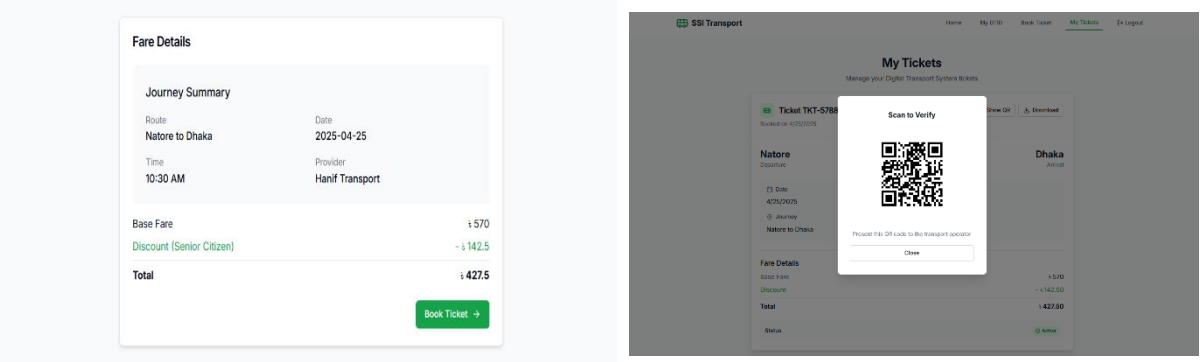


Fig 11: Fare Details Page & QR

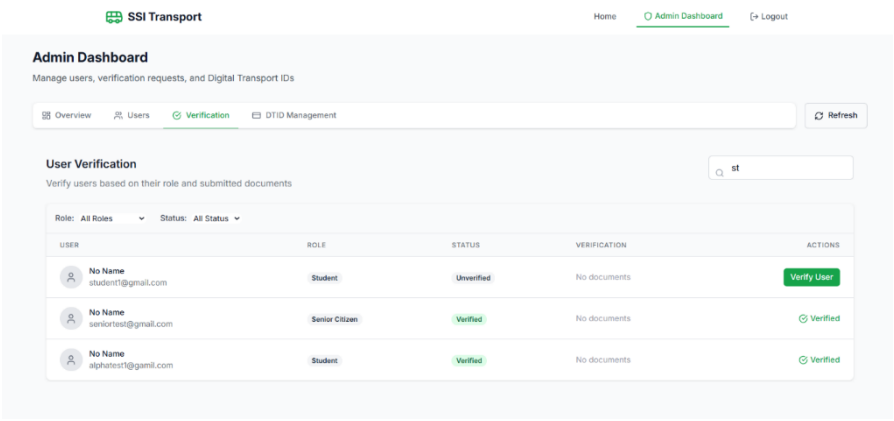


Fig 12: User Verification

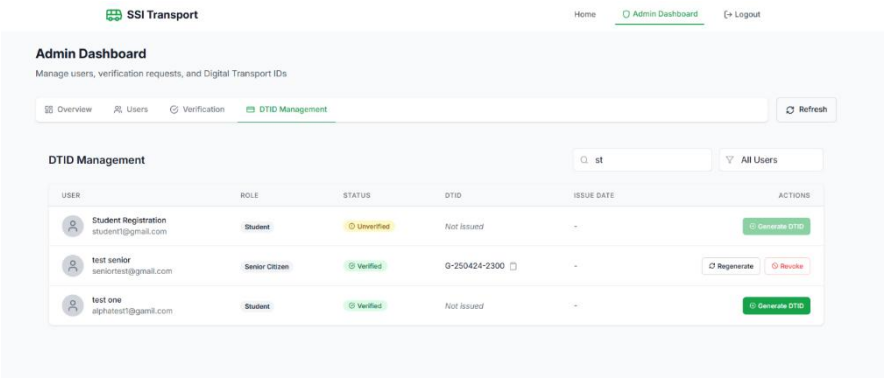


Fig 13: DTID Issue

Fig 12 & Fig 13 represent the admin/BRTA dashboard features. In fig 14 showing admin can verify hash credential of user upload document through verified blockchain nodes. The blockchain nodes check and verify user credential. Then admin issue DTID to every verified user (fig 13).

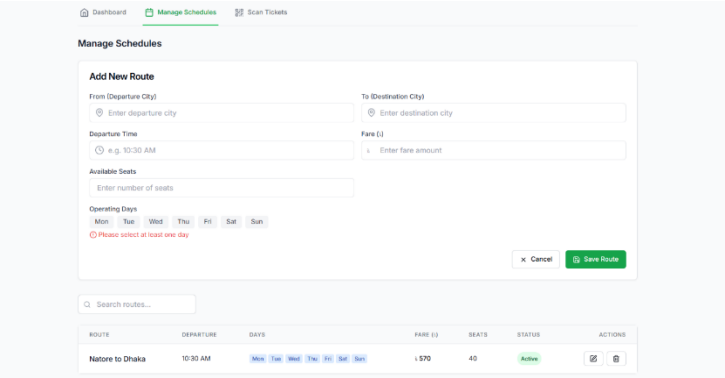


Fig 14: Schedule Management Page (TP)

Fig 14 showing schedule management page, where each transport provider can update delete every schedule of their transport and fig 15 show ticket verification page and status.

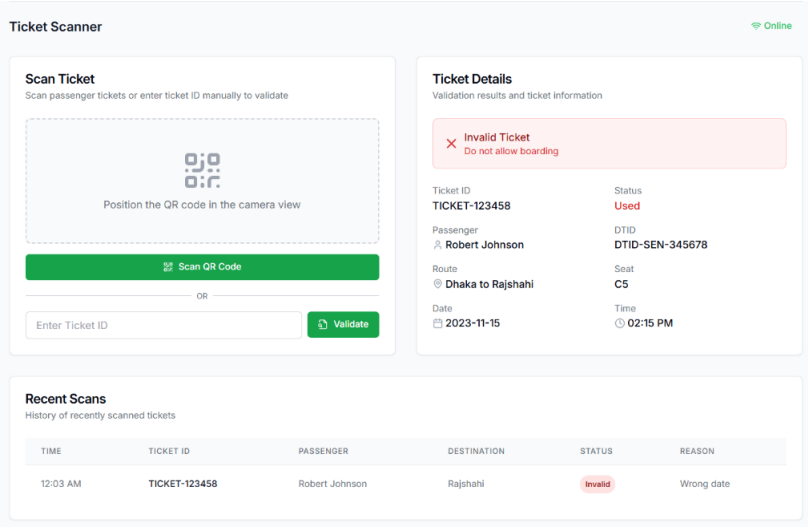


Fig 15: Ticket Verification Page

3.2 Detailed Methodology and Design

This section outlines the technical methodology and system design underpinning the proposed blockchain-based Self-Sovereign Identity (SSI) framework for Bangladesh's public transport infrastructure. Building upon the conceptual methodology presented in Section 3.1, this portion focuses on the architecture, technologies, components, and operational workflows that enable secure identity issuance, credential validation, ticketing automation, and decentralized fare management.

At the heart of the system is a Hyperledger Fabric permissioned blockchain network, which forms the trust layer between various actors=including the Bangladesh Road Transport Authority (BRTA), transport providers, verification institutions (e.g., universities, banks, govt agencies), and the end users. The platform supports Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), empowering users to control their identities via a digital wallet while ensuring that no sensitive data is stored on-chain. The flow of credentials from issuance to transport validation is cryptographically protected, and smart contracts are used to manage ticketing, fare locking, and revenue disbursement without the need for intermediaries. Additional layers, such as Zero-Knowledge Proofs (ZKPs) and middleware for interoperability, ensure privacy, offline support, and system-wide synchronization.

3.2.1 System Architecture

The system architecture, illustrated in Figure 18, defines a decentralized, secure, and privacy-protecting infrastructure for managing digital identity, ticketing, and fare transactions in Bangladesh's public transport sector. Built on the Self-Sovereign Identity (SSI) model and powered by Hyperledger Fabric, the framework facilitates coordination between various actors such as passengers, credential issuers, verifiers, transport provider and governance authorities in a secure blockchain environment. The lifecycle of ID starts from when a passenger starts the process of registering in a decentralized digital wallet (user). In this wallet, the user has Verifiable Credentials (VCs) issued by some trusted nodes of identity verification, such as government departments, universities and banks. These credentials are verified attributes like age, student, or income status. If the authentication is successful, then a Digital Transport ID (DTID) is issued by the Bangladesh Road Transport Authority (BRTA) as the main issuing entity. This DTID is issued to the user as a signed Verifiable Credential in the user's wallet, which allows the user to securely interact with the transport ecosystem. Using the DTID, the passenger can purchase tickets via the wallet interface. The system generates a QR code or NFC token that represents the digital ticket. When the user boards a vehicle, the transport provider or verifier scans the token to initiate ticket verification. Rather than accessing any personal data, the verifier queries the blockchain to check credential validity using Zero-Knowledge Proofs (ZKPs). The system returns only a cryptographic validation result, ensuring privacy and security at all times. Ticket purchases and fare operations are executed via smart contracts on the blockchain. These contracts handle fare calculations, apply applicable discounts (e.g., for students or seniors), and lock the fare amount in a simulated escrow. Upon journey completion, the contract automatically triggers payment disbursement to the respective transport provider. All relevant credential hashes, ticket data, and transaction records are stored in a tamper-proof hash store on the blockchain ledger for transparency and auditability. Oversight is maintained by a governance authority, which enforces legal frameworks, access control policies, and system rules. This governance layer ensures that each participating entity whether issuer, verifier, or transport operator functions in accordance with national transport policies and data protection standards.

As depicted in Figure 18, the architecture integrates identity issuance, verification, ticketing, and fare management into a unified, decentralized flow. It allows for user-controlled identity, verifiable trust between parties, and automation of fare operations, while upholding privacy and ensuring interoperability across all transport modes in Bangladesh.

