Decentralized Identity Verification: A Blockchain-Based Framework for Self-Sovereign Identity (SSI) with Issuer Trust Registry

by

Faiaz Mohammad Tiham
24141271
Ashiqur Rahman Fahim
20101496
Gazi Md. Julcarnine
20101360
Hossain Mohammed Usman
20101053

A thesis submitted to the Department of Computer Science and Engineering
in partial fulfillment of the requirements for the degree of
B.Sc. in Computer Science

Department of Computer Science and Engineering
Brac University
October 2024

Declaration

It is hereby declared that

1. The thesis submitted is my/our own original work while completing degree at Brac University.
2. The thesis does not contain material previously published or written by a third party, except where this is appropriately cited through full and accurate referencing.
3. The thesis does not contain material which has been accepted, or submitted, for any other degree or diploma at a university or other institution.
4. We have acknowledged all main sources of help.

Student's Full Name & Signature:

Faiaz Mohammad Tiham
24141271

Ashiqur Rahman Fahim
20101496

Gazi Md. Julcarnine
20101360

Hossain Mohammed Usman
20101053

Approval

The thesis titled "Decentralized Identity Verification: A Blockchain-Based Framework for Self-Sovereign Identity (SSI) with Issuer Trust Registry" submitted by

1. Faiaz Mohammad Tiham (24141271)
2. Ashiqur Rahman Fahim (20101496)
3. Gazi Md. Julcarnine (20101360)
4. Hossain Mohammed Usman (20101053)

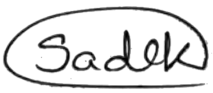
Of Summer, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on 22nd October 2024.

Examining Committee:

Supervisor:
(Member)

Muhammad Iqbal Hossain, PhD
Associate Professor
Department of Computer Science and Engineering
Brac University

Co-Supervisor:
(Member)



Md. Sadek Ferdous, PhD
Professor
Department of Computer Science and Engineering
Brac University

Head of Department:
(Chair)

Sadia Hamid Kazi, PhD
Chairperson and Associate Professor
Department of Computer Science and Engineering
Brac University

Abstract

In an era where data security and privacy breaches are alarming, blockchain technology could greatly enhance different identification systems like passports, national identity cards (NIDs), driving licenses, etc. We explore the idea of a blockchain-powered identity verification system in this research where individuals' identity information is safely kept on a decentralized ledger. The principal goal of this research is to find out the possible advantages and difficulties of incorporating blockchain systems into personal identity verification systems. We thoroughly assess the built-in cybersecurity attributes of blockchain, including decentralization, immutability, and cryptographic security, which collectively establish it as a perfect choice for authenticating and safeguarding personal identity data. Moreover, the research dives into topics concerning data privacy, surveillance, and individual rights. The primary emphasis of this research is on the smooth incorporation of a blockchain-driven identity verification system centered on Self-Sovereign Identity (SSI). Furthermore, this thesis highlights the critical role of issuers in the Self-Sovereign Identity System (SSI) and addresses the inherent issue of Issuer Trust for verifiers. To address the issue, this study introduces the concept of an Issuer Trust Registry to ensure trustworthiness when issuing credentials. The research studies how blockchain can streamline identity verification for authentication while creating driver's licenses, bank account openings, SIM card registrations, land registrations, etc., thereby mitigating fraudulent activities in the cyber world and enhancing overall security. When we increase the security, we can optimize the personality verification of authentication. In conclusion, this research proposes a comprehensive study of the role of blockchain technology in reimagining personal identification systems for the digital age.

Keywords: Blockchain, Data Security, Cybersecurity, Cyberworld, Self-Sovereign Identity (SSI), Identity Verification, National Identity (NID), Issuer Trust Registry;

Acknowledgement

First and foremost, all praise is due to Almighty Allah, through whose grace we have been able to complete our thesis successfully without any significant obstacles.

Secondly, the supervisor Muhammad Iqbal Hossain, PhD for his kind support and motivation. His insightful guidance was crucial in advancing our work.

Thirdly, the co-supervisor, Dr. Md. Sadek Ferdous, PhD guided us with his proper instructions and constant support with our thesis planning and work.

Fourthly, the Research Assistant, Md. Yeasin Ali helped us as a mentor. Throughout the thesis, he gave constant theoretical and technical support to us.

Finally, we would like to express our deepest gratitude to our beloved parents. Their constant support and heartfelt wishes have been instrumental in bringing us to the completion of a thesis, and none of this would have been possible without them.

Table of Contents

Declaration i

Approval ii

Abstract iii

Acknowledgment iv

Table of Contents v

List of Figures vii

List of Tables viii

Nomenclature ix

1 Introduction 1
- 1.1 Motivation . . . 3
- 1.2 Problem Statement . . . 3
- 1.3 Research Objectives . . . 4
- 1.4 Structure . . . 5

2 Background 6
- 2.1 Self Sovereign Identity (SSI) . . . 6
  - 2.1.1 Principles of SSI and SSI Roles . . . 6
  - 2.1.2 Decentralized Identifier (DID) . . . 8
  - 2.1.3 Verifiable Credentials (VC) . . . 8
  - 2.1.4 Identity Wallet . . . 9
  - 2.1.5 Trust . . . 9
- 2.2 Blockchain . . . 9

3 Literature Review 11

4 System Proposal 20
- 4.1 Proposed Model . . . 20
- 4.2 Methodology . . . 21
- 4.3 Threat Modeling . . . 22
- 4.4 Requirement Analysis . . . 23
  - 4.4.1 Functional Requirements (FR) . . . 23
  - 4.4.2 Security Requirements (SR) . . . 23

4.4.3 Privacy Requirements (PR) 24

5 Architecture and Implementation **25**
5.1 Architecture 25
5.2 Implementation 26
5.2.1 ACA-Py Framework 26
5.2.2 Hyperledger Fabric 29
5.3 Use-case and Protocol Flow 31
5.3.1 Data Model and Algorithms 32
5.3.2 Protocol Flow for Issuing Verifiable Credential 35
5.3.3 Protocol Flow for User Identity Verification 37
5.3.4 Protocol Flow for Issuer Authenticity Verification 39

6 Discussion **42**
6.1 Requirements Analysis 42
6.1.1 Functional Requirements (FR) 42
6.1.2 Security Requirements (SR) 43
6.1.3 Privacy Requirements (PR) 43
6.2 Research Objectives Analysis 44
6.3 Advantages 45
6.4 Challenges and Limitations 45
6.5 Comparison with Existing Relevant Research Studies 46
6.6 Future Work 50

7 Conclusion **51**

Bibliography **55**

List of Figures

2.1 SSI Trust Triangle 7
2.2 Decentralized Identifier (DID) 8

3.1 The NIDBC Framework [4] 13
3.2 Access control flow enforced by the SSIBAC model [9] 15
3.3 Health Passport Prototype [32] 16
3.4 Integration of TRAIN into W3C VC SSI ecosystem [20] 18

4.1 Methodology Diagram 21

5.1 System Architecture Diagram 25
5.6 Credential Delivered 36
5.2 Issuer Invitation 37
5.3 NID Form 38
5.4 Issued Credential in Wallet 39
5.5 Accepted Issued Credential in the Wallet 39
5.7 Invitation from Verifier 40
5.8 Verifier Proof Request 41
5.9 Share/Decline Proof Request 41

List of Tables

5.1 Cryptographic Notations 32
5.2 Data Model 33
5.3 Getting VC from the Issuers 36
5.4 Identity Verification by Verifier 37
5.5 Issuer Trust Verification Protocol using Fabric Ledger with HTTP(S) 40

6.1 Comparison with the Existing Research on Identity Verification . . . 48
6.2 Comparison with the Existing System Architectures 49

Nomenclature

The next list describes several symbols & abbreviation that will be later used within the body of the document

DID	Decentralized Identifier
FR	Functional Requirement
NID	National Identity
PR	Privacy Requirement
RO	Research Objective
SR	Security Requirement
SSI	Self-Sovereign Identity
VC	Verifiable Credential
VP	Verifiable Presentation

Chapter 1

Introduction

In the age of rapid technological advancement and digital transformation, the security and management of personal identity data have become vital issues for governments and organizations worldwide. National identity systems—comprising Passports, National Identity (NID) cards, Driving Licenses, Birth Certificates, etc.—form the cornerstone of how individuals access essential services, assert their rights, and participate in society. These identity documents serve a critical function, enabling individuals to authenticate themselves in various situations, including voting, healthcare access, financial transactions, and travel. However, traditional methods of storing, verifying, and managing such identities have encountered significant challenges, particularly with respect to data breaches, identity theft, forgery, and security vulnerabilities. As the world continues to digitalize, it becomes imperative to explore more secure and efficient mechanisms for managing identity information.

Blockchain has emerged as a promising solution in the field of technology [6]. Blockchain technology, at its core a decentralized and unchangeable system for keeping records, offers a new way of managing identity that supports self-sovereign identity (SSI) principles and minimizing data [38]. These principles highlight the importance of allowing individuals to have control over their personal data, so they can manage, share, and safeguard it without depending on centralized authorities that could lead to potential data misuse or security breaches. By utilizing blockchain's encryption algorithms and agreement methods, governments and institutions can create secure identity management systems that prioritize user needs while addressing key privacy, security, and fraud issues. Blockchain provides a tamper-resistant infrastructure, making it a perfect technology for securely storing and managing personal identity data without unauthorized access.

The aim of this research paper is to investigate the potentiality of an identity management system based on blockchain that could include various forms of identities (e.g. NID cards, passports, driving licenses, etc.) so as to cover almost all types needed in modern society. In this study, we have discussed how blockchain implementation can influence identity management not only in technical aspects but also in socio-political. It pays attention to the blockchain superpowers — security features built into it that make it a good fit for personal data management, decentralization, cryptographic security, and immutability. Identity verifications made possible through blockchain are superior in quality and efficiency as a secure mode

of authentication providing prevention from frauds on various critical areas such as banking, land registration or sim card registrations, etc.

This study has mainly focused on incorporating the idea of Self-Sovereign Identity (SSI) into its personal identity framework. The states that the centralized entities should refrain from controlling their life data, but instead such personal identity data-related ideas represented by SSI have to take a full turn in this regard. In fact, blockchain is an essential part of the SSI model because it offers a distributed architecture for issuing identities and verifying them with cryptographic protocols that enable many organizations to provide secure services while protecting personal data. This trust infrastructure is designed to enable the issuance and exchange of identity information between trusted issuers, holders, and verifiers - a complete ecosystem that gives users all benefits of internet identities without suffering as a result of global data risk.

The most essential part of an SSI system is the role played by issuers — usually, a trusted body such as a government or financial institution who verifies importantly that someone is really an authentic person [22]. We have proposed in this study to introduce a decentralized "Issuer Trust Registry" based on blockchain which verifies and attests for reliable issuers that can secure identity verifiers about certificates not being counterfeit or misrepresented. The Issuer Trust Registry is the trust layer in SSI ecosystem which makes sure an identity verification procedure not only happens between two or more DID controllers, but these DIDs themselves are also trustworthy.

This research also examines the ethical, legal, and societal implications of using blockchain technology for identity management. While the security benefits are considerable, implementing blockchain-based identity systems brings up issues related to surveillance, data privacy, and the power dynamics between governments and citizens. It is essential to critically assess ethical questions regarding who has control over access to the ledger, the risks of misusing stored identity information, and the significant influence of state authorities in the digital era. Additionally, this thesis investigates the regulatory frameworks needed to facilitate blockchain adoption, emphasizing legal challenges concerning privacy laws, data ownership, and cross-border identity management.

This research assesses the potential of blockchain technology in reconstructing personal identity systems. It addresses the viability of managing several identity possessions using blockchain technology as well as its relation to self-sovereign identity and issuer trust registry systems. The purpose of this study is to identify how best this revolutionary technology can be adopted by governments and peaceful institutions in order to make identity verification processes more secure and efficient and also more transparent as possible. It also touches upon the issues, challenges, and opportunities that accompany this shift and suggests solutions on how one will be able to use blockchain technology to improve the current shortcomings of systems employed in managing people's identities without going to extremes ethically and legally as we prepare for a digital world of citizenship.

1.1 Motivation

As Bangladesh and the world become more reliant on digital systems, the risks associated with cyber threats, data breaches, and identity theft are growing. In Bangladesh, the situation is further complicated by corruption, where identity data is often leaked or sold to unauthorized parties, compromising the privacy and security of citizens [37]. Additionally, the current identity verification systems, such as NID cards and passports, are inconvenient to carry, lack portability, and are vulnerable to misuse. For example, even when purchasing a SIM card from a telecom operator, individuals need to present their full NID card to the vendors which raises privacy and security concerns. Our research addresses these critical issues by proposing a blockchain-based identity verification system that offers more secure, portable, and efficient identity verification. Blockchain's tamper-resistant technology can protect sensitive personal information from being leaked or sold which ensures the privacy of citizens. Its decentralized architecture provides stronger security than the current centralized identity data storing mechanism, making it an effective solution to prevent data breaches and identity fraud. In this system, a wide range of stakeholders will be benefited. Citizens will be able to enjoy greater security, privacy, and convenience in managing their personal information, with the added portability of digital identity verification. Financial institutions and businesses will also benefit by having a more secure and efficient system for customer verification, reducing the risk of fraud and improving overall service delivery. By addressing the challenges of data security, privacy, corruption, and inefficiency in the current system, this study has the potential to transform identity management in Bangladesh. It not only strengthens national security and enhances the privacy of individuals but also creates a safer, more convenient environment for both public and private sectors.

1.2 Problem Statement

People need to provide personal information like date of birth, photo, fingerprint, address, etc. to verify identity while applying for different government services like driving license, bank account opening, sim card registration, land registration, etc. It creates a huge data breach scope as the databases of these websites are not secured enough.