3.2.1.1 Hyperledger Fabric Platform

The foundational infrastructure of the proposed transport identity system is built on Hyperledger Fabric, an enterprise-grade, permissioned blockchain platform that offers modularity, scalability, and privacy-focused architecture. Unlike the public blockchains, Hyperledger Fabric does support fine-grained access control, so that only identity-based entities such as government authorities, banks and transport providers can join and access data for their need on private channels. It is great for handling personal identity information, such as user details, tickets and similar real time fare and managing in a secured and audit-able way. In the architecture, the user receives the Decentralized Identifier (DID) by the wallet interface and it gets anchored on the blockchain. These DIDs are associated with cryptographically verifiable public key metadata and used for secure peer-to-peer communications and digital verification of digital signatures. Nothing personal is ever written to the ledger. Instead, just the (hashed) representations and cryptographic proofs are stored, maintaining the privacy of the parties and their information whilst allowing for trustworthy, verifiable engagements.

Credential issuance, verification and ticketing workflows are governed by smart contracts (i.e. chain-code in Fabric). The channel-based architecture of Fabric makes it possible for data to be shared only between legitimate parties. Additionally, evidence of a discount for students, for example, at one university is disclosed only to BRTA and the university, but not to other users in the system. By leveraging DIDs, VCs, and programmable smart contracts in a federated ledger, Hyperledger Fabric offers a decentralized but trusted identity verification system for all the transport providers.

3.2.1.2 Decentralized Identity Managements

The system is based on the Self-Sovereign Identity (SSI) model, allowing users to own and manage their digital identity through a decentralized mobile wallet. This wallet creates a DID for every user and acts as the front end to submit and manage VCs. At registration time, users submit digital proofs of their identity (such as national ID, student status, or bank account verification) to authorized issuers (e.g., universities, banks, government agencies), who cryptographically validate them. When verified, these issuers issue digitally signed Verifiable Credentials, which get stored inside the user's wallet, not the blockchain. Upon multi-party verification, the Bangladesh Road Transport Authority (BRTA) releases a Digital Transport ID (DTID) which is a reusable, cryptographically signed credential that serves as the user's single transport identity across buses, trains, metros and ferries. When it comes to travel, users identify themselves via their DTID when providing their QR code or NFC token. The tokens are validated through Zero Knowledge Proofs (ZKPs), thus no personal information is revealed in the process. For instance, a student can show his or her discount eligibility without disclosing the name, university, or ID number. And the wallet stores a cached copy of the credentials so they can be checked offline in areas with slow or intermittent internet access. When connection restored, all outstanding verification logs are synced with blockchain to ensure auditability and transaction consistency.

Under the identity model, users maintain direct control over their credentials, so

transport providers and regulators can verify authenticity in a secure, privacy-preserving, and decentralized fashion..

3.2.1.3 Zero-Knowledge Proofs (ZKPs)

ZKPs are a fundamental privacy primitive of the proposed system. ZKPs enable a user (the prover) to prove to another party (the verifier—e.g., a transit operator or authority) that a statement is true (e.g., that the user is entitled to a fare discount) without revealing any underlying information. Such a cryptographic method has the advantage of data minimization; one does not have to reveal specific sensitive attributes, such as a student's name, date of birth, characteristics of the university that the student attends. In the context of this framework, ZKPs are deeply embedded in the design of VCs and DTID. When a user purchases a ticket or provides evidence at a checkpoint, the transport operator is sent no more than binary outcome (e.g., valid/invalid) in response to a ZKP-based query. This eliminates the need for third-party "verifiers" and ensures that validation is trustless, meaning integrity is guaranteed by cryptographic proof rather than the need to trust an organization. Aside from privacy, ZKPs are also crucial for system security. ZKPs are inalienable and tamper-evident, deterring impersonation and unauthorized modification of the credentials. Furthermore, their decentralized nature makes them suitable for both offline or temporary distributed systems, a requirement in the context of real-world public transportation, where internet connectivity might not be constant. Using ZKPs in both tickets and identity verification, it offers a method for privacy-preserving on-chain proving that does not leak data about riders, while preserving operational soundness.

3.2.1.4 Cryptographic Signatures & Access Control

To guarantee the verifiability and the provenance of the identity credentials, trust is built on the digital signatures and on role-based access control system implemented inside the overlay system Hyperledger Fabric. Each VC is cryptographically signed by the issuer (i.e. BRTA, university, financial institution etc.,) where issuer's own private key is used. Upon a user submitting the credential, the verifier can verify the validity of the certificate with the issuer public key, thus providing non-repudiation and tamper proofness. Fabric user space user space processes can only access system resources through Fabric's channelized hierarchy and ACLs. These mechanisms specify that certain nodes are entitled to execute certain actions, for instance, issuing a credential, verifying an identity, or validating a ticket. These access rules are put into effect in real-time via smart contracts to make sure that only involved participants interact with the right set of data.

Through the use of cryptographic-signed unlinked references with fine granularity of access control, the system realizes the authenticated and authenticatable data exchange while preserving the privacy of the users. It enables horizontal scalability by node specialization, while vertical compliance is possible as well (e.g., through regulatory supervision), which makes the approach resilient against data misuse and unlawful access.

3.2.1.5 Blockchain Node Roles and Responsibilities

The system works under a permissioned blockchain, in which every participant in the organization maintains a node that performs the assigned role. This architecture guarantees decentralized, trustless, and democratic amongst participants in the network.

- Issuer Nodes such as BRTA, universities and banks validate the end-user provided credentials and issue cryptographically signed VCs. These credentials are the

underpinning of the identity model.

- Transport provider Nodes that control the issuing of tickets, the validation of DTIDs and ticketing related transactions. These nodes process identity credentials through use of the smart contracts and write into the DLT the flow of the issuing and payment of tickets.

- Regulatory Nodes: Managed by BRTA, they supervise network integrity, policy rules enforcement, and audit without compromising any sensitive user information. This criterion enables the network to be complaint with the law, can monitor network health and can coordinate the system.

Ledger consensus is conducted among all nodes, achieving consistency, non-repudiation, and transparency of data. This distributed trust model eliminates the need for centralized authorities, reduces single points of failure, and enables verifiable, role-specific operations across all actors in the ecosystem

3.2.1.6 Data Privacy & GDPR Compliance

Although Bangladesh does not yet enforce a formal equivalent to the General Data Protection Regulation (GDPR), the proposed system architecture is designed to align with globally recognized data protection principles. These safeguards are built directly into the technical infrastructure of the platform to ensure both compliance readiness and ethical handling of personal information.

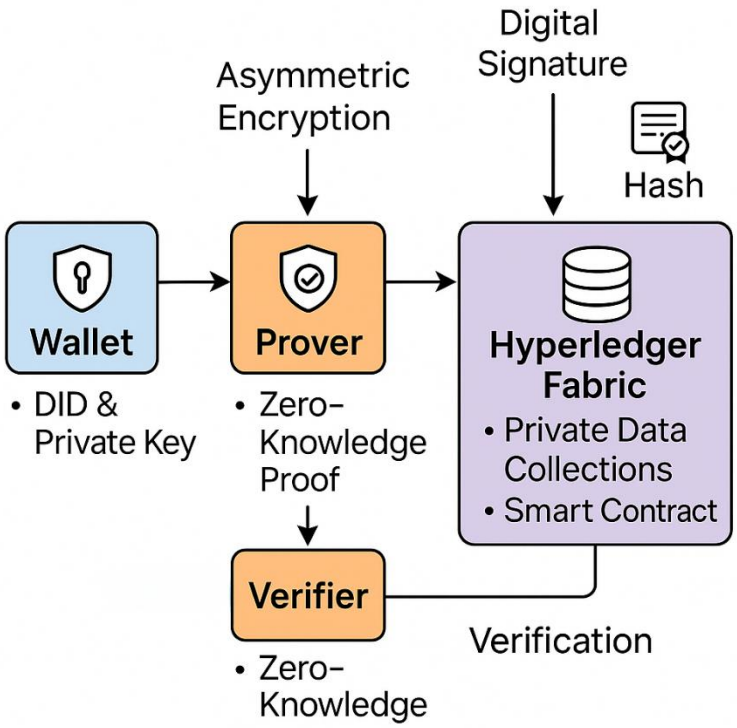


Fig 16: Privacy Architecture

The system complies with data minimization mandates by not storing any raw personal data on-chain. Instead, a record of only hashed forms or cryptographic signatures of credentials are logged, which means even if the blockchain gets leaked, no personally identifiable information about the users is leaked. In addition, the architecture allows

users to withdraw the Verifiable Credential (VC) access and request DTID invalidation via off-chain revocation lists, and thus enable individuals to manage their identity as they wish. Limited purpose is also by design. Each credential like student status or financial eligibility is issued to a direct use case and it cannot be reused elsewhere it is not supposed to be. The communication between the different system components is encrypted by industry standard protocols (such as AES-256, TLS), and the saved VCs are digitally signed to ensure authenticity.

Furthermore, selective disclosure with ZKPs Guarantees that a user is able to verify claims (e.g., the age or discount eligibility) without leaking superfluous personal characteristics. These embedded privacy protections work in combination to help comply with international data protection norms, and to prepare the platform for integration into future legislation in Bangladesh.

3.2.1.7 Smart Contracts for Fare & Identity Automation

Smart contracts are chaincode deployed within the Hyperledger Fabric, which we implemented as the autonomous logic engine of the system. They allow for manual free processing, automating key transport functions based on prior rules and trusted identity attributes.

The first primary service is machine validation of identity. When a user tries to make a reservation or get check-in status at a station, smart contracts verify the digital signatures of their DTID and Verifiable Credentials. Moreover, the smart contract imposes eligibility criteria on fare groups or access to transportation depending on the user's role (e.g., student, senior citizen). Secondly, a dynamic pricing scheme and its associated discounting process are encoded in the smart contract. Fare calculations that are dependent on travel details, e.g. route, distance and user-category, are on-going updated using validated data in the user´s DTID. Upon verification, the smart contract

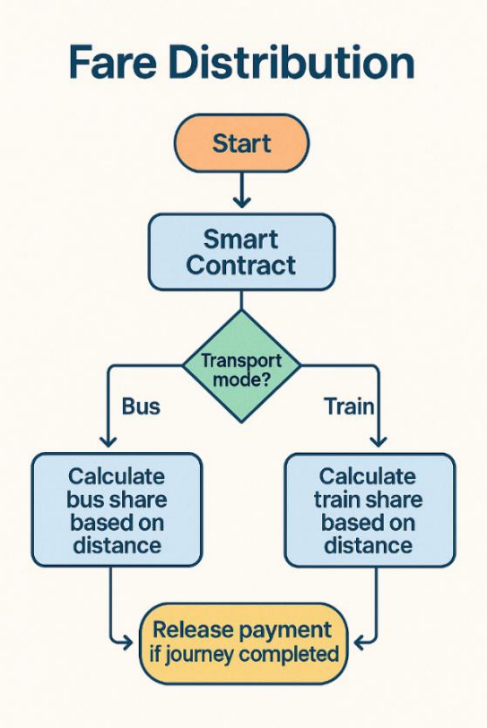


Fig 17: Smart Contract Fare Payment

freezes the fare in a virtual escrow to mimic safe and conditional payment holding. After completing a trip, the contract handles the fare distribution, triggering the automatic

release of the hold back to the transport provider. All operations including ticket issuing, fare locking, payment release are written to the blockchain, enabling the entire history to be audit trail for regulatory and other purposes. Smart contracts, by reducing the cost of 'negotiating and enforcing passenger-provider exchanges,' effectively remove intermediation costs and minimize the potential for fraud, such that a code automatically executes and insulates the transportation provider from human decision in carrying out policy.