There are a lot of technical threats for an individual for example, fake banking transactions and Online shopping, Credit card fraud, Blackmail, and Social media ID fraud can be caused by the breached data.

According to TechCrunch, details of individual citizens including full name, NID card number, mobile number, and email address are leaked on a government website of Bangladesh [31]. The leak was found by Viktor Markopoulos, a cybersecurity researcher who accidentally looked upon the website while looking for an SQL problem. This personal information may be used to verify birth registration records as well as access, modify, and/or delete applications. In a report, BBC News states that malware on an ATM network compromised the security of more than 3.2 million debit cards in India, leading to fraudulent transactions and reputational damage to

institutions [3]. As a result, consumers have expressed concern about the breach, which significantly affects the economy.

Current methods of identity verification on the Internet, especially age verification, are not as effective as they should be. There is a significant lack of a reliable and accurate age verification process, with significant gaps in ensuring online safety, especially for minors. This gap stems from reliance on self-declaration and vulnerabilities in the birth certificate registration process, enabling potential manipulation. As a result, young people have easy access to information and content that could be harmful to them, primarily due to the absence of a robust age verification system beyond a simple "Yes, I'm over 18" button [26].

As we see, this kind of data leakage or verification problem is getting worse, thus we need to find an effective solution that will help our general public to prevent this data leakage and proper authentication of important information.

1.3 Research Objectives

The main objective of this research is to approach the practicality and effectiveness of implementing a blockchain-based personal identification system with the objective of data security, privacy, accessibility, immutability, and overall system integrity. Making the already existing system robust and more foolproof is also one of its goals. Already existing verification system is extremely vulnerable and easy to fraud. Implementation of Self-Sovereign Identity (SSI) with the Issuer Trust Registry will provide more trust and a secure identity verification system. This research aims to achieve the following objectives:

RO1: Enhancing Identity Verification
Sub-objective 1.1: Develop and implement a secure identity verification process utilizing blockchain technology to ensure the authenticity of personal identities.
Sub-objective 1.2: Compare and evaluate the performance of the SSI-based verification system against traditional methods and improvements in accuracy, security, portability, and privacy.

RO2: Reviewing the Existing Research Perspective
Analyze the limitations and strong points of existing identity verification models, and address these shortcomings within the proposed architecture, providing a foundation for future enhancements and research directions.

RO3: Empowering Users with Control over Their Data
Sub-objective 3.1: Design and implement a consent-based data access system that restricts third-party intruders' access to user data without user consent. This will include the integration of a notification alert to inform users when third parties request access to their personal data.
Sub-objective 3.2: Evaluate the effectiveness of the notification system in empowering users with control over their own data privacy, and assess user satisfaction with these privacy controls.

RO4: Integrating Self-Sovereign Identity (SSI) and Ensuring the Issuers Trust
Sub-objective 4.1: Implement a public key-based verification system that restricts unauthorized third-party access to user data, and evaluate its integration with a range of identity systems, including national identification cards, driver's licenses, and passports.
Sub-objective 4.2: Establish an Issuers Trust Registry within the SSI framework, ensuring that only authentic identity issuers are authorized, thereby enhancing security, trust, and reliability.

RO5: Ensuring Data Immutability and a Tamper-Proof System
Implement data immutability features using blockchain technology, ensuring that user data remains tamper-proof and protected against unauthorized modifications.

1.4 Structure

This thesis is organized into seven chapters, each building on key aspects of the research.

Chapter 1: Introduction introduces a research problem ready to be solved, with specific attention to blockchain-based identity verification, and states the motivation (Section 1.1), aims, and questions answered. Moreover, this chapter consists problem statement (Section 1.2) and research objectives (Section 1.3).

Chapter 2: Background discusses some fundamentals of Self-Sovereign Identity (SSI) (Section 2.1) and blockchain (Section 2.2) and will build a theoretical foundation with relevant literature.

Chapter 3: Literature Review examines existing research on identity verification and blockchain technologies, identifying gaps that justify further investigation.

Chapter 4: System Proposal presents the proposed model (Section 4.1), methodology (Section 4.2), threat modeling (Section 4.3), and requirements (Section 4.4) of the blockchain-based identity verification system, highlighting its benefits and challenges.

Chapter 5: Architecture and Implementation details the technical implementation, including blockchain components (Section 5.2 and Section 5.1) and the Issuer Trust Registry. Moreover, this chapter also includes use-case and protocol flow (Section 5.3).

Chapter 6: Discussion evaluates the findings of the investigation and its strengths and weaknesses concerning its comparison along with the previously existing models (Section 6.5) and future works (Section 6.6) of our proposed system.

Chapter 7: Conclusion summarizes the research contributions and suggests future directions for innovation in secure identity management.

Chapter 2

Background

This section presents a brief introduction to Self-Sovereign Identity (SSI) (Section 2.1) and Blockchain technology (Section 2.2).

2.1 Self Sovereign Identity (SSI)

The digital movement of individuals' ownership and control over their identity without depending on any administrative authority is emphasized as Self-sovereign Identity [30]. With SSI people can manage and control their identifying information digitally such as birth certificates, and degree licenses. This is very much like a physical card system in the offline world but digitally managed. SSI approach makes a person, business, and IoT entities interact in the digital world with freedom and trust similar to offline interaction. SSI allows holders to handle their identity elements, controls access to credentials, and authenticate their identity using a digital wallet. The system system eliminates the need to surrender personal information to numerous databases reducing the risk of identity theft. In a Self Sovereign identity system, individuals become the sovereign controllers of their digital existence, independent of any organization, ensuring greater security and autonomy.

2.1.1 Principles of SSI and SSI Roles

Self-sovereign identity is a decentralized digital identity system that gives them control of a person's identity information [17]. In this model, there are three main roles.

Issuer: The issuer is the entity that issues the digital identities or verifiable credentials to a holder [17]. This could be government, service provider, agency, or any other entity. There could be multiple types of information such as personal details, qualifications, membership, or any other attributes. To make the identity tamperproof and verifiable the issuer put digital signatures in credentials. The signatures ensure the integrity and authenticity of these credentials. In the SSI model the holder's information is not stored by the issuer instead the holder gets to store these credentials in their digital wallet.

Holder: The entity that owns and controls its information is called the holder [17]. This role is held by the person or the organization to whom the identity credentials were issued by the issuer. Holders can store their credentials in a digital wallet

or any secured repository. The wallet stays under their control and they can give permission to which piece of information they like to share and with whom. The SSI model gives better privacy and control as the holder gets to decide who to give personal information.

Verifier: The entity that needs to verify specific claims and attributes of holder [17]. Service providers, employers, government agencies or any other entity requiring identity verification could fill this role. Verifiers do not hold a central database of user information. Instead, Holders present their verifiable credentials to the verifier. The verifier can ask for specific information from the holder and holders then present the required information allowing the verifier to verify the authenticity of the information from the blockchain.

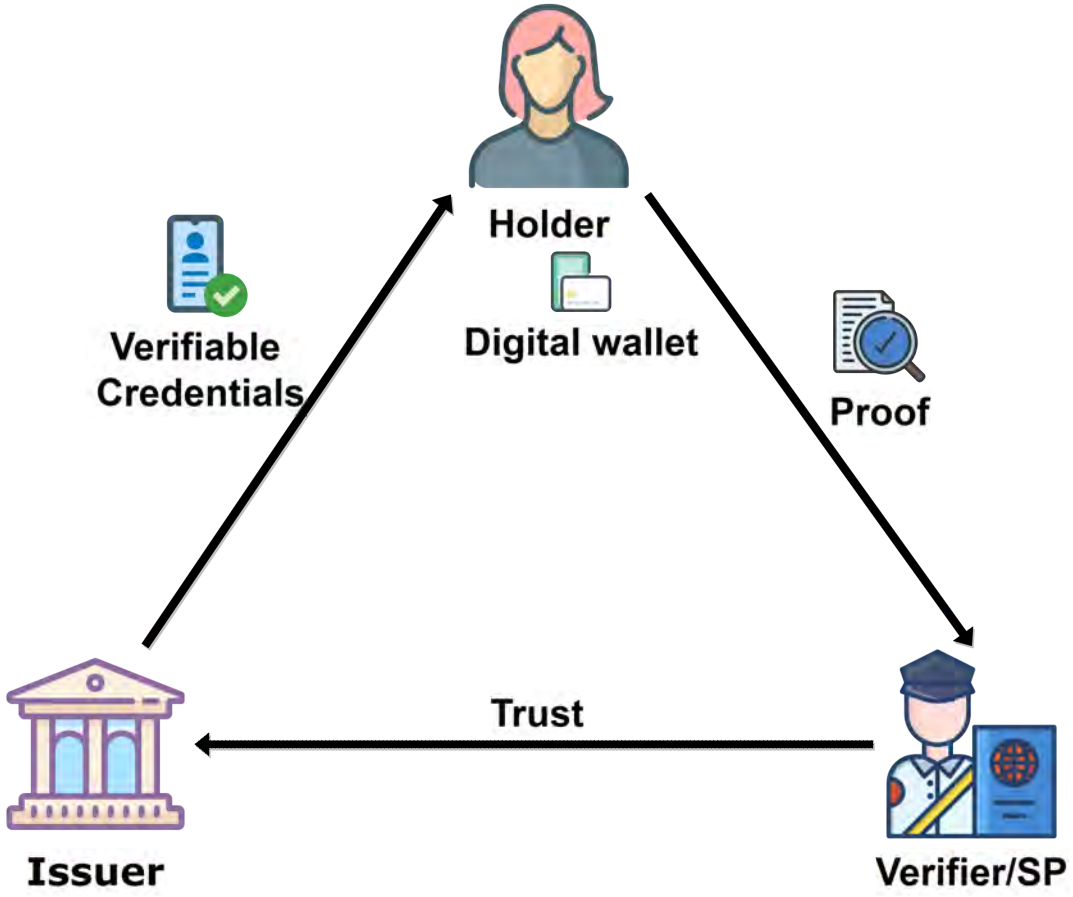


Figure 2.1: SSI Trust Triangle

In SSI the relationship between the Issuer, Holder, and Verifier is known as the trust triangle like in Figure 2.1. This shows if the credentials are only trustable on how much trust the verifier has in the issuer. The verifier in this case takes a decision on how much trust assurance it has in the issuer.

2.1.2 Decentralized Identifier (DID)

A decentralized Identifier is one of the most important entities in the SSI model [33]. Decentralized Identifiers (DID) are comparatively a new type of identification system that enables decentralized digital identity verification. DID methods are the mechanisms by which a particular type of DID and its associated DID documents are created, resolved, updated, and used cryptographic proofs such as digital signatures. DID could refer to any subject that the controller of that DID wants to verify for example: person, organization, objects, data model abstract entity etc. Compared to federated identifiers, DID is designed with the goal that it may be separated from the centralized registry, certification authorities, or identity providers. DIDs can express cryptographic material, verification methods, or services. This can be used by a DID controller to prove control of the DID. A simple DID contains 3 parts like in Figure 2.2

- **DID URI Scheme Identifiers:** These are uniform resource identifiers (URIs) used in DIDs (Decentralized Identifiers) to uniquely identify an entity or resource on the web. The URI scheme defines how the DID is formatted and resolved across different decentralized systems.
- **Identifier for the DID Method:** This specifies the method used to create and manage a DID on a particular blockchain or decentralized network. It defines the rules for how DIDs are generated, read, updated, and deactivated on that specific ledger or network (e.g., did:example where "example" is the DID method).
- **DID Method-Specific Identity:** This refers to the unique identity created by the DID method, often a method-specific identifier that is tied to the DID and represents a specific entity within that method's scope. It is used to locate and interact with the entity's public information or keys within the decentralized system.

Figure 2.2: Decentralized Identifier (DID)

2.1.3 Verifiable Credentials (VC)

Credential refers to pieces of paper or plastic that we carry around to prove our identity like driving license, national identity card, credit card, etc. [17]. Every

credential contains a set of claims about the identity of the credential holder. In SSI these claims are created by the issuer. Those who get the verifiable credential are the holders and they can keep it in their digital wallet. The VC also contains metadata and DID. This will be used by the verifier to verify the identity of the holder.

2.1.4 Identity Wallet

An identity wallet is a digital tool designed to securely store and manage a user's identity credentials and personal information [24]. It allows users to control their digital identity, providing a convenient way to access and share personal information, such as identification documents, certificates, and verifiable credentials while maintaining privacy and security. Identity wallets are especially important in a world where digital interactions are becoming more common, allowing individuals to prove their identity in various contexts, such as online transactions, service access, and identity verification. Some existing types of Identity wallets are Bifold Wallets, Multifold Wallets, Decentralized Identity Wallets, Centralized Identity Wallets etc.

2.1.5 Trust

In Self-Sovereign Identity (SSI), trust plays a central role in how individuals and entities manage and verify identities without relying on a central authority. The trust model in SSI is decentralized, meaning individuals, known as holders, have control over their own identity data and can share it directly with verifiers, while issuers create and verify credentials [15]. Trust is established through cryptographic proofs, where the verifier trusts the credential based on its authenticity and the reputation of the issuer, rather than relying on a centralized institution.

In SSI, trust is also rooted in blockchain or distributed ledger technologies (DLTs), which provide a transparent, immutable record of issued credentials and DIDs. This ensures that both issuers and credentials can be verified through decentralized, consensus-driven mechanisms, reducing the need for intermediaries. The trust framework in SSI empowers users by allowing them to control who accesses their data, while also providing verifiable, secure interactions between issuers, holders, and verifiers, all based on cryptographic assurance rather than centralized trust.

2.2 Blockchain

Blockchain is a profoundly secure distributed ledger that isn't in charge of any authority [5]. A blockchain is decentralized in contrast to a conventional ledger, which is managed by a single authority. Every transaction is regarded as a digital document that requires a signature. At the point when somebody needs to add another exchange to the blockchain, they sign it carefully and utilize their private key. Exchanges are assembled into blocks. Once a block is made and connected to the block before utilizing the hash of that block, it becomes extremely challenging to modify it. Changing an exchange would require recalculation of the hash of the block. Since the hash of the block that is preceding, is additionally essential for the hash, messing with an exchange is promptly observable as each new block is reproduced among

the peers in the organization. This characteristic makes blockchain an ideal solution for applications requiring secure and transparent record-keeping, such as financial transactions, supply chain management, and identity verification.

There are several types of blockchain networks, each designed to meet different needs and use cases [41]. Public blockchains, like Bitcoin and Ethereum, are open to anyone, allowing users to join the network, validate transactions, and access transaction data freely. These blockchains are fully decentralized, providing complete transaction visibility and fostering a trustless environment. On the other hand, private blockchains are restricted to specific organizations or individuals, requiring permission to access the network. Examples include Hyperledger Fabric, which is often used by enterprises for internal processes, as it offers enhanced privacy and control over data.

Consortium blockchains represent a middle ground between public and private systems, where a group of organizations governs the network, allowing multiple entities to participate while maintaining some degree of privacy. This setup is often employed in industries like banking, where multiple financial institutions collaborate without exposing all their transactional data to the public. Finally, hybrid blockchains combine elements from both public and private blockchains, allowing for certain data to remain private while permitting other data to be public. Dragonchain is an example of a hybrid blockchain, offering flexibility in how data is managed and shared.

Overall, blockchain technology is transforming the landscape of data management and transaction verification across various sectors by offering enhanced security, transparency, and decentralization. Its applications are rapidly expanding, with potential uses ranging from cryptocurrencies and digital identities to supply chain traceability and smart contracts, thereby reshaping traditional business models and fostering innovation.

Chapter 3

Literature Review

In recent years there have been various studies that focused on different identity verification systems. We have studied the application of blockchain technology in secure identity management and verification across different fields such as passport authentication, open banking, national identity systems, land registries, and healthcare. The main purposes of these studies include the use of decentralized architectures, such as Self-Sovereign Identity (SSI), to enhance security, privacy, and transparency in digital identity systems, while mitigating issues like identity theft and data leakage.

Htet et al. discussed using blockchain technology in a digital secure identity management system for passports in Myanmar in their paper [11]. The aim of this proposed system was to prevent counterfeiting of passports. The main goal of this research was to ensure that each person can only hold one valid passport. All passport offices will be connected with each other as a chain where the information regarding passports will be securely shared among colleagues which can prevent the illegal duplication of passports and guarantee passport authentication. This approach makes the system decentralized. The study explained the working procedures of blockchain technology. The proposed model of the study was executed based on a fully distributed mode. It checks if transactions are validated, approved, and recorded by all the members of the blockchain. This technique is different from storing data in a central database which prevents passport fraud. The article further previewed various components within a block, including the block version number, a timestamp, the Bits field, the computed Merkle root hash for all transactions, the nonce, and the hash of the header obtained from the previous block. Besides, the proposed system only focused on passport data management which can be further extended in various fields like driving licenses, national identity cards (NID), and many more.

Liao et al. discussed the requirements and challenges of building an open banking scenario using blockchain in their paper [21]. The paper reviewed related research and presented an ecosystem, operational model, smart contract design, and backend elements. Additionally, this paper also introduced the BIMAC architecture, which serves as a blockchain-based framework. Which is used for managing and controlling identity. BIMAC utilizes smart contracts and stateless authentication. This establishes a highly secure platform for managing personal information. The use of access control techniques, such as role-based access control (RBAC) was also described to

ensure privacy and transparency. It included a notarization mechanism, audit trail, and privacy protection for security purposes. The paper reviewed five unique types of blockchain research with different aspects. They suggested different approaches to implementing blockchain in the open banking ecosystem. Though these five studies had their own unique approaches, they could not solve the problem alone. They needed to be combined and improved to serve a more comprehensive solution. This paper concluded by mentioning the benefits of BIMAC. It is an efficient authentication framework for mitigating the costly KYC (Know Your Customer). Additionally, public key cryptography (ECC) and digital signature techniques (ECDSA) are employed within the BIMAC ecosystem to handle customer information.

Alilwit et al. discussed the challenges associated with conventional authentication systems, such as identity theft and data leakage in their study [8]. The study proposed a solution using blockchain technology, offering secure access to online services for customers. The technique utilized a prototype-based E-pass that protected sensitive information from being exposed. Given that identity theft is a significant threat in the digital age, traditional authentication systems face numerous problems. The paper explored the limitations of the current AAA (Authentication, Authorization, and Accounting) infrastructure used by service providers, including data theft and breaches, and introduced blockchain features like blocks and smart contracts. It recommended Ethereum or other blockchain-based platforms as suitable solutions due to their advantages in data ownership and security. Finally, the study concluded that users showed interest in blockchain-powered digital identities.

Alsayed et al. explained the concept of digital identity and management (IDM) in detail and suggested a revolutionary decentralized architectural model for IDM on the Ethereum platform [7]. The proposed model enhanced security in current IDM implementations. The article included three tests that highlighted the security benefits of DNS-IdM, considering the overall findings of the investigation. This study proposed a decentralized identity management architecture with attribute-related validation that maximized security. Furthermore, the paper suggested minimal disclosure using RP smart contracts, which could be updated based on the user's best interests before being uploaded to the network. The primary goal was to achieve a decentralized environment through self-sovereign identity management, utilizing the best possible strategies for privacy, performance, and security.

Fathiyana et al. proposed a functional model of a secure national identity storage system in Indonesia integrated with blockchain technology in their research paper [19]. This system aimed to address the challenges associated with information systems that were not interconnected, which had been developed by government agencies responsible for issuing national identification numbers. Additionally, it sought to prevent user organizations from misusing data retrieved from the Population Data Utilization Program. After comparing different blockchain architectures, Hyperledger Fabric was selected as the platform for implementing this system. The study provided a detailed overview of the proposed system and discussed the requirements for the research. The study primarily focused on developing an integrated storage security system using blockchain technology for the Ministry of Interior's population data utilization program. The history of the implementation of a national popu-

lation database center by the Indonesian government of the Republic of Indonesia was also included in the paper. The document explained how an electronic identity card could be used as a valid legal reference and data source for various government services with high security.

Chalaemwongwan et al. proposed two types of authentication techniques: document authentication and user authentication in their research [4]. Document authentication techniques incorporated variable laser pictures, visualizations, watermarking, one-way functions, and protocols. User authentication techniques included biometric attributes, behavioral qualities, PINs, passwords, and one-time passwords. The paper also examined the utilization of blockchain technology for transactions and the challenges related to security in public ID record systems. The paper concluded with a review of consensus algorithms for blockchain network evaluation and the performance outcomes of the implemented system.

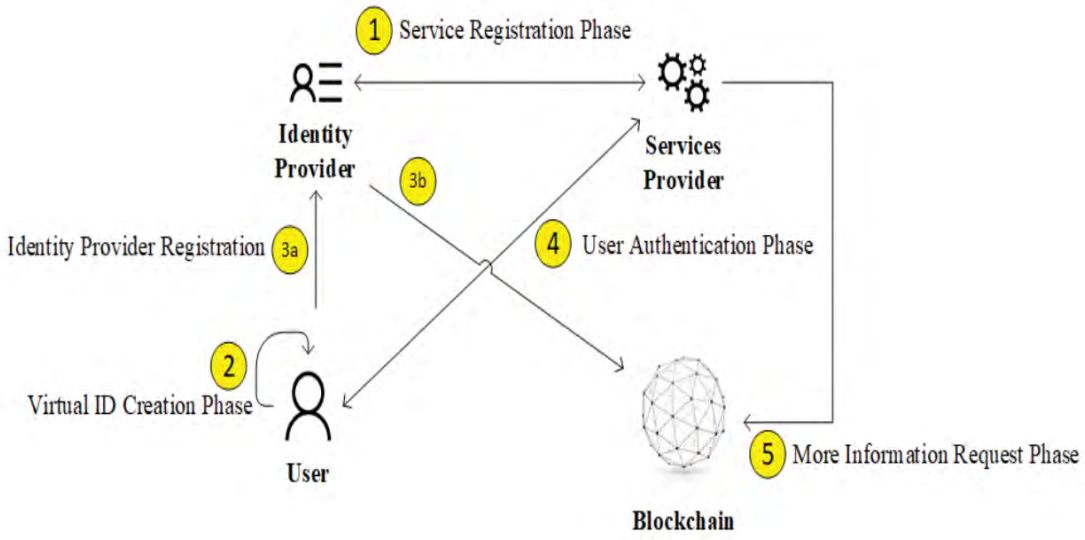


Figure 3.1: The NIDBC Framework [4]

The system architecture diagram of Chalaemwongwan et al. (Figure 3.1), the National Digital Identity Blockchain Framework (NIDBC) consists of five coordinated phases that aid secure digital identity management using blockchain [4]. It begins with the Service Registration Phase (1), where the service provider (SP) registers with the identity provider (IP) to access user identity services. Next, in the Virtual ID Creation Phase (2), users create a virtual ID (VIDu) from their public key to ensure privacy. The Identity Provider Registration Phase (3a, 3b) involves the IP registering the user's VIDu on the blockchain and providing necessary identity verification for SPs through the blockchain. In the User Authentication Phase (4), when a user requests a service, the SP uses the blockchain to authenticate the user's VIDu and public key. Lastly, the More Information Request Phase (5) allows SPs to request additional information from the blockchain when necessary, ensuring secure and authorized access to user data.

Shuaib et al. explained a methodical paper that aimed to identify the most suitable self-sovereign identity (SSI) for the blockchain-based land registry [25]. The review

methodology included research questions, data sources, search methodology, inclusion and exclusion criteria, and a description of the screening and final selection process. By integrating the principles of SSI, SSI's role in data flows, blockchain technology, and its application to SSI and its use in the land registry system, the work offered a comprehensive assessment of the relevant literature required for this study. The study also discussed how SSI addressed the issue of non-compliance with identification requirements in the blockchain-based land registration architecture. Finally, the paper proposed various blockchain-based SSI solutions based on the defined criteria.

Datta et al. proposed a technique for enabling information sharing in response to third-party data access requests [10]. The approach empowered citizens with an access authorization system while providing data to third parties. The proposed architecture granted citizens control over their data sharing, where access to information and the attributes to be shared were subject to each citizen's consent. The paper also referenced the implementation of a model to test the effectiveness of the proposed architecture. Extensive experimentation was necessary to assess all relevant parameters, relying heavily on powerful computers at a large scale. Which depended on securing funding. The proposed system enabled citizens access to their data in cases third-party organizations requested it. Additionally, the research explored how blockchain could be used to design a secure management system for a "smart national identity card." This architecture would provide protection against unauthorized data tampering. Also, the system's distributed ledger would ensure flexibility even in the event of node failure. Citizens can still control who access their data, even when third-party organizations make requests.

Páez et al. discussed the authentication methods for electronic identity documents (e-ID) [13]. The paper mentioned two types of authentication methods: document authentication and user authentication. Document authentication included changeable laser images, holograms, watermarking, one-way functions, and protocols, while user authentication comprised biometric characteristics, behavioral characteristics, PINs, passwords, and public-key cryptography. This study also proposed a private model (TCA) for e-ID systems to enhance security. Furthermore, the method of implementation and the performance results of the proposed system were addressed in the paper, demonstrating its high efficiency, limitations, and ability to preserve established information. Tests were performed to validate the consensus algorithm's effectiveness in terms of CPU usage, cache memory consumption, and the time spent on mining and broadcasting. The results showed that the TCA (Tournament Consensus Algorithm) was efficient and did not consume excessive computational power, while still maintaining blockchain security. This differentiated it from other algorithms, such as PoW and PoS, which used more power and raised more security concerns, particularly in private blockchains.

Mahula et al. described the opportunities and challenges of implementing Self-Sovereign Identity (SSI) for the public space in Belgium [16]. The study included various interviews. Such as identity specialists, executives and SSI practitioners. The primary motive was to facilitate communication and provide simple utilization of SSI, enabling individuals to move freely, acquire credentials from multiple sources

and apply them as needed. Although, multiple challenges can arise in the way of achieving this like ease of user experience and the need for a trustworthy security framework etc. Furthermore, the research emphasized the importance of beginning with low-risk use cases and gradually adopting Self-Sovereign Identity (SSI). The research proposed that despite all these challenges, SSI still has the potential to improve communication and provide individuals more control over their data within the public domain.

Belchior et al. proposed the SSIBAC model, which combined self-sovereign identity with attribute-based access control [9]. The central concept of SSIBAC was to design Verifiable Credentials (VCs) to secure access control policies, stored at the Policy Retrieval Point (PRP), that were parsed by an underlying Access Control Model (ACM), to achieve context-based privilege and ensure data security. The paper provided a model using ABAC, reported on evaluation results, and highlighted related studies. It discussed the threat model and security requirements, as well as the challenges associated with traditional access control models. The paper also examined several limitations. Verifiers acted as single points of failure because the system's trust was heavily dependent on a single access control engine. Another limitation was that, although SSIBAC could mitigate the data privacy issue, it might have been more time-consuming than traditional centralized access control systems. The paper offered an overview of access control systems and the components involved in the access control process.