3.2.1.8 Middleware

The The middleware acts as a communication and coordination platform for the entire system. It supports interoperability between the blockchain, wallet, smart contract, and validator modules at real-time/ instant speeds. This layer is particularly important in orchestrating authentication flows, running smart contracts, and offline synchronization. When a user takes actions (booking a ticket or scanning a DTID at a checkpoint) the middle layer ensure that the user possesses all the necessary credentials by contacting the blockchain using Zero-Knowledge Proofs of knowledge. It then gets a simple "valid" or "invalid" response and sends back to the service provider through the transport provider completely in privacy (with speed and without any personal data exposure underneath).
The middleware layer is responsible for the real-time validation, as well as the smart contract triggering such as fare calculation, booking confirmations, and releasing the payment (cfr. section 3.2.1.7). These functions are hidden from the user (business logic is automated behind doors). Of importance, the middleware takes care of offline verification cases. The middleware keeps a copy of the blockchain state in cache and permits local validation of DTIDs when transportation checkpoints are disconnected. Upon re-connection to the internet, the middleware synchronizes transaction records with the blockchain ledger ensuring data consistency and continuity across devices.
By separating the user interface from the blockchain and incorporating a fault-tolerant communication, the middleware guarantees that the platform holds both a solid foundation and applicability to a broad spectrum of practical transport contexts.

3.2.1.9 Verification Mechanisms

The identity verification process in the proposed system is based on the Self-Sovereign Identity (SSI) and aims to work securely and privately and efficiently in a decentralized system. This model controls the entire lifecycle of user identity from the time of submission of initial credentials through to transport authentication and does so without mandating a centrally trusted authority to store or verify any data. At signup time, a user submits her personal documents to well-known verifiers like universities, banks, or government offices. These verifiers verify the claims and produce digitally signed Verifiable Credentials (VCs), which are added to the user's digital wallet. Upon validation, the BRTA provides the Digital Transport ID (DTID) as a mobile utility, steady and free-of-charge with regard to the end-user in the transport utility-system. Upon booking a ticket or entering a checkpoint, the user is presented with the DTID via a QR code or NFC. The verifier node then explores the blockchain to see whether the credential is valid by using Zero-Knowledge Proofs (ZKPs) to ensure the transaction is never compromised with any sensitive information. Just a plain permissions signal is sent back. Privacy is retained, and trust is built. This system also incorporates cryptographical digital signatures for every transaction with the user's public key linked to his identity. This makes every proof of identity inalterable, resistant to being denied, and impossible to be forged. In case of an off-line verification, a pre-signed validation token is used, being re-synced with the blockchain when the device comes on line. With verifiable credentials, ZKPs, offline-ready workflows and cryptographic assurance, the identity verification

mechanism delivers secure access, fraud prevention and privacy protection that is a perfect fit for the operational context of public transport in Bangladesh.

3.2.2 System Actors and Stakeholders

The Self-Sovereign Identity (SSI) model, as adopted in the proposed transport identity system, is built upon three fundamental roles: the Issuer, the Holder, and the Verifier. These roles collectively facilitate a decentralized identity framework in which data ownership resides with the individual, trust is distributed among verified authorities, and privacy is maintained throughout the credential lifecycle.

In this blockchain-enabled architecture, these abstract roles are embodied by real-world stakeholders such as passengers, regulators, financial institutions, and transport providers each contributing to a secure and interoperable identity ecosystem (see Figure 18). The subsections below outline the responsibilities of these actors and their alignment with the technical and governance layers detailed in Sections 3.2.1.1 to 3.2.1.9.

1. Passengers (Holders)

Passengers act as Holders in the SSI framework. They initiate the registration process through the decentralized wallet application, submitting credentials such as National ID, student verification, or bank account details. Upon successful verification, users receive a Digital Transport ID (DTID) a cryptographically signed Verifiable Credential (VC) that is securely stored in their digital wallet (refer to Section 3.2.1.2). Passengers use the DTID to authenticate at transport checkpoints via QR codes or NFC tokens, with verification performed through Zero-Knowledge Proofs (ZKPs) to ensure privacy (Section 3.2.1.3). Ticketing, fare calculation, and payment deduction are handled automatically via smart contracts (Section 3.2.1.7), with no manual interaction required by the user.

2. BRTA (Issuer and Regulator)

The Bangladesh Road Transport Authority (BRTA) fulfills the dual role of Issuer and Regulatory Node. As the central credential authority, BRTA issues DTIDs after validating user-submitted credentials, which are processed and confirmed by identity verification nodes (Section 3.2.1.5). As a regulator, BRTA enforces access policies, audits network health, and oversees legal governance (Section 3.2.1.6). Crucially, BRTA never stores or views raw personal data; it interacts solely with hashed or cryptographically signed credentials to preserve user privacy.

3. Educational Institutions (Issuer Nodes)

Universities and accredited academic bodies operate as Issuer Nodes by validating claims related to student status. Upon successful validation, they issue VCs that support transport-related benefits, such as student fare discounts. These VCs are digitally signed and verifiable through public keys embedded in the blockchain (Section 3.2.1.4). Educational issuers interact with BRTA and middleware to enable policy-compliant identity verification (Section 3.2.1.8).

4. Financial Institutions (Issuer Nodes)

Banks and mobile financial service providers (e.g., bKash, Nagad) act as Issuer Nodes responsible for verifying user payment methods. These institutions issue VCs attesting to the user's financial standing or payment credentials. These VCs are subsequently used by smart contracts for secure fare deduction and escrow operations (Section 3.2.1.7). Similar to educational issuers, financial institutions operate in a permissioned role, with data sharing restricted to authorized channels (Section 3.2.1.1).

5. Transport Providers (Verifiers)

Public and private transport operators function as Verifiers. At boarding points, they scan the DTID presented by the passenger via QR or NFC. The provider's node then invokes ZKP-based validation logic, querying the blockchain without retrieving or exposing any personally identifiable information (Section 3.2.1.3). If the ticket is valid, the system authorizes access; if not, entry is denied. Once the journey is completed, the verifier's node triggers the smart contract to release payment from escrow to the appropriate service provider (Section 3.2.1.7).

6. Identity Verification Nodes

Identity verification is distributed among trusted organizational nodes, including government agencies, financial bodies, and educational institutions. These nodes validate user claims and issue VCs as cryptographic attestations. They do not store identity documents themselves but interact with the system through Fabric's channel-based

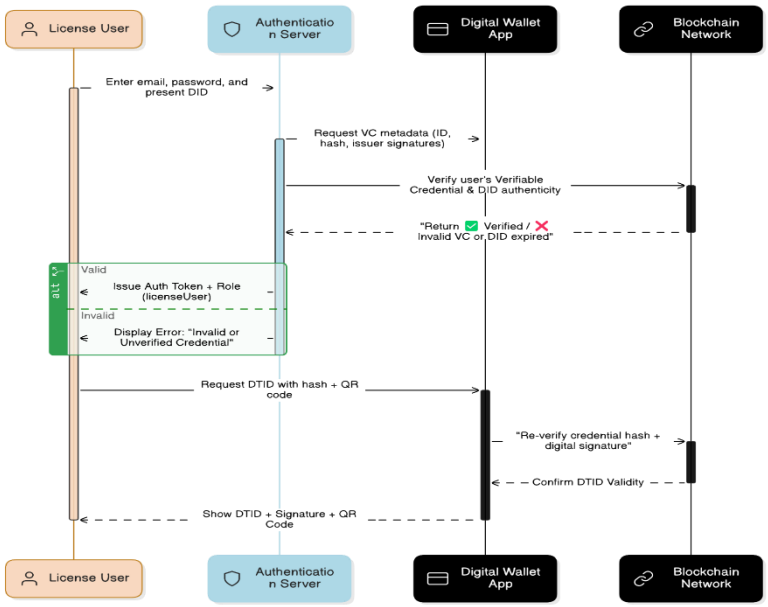


Fig 18: User Authentication Sequence diagram

access model, which enforces strict privacy and policy compliance (Section 3.2.1.4).

This actor-based model upholds the principles of decentralized identity by separating control among multiple trusted authorities. Each entity operates independently but within a cryptographically secured framework, reducing reliance on any single authority. As a result, the system ensures trustless verification, enhanced data privacy, and operational transparency across the national transport infrastructure.