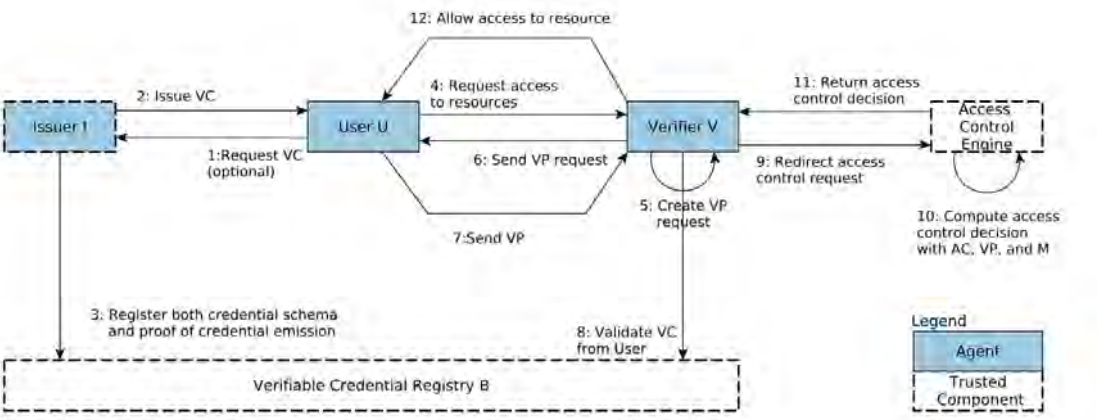


Figure 3.2: Access control flow enforced by the SSIBAC model [9]

The proposed architecture diagram (Figure 3.2) of Belchior et al. presents the interaction between various entities in a Self-Sovereign Identity Based Access Control (SSIBAC) model [9]. The process begins with the user (U) requesting verifiable credentials (VC) from an issuer (I). Once the issuer generates the VC, it registers the credential schema and proof of emission with a verifiable credential registry. The user then executes a request to access a resource from the verifier (V). The verifier initiates a verifiable presentation (VP) request based on access control policies and sends it to the user. The user responds by providing a VP, which the verifier validates against the verifiable credential. If valid, the verifier forwards the request to the access control engine, where a decision is computed based on the access control policies, VP, and additional metadata. The engine returns its result, which, if posi-

tive, grants the user access to the resource.

George et al. extensively discussed the technical feasibility of a blockchain-based Self-Sovereign Identity (SSI) system, referred to as the 'Health Passport,' in this study [32]. This system was essentially a decentralized digital wallet that allowed users to manage all their health-related history and information in one place. The paper thoroughly analyzed the design, architectural components, and complex functionalities. The proposed system was based on blockchain technology using the self-sovereign identity (SSI) model. It was intended to verify credentials (VCs) for securely creating, sharing, verifying, and revoking health credentials. To create the Health Passport for an SSI-based credential verification system, the study utilized agent-oriented modeling (AOM). The technological feasibility of the Health Passport was also discussed in the paper. The system was integrated with a PHR (Personal Health Record) and presented proof built on Hyperledger Aries and Hyperledger Indy. Finally, the paper concluded with a thoughtful investigation of potential future research directions in this dynamic field, showcasing a commitment to improvements and advancements in blockchain-based identity management systems for healthcare.

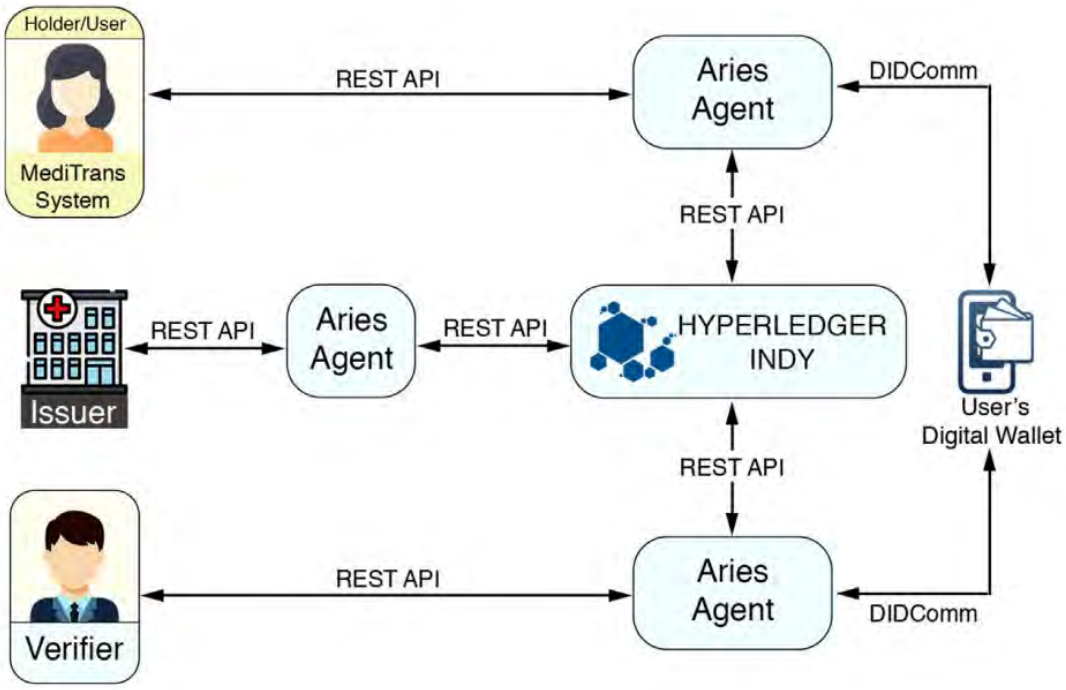


Figure 3.3: Health Passport Prototype [32]

The proposed system diagram (Figure 3.3) by George et al. shows a blockchain-based self-sovereign identity (SSI) solution integrated with the Personal Health Record (PHR) system, MediTrans [32]. The architecture involves several key agents: the issuer, holder/user, verifier, and Hyperledger Indy as the decentralized ledger. The MediTrans system interacts with the Aries Agent to manage user requests and health data through REST API connections. The issuer, typically a healthcare provider, issues verifiable credentials (VCs) such as health passports to users after verifying medical records. These credentials are stored securely in the user's digital

wallet and can be presented to verifiers (e.g., immigration officers) through secure DIDComm communication. The Hyperledger Indy ensures trust and immutability in credential verification.

Bandara et al. introduced "Casper", a blockchain-based self-sovereign identity platform that addressed security and privacy issues inherent in centralized data storage in their study [14]. The paper emphasized the increased risk of data fraud and attacks due to centralized control, as well as concerns about immutability and data provenance. Casper mitigated these risks by adopting a self-sovereign identity (SSI) architecture that stored personal data on users' mobile devices while limiting distributed blockchain storage to identity proofs. The platform introduced a decentralized approach to inter-bank 'Know Your Customer' (KYC) platforms, enabling users to manage and share their customer data securely through their mobile or digital wallets. Through blockchain and SSI, 'Casper' ensured a secure, decentralized, and verifiable identity, offering applications not only in banking but also in healthcare and government sectors. This comprehensive solution enhanced data privacy, traceability, and decentralized control.

Naik et al. discussed the major criteria for evaluating self-sovereign identity (SSI) models in their research [12]. The authors pointed to the importance of open standards and forums. Such as the Organization for the Development of Structured Information Standards (OASIS), the Decentralized Identity Foundation (DIF) and the World Wide Web Consortium (W3C), for facilitating the SSI solutions. The paper described the evolution of three Identity Management (IDM) models. Those are Centralized IDM, Federated IDM and Self-Sovereign IDM. The proposed model was the Self-Sovereign IDM model, also known as IDM 3.0. This eliminates the third-party IDP and offers a direct connection between client and an organization. It also mentioned the critical issues of ownership of confidential personal data by giving the user full control using a Digital Wallet. Besides, the paper also discussed certain constraints of the Self-Sovereign Identity (SSI) model. One of the main limitations of this paper was scalability. As a collection of accepted standards and processes provided by standard organizations was necessary for the successful implementation of SSI models.

Mukta et al. discussed a blockchain-based decentralized identity management system [23]. This paper aims to address the issues of trust deficits between issuers and verifiers in the current (SSI) model. The authors presented a multi-layered issuer authorities framework, which emphasises the critical role of the Governing Body as the root authority in the chain and the Policy Authority (PA). And that is responsible for defining policies for issuance of credentials. The paper introduced the concept of 'supporting credentials' to enable personal issuers to establish trusted relationships with verifiers. Blockchain technology is leveraged to build a decentralized trust infrastructure that supports personal issuers. The proposed solution centers on resolving the trust gap in SSI systems by incorporating decentralized credential management and introducing supporting credentials for personal issuers. The paper focused on enhancing trust in SSI systems, especially through blockchain technology. Though it did not explicitly discuss the limitations of the proposed system.

Chadwick et al. proposed a conceptual model for establishing trust in self-sovereign identity (SSI). The model aims to allow users wallets that contain W3C Verifiable Credentials (VCs) to assess whether the verifier could be trusted to comply with GDPR regulations, enabling the safe sharing of personal identifying information within their VCs [27]. The authors discussed the implementation of this model using the TRAIN trust infrastructure. They also discussed how wallets could interact with verifiers using various trust infrastructures. The research highlighted the critical importance of both technical and administrative trust levels, which were enforced through cryptography and standard trust lists to ensure the integrity and reliability of the verifiable credentials. Moreover, the study emphasizes the importance of further investigation into trust in wallet software, identifying it as a promising avenue for future research and development. While the paper focused on enhancing trust in SSI verifiers, especially in the context of GDPR compliance,however, it did not explicitly discuss the limitations of the proposed model and the practical implementation of their trust model.

Jeyakumar et al. proposed a novel approach to establishing trust in verifiable credential issuers using the TRAIN infrastructure [20]. The proposed model emphasized the need for a holistic approach to trust management in self-sovereign identity (SSI) ecosystems, addressing both technical and institutional trust. The TRAIN infrastructure leveraged the Domain Name System (DNS) to enable individual and distributed trust decisions, providing a novel solution to the trust and governance challenges in SSI. The document discussed related work and initiatives in the field, such as the development of trust registry frameworks, and highlighted ongoing efforts to integrate TRAIN with other components. However, it acknowledged the limitations and future work required for the integration of TRAIN with other components, such as the VC holder, and emphasized the need for further specification by relevant foundations. The proposed model aimed to enhance the credibility of VC issuers and contribute to the establishment of trust in SSI ecosystems.

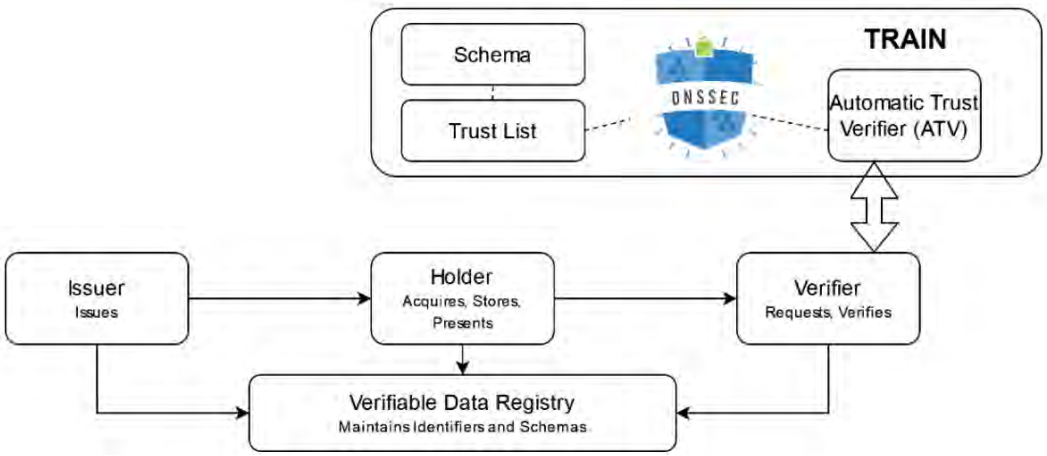


Figure 3.4: Integration of TRAIN into W3C VC SSI ecosystem [20]

The system diagram of Jeyakumar et al. (Figure 3.4) illustrates how the TRAIN (TRust mAnagement INfrastructure) operates within a Self-sovereign Identity (SSI) ecosystem [20]. The process begins with the "Issuer" who issues verifiable creden-

tials to a "Holder." The Holder is responsible for acquiring, storing, and presenting these credentials to a "Verifier," who requests and verifies the credentials. To manage trust, a "Verifiable Data Registry" maintains identifiers and credential schemas that the Holder interacts with. At the core of trust management, the TRAIN system integrates a DNSSEC-based infrastructure to ensure secure trust verification. It includes key components such as the "Schema" and a "Trust List," which are linked to an "Automatic Trust Verifier" (ATV). This verifier helps the Verifier check the authenticity of credentials by validating trust against established trust lists, ensuring a robust and decentralized trust system without the need for third-party intermediaries.

De Salve et al. proposed a multi-layer trust framework for Self Sovereign Identity (SSI) on blockchain. The framework aims to manage trust relationships among different SSI actors, including issuers, verifiers, and holders of credentials. It leverages a multilayered architecture and blockchain technology to establish, record, and verify trust relationships, enhancing the security and reliability of SSI systems [28]. The model addresses the trust requirements of verifiers by considering trust preferences expressed for specific contexts, trust relationships among all verifiers for the same context and relationships between issuers. It also incorporates the concept of a Web of Trust (WoT) to enable verifiers to rate issuers' trustworthiness and associate trust scores with particular contexts. The proposed model aims to enhance the security of SSI by supporting users' interactions, even with completely unknown entities. The paper also included a security analysis of the proposed framework, which demonstrates its ability to enhance the security of SSI with a trust evaluation scheme. Besides, a performance evaluation of the framework was also addressed. Which highlights effectiveness in managing trust relationships and supporting trustworthy decisions in various use cases.