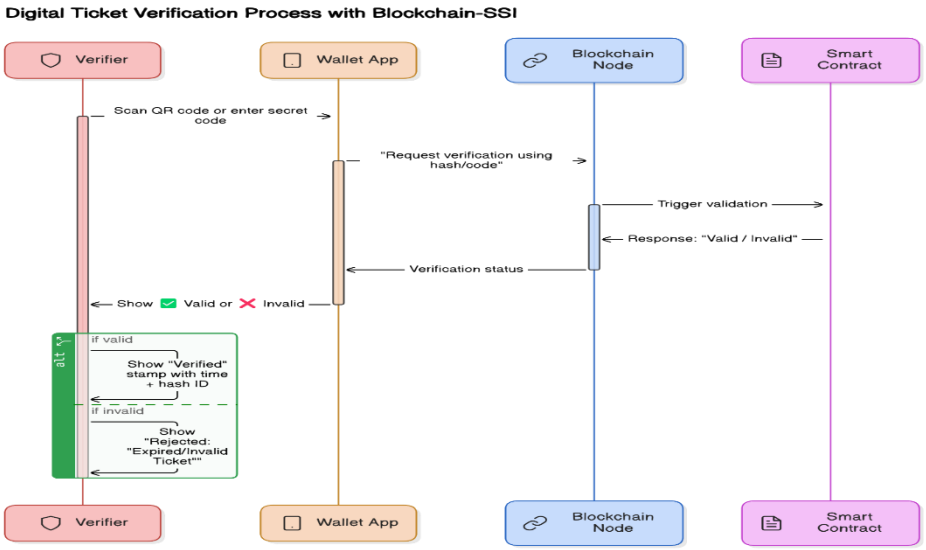


Fig 19: Ticket Verification Sequence diagram

3.2.3 Use Case

This section illustrates the practical operation of the proposed Self-Sovereign Identity (SSI)-based transport system through a series of interconnected use cases. Each use case corresponds to a phase in the identity lifecycle, from registration to post-travel fare distribution. The cryptographic workflows, credential issuance, smart contract interactions, and blockchain verification processes are described using formal notations as outlined in Table 2.

Cryptographic Notations

Table 2: Cryptographic Notation

Notations	Description
U	User(passenger)
P	Transport provider
B	Blockchain Network
SC	Smart Contract
A	Authentication Authority BRTA
$DTID$	Digital Transport ID
E	Education institution (Blockchain Nodes)
BN	Bank nodes
GN	Government node (NID)
K_U^{priv}, K_U^{pub}	Public & private key pair of user U
K_P^{priv}, K_P^{pub}	Public & private key pair of transport provider P
K_A^{priv}, K_A^{pub}	Public & private key pair of authentication authority A
K_E^{priv}, K_E^{pub}	Public & private key pair of educational institution E
K_BN^{priv}, K_BN^{pub}	Public & private key pair of bank BN
K_GN^{priv}, K_GN^{pub}	Public & private key pair of Government NID GN
$\sigma_X(M)$	Digital signature of the message M by entity X
$H(M)$	Cryptographic hash of message M
$E_{nck}(M)$	Encryption of message M using key K
$D_{eck}(C)$	Decryption of ciphertext C using key K

User Registration

User onboarding begins with identity setup through a decentralized wallet. This process ensures that each passenger has a verifiable and privacy-preserving identity stored securely.

M1: The user (U) interacts with their digital wallet (WU) to generate a key pair (KUpriv, KUpub) and identifier (IDU).
M2: The wallet returns (IDU , KUpub) to the user.
M3: The user submits (IDU , KUpub, identity credentials) to the Authentication Authority (A).
M4: (A) requests verification from (E, BN, GN), collecting their digital signatures.
M5: If verified, a Digital Transport ID (DTID) is issued and stored on the blockchain.

Transport Provider Registration

To ensure regulatory compliance, transport operators must register through BRTA and receive credentials before being allowed to participate in the system.

M1: The transport provider (P) generates key pair (KPpriv, KPpub) and identifier (IDP) using wallet(W).
M2: The provider submits (IDP, KPpub , business credentials) to (A).
M3: (A) verifies transport licenses with regulators and assigns a Transport Provider ID (TPID).
M4: The TPID is stored on the blockchain and linked to smart contracts for ticket processing.

DTID issuance

The DTID represents a unified transport identity for the user, secured cryptographically and stored immutably.

M1: (A) collects verification from (E, BN, GN) and confirms credentials.
M2: A DTID is generated, cryptographically signed by (A), and stored on the blockchain.
M3: The user receives the DTID and links it to their wallet.
M4: The DTID is used for transport authentication.

Ticket Booking

Ticket purchase is initiated through the user's wallet and processed autonomously using smart contracts to ensure integrity and automation.

M1: The user (U) submits a booking request (DTIDU, Route, Fare) to (SC).
M2: (SC) verifies (DTIDU) and locks the fare in escrow.
M3: The transport provider (P) receives a booking confirmation.
M4: A QR code/NFC-based digital ticket is generated and stored in the user's wallet.

Verification & Payment Process

The user's journey is cryptographically validated, and fare is distributed post-travel, eliminating third-party intermediaries.

M1: The user () scans their QR code/NFC tag at the entry point.
M2: The transport provider () verifies the DTID using blockchain records.
M3: The journey begins, with the fare remaining locked in escrow.
M4: At the destination, the user scans their ticket again for exit verification.
M5: The smart contract () processes the transaction and automatically distributes

payments to transport providers.

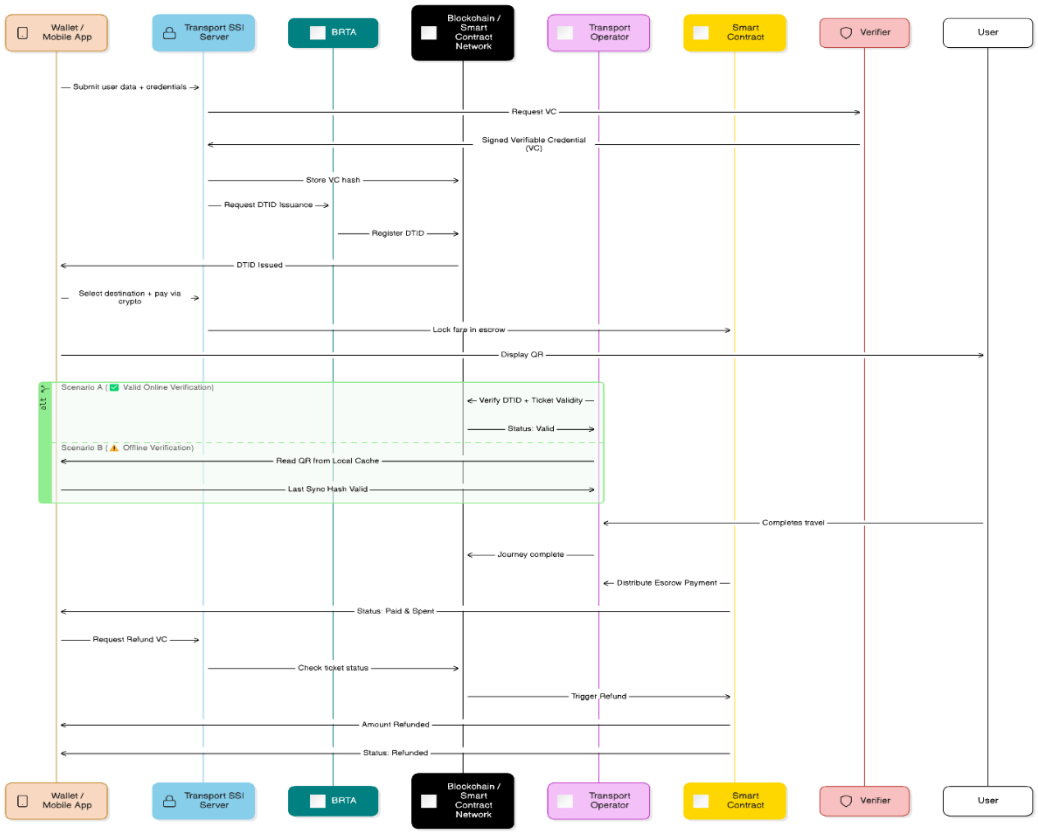


Fig 20: Full System Sequence Diagram

Offline Support and Resilience

In scenarios where internet connectivity is limited, the system allows local verification using pre-signed cryptographic tokens. These tokens are validated at entry and stored locally. Upon reconnection, the wallet syncs offline logs to the blockchain, ensuring integrity and preserving the audit trail (cf. 3.2.1.2, 3.2.1.8).

3.2.4 Algorithms

This section outlines the core algorithms used in the proposed Self-Sovereign Identity (SSI)-enabled transport system. While the implementation was simulated using React and Firebase, the algorithmic design reflects how the full system would function in a blockchain-integrated environment. Each algorithm supports a major process within the system: user registration, ticket booking, and ticket verification. These algorithms are designed to be modular, scalable, and privacy-preserving, aligning with the architectural principles described earlier.

Algorithm 1: User Registration

Input:
userType: User role ("passenger")
userWallet: Unique wallet address
credentials[]: Verifiable documents

Output:
Issued Digital Transport ID (DTID)

Steps:
Validate userType; if invalid, terminate.
Verify credentials through authorized entities.
If verification fails, return an error.
Generate a digital signature from credentials and userWallet.
Check if the wallet is already registered.
If not, create a DTID linked to the wallet and signature.
Store the DTID and user info on the blockchain.
Log the registration event.
Return confirmation and DTID.

Algorithm 2: Ticket Booking

Input:
userWallet, fromLocation, toLocation, transportMode, fareAmount

Output:
Unique ticket ID

Steps:
Validate the user's DTID.
Check if user is allowed to book.
Check transport availability for selected route.
Calculate and lock fare.
Assign route to a new ticket.
Generate a QR code for the ticket.
Store ticket info in system.
Return ticket ID.

Algorithm 3: Ticket Verification

Input:
ticketId, userWallet, isEntry (True = Boarding, False = Exiting)

Output:
Verification status and action log

Steps:
Confirm ticket belongs to the user.
Verify ticket integrity and expiry.
If isEntry:
Confirm not previously scanned.
Log entry and update ticket to "InTransit".
If isExit:
Confirm not already exited.
Log exit, mark as "Completed", and release payment.
Return success message.

3.3 Project Plan

This section outlines the timeline and phased activities that guided the system's design and development. This section outlines the timeline and phased activities that guided the system's design and development.

This section outlines the timeline and phased activities that guided the system's design and development.

Table 3: Project Plan

Phase	Description
Problem Identification (Month 1)	Identify the core problem of public transport in Bangladesh. Also review existing transport system. Identified need to update system. Need Decentralization, Privacy & Security.
Literature Review (Months 1-2)	In depth review on SSI frameworks, Blockchain in transport system, smart contract based automation.
System Architecture Planning (Months 3-4)	Design a Blockchain SSI enabled transport system, define stakeholders, develop some diagram.
Prototype Planning (Months 5-6)	Create a frontend prototype for visualization without backend.
Writing (Month 7)	Compiled and documented the entire conceptual framework. Create diagram, system maps for support explanation.
Refinement & Finalization (Month 7+)	Revise and refine based on supervisor feedback and academic standards.