Eer et al. proposed a decentralized trust framework for Self-Sovereign Identity (SSI), introducing a design for a trust registry along with a mechanism to facilitate a web of trust among identity issuers and verifiers [29]. The study emphasized the importance of human trust in SSI, employing a bottom-up approach to ensure the trustworthiness of the system. The model mentioned challenges in digital identity systems by motivating active and honest stakeholder participation within the trusted registry. Which offers a promising solution to manage trust relationships in a decentralized manner. However, the paper highlighted some limitations such as the need for further experimentation and evaluation of the zero-knowledge extension to their protocol. It also pointed out scalability challenges due to reliance on maintainers to preserve privacy within the directed graph and the high cost of generating non-interactive zero-knowledge proofs (ZKP). Despite all these challenges, the paper provides important insights into decentralized trust frameworks for SSI. It addressed further research to mitigate the limitations and validate the model's effectiveness.

Chapter 4

System Proposal

In this section, we introduce our proposed model (Section 4.1), a threat model (Section 4.3), and examine various functional, security, and privacy requirements (Section 4.4) for our system.

4.1 Proposed Model

We propose a Self-Sovereign Identity (SSI) blockchain model with an integrated Issuer Trust Registry as a comprehensive solution for secure, scalable, and privacy-centric identity management (Figure 5.1). Our model provides individuals with full control over their identity data while addressing critical concerns of trust, privacy, and scalability. By decentralizing identity verification processes and eliminating reliance on centralized authorities, this model mitigates risks associated with data breaches and unauthorized access.

The SSI model leverages the blockchain's cryptographic safeguards and immutable ledger, ensuring that identity records are tamper-proof and securely stored [30]. The introduction of an Issuer Trust Registry enhances the credibility of identity issuers by establishing a trusted mechanism to verify their authenticity. This approach tackles one of the significant challenges in SSI systems—ensuring that identity verifiers can trust the credentials issued, thus making the verification process more secure and reliable.

Additionally, the SSI blockchain model incorporates consent-based data sharing, empowering users to manage their personal data autonomously. Individuals can grant access to third parties only when explicitly necessary, safeguarding their privacy while adhering to legal regulations. The model's architecture is optimized for scalability, making it capable of handling nation-scale identity systems, including national identification cards, passports, driving licenses, and other crucial identity holdings (Figure 5.1). Its cost-efficient design, combined with a seamless user experience, makes this model an ideal solution for large-scale identity management systems.

Compared to traditional identity systems and existing blockchain-based solutions, this SSI model offers a more robust, privacy-preserving, and trust-driven solution for national identity management. It enhances security and user control, offering

a comprehensive framework that aligns with modern regulatory and technological demands.

4.2 Methodology

This research follows the Design Science Research Methodology (DSRM) (Figure 4.1), beginning with Threat Modeling and progressing through six stages: Requirement Analysis, System Design, System Development, Threat Mitigation, Demonstration, and Evaluation [1].

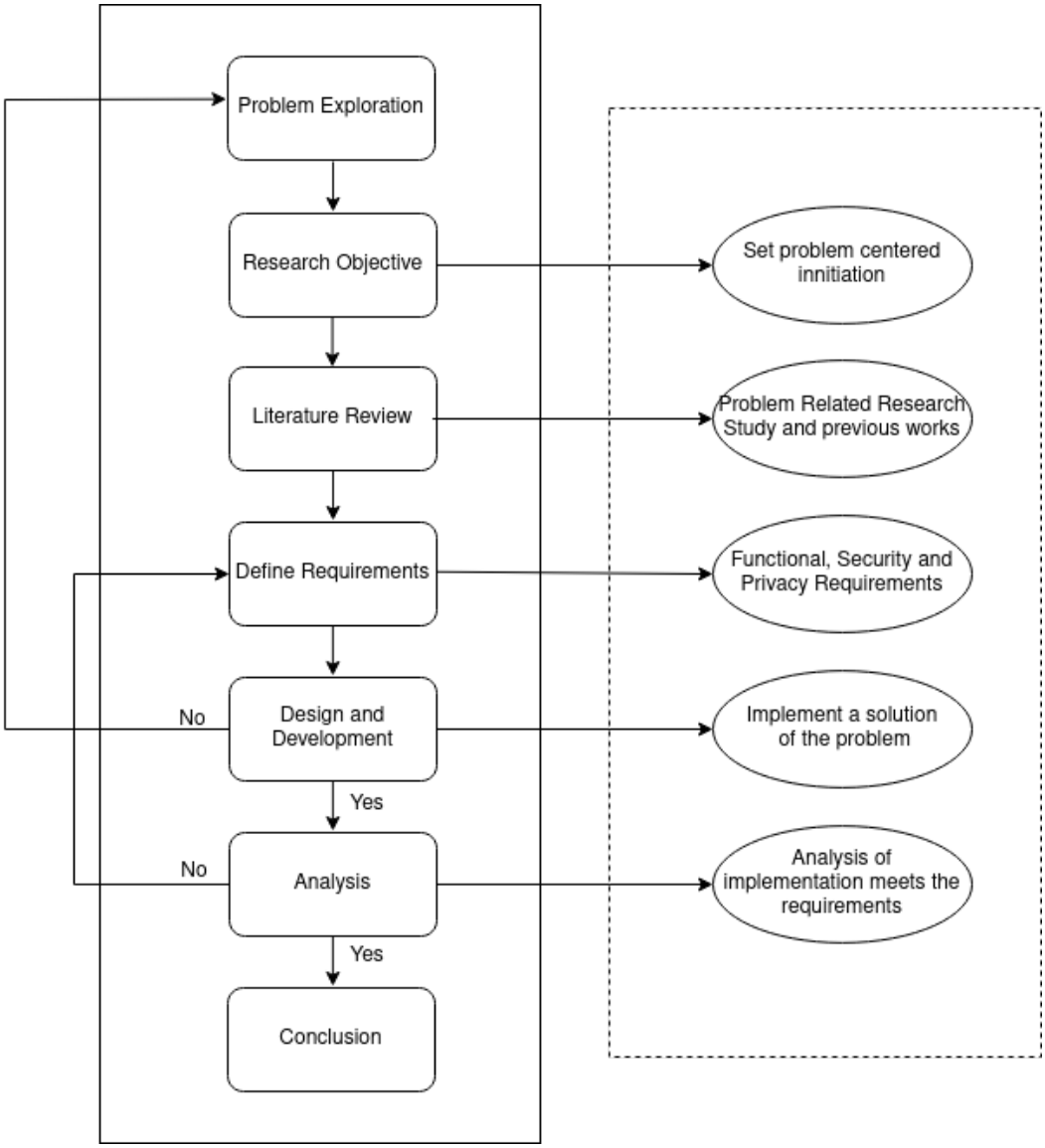


Figure 4.1: Methodology Diagram

Using the STRIDE framework, we identify potential security risks, such as Spoofing and Tampering, and address them in the SSI system architecture [2]. We define the system's functional needs, such as issuing verifiable credentials and managing decentralized identifiers, while ensuring data security and privacy through user consent (Section 4.4). The architecture is built with Issuers, Holders, Verifiers, and an Issuer Trust Registry. Blockchain technology ensures secure and decentralized

identity verification (Section 5.1). The system is implemented using the ACA-Py framework and Hyperledger Fabric (Section 5.2). Cryptographic techniques, selective disclosure, and safeguards against attacks are integrated into the framework (Section 4.4.2 and Section 4.4.3).

We represent a research methodology flowchart (Figure 4.1), outlining the steps from problem exploration to conclusion. It starts with defining the research problem, followed by research objectives, reviewing and comparing the literature review, and explaining functional, security, and privacy requirements. The design and development phase follows, where the model is implemented. Afterward, an analysis is conducted to verify if the proposed model meets the requirements. If it meets the requirements, the process concludes, otherwise, it loops back to rework the design. The right side offers a detailed understanding of each stage of the process.

4.3 Threat Modeling

We use the STRIDE threat modeling framework [2] to identify the security concerns of our system. When applying this model to an identity verification system built on Self-Sovereign Identity (SSI) principles, it's essential to account for the decentralized characteristics of SSI. Unlike traditional models that rely on a central authority, SSI empowers individuals to have full control over their digital identities. This decentralized approach introduces unique considerations for potential threats and vulnerabilities.

By examining the STRIDE framework in the context of an SSI-based identity verification system, we can address each component as follows:

T1. Spoofing: Unauthorized or out of the SSI system attackers or users attempting to impersonate authorized users (Holder).

T2. Tampering: Issuer or Verifier tampering with the data in the SSI system, potentially compromising the integrity of the NID information like leaking private DID.

T3. Repudiation: Issuer can deny or assert Holder's request.

T4. Information Disclosure: Unauthorized attackers could get an authorized user's VC metadata through the Issuer without the permission of the user.

T5. Denial of Service (DoS): Might disrupt the update and usability of the whole SSI-based system.

T6. Elevation of Privilege: Unauthorized attackers might gain higher levels of access or control within the SSI system.

Along with these, we have taken into consideration another risk that is essential for safely obtaining access to restricted online services:

T7. Replay: The Holder's request could be intercepted by an unknown attacker, who would subsequently send it later to initiate a replay attack.

Privacy threats primarily arise from the absence of user control over privacy. Based on this assumption, the identified threats are as follows:

T8. Lack of consent: VC is released without the user's agreement.

T9. Lack of controls: Users (Holder) have limited control over how specific claims are disclosed to other organizations (Verifier).

4.4 Requirement Analysis

Requirement analysis for the Self-Sovereign Identity (SSI) model is essential to precisely define the goals, functionalities, and highlights of the framework [30]. It ensures that the SSI system meets privacy, security, and usability requirements by assisting in the comprehension of the particular requirements of users. Through necessity examination, potential threats can be distinguished and addressed early in the development cycle, prompting a more compelling and easy-to-use SSI implementation.

4.4.1 Functional Requirements (FR)

The functional requirements of our proposed model are outlined in the following part:

FR1. Multiple issuers (eg. NID office, Passport office) as SSI agents must be added to the system to provide VC and DID to the requested holder (user).

FR2. The system must have a digital wallet (SSI Wallet) to store the VC and public DID for verification and maintain their digital identities.

FR3. The verifier (third-party organization) will verify users through VC using public DID.

FR4. Authentic issuers are registered in the Issuers Trust Registry, which is maintained using Hyperledger Fabric.

FR5. The verifier verifies the issuer from the previously created Issuers Trust Registry.

4.4.2 Security Requirements (SR)

We now introduce a set of security requirements aimed at mitigating the identified security threats (Section 4.3).

SR1. The system should have cryptographic authentication mechanisms, such as

decentralized identifiers (DIDs) and verifiable credentials (VC), and ensure that only the authorized user (holder) has control over their private keys (private DID). It will mitigate the T1 threat.

SR2. Leverage the cryptographic properties of DLT (Distributed Ledger Technology) or decentralized consensus mechanisms to ensure data integrity. This will mitigate the T2 threat.

SR3. Use smart contracts or digital signatures to provide non-repudiation evidence to mitigate the T3 threat.

SR4. Use selective disclosure mechanisms provided by verifiable credentials or permission mechanisms to share only the necessary information and use encryption techniques to protect sensitive data. It will mitigate the T4 threat.

SR5. The system must have to take steps to stop DoS attacks to mitigate the T5 threat.

SR6. Use a decentralized application or access control system with the least amount of privilege of user's data so that it can mitigate the T6 threat.

SR7. Replay attacks must be blocked by the system in order to solve the T7 threat.

4.4.3 Privacy Requirements (PR)

Privacy requirements play a crucial role in addressing privacy threats. We have identified only one privacy requirement, which is outlined in the following:

PR1. Every VC must only be issued if the user (Holder) has verified and given their approval, according to the system. Threats T8 and T9 are addressed by this.

Chapter 5

Architecture and Implementation

In this chapter, we discuss key components of our architecture (Section 5.1) and implementation. The model is designed to ensure secure, scalable, and privacy-centric identity management, integrating an Issuer Trust Registry to enhance the credibility of identity issuers. This approach mitigates risks associated with centralized identity systems by providing individuals with full control over their identity data, empowering them to manage and share data securely. The following section dives into the specific details of the proposed model and its architectural framework.

5.1 Architecture

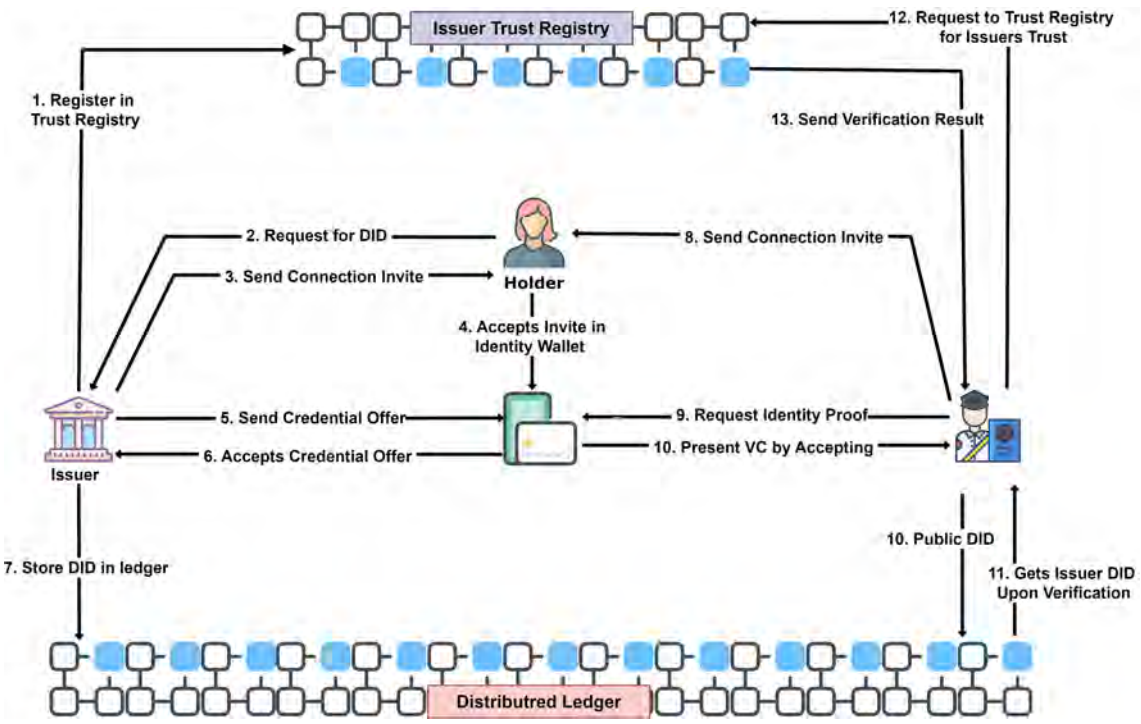


Figure 5.1: System Architecture Diagram

In the proposed Self-Sovereign Identity (SSI) model, three primary roles are involved: the Issuer, the Holder, and the Verifier, as illustrated in the system architecture (refer to Figure 5.1). In our system, the Issuer represents trusted entities such as the

government or accredited institutions responsible for issuing identity credentials. The Holder is the individual or citizen who owns and manages their digital identity, while the Verifier is a third-party organization, such as a bank or government service, that requires identity verification.