3.4 Task Allocation

The following table outlines the division of work and responsibilities across the research timeline. Each task aligns with specific project objectives and deliverables.

Table 4: Task Allocation

Task	Describe
Problem Identification	Defined the main challenges in Bangladesh public transport.
Objective Set	Outlined research objective based on blockchain, SSI.
Literature Review	Reviewed some related research paper, case studies related to SSI, blockchain and digital transport system.
System Requirement Analysis	Identified some functional and non functional requirement for the proposed system.
Architecture design	Designed high-level architecture including data flow, blockchain interaction.
Diagram Development	Created some visual diagrams.
Report Writing	Documented all the phases of each and every task.

Refinement	Reviewed and refine the written for clarity and academic standard.

3.5 Summary

This chapter presented the detailed design and methodology of a blockchain-based Self-Sovereign Identity (SSI) system tailored for the public transport ecosystem in Bangladesh. It focused on the integration of Hyperledger Fabric, decentralized digital wallets, cryptographic credentials, and smart contracts to create a secure and privacy-preserving transport infrastructure. Each architectural component such as credential issuance, ZKPs, middleware, and identity verification was aligned with SSI principles to enable user-controlled, trustless authentication and ticketing. The overall methodology reflects a decentralized, scalable, and regulatory-compliant approach to digital identity in public transportation.

Chapter 4

Implementation and Results

4.1 Environment Setup

This chapter details the technical environment and development process for the blockchain-enabled SSI TPS prototype. It describes the system architecture, tools used, and how the final working prototype was built and tested. Although full blockchain integration was beyond the scope of the current implementation phase, a complete simulation environment has been successfully developed to validate all user workflows and role-based functionalities.

4.1.1 Technology Stack

The system was developed as a web-based application using modern frontend and backend technologies. The frontend interface was built with React.js, a component-based JavaScript library ideal for managing complex user flows. Tailwind CSS was used to ensure a modern, responsive, and accessible user interface. For the backend, Firebase

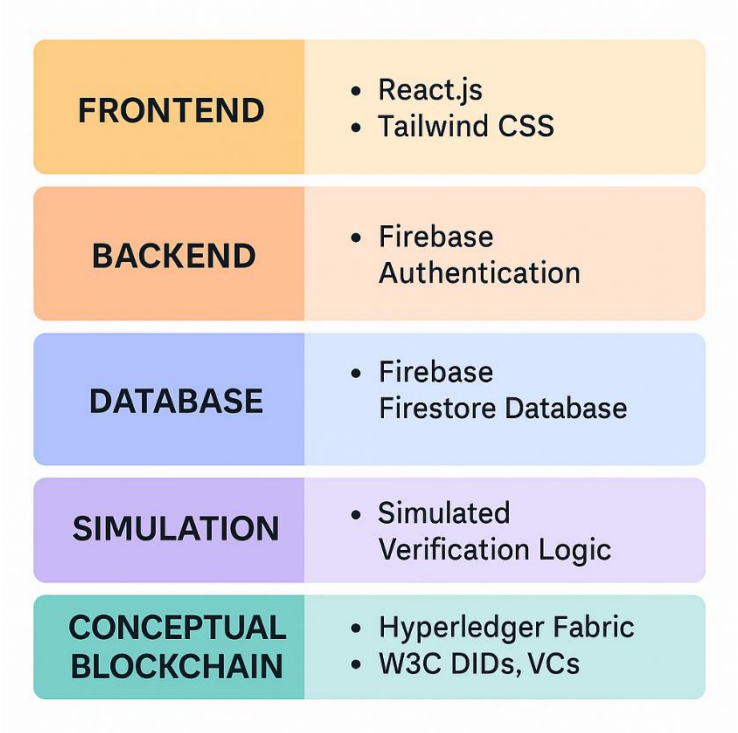


Fig 21: Tech Stack

was chosen to handle authentication, real-time database storage, and hosting, which allowed for rapid development and smooth role-based access control. Although actual blockchain integration (e.g., Hyperledger Fabric) was not implemented in this version, the system design and architecture fully anticipate its future inclusion. The concept assumes integration with a permissioned blockchain network where BRTA and other verification institutions act as nodes, and smart contracts manage fare locking and distribution. The standards proposed for identity management include W3C Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), which are widely recognized within SSI frameworks.

4.1.2 Prototype Development

A fully functional prototype was developed to simulate the user experience and operational flow of the system. The web application includes three dashboards:

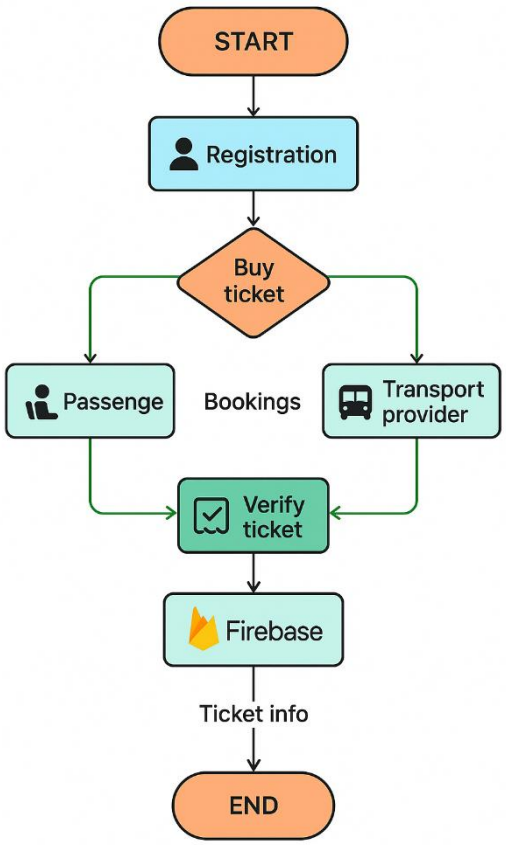


Fig 22: Prototype flow

User Dashboard: Allows users to register under one of three categories - student, senior citizen, or regular. The registration process collects identity data and enables users to upload supporting documents but the document directly not uploaded to BRTA, only an encrypted hash can see BRTA. Based on user role, the system automatically applies fare discounts after verification. Once verified, users receive a Digital Transport ID (DTID) represented by a QR code and a physical code, which is used for booking and boarding. However, NFC card integration was not implemented in this phase.

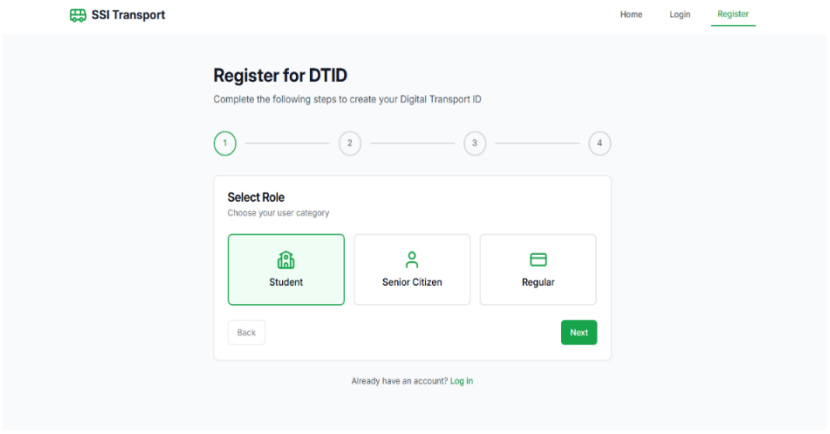


Fig 23: User Registration process (Role selection)

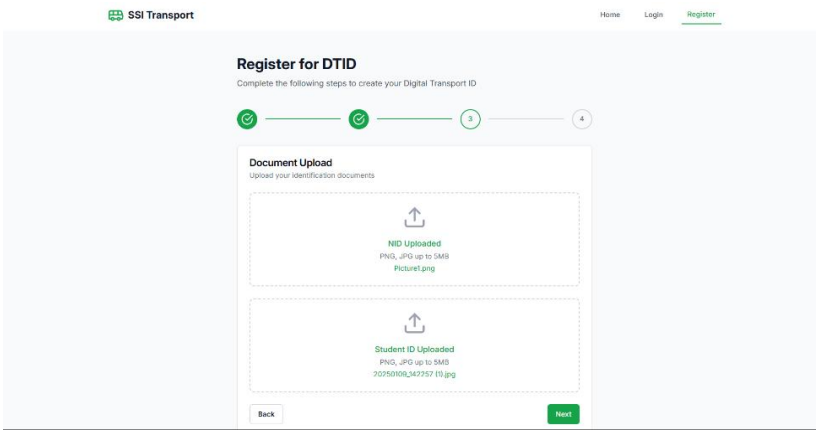


Fig 26: User Registration process (Doc Upload)

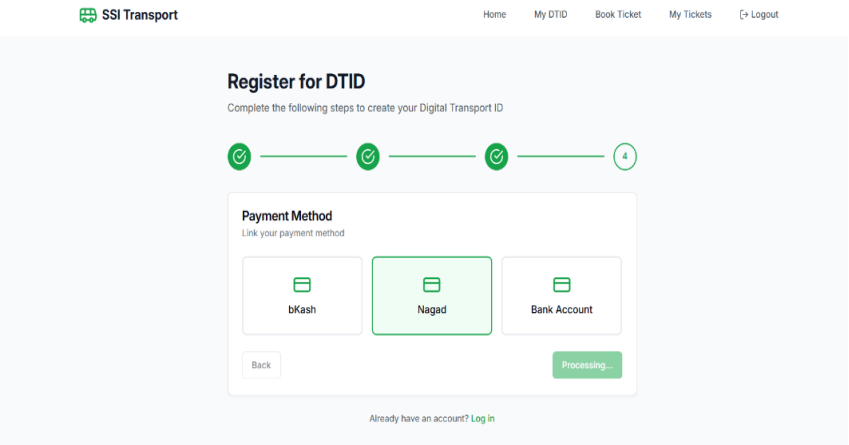


Fig 25: User Registration process (Payment Method)