The architecture also includes three additional entities: the Identity Wallet, Distributed Ledger, and the Issuer Trust Registry. The Issuer and Verifier are connected to the Issuer Trust Registry. The Issuer Trust Registry is a distributed ledger (Hyperledger Fabric), ensuring that only trusted and verified issuers can participate in the identity issuance process, thereby addressing the trust concerns between the Issuer and the Verifier. When the Holder requests a Verifiable Credential (VC), the Issuer creates a signed VC along with the Holder's private Decentralized Identifier (DID) and issues it to the Holder. The Holder receives and stores the VC in their Digital Wallet, owning complete control over their identity data.

When the Verifier needs identity verification, the Holder presents the VC through the Digital Wallet to the Verifier. The Verifier then checks the authenticity of the signed VC by referencing the Holder's public DID, which is stored on the blockchain. Blockchain technology is structured to this process as it stores the DIDs in a tamper-proof and verifiable registry. This ensures that identity verification is secure, decentralized, and trustworthy. The system's credibility is further strengthened by validating the trustworthiness of Issuers by the Issuer Trust Registry stored on the blockchain, allowing Verifiers to rely on the authenticity and integrity of the identity data they are checking. This architecture ensures that users have full control over their data while benefiting from the security and transparency of the blockchain. The SSI model's integration with blockchain's decentralized features, cryptographic security, and immutable records addresses the scalability and security challenges of national-scale identity management. The system enhances data privacy, eliminates the risks of centralized data breaches, and ensures seamless, trusted identity verification processes.

5.2 Implementation

This implementation section focuses on the integration of the ACA-Py framework and Hyperledger Fabric to establish a decentralized and secure identity management system. Utilizing these technologies, the system allows for the creation, storage, and exchange of verifiable credentials to ensure both privacy and security in a decentralized identity network. The proposed architecture supports Self-Sovereign Identity (SSI) that enables individuals to control their identity data by maintaining trust, scalability, and resistance to data breaches.

5.2.1 ACA-Py Framework

Aries Cloud Agent Python (ACA-Py) is an open-source agent framework that is built on the Hyperledger Aries project [36]. ACA-Py provides a foundational framework to build, deploy, and manage agents which interact with decentralized identity networks (blockchain networks) to facilitate secure communication, credential issuance, and identity verification in Self-Sovereign Identity (SSI) systems. It supports key SSI

functionalities eg. verifiable credentials, digital wallets, and cryptographic proofs, making it an ideal platform for developing identity solutions that give individuals control over their data.

ACA-Py Architecture: The ACA-Py framework is designed in a modular, flexible architecture that allows for flawless integration with various decentralized identity networks. The main components of ACA-Py include:

1. Agents: In ACA-Py, an agent represents an autonomous entity able to create, store, and exchange verifiable credentials. Agents communicate with each other through secure and peer-to-peer channels.

2. Indy Ledger Interaction: ACA-Py agents interact with Hyperledger Indy, a distributed ledger purpose-built for identity management, which stores decentralized identifiers (DIDs), credential definitions, and revocation registries. This enables secure, tamper-proof verification of identity data.

3. Protocols and Messaging: ACA-Py uses the DIDComm protocol to facilitate secure message exchanges between agents. DIDComm is a decentralized communication protocol designed specifically for SSI use cases. It ensures end-to-end encryption, privacy, and secure data transfer between identity holders, issuers, and verifiers.

4. Verifiable Credentials: One of ACA-Py's primary features is its ability to issue and verify verifiable credentials (VCs), which are cryptographically signed pieces of identity information. These credentials can be presented by individuals to verify their identity without exposing unnecessary personal information.

5. Secure Storage (Wallet): ACA-Py uses a digital wallet to securely store cryptographic keys, verifiable credentials, and other personal data associated with a user's identity. These wallets ensure that users maintain full control over their identity information, which aligns with the principles of self-sovereign identity.

6. Connection Protocols: ACA-Py supports the establishment of secure, trust-based connections between entities through decentralized identifiers (DIDs). This allows individuals to manage their own connections with organizations and services, further enhancing privacy and control.

ACA-Py Properties: The ACA-Py framework was chosen for our blockchain-based personal identification system due to several key features that align perfectly with the principles and goals of Self-Sovereign Identity (SSI) [34]:

1. Decentralization and Privacy: ACA-Py enables a decentralized identity model where individuals, not centralized authorities, control their identity data. The use of verifiable credentials allows individuals to selectively share their identity information with verifiers, ensuring privacy and minimizing the risk of data exposure.

2. Interoperability: ACA-Py is built on open standards and protocols (e.g., DIDComm, verifiable credentials), ensuring that it can interoperate with other decentralized identity solutions and blockchain networks. This is critical in building a system that can scale and work across different industries and regions.

3. Secure Credential Management: The framework's support for cryptographically signed verifiable credentials ensures that identity data cannot be forged or tampered with. This makes ACA-Py highly suitable for secure identity management across various use cases, such as national identity cards, passports, driving licenses, and bank accounts.

4. Indy Ledger Integration: By leveraging Hyperledger Indy as its default ledger, ACA-Py provides a decentralized, tamper-resistant ledger for registering DIDs and storing credential schemas. This ensures that verifiers can trust the credentials presented to them without relying on a central authority.

5. Self-Sovereign Identity Support: ACA-Py inherently supports SSI through features like decentralized identifiers (DIDs) and digital wallets. This allows individuals to manage their identity credentials without the need for third-party intermediaries, reducing the risk of data breaches and enhancing personal privacy.

6. Trust Framework through Issuer and Verifier Roles: In an SSI ecosystem, trust is established through the relationships between issuers, holders, and verifiers. ACA-Py facilitates these roles by providing a secure infrastructure for credential issuance and verification. By implementing an Issuer Trust Registry, we further ensure that only trusted entities can issue credentials, and verifiers can rely on the validity of these credentials with confidence.

Role of ACA-Py in Our System: In our blockchain-based personal identification system, ACA-Py plays a pivotal role in enabling secure, decentralized management of identity credentials. The following key features of ACA-Py enhance the reliability and security of our system:

1. Credential Issuance and Verification: Through ACA-Py, government agencies or trusted institutions can issue verifiable credentials such as National Identity (NID) cards, passports, and driving licenses. These credentials can then be stored in a user's digital wallet, enabling secure identity verification during critical processes like bank account openings or land registrations.

2. Reduced Fraud and Identity Theft: By decentralizing identity data and enabling cryptographic proofs through verifiable credentials, ACA-Py reduces the risk of identity theft and fraud. Users can prove their identity without having to expose sensitive information, thereby enhancing both security and privacy.

The ACA-Py framework provides the foundational infrastructure for implementing a secure, decentralized Self-Sovereign Identity (SSI) system. Its support for decentralized identifiers, verifiable credentials, and secure communication protocols

aligns perfectly with the objectives of this research. By integrating ACA-Py into our blockchain-based personal identification system, we can offer a robust solution that enhances data privacy, security, and trust in identity verification processes, ultimately transforming how personal identity information is managed and shared in the digital age.

5.2.2 Hyperledger Fabric

Hyperledger Fabric is a permissioned blockchain framework developed as part of the Hyperledger initiative by the Linux Foundation [18]. It has a flexible, modular architecture that is appropriate for enterprises requiring secure and private transaction handling. As opposed to public blockchains, where open participation is allowed in, in Hyperledger Fabric, it follows the permissioned model. This ensures that all users are verified and authorized, thus suitable for applications that require increased control and oversight.

A key feature of the Hyperledger Fabric support for private channels. Private channels allow a selected set of participants in a network to transact in confidence, keeping the transactions private, observable only to them. Hence, Fabrics turn out to be very important in sectors related to health care, supply chain, and finance, where the data of interest needs to be kept confidential. What's more, Fabric's modular consensus lets organizations choose a consensus protocol that best works for their network, permitting flexibility to take the lead in performance, security, and scalability.

Hyperledger Fabric's support for smart contracts, referred to as chaincode, adds to its versatility by enabling the automation of business processes within secure, tamper-resistant environments. Unlike public blockchains, Fabric's modular design allows essential components such as identity management, consensus, and governance to be customized to fit the unique requirements of the organization or industry using it.

Hyperledger Fabric Architecture: Hyperledger Fabric's architecture is composed of various modular components that collaborate to deliver a secure and scalable blockchain solution:

1. Permissioned Network: The permissioned nature of Fabric provides access to the network and interaction with the network only to the verified and authorized participants. This builds trust and allows control over who views or validates the transactions.

2. Private Channels: Participants can create private channels for their confidential transactions. These channels will enable the selected members of the overall network to share data in privacy, preserving integrity by means of blockchain.

3. Smart Contracts: Chaincode is used to refer to smart contracts in Fabric. Chaincode enables developers to define the logic of the transactions that will be automatically executed in an agreement without intermediaries.

4. Pluggable Consensus Mechanism: The consensus mechanism of Fabric is modular and flexible. This feature of Fabric provides ease for an organization to select a consensus algorithm in order to meet specific performance and security requirements.

5. Scalability and Performance: Being optimized for high transaction throughput, Fabric is suited for enterprise applications in which not only speed but reliability is important.

6. DID Support: Yes, it does. Fabric supports decentralized identity models enabling participants to securely manage their identities according to the principles of privacy and user autonomy.

Role of Hyperledger Fabric in Our System: In our blockchain-based personal identification system, Hyperledger Fabric plays a critical role in enabling the secure and decentralized management of identity data through the Issuer Trust Registry [35]. The following key components illustrate how Fabric enhances the security, reliability, and scalability of the system:

1. Issuer Trust Registry: Hyperledger Fabric provides the foundation for the Issuer Trust Registry, a key component of our identity system. By leveraging Fabric's permissioned blockchain, we can ensure that only trusted entities (issuers) are allowed to register and issue credentials. This registry serves as a verification mechanism for verifiers to ensure that the credentials they receive originate from an authenticated source.

2. Decentralized and Secure Credential Issuance: Fabric's support for decentralized identifiers and verifiable credentials ensures that identity credentials issued by government agencies or trusted institutions are tamper-proof. These credentials, stored on the blockchain, can be verified securely by any participant in the network.

3. Private and Secure Communication: Fabric's private channels allow for confidential communication between the Issuer Trust Registry and verifiers, ensuring that sensitive identity data is only shared with authorized entities. This further reduces the risk of data breaches and enhances the overall privacy of the identity verification process.

4. Reduced Fraud and Tampering: By decentralizing the issuance and verification of identity credentials, Hyperledger Fabric significantly reduces the risk of fraud and identity theft. The immutability of blockchain records ensures that once a credential is issued and stored on the ledger, it cannot be altered or forged.

Hyperledger Fabric provides the essential infrastructure for implementing a secure, permissioned Issuer Trust Registry within our blockchain-based personal identification system. Its support for decentralized identities, private channels, and verifiable credentials aligns seamlessly with the objectives of Self-Sovereign Identity (SSI), enabling secure and private identity verification processes. By leveraging the strengths of Hyperledger Fabric, we have created a system that not only enhances trust and

security but also ensures the scalability and flexibility needed to accommodate various use cases across industries. Ultimately, Fabric's permissioned architecture and modularity make it the ideal platform for building a robust and trustworthy identity verification ecosystem in the digital age.

5.3 Use-case and Protocol Flow

In this section, we explore the use cases for issuing and transferring identity verification credentials within a blockchain-based personal identification system [39]. The core objective of these use cases is to demonstrate how identities are securely issued, claimed, and transferred in a decentralized environment based on Self-Sovereign Identity (SSI). The use cases address both the initial issuance of identity credentials and the subsequent verification of the credentials when required. The following scenarios outline the key activities involved in these processes:

Initiating the Connection: A secure peer-to-peer (P2P) asynchronous communication channel is established between the system entities—namely, the identity issuer, holder, and verifier—using the SSI framework. This ensures that identity details and credentials are shared securely, adhering to privacy and authentication standards.

Issuing Verifiable Credentials (VCs) to Identity Holders: Identity-issuing authorities, such as governments or accredited institutions, issue a Verifiable Credential (VC) to individuals. This VC acts as proof of the individual's identity, similar to traditional documents like passports or national IDs. The VCs are cryptographically signed and stored on a decentralized blockchain ledger, ensuring their authenticity and immutability.

Secure Storage of VCs and Claiming Attributes: The issued VC and any associated claiming attributes (e.g., keys, tokens) are securely stored in the holder's digital wallet. These wallets are cryptographically secured, preventing unauthorized access. Simultaneously, identity issuers (e.g., governments or banks) store these identity credentials on the blockchain, maintaining a decentralized record that ensures both transparency and security.

Requesting Proof of Identity: In situations where identity verification is required (e.g., opening a bank account or registering a SIM card), the verifier requests proof of the VC from the holder. The request is made through the established P2P connection, ensuring a secure and seamless verification process. This step replaces traditional authentication methods, streamlining the identity verification process while maintaining high security.

Issuer Trust Registry for Verifiable Credentials: A key challenge in the SSI model is ensuring the trustworthiness of identity issuers. The Issuer Trust Registry, a blockchain-based component, addresses this by acting as a decentralized trust layer between issuers and verifiers. Before accepting verifiable credentials, verifiers consult the registry to confirm the issuer's credibility. It is assumed that authentic issuers have been pre-approved and belong to a whitelisted consortium of trusted

entities. This ensures that identity data originates from reliable sources, mitigating the risk of fraud and enhancing the security and reliability of the entire system.

Through these use cases, this research illustrates the end-to-end processes involved in a blockchain-based identity management system. By adopting a decentralized and secure approach, the system enhances trust, privacy, and security for identity holders and verifiers alike, creating a more efficient and reliable model for personal identification in the digital age.

5.3.1 Data Model and Algorithms

Different cryptographic symbols or notations have been used throughout the proposed protocol and data model. To enhance clarity, these notations are summarized in Table 5.1.

Notation	Description
N_i	A Fresh Nonce
U	User (or Actor) requesting or holding a Verifiable Credential
MD	Mediator
I	Issuer (Entity responsible for issuing Verifiable Credentials)
Web	Website of Issuer or Verifier
W	Mobile Wallet
V	Verifier (Entity requesting proof of the verifiable credential)
B	Blockchain (Distributed ledger used to store public key data and proofs)
K_Y^X	Public Key of Y for X ; where X = $U \vee$ X = $MD \vee$ X = $I \vee$ X = V and Y= $I \vee$ Y = $MD \vee$ Y = $U \vee$ Y = V
$K_Y^{-1\|X}$	Private Key of Y for X; where X = $I \vee$X = U and Y= $U \vee$Y = I
DID_Y^X	Decentralised Identifier of Y for X
VC	Verifiable Credential (a digital document issued by an authority, containing verified attributes)
VC_Y^X	A VC issued by Y to X
F	Hyperledger Fabric
$[\ \ldots\ ]_{HTTPS}$	Indicates that the message is transmitted over HTTPS, ensuring encryption and integrity of the data
$\{\ \}\ K_Y^X$	Encryption operation using a public key
$\{\ \}\ K_Y^{-1\|X}$	Signature using a private key $K_Y^{-1\|X}$
$\{\ \}\ K_{XY}$	Encryption operation using a symmetric key K
[...]	Brackets represent the contents of a message (e.g., credentials, proofs, signatures)

Table 5.1: Cryptographic Notations

The data model shown in Table 5.2 illustrates a request-response structure that supports identity management and verification processes. This model accommodates various actions, which are grouped into requests (*req*) and their corresponding responses (*resp*). Each action carries a specific set of data points and parameters that ensure secure communication and verification within the system. The requests include six key types: *identityCreationReq*, *attributeReq*, *identityClaimReq*, *launchProofReq*, *applyForIdentityProof*, *identityProofReq*, and *DIDLookupReq*. Similarly, the system responds to these requests with the corresponding responses: *identityCreationResp*, *attributeResp*, *identityClaimResp*, *identityClaimAck*, *launchProofResp*, *identityProofResp*, and *DIDLookupResp*. Additionally, the system includes *VCVerificationResult* to provide verification results for the verifiable credentials.

- *identityCreationReq* initiates the identity creation process, containing a URL. The corresponding *identityCreationResp* returns a URL as a response.

req	$\triangleq\langle$*identityCreationReq*, *attributeReq*, *identityClaimReq*, *launchProofReq*, *applyForIdentityProof*, *identityProofReq*, *DIDLookupReq*$\rangle$
resp	$\triangleq\langle$*identityCreationResp*, *attributeResp*, *identityClaimResp*, *identityClaimAck*, *launchProofResp*, *identityProofResp*, *DIDLookupResp*, *VCVerificationResult*$\rangle$
identityCreationReq	$\triangleq\langle url_i, N_1\rangle$
identityCreationResp	$\triangleq\langle url_i, N_1\rangle$
attributeReq	$\triangleq\langle attr_1, attr_2, attr_3, ..., attr_n\rangle$
attributeResp	$\triangleq\langle(attr_1, val_1), (attr_2, val_2), (attr_3, val_3), ..., (attr_n, val_n)\rangle$
identityClaimReq	$\triangleq\langle$*Requesting Certificate, attributeResp*$\rangle$
identityClaimResp	$\triangleq\langle VC_I^U\rangle$
VC_I^U	$\triangleq\langle(attr_1, val_1), (attr_2, val_2), (attr_3, val_3), ..., (attr_n, val_n)\rangle$
identityClaimAck	$\triangleq\langle$*Credential stored in holder wallet successfully*$\rangle$
launchProofReq	$\triangleq\langle url_i, N_1\rangle$
launchProofResp	$\triangleq\langle url_i, N_1\rangle$
identityProofReq	$\triangleq\langle attr_1, attr_2, attr_3, ..., attr_n\rangle$
identityProofResp	$\triangleq\langle VC_I^U\rangle$
VC_I^U	$\triangleq\langle(attr_1, val_1), (attr_2, val_2), (attr_3, val_3), ..., (attr_n, val_n)\rangle$
DIDLookupReq	$\triangleq\langle$*IssuerDID*$\rangle$
DIDLookupResp	$\triangleq\langle$*IssuerDIDStatus*$\rangle$
VCVerificationResult	$\triangleq\langle url_i\rangle$

Table 5.2: Data Model

- *attributeReq* requests specific attributes about an identity, which includes a list of attributes $(attr_1, attr_2, \ldots, attr_n)$. The *attributeResp* contains the requested attributes in the form of attribute-value pairs ($(attr_1, val_1)$, $(attr_2, val_2)$, …, $(attr_n, val_n)$).

- *identityClaimReq* is used for requesting a verifiable credential and it utilizes data from *attributeResp*. The *identityClaimResp* provides a verifiable credential (VC) containing attributes associated with the request.

- *identityClaimAck* acknowledges that the credential has been successfully stored in the holder's wallet.
- *launchProofReq* initiates the process of launching proof of identity, where a URL are sent. *launchProofResp* provides a URL as a response to confirm the proof launch.
- *identityProofReq* requests a proof of identity, while *identityProofResp* responds with the verifiable credential (VC) as proof of identity.
- *DIDLookupReq* and *DIDLookupResp* handle decentralized identity (DID) lookup, with the former requesting the status of an issuer's DID and the latter providing the current DID status.
- *VCVerificationResult* returns a URL with the result of the verifiable credential verification process.

This data model ensures that all identity management processes within the proposed system are handled securely, utilizing decentralized identifiers and verifiable credentials. Each action either requests or delivers critical identity data, ensuring that all participants in the system can securely verify identities and associated attributes.

Next, we show some of the important functions of the VC issuance and verification process in two different algorithm snippets (Algorithm 1 and Algorithm 2).

Algorithm 1 Algorithm Snippet for `identityProofStatus` function

```
Start
...
function identityProofStatus(data)
    walletResponse ←receive response from identityProofRequest(data)
    if response then
        verified ←checkSignature(walletResponse.DID^I, walletResponse.K^I )
        if verified then
            globalAttributes ←walletResponse.VC_W^U
            fabricTrust ←globalAttributes.DID
            return True
        else
            return False
    else
        return False
    end if
end function
...
```

The algorithm snippet for the identityProofStatus function outlines the steps an issuer follows to verify an identity-proof (Algorithm 1). The process begins by getting a response from the identityProofSRequest function. This function gets data from a user's wallet. If a response is received, the algorithm checks the signature of the wallet response using a DID^I and K^I. If the verification is successful the wallet

response is assigned to a global variable. To verify the issuer the issuer's DID is passed to the fabricTrust function. The function then returns True if all checks pass; otherwise, it returns False at failure points in the process.

Algorithm 2 Algorithm Snippet for `identityProofRequest` function

```
1: Start
2: ...
3: function IDENTITYPROOFREQUEST(req, resp)
4:     requiredAttributes ←from Verifiers request body
5:     data ←presentationProofResponseTemplate(requiredAttributes)
6:     proofStatus ←proofStatus(data) if U accepts
7:     if proofStatus then
8:         revealeAttributes ←revealed attributes form wallet
9:         revealeAttributes.did ←public DID of issuer
10:        return reavealeAttributes
11:    else
12:        return False
13:    end if
14: end function
15: ...
```

The identityProofRequest function handles the verification process from the holder's end (Algorithm 2). It starts by extracting the required attributes from the verifier's request. These attributes are then packaged into a proofResponseTemplate following schema. The function proceeds by checking the status of the proof using the provided data. If the proof is valid, it extracts the revealed attributes from the wallet. It also includes the public DID^I of the issue. It returns these attributes. If the proof status check fails, the function returns False, indicating an unsuccessful verification process.

5.3.2 Protocol Flow for Issuing Verifiable Credential

In this use-case, we outline the steps for issuing a Verifiable Credential (VC) to U, with interactions between several entities: the User U, the *Web*, the Mediator *MD*, and the Issuer I. The detailed protocol flow of this section is presented in Table 5.3. Each step corresponds to the technical notation outlined in Table 5.1. We denote the steps as $M1$ to $M8$.

1. U initiates the process by sending an identity creation request, *identityCreationReq*(url) to the *Web*. This request is made over a secure HTTPS connection, as indicated by HTTPS (M1 in Table 5.3).

2. *Web* responds to U's request by returning an identity creation response, *identityCreationResp*(url) over HTTPS (Figure 5.2). This establishes a secure identity creation session between U and *Web* (M2 in Table 5.3).

M1	$U \rightarrow Web : [N_1, \textit{identityCreationReq(url)}]_{\text{HTTPS}}$
M2	$Web \rightarrow U : [N_1, \textit{identityCreationResp(url)}]_{\text{HTTPS}}$
M3	$U \rightarrow MD : [I, \{N_2, \textit{identityClaimReq}\}_{K_I^U}]_{K_{MD}^U}$
M4	$MD \rightarrow I : [\{N_2, \textit{identityClaimReq}\}_{K_I^U}]_{K_I^{MD}}$
M5	$I \rightarrow MD : [U, \{N_2, \textit{identityClaimResp}\}_{K_U^I}]_{K_{MD}^I}$
M6	$MD \rightarrow U : [\{N_2, \textit{identityClaimResp}\}_{K_U^I}]_{K_U^{MD}}$
M7	$U \rightarrow MD : [I, \{N_2, \textit{identityClaimAck}\}_{K_I^U}]_{K_{MD}^U}$
M8	$MD \rightarrow I : [\{N_2, \textit{identityClaimAck}\}_{K_I^U}]_{K_I^{MD}}$

Table 5.3: Getting VC from the Issuers

3. U generates an identity claim request, *identityClaimReq* containing identity information and encrypts it with public keys of both the Issuer I (K_I^U) and MD (K_U^{MD}). This encrypted request is then sent to MD, ensuring confidentiality and integrity of the claim data (M3).

4. MD forwards the identity claim request *identityClaimReq* to the Issuer I (M4). The request contains the identity information encrypted with K_I^{MD}, ensuring that I can securely validate the request.

5. The Issuer I validates the identity claim and responds by generating an identity claim response *identityClaimResp* (M5). The response is encrypted to ensure confidentiality. This response is sent back to MD (Figure 5.3).

6. MD forwards the encrypted identity claim response *identityClaimResp* to U (M6). The response is encrypted, which ensures that only U can decrypt and read the response (Figure 5.4).

7. After verifying the identity claim, U sends an identity claim acknowledgment *identityClaimAck* back to MD (M7). This acknowledgment is encrypted ensuring that I can validate the acknowledgment (Figure 5.4).

8. MD forwards the identity claim acknowledgment *identityClaimAck* to the Issuer I (M8). This step concludes the protocol, confirming that U has received and validated the issued identity credential (Figure 5.6).

Figure 5.6: Credential Delivered

Now, U has successfully completed the VC issuance process and got a VC, with all identity claims securely exchanged and acknowledged (Figure 5.5).

Figure 5.2: Issuer Invitation

5.3.3 Protocol Flow for User Identity Verification

In this section, we describe the protocol flow for verifying a Verifiable Credential (*VC*) of a user. The process involves the User U, the *Web*, the Verifier V, and the Mediator *MD*. The detailed protocol flow of this section is presented in Table 5.4. Each step corresponds to the cryptographic notation outlined in Table 5.1, every step is denoted by M1 to M8.

M1	$U \rightarrow Web : [N_1, \textit{launchProofReq(url)}]_{\text{HTTPS}}$
M2	$Web \rightarrow U : [N_1, \textit{launchProofResp(url)}]_{\text{HTTPS}}$
M3	$U \rightarrow Web : [N_1, \textit{applyForIdentityProof(url)}]_{\text{HTTPS}}$
M4	$V \rightarrow MD : [U, \{N_2, \textit{identityProofReq}\}_{K_U^V}]$
M5	$MD \rightarrow U : [\{N_2, \textit{identityProofReq}\}_{K_U^V}]$
M6	$U \rightarrow MD : [V, N_2, \{\text{identityProofResp}\}_{K_V^U}]$
M7	$MD \rightarrow V : [N_2, \{\text{identityProofResp}\}_{K_V^U}]$
M8	$V \rightarrow U : [N_3, \textit{submitIdentity(url)}]_{\text{HTTPS}}$

Table 5.4: Identity Verification by Verifier

1. U initiates the verification process by sending a proof request *launchProofReq*(url) to the verifier's website (*Web*). This request is made over a secure HTTPS connection (M1 in Table 5.4).