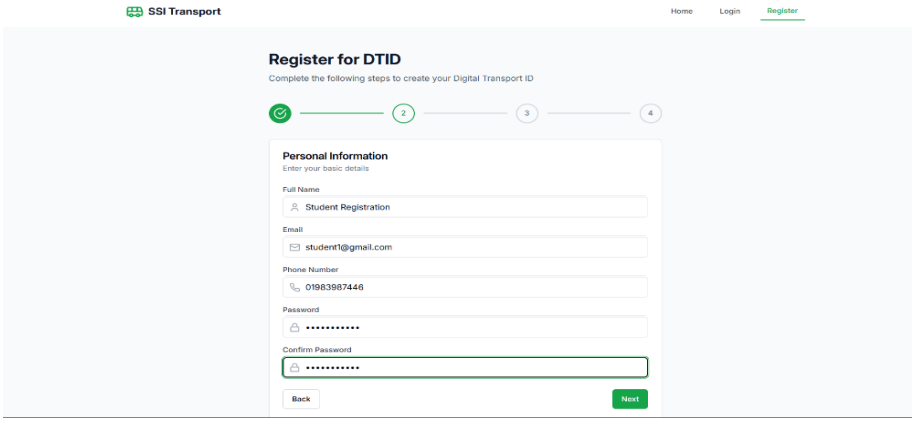


Fig 24: User Registration process (Form Fill-Up)

Figures 26–29 showcase UI screenshots illustrating the DTID registration process. After registration user only see verification status. After registration, BRTA or the designated admin can view the registered user list filtered by role. After that admin request verification to the nodes (Educational institution, Banks, Govt). After verification admin generate DTID for the verified user. And user can see their DTID and book ticket and get their discount according to the role. All UI screenshot are attached on Chapter 3 and Subsection 3.1.6.

4.2 Comparative Analysis

Traditional identity management systems assume that public transport operates off of the centralized databases of public authorities or transport operators. Such systems make it necessary for passengers to register separately for different transport services, resulting in fragmented identity records, redundant verification processes, and security vulnerabilities. Because these systems are centralized, they are susceptible to data breaches, identity theft, and unauthorized access since a single point of failure can lead to the compromise of the entire user database. Moreover, passengers must carry physical tickets, smart cards, or identity documents, which can easily get lost and can be vulnerable to fraud, and the ticketing system can be operationally inefficient. Unlike the conventional databases based models, the blockchain-based Self-Sovereign Identity(SSI) framework does not depend upon the centralized database to provide role-based access, rather, it uses decentralized identity verification through VCs, ZKPs and smart contracts. Passengers have ownership and control of their identity credentials, which are securely stored in their digital wallet, ensuring that personal data is kept private and tamper-proof. The proposed system allows transport providers to authenticate users without revealing any underlying personal information directly to them, which is not possible in traditional systems where direct access to sensitive, personally identifiable information (PII) is required for identity verification, thus ensuring privacy-by-design authentication. Additionally, central identity systems depend on manual fare processing and ticket validation, which are susceptible to human error, lag, and fraud. By means of smart contracts, it achieves the automatic ticket issuance, the fare deduction and payment. It improves efficiency, reduces costs, and organizes transportation access to passengers by eliminating the requirement for physical cards or paper documents of identity. Furthermore, existing legacy systems need to address compatibility challenges when each transporter has its own database and validation system. This makes it difficult to travel on a bus, then a train, then a metro and then a ferry, and mandates that commuters have to register multiple times. In this, the blockchain-based approach can enable a common interoperable identity framework where passengers will be free to use their DTID for any transport service. This makes for an improved user interface and adds even more convenience while achieving sounder fraud prevention and operational efficiency. It is based on decentralized identity principles and blockchain technology, which emphasizes the need to move closer to decentralized identification systems for public transportation.

Table 5: Comperative Analysis

Feature	Blockchain-Enabled Self-Sovereign Identity for Seamless Public Transportation in Bangladesh	Leveraging self-sovereign identity & distributed ledger technology in renewable energy certificate ecosystems	Blockchain-Based Transaction Verification Infrastructure in Public Transportation	RideChain: A Blockchain-Based Decentralized Public Transportation Smart Wallet	Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation
DID's	☑	☑	☑	☑	☑
VCs	☑	☑	☑	☑	☑
ZKPs	☑	✗	☑	✗	☑
Offline Functionality	☑	✗	✗	✗	✗
SSI	☑	☑	☑	☑	☑
Dynamic Pricing	☑	✗	✗	✗	✗
Interoperability	☑	☑	☑	☑	✗
Cost-Effective	☑	✗	☑	☑	☑

4.3 Results and Discussion

This section describes the results from a prototype of a simulation of the proposed blockchain-based SSI transport system. The whole simulation was developed using React

for the front-end and Firebase for the authentication, data management and real-time interactions. While a full blockchain backend (e.g., Hyperledger Fabric) was not deployed due to time and resource constraints, all critical workflows were replicated to accurately demonstrate system functionality and user experience. Although Firebase lacks the decentralized features of blockchain, it was used to simulate key processes such as credential verification, fare locking, and role-based access in a centralized environment. This approach allowed the team to test user workflows and validate system logic, while maintaining future readiness for integration with Hyperledger Fabric.
While actual cryptographic ZKPs were not used, the system design reflects ZKP principles by enabling verification without exposing the underlying credential data. For example, credential validity was confirmed using encrypted hashes instead of raw documents, simulating the privacy-preserving approach of ZKPs.

Prototype Highlights

The React-Firebase-based prototype successfully demonstrated the key operational aspects of the proposed model, including:

- User Registration and Credential Submission: Users were able to register through a clean, intuitive React interface. Upon registration, users could upload essential credentials such as NID, student certificates, and banking information. The simulation ensured privacy by storing cryptographic representations (simulated hash equivalents) of the credentials in Firebase, instead of raw data.
- Role-Based Credential Verification: Simulated institutional nodes (educational institutions, financial entities, and government authorities) accessed Firebase to verify user-submitted credentials. This mimicked a decentralized identity verification process, where each authority independently attested to the user's claim (e.g., student status or bank linkage).
- Digital Transport ID (DTID) Issuance: Upon successful verification, BRTA generated a Digital Transport ID (DTID) for each user. The DTID was stored in the user's profile and functioned as the user's verifiable identity for future ticketing and travel interactions.
- Ticket Booking and Escrow Simulation: Users could seamlessly book tickets through the UI by selecting transport mode, route, and preferred travel time. Upon booking, the fare was simulated to be "locked in escrow" and a QR code or NFC-based ticket was generated, reflecting what would happen with a real blockchain-based smart contract.
- Offline Verification Logic: A significant feature implemented was offline ticket validation. The system allowed transport providers to verify tickets using previously synced data, stored locally through Firebase caching, simulating verification in low-connectivity areas. This function is essential for remote regions in Bangladesh where real-time internet access is limited.
- Privacy and Security Emulation: Although Zero-Knowledge Proofs (ZKPs) were not implemented cryptographically, the system was designed to reflect ZKP principles ensuring that verifiers could confirm credential authenticity without accessing the actual sensitive data. This was achieved through logical abstraction and simulation workflows.
- Multimodal Transport Interoperability: The prototype supported a unified user experience across different transport types (bus, train, ferry). Users used a single DTID to interact with various services, thus validating the system's interoperability goal.

The React-Firebase simulation validated the practicality and usability of the proposed

SSI-based decentralized identity model in the context of public transport. The results clearly demonstrated how such a system can:

- Reduce repetitive identity checks and eliminate the need for paper-based documentation.
- Ensure user privacy by eliminating centralized personal data storage.
- Offer an interoperable experience across multiple transport services.
- Simulate smart contract-based fare locking and payment distribution, improving transparency and reducing human error.
- Enable offline ticket validation, addressing real-world constraints such as limited internet coverage in rural Bangladesh.

While this simulation used Firebase as the backend, it was intentionally designed with modularity so it can be upgraded in the future to integrate real blockchain platforms like Hyperledger Fabric. The design choices made during development such as role-based access control, simulated credential signing, and identity lifecycle flow reflect the core logic of a decentralized and privacy-focused ecosystem.
Overall, the prototype confirms that even in a simulated environment, an SSI-powered identity and ticketing system has the potential to significantly improve security, user control, and operational efficiency in Bangladesh's fragmented public transport infrastructure.

4.4 Summary

This chapter presented the simulation environment and prototype validation for the proposed blockchain-based Self-Sovereign Identity (SSI) system in public transportation. The operation was a success, proving that the core identity/verification/ticketing flows (including offline support) worked as intended. Comparative analysis validated the superiority of the proposed distributed model compared to conventional systems in security, privacy/efficiency and scalability. These results confirm the feasibility of real-world application and present a solid basis for further development stages.

Chapter 5

Engineering Standards and Design Challenges

This chapter describes the design choices, engineering principles and technical standards of the Blockchain-Enabled Self-Sovereign Identity (SSI) Transport System. It also explores the implications of the system at societal, sustainable, ethical level. The latter part of this chapter provides a mapping of the project with complex engineering problem-solving and engineering activities based on national accreditation guidelines.

5.1 Compliance with the Standards

The system follows a set of software, hardware and communication standards essential for interoperability, privacy and security.

5.1.1 Software Standards

- W3C DID - Enables decentralize identity management without any third parties.
- W3C VC - Used to issue digitally signed student ID, NID, and bank credentials;
- Hyperledger Fabric - It Enables permissioned smart contracts for fare handling and credential validation.

5.1.2 Hardware Standards

NFC smart cards are used for offline entry and exit verification, the system will use ISO/IEC 14443 (NFC Cards), while a barcode-only system is an alternative. NFC technology is favoured for its quick and secure performance, as well as its lack of necessity for internet connectivity, a must-have in places like Bangladesh. Barcodes, on the other hand, are not as secure as QR codes, thus making them less secure and reliable for offline use compared to QR codes. QR Codes, following ISO/IEC 18004, have been designated as the universal digital ticket format due to their broad device compatibility and low-cost implementation, improving accessibility and ease of integration across platforms.

5.1.3 Communication Standards

For the proposed system, HTTPS is adopted for the communication protocol, in order to achieve a secure exchange of data between the wallet and the backend server. Furthermore, RESTful APIs in JSON format have been developed to allow smooth exchange in a decentralized identity and ticketing system.

5.2 Impact on Society, Environment and Sustainability

This paper introduces the Blockchain-Enabled Self-Sovereign Identity (SSI) Transport System, not only as a technological breakthrough but also as a socially responsible and morally motivated model based on humanitarian principles. The chapter concludes the paper with a discussion about the larger picture of the system, how it affects people, what it adds to the environmental issues, the ethical questions, and what the strategy it should be for the system to be long-lasting in the Bangladesh public transport situation.

5.2.1 Impact on Life

DTID is an intelligent architecture that reduces the complexity of travel for citizens by

ensuring seamless access to whatever mode of transport (automated fare collection in bus/train/metro/ferry) they choose via a single secure ID system. The enhancement of providing privacy-preserving identity also allows for the protection of personal data and reduction of their misuse or unauthorized access. One of the primary advantages of the system is that it ensures fair fares for passengers - students and pensioners with concessionary travel passes are already being automatically checked without having to disclose personal information in the process.

5.2.2 Impact on Society & Environment

The system creates an accessible, equitable and user friendly transit system for the society. By offering a singular digital interface to a range of travel options, it democratizes access between urban and rural populations. From an environmental point of view, it promotes the use of public transport through improving the travel experience and merging multiple transport networks into a single system. This transition could decrease reliance on privately owned vehicles, leading to less emissions and traffic in cities. In addition stadium access is on digital device thereby minimizing paper ticketing and the waste. By reducing corruption space and increasing transaction transparency in smart contracts the system would also support the (re-)establishment of trust between citizens and the government in transport governance and digital public services.

5.2.3 Ethical Aspects

From the ethical point of view, the system was largely built following the principles of user's autonomy and data sovereignty. Use of SSI principles allows users to maintain the ownership of their Identity and share only the information required to verify their Identity. This technique effectively mitigates identity theft and lowers centralized risks through the decentralization of data ownership. Moreover, the system is fair as it offers access equally to everybody no matter if rich or poor. All user, regardless of Incomes, get EQUAL Privacy and Usability. With such architecture the tracking or surveillance is prevented and respecting ethical standards of the digital infrastructure.

5.2.4 Sustainability Plan

The system is designed to be sustainable. By using open and interoperable standards like W3C DID and Verifiable Credentials, the platform is set up to work with any new technology and to be easily maintained. The blockchain does not involve the use of flashy or otherwise impractical uses of energy, as well as being able to scale as more efficient solutions for consensus emerge. The adoptability of the system is also dependent from the model of implementation. It can unlock strategic private sector investment, thereby also reducing up front public sector investment and increasing adoption, by promoting public-private partnerships, such as with existing mobile financial service providers. This model ensures the financial and operational sustainability in the long run, and at the same time doesn't ignore the public interest.

5.3 Project Management and Financial Analysis

This section details an approximate budget plan for the production of the prototype, bare and alternate. It also justifies every expenditure.

Table 6: Financial Analysis

Item	Estimated Budget	Alternative Budget	Rationale
Paper & Printing	2000	1500	Paper, printing & Binding.
Research Material	1000	00	Free Journal, open source.
Design & Diagram	2000	1000	Canva, Edrawmax

Frontend Design	5000	3000	Basic UI UX with animation

5.4 Complex Engineering Problem

This is a practical complex problem of real life, with a variety of stakeholders, of regulatory and security nature. The problem is then linked to the complex engineering PSIs and KDs below.

5.4.1 Complex Problem Solving

The EP indicators (EP1–EP7) of complex problems are framed beneath for the context of Bangladesh public transportation.

Mapping with Knowledge Profile for EP1

Table 7: Knowledge Profile

EP1 Dept of Knowledge	EP2 Range Of Conflicting Requirements	EP3 Depth of Analysis	EP4 Familiarity of Issues	EP5 Extent of Applicable Codes	EP6 Extent Of Stake-holder Involvement	EP7 Interdependence
✔	✘	✔	✔	✘	✘	✔

EP1 (Depth of Knowledge): The project exhibits an outstanding depth of engineering knowledge, especially within the identity systems, decentralized technology, cryptography, and smart contract development space. The combination of the pair: SSI and blockchain represents maturity in systems of systems and privacy by design engineering.

EP2 (Range of Conflicting Requirement): User privacy, regulatory compliance, and interoperability are all relevant areas that are conceptually touched upon by the project; however space for conflicting requirements was not addressed through real-world stakeholder negotiation or design trade-off analysis. No to a sufficient engineering depth to solve these conflict in practice; and could be attributed to the current prototype phase. Thus, this requirement is only partially fulfilled.

EP3 (Depth of Analysis): The project demonstrates strong technical breakdowns of blockchain identity flows, smart contracts, and privacy mechanisms like ZKPs. Each part—from DTID issuance to fare settlement—was analyzed to ensure secure, efficient, and scalable integration.

EP4 (Familiarity of Issues): The idea of using decentralized identity and blockchain for transportation new, especially when seen on the socio-technical aspect based on Bangladesh. Therefore, the project deals with a low familiar area that needs the translation of world-wide systems standards to local infra-structure and policy conditions.

EP5 (Extent of Applicable Codes): The system uses universal standards, W3C DID/VC,

and NFC and QR protocols. However, these sources serve merely as guidance and are not actually adopted or tried in a court room, in a manufacturing production retrieval system. No actual integration into government/traffic regulation is present (such as Bangladesh's own Digital Security Act enforcement), so the applicable code is technically actually minimal.

EP6 (Extent of Stakeholder Involvement): Design involves multiple stakeholders, It was involved BRTA, Financial Institutes and transport operator directly in engagement, feedback and collaboration in development. All of the stakeholder needs were assumed and not taken from real conversations, so stakeholder engagement is limited. As such, this falls short of real-world stakeholder engagement.

EP7 (Interdependence): In the project, the level of the dependence between its subsystems (i e., the identity check, the interaction of the user and the smart contract, payment receipt, and the system of the operator of the transport). Failure or delay in any of the components can have an effect on the entire service flow, and a strong coordination and fail-safety is required among them.

Table 8: Knowledge Profile 2

K3 Engineering Fundamentals	K4 Specialist Knowledge	K5 Engineering Design	K6 Engineering Practice	K8 Research Literature
✔	✔	✔	✔	✔

K3 - Engineering Fundamentals: The System fundamentals are based on core engineering principles such as secure communication, modular system design, public key cryptography, and distributed ledger architecture. Fundamental concepts of data structures, networking, and cyber security were used extensively.

K4 - Specialist Knowledge: This contribution shows expertise in the field of distributed digital identity, automated processes with blockchain and in transportation ticketing systems. The depth in this area is presented in the utilization of W3C SSI protocols and permissioned blockchain platforms such as Hyperledger Fabric.

K5 - Engineering Design: The structure of the system called for novel problem solving and abstraction. Issues were framed in terms of the balance between user needs, privacy wishes, and institutional requirements, resulting in a world-wide, cryptographically-secure ticket advisory system.

K6 - Engineering Practice: Practical engineering was performed by producing frontend prototypes, interactive wireframes, identity flows and system integration logic. All of our design choices were based upon well-established international software development and UI/UX practices.

K8 - Research Literature: This project is strongly grounded in secondary research. Established frameworks, standards documentation (W3C, ISO), and global case studies in SSI and smart mobility were reviewed and synthesized to design a contextually appropriate system

5.1.1 Engineering Activities

This section presents a mapping between the project and the range of recognized engineering activities, in accordance with national and international accreditation criteria. These activities are assessed across multiple dimensions, including complexity, innovation, and societal impact. The following mapping demonstrates how this project meets the attributes of professional engineering work.

Table 9: Engineering Activities

EA1 Range of resources	EA2 Level of Interaction	EA3 Innovation	EA4 Consequences for society and environment	EA5 Familiarity
✔	✔	✔	✔	✔

EA1: The project integrates software frameworks (React, Tailwind, Hyperledger), blockchain toolkits, digital identity libraries, and design software. The need to work across these platforms demonstrates a broad and effective use of engineering resources.

EA2: The work involves multidisciplinary collaboration between engineering domains (software, transport systems, cryptography) and institutional entities. Interaction spans both human and machine systems, emphasizing communication between users, verification bodies, and backend infrastructure.

EA3: The application of Self-Sovereign Identity in public transport is a novel innovation within the context of Bangladesh. The introduction of the Digital Transport ID (DTID) and automated, contract-based fare distribution are both creative and unprecedented in this sector.

EA4: The project considers its societal impact thoroughly, with built-in support for digital equity, environmental sustainability, and ethical data practices. By encouraging public transport use and eliminating paper-based ticketing, the design aligns with sustainability goals.

EA5: Due to the unique challenges associated with blockchain adoption in a regulated public infrastructure, this work operates in a domain with low existing familiarity. As such, it contributes to emerging knowledge and set a precedent for future deployments.

5.2 Summary

This chapter has discussed the engineering standards, design considerations, and issues faced in the development of the purposed SSI-based transport system. It described adherence to the applicable software, hardware, and communication standards, analyzed societal and ethical considerations, included a sustainability plan. A financial and administrative summary was also prepared, demonstrating the project's economic feasibility. Lastly, the work was related to complex engineering problem-solving as well as activities, which indicated that the system covered the range and depth required for current engineering solutions.

Chapter 6

Conclusion

This chapter wraps up the project work. It provides an overall summary of major findings, analyses the current limitations, and recommends for potential future improvements to the proposed blockchain-based decentralized identity scheme.

6.1 Summary

The proposed system present a Blockchain enabled Self Sovereign Identity (SSI) framework for seamless public transportation in Bangladesh. This system ensure secure, decentralized and privacy preserving identity management. The proposed system integrate Verifiable Credential, Zero Knowledge Proofs, Digital signatures and Smart Contracts for trustless secure authentication, automatic fare payment process and immutable transaction records. Using Hyperledger Fabric, the system guaranteed secure identity verification process, ticket buying, fare payment. This system eleminate intermediaries and third parties and centralized management. This architecture improve data security, fraud prevention and enhance operational efficiency in fragmented transport system. This architecture connect all the fragmented transport system in an one system. Using one DTID pubic can use any transport. After every journey fare automatically deduct from wallet and fare distributed to the transport provider.

6.2 Limitation

Despite the promise of a decentralized, privacy-preserving transport identity system, this research remains a conceptual and simulated effort. Several limitations, both theoretical and technical, must be acknowledged.