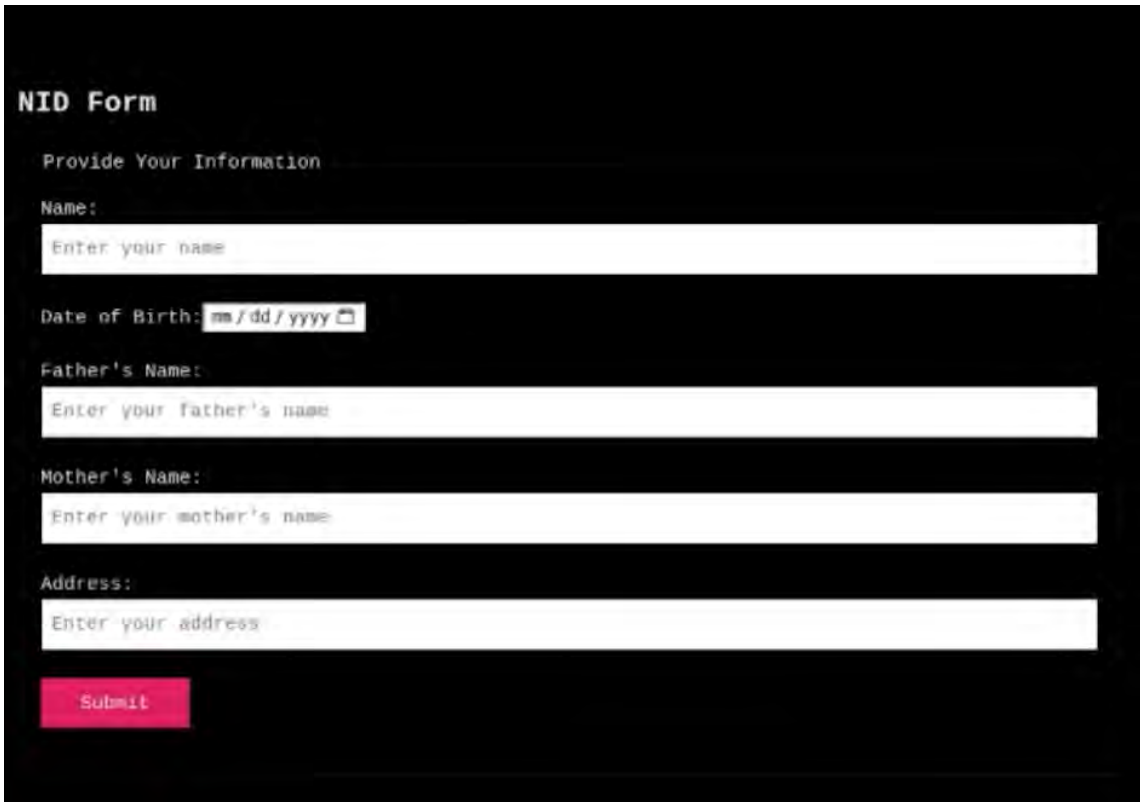


Figure 5.3: NID Form

2. *Web* responds by sending a proof response *launchProofResp*(url) to U over HTTPS. This establishes a session between U and *Web* for proof generation (M2 in Table 5.4).

3. U sends an application for identity proof *applyForIdentityProof*(url) to *Web* (Figure 5.7), initiating the proof generation process over HTTPS (M3).

4. V sends an identity proof request *identityProofReq* to *MD*, containing identity information encrypted with the public key of the User K_U^V (Figure 5.8). This ensures that the identity proof request is securely transmitted (M4).

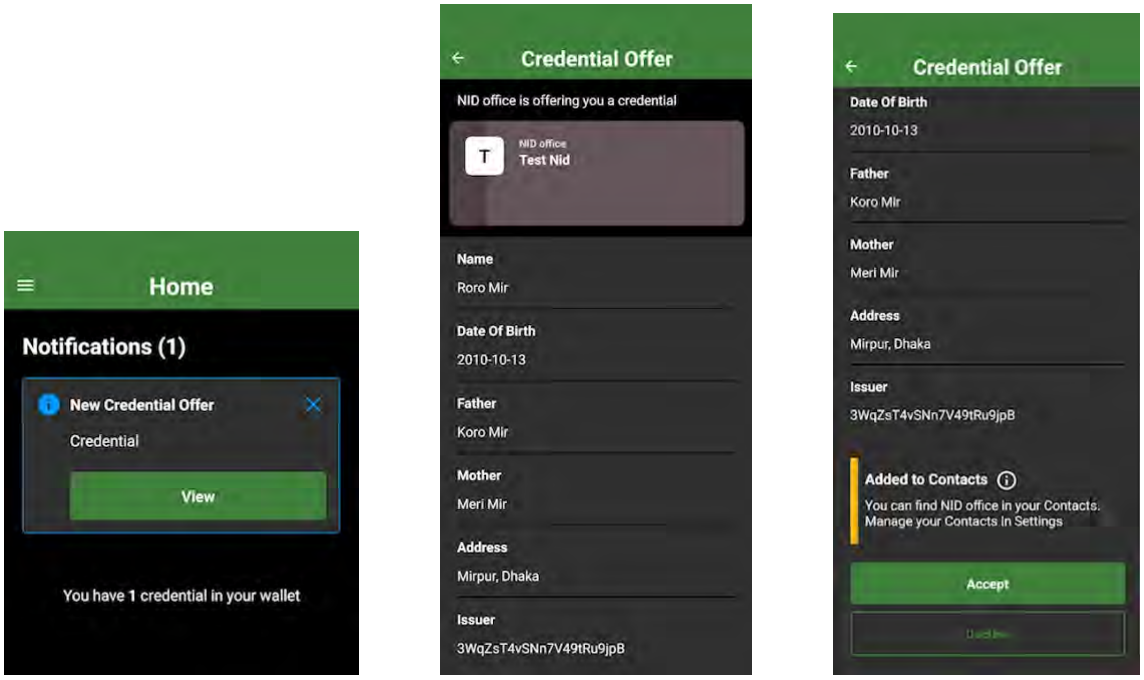
5. *MD* forwards the identity proof request *identityProofReq* to U, encrypted with the public key of U (K_U^V), ensuring that only U can decrypt it (M5).

6. U responds to *MD* with the identity proof response *identityProofResp* (Figure 5.9), verifying that U has the credentials requested by V (M6).

7. *MD* forwards the identity proof response *identityProofResp* back to V, ensuring the integrity and authenticity of the response by encrypting it with K_I^{-1} (M7).

8. V sends the identity submission response *submitIdentity*(url) to U, completing the verification process over HTTPS. The proof of identity has now been securely verified (M8).

Now, U's identity has been successfully verified, and the Verifier V can confidently accept the Verifiable Credential VC as proof of identity.



(a) Issued Credential Notification

(b) Check Issued Credential

(c) Accept/Deny Issued Credential

Figure 5.4: Issued Credential in Wallet

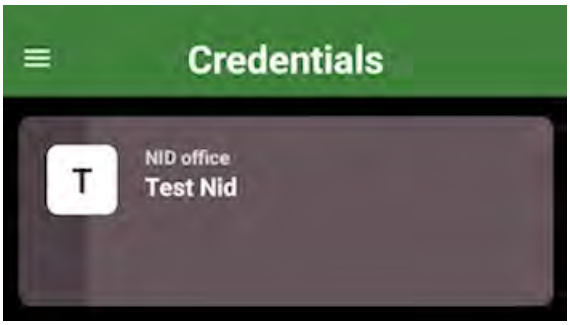


Figure 5.5: Accepted Issued Credential in the Wallet

5.3.4 Protocol Flow for Issuer Authenticity Verification

In this use case, we outline the steps for Issuer Trust Verification, with interactions between several entities: the User U, the Verifier, and the Hyperledger Fabric F. The detailed protocol flow of this section is presented next in Table 5.5.

1. The user (U) presents a verifiable credential (VC) to the verifier (V). This presentation typically contains the URL of the VC, which allows the verifier to access and validate it through an HTTPS request and get the Issuer's DID ($launchProofReq$(url)) (M1 in Table 5.5). This DID will be used to further verify the trustworthiness of the issuer by interacting with a trusted fabric ledger.

2. The verifier (V) sends a lookup request to the Hyperledger Fabric (F) to query the status of the issuer's DID ($DIDLookupReq$) (M2 in Table 5.5). This request is made over HTTPS, containing the issuer's DID as the parameter.

Figure 5.7: Invitation from Verifier

M1	$U \rightarrow V : [VCPresentation(\text{url})]_{HTTPS}$
M2	$V \rightarrow F : [DIDLookupReq, IssuerDID]_{HTTPS}$
M3	$F \rightarrow V : [DIDLookupResp, IssuerDIDStatus]_{HTTPS}$
M4	$V \rightarrow U : [VCVerificationResult(\text{url})]_{HTTPS}$

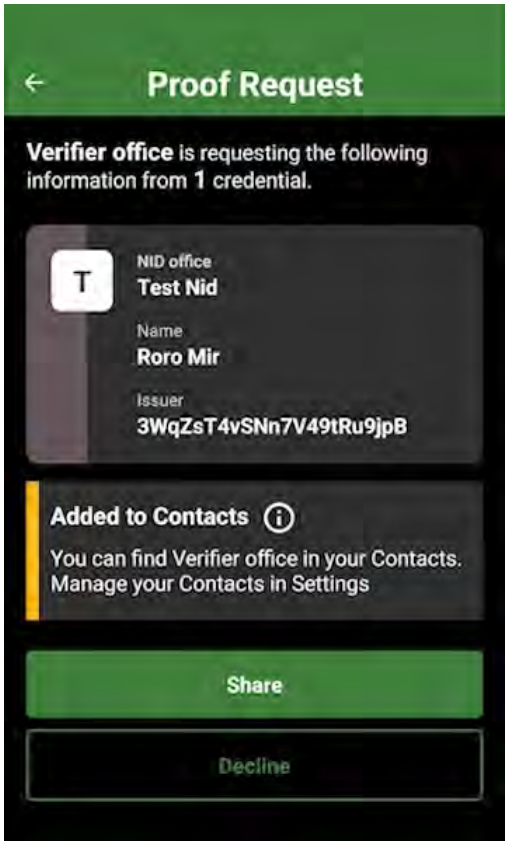
Table 5.5: Issuer Trust Verification Protocol using Fabric Ledger with HTTP(S)

3. The Hyperledger Fabric (F) responds to the verifier (V) with the result of the lookup request (*DIDLookupResp*) (M3). This response contains the status of the issuer's *DID* (*IssuerDIDStatus*), which confirms whether the issuer is trusted and recognized by the ledger.

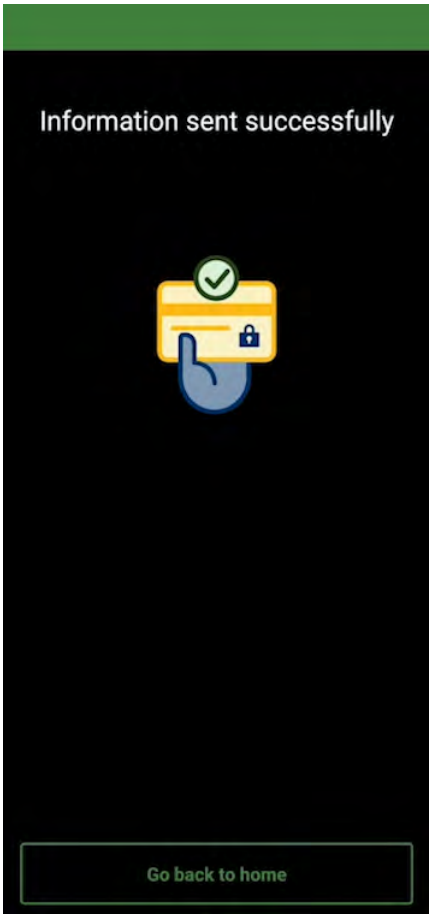
4. The verifier (V) returns the verification result to the user (U) via an HTTPS request (*VCVerificationResult*(url)) (M4). The result includes a URL indicating the verification outcome, which informs the user whether the presented *VC* has been successfully verified.

This protocol flow ensures that the verifier can check the trustworthiness of the issuer itself of a verifiable credential using a Hyperledger Fabric ledger, ensuring security and trust through an Issuer Trust Registry-based system.

Figure 5.8: Verifier Proof Request



(a) Share/Decline Proof Request



(b) Shared Identity Successfully

Figure 5.9: Share/Decline Proof Request

Chapter 6

Discussion

In the following section, we discuss the functional, security, and privacy requirements which are necessary for the successful implementation of the Self-Sovereign Identity (SSI) model. The analysis shows the essential features that ensure the system's scalability, security, and privacy while addressing potential security threats and challenges. Each requirement is tied to specific properties of the system architecture, providing a comprehensive framework for secure identity management and verification.

6.1 Requirements Analysis

The requirements analysis describes the key functionalities and security measures needed for developing a robust decentralized identity system (Chapter 4). This analysis focuses on making sure that the system meets its goals of secure, user-controlled identity verification while addressing privacy and security concerns. In the following section, we will get details of the specific functional requirements that the system must satisfy to ensure its operational success.

6.1.1 Functional Requirements (FR)

The main goal of this thesis was to develop a more secured and scalable decentralized identity verification system using Self-Sovereign Identity