Concept-Based Limitations

- **Smartphone and Digital Literacy Requirements:** The proposed system assumes that every user will possess a smartphone and have sufficient technical literacy to operate a decentralized wallet, book digital tickets, and interact with digital credentials. In Bangladesh, a significant portion of the population—especially in rural or low-income areas—either lacks access to smartphones or the digital knowledge needed to use such systems effectively.
- **Dependence on Stakeholder Participation:** The success of the system depends heavily on the active involvement of BRTA, transport providers, financial institutions, and identity verification bodies. No formal collaboration has occurred in this phase, and the willingness or readiness of these parties remains unverified.
- **Legal and Policy Barriers:** Although the architecture references GDPR, W3C DID standards, and digital laws, the system has not been tested or reviewed under the actual legal and regulatory framework of Bangladesh. Full compliance with local data protection laws and transport regulations is yet to be evaluated.
- **National Infrastructure Constraints:** Nationwide deployment would require significant upgrades to existing transport and IT infrastructure, especially in rural or under-resourced areas. Issues like inconsistent network availability, limited electricity, and lack of digital payment systems in some regions could obstruct system adoption.

Simulation and Prototype Limitations

- **No Real Blockchain Deployment:** The current implementation uses Firebase and React to simulate blockchain functionalities. It does not incorporate a real permissioned blockchain (e.g., Hyperledger Fabric), and therefore lacks decentralization, consensus mechanisms, and immutable ledger storage.
- **Absence of Cryptographic Proofs:** Core components such as digital signatures, verifiable credentials (VCs), and Zero-Knowledge Proofs (ZKPs) are not implemented in the prototype. As a result, security, privacy, and trust assumptions have not been demonstrated technically.
- **Simulated Offline Verification:** Offline ticket verification via QR codes or NFC is conceptually outlined, but actual implementation of device-level validation and blockchain state caching is not present. Hardware integration and local syncing logic remain untested.
- **No Financial Gateway Integration:** Fare transactions, ticket payments, and revenue disbursements are emulated within Firebase and are not connected to actual financial services like bKash, Nagad, or bank APIs. Real-time payment automation and escrow handling are conceptual only.

These limitations highlight the current gap between theoretical feasibility and real-world applicability. To progress toward deployment, future work must focus on blockchain integration, stakeholder onboarding, user training strategies, legal validation, and rigorous field testing in both urban and rural contexts.

6.3 Future Work

To elevate this system from a simulation to a production-ready solution, the following future directions are proposed:

- **Blockchain Integration (Hyperledger Fabric):** Implement actual chain-code smart contracts for DTID issuance, credential verification, and automated fare processing on a permissioned blockchain.
- **Cryptographic Features:** Incorporate Verifiable Credentials (VCs), Decentralized Identifiers (DIDs), and Zero-Knowledge Proofs (ZKPs) using libraries like Hyperledger Aries or zk-SNARKs.
- **NFC & Offline Hardware Testing**: Test and implement NFC-based offline DTID verification using mobile hardware and local secure storage with automatic sync logic.
- **Integration with BRTA & Transport APIs:** Partner with BRTA and local transport operators to deploy the system in a pilot area (e.g., Dhaka metro or intercity bus terminals) for field testing.
- **Payment Gateway Integration:** Add real-time payment handling through mobile financial services (e.g., bKash/Nagad) and escrow contracts for automatic fare distribution.
- **Security & Penetration Testing:** Conduct full-scale security audits to verify data protection, fraud resistance, and operational resiliency in high-load scenarios.
- **AI Integration for Predictive Analytics:** Use AI/ML models to analyze user travel patterns, detect anomalies, predict peak demand, and optimize route planning or dynamic pricing in real time.
- **Loyalty and Reward System:** Introduce a blockchain-based loyalty program where frequent travelers earn digital points or tokens that can be redeemed for discounts,

rewards, or services across transport providers.

- **Global Interoperability and Collaboration:** Design the system to support international interoperability (e.g., using W3C standards) and collaborate with similar SSI-based transport identity systems in other countries, enabling cross-border travel identity support.

References

[1] G. K. A. M. R. R. M. M. A. Lukas Stockburger, "Blockchain-enabled Decentralized Identity Management: The Case of Self-Sovereign Identity in Public Transportation," *Blockchain: Research and Applications,* vol. 2, p. 100014, 2021.

[2] N. T. Alexandru-Cristian Careja, "Digital Identity Using Blockchain," *Procedia Computer Science,* vol. 221, no. 2023, pp. 1074-1082, 2023.

[3] A. T. a. C. C. S. Martín, " A Study of Blockchain Adoption in the Rail Sector," *Transportation Research Procedia,* vol. 72, pp. 1396-1403, 2023.

[4] U. C. U. H. W. P. Md Sadek ferdous, "Leveraging self-sovereign identity & distributed ledger technology in renewable energy certificate ecosystems," *Journal of Cleaner Production,* vol. 422, p. 138355, 2023.

[5] A. I. W. P. Md Sadek Ferdous, "SSI4Web: A Self-sovereign Identity (SSI) Framework for the Web," *5th International Congress on Blockchain and Applications (LNCS, Springer),* 2022.

[6] C.-R. S. S. H. P. L. L. Z. Yan Zhuang, "Self-Sovereign Identity Empowered Non-Fungible Patient Tokenization for Health Information Exchange Using Blockchain Technology," *Computers in Biology and Medicine,* vol. 157, p. 106778, 2023.

[7] G. K. A. M. R. R. M. M. A. Lukas Stockburger, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain: Research and Applications,* vol. 2, p. 100014, 2021.

[8] I. S. L. A. Alex Grech, "Blockchain, Self-Sovereign Identity and Digital Credentials: Promise Versus Praxis in Education," *Frontiers in Blockchain,* vol. 4, p. 12, 2021.

[9] L. W. T. L. Jiayang Yao, "Blockchain-Based Voting System," *Computer System Networking and Telecommunications,* vol. 3, no. 1, p. 9, 2020.

[10] G. Kortemeyer, "Self-Sovereign User Scenarios in the Educational Domain," *ETH Zurich,* 2023.

[11] J. J. B. P. L. H. E. Araceli Queiruga-Dios, " Self-Sovereign Identity in University Context," *FRUCT Association,* Vols. 2022-april, pp. 259-264, 2023 Proceedings of the 31st Conference .

[12] N. H. T. K. G. L. P. A. M. Sroor, "How Modeling Helps in Developing Self-Sovereign Identity Governance Framework," *Procedia Computer Science,* vol. 204, pp. 267-277, 2022.

[13] D. D. F. M. P. M. L. R. A. P. A. De Salve, "A Multi-Layer Trust Framework for Self-Sovereign Identity on Blockchain," *Online Social Networks and Media,* Vols. 37-38, p. 100265, 2023.

[14] A. N. P. N. M.M. Ibrahimy, " Blockchain-based Governance Models Supporting Corruption-Transparency," *Blockchain: Research and Applications,* vol. 5, p. 100186, 2024.

[15] R. S. M. G. T. H. K. Gulshan Kumar, "BRON: A Blockchained Framework for Privacy Information Retrieval in Human Resource Management," *Heliyon,* vol. 10, p. 33393, 2024.

[16] J. F. F. T. F. M. C. Sérgio Guerreiro, "Integrating an Academic Management System with Blockchain," *Blockchain: Research and Applications,* vol. 3, p. 100099, 2022.

[17] H. G. S. B. Syrine Sahmima, "Edge Computing: Smart Identity Wallet Based Architecture and User Centric," *Procedia Computer Science,* vol. 159, pp. 1246-1257, 2019.

[18] X. L. P. F. S. S. C. H. D. B. N. R. K. D. Z. Eranga Bandara, "A Blockchain-Empowered and Privacy-Preserving Digital Contact Tracing Platform," *Information Processing and Management,* vol. 58, p. 102572, 2021.

[19] V. D. A. S. L. A. P. Francesco Buccafurri, "Enforcing Security Policies on Interacting Authentication Systems," *Computers & Security,* vol. 140, p. 103771, 2024.

[20] M. K. G. C. M. P. R. T. L. K. Aarti Amod Agarkar, "Blockchain-Aware Decentralized Identity Management and Access Control System," *Measurement: Sensors,* vol. 31, p. 101032, 2024.

[21] M. S. F. Sadman Sakib Akash, "A Blockchain-Based System for Healthcare Digital Twin," *IEEE Access,* vol. 10, pp. 50523-50547, 2022.

[22] M. A. S. M. S. F. M. J. M. C. M. S. R. Md. Abdul Hannan, "A Systematic Literature Review of Blockchain-Based e-KYC Systems," *omputing,* vol. 105, pp. 2028-2118, 2023.

[23] M. A. S. M. S. F. M. J. M. C. M. S. R. Md. Abdul Hannan, "A Systematic Literature Review of Blockchain-Based e-KYC Systems," *Computing,* vol. 105, pp. 2089-2118, 2023.

[24] A. V. Leonardo Perugini, "On the Integration of Self-Sovereign Identity with TLS 1.3 Handshake to Build Trust in IoT Systems," *Internet of Things,* vol. 25, p. 101103, 2024.

[25] A. L. a. S. Butakov, "Trust Framework for Self-Sovereign ID in Metaverse Health Care Applications," *Data Science and Management,* 2024.

211-15-4020

ORIGINALITY REPORT

13%	10%	7%	9%
SIMILARITY INDEX	INTERNET SOURCES	PUBLICATIONS	STUDENT PAPERS

PRIMARY SOURCES

1	Submitted to Daffodil International University Student Paper	3%
2	dspace.daffodilvarsity.edu.bd:8080 Internet Source	2%
3	Submitted to United International University Student Paper	1%
4	Submitted to Ghana Technology University College Student Paper	<1%
5	Submitted to Melbourne Institute of Technology Student Paper	<1%
6	Konstantinos Loupos. "About the Editor", Now Publishers, 2025 Publication	<1%
7	d197for5662m48.cloudfront.net Internet Source	<1%
8	arxiv.org Internet Source	<1%
9	Submitted to University of Northumbria at Newcastle Student Paper	<1%
10	Submitted to Victorian Institute of Technology Student Paper	<1%
11	export.arxiv.org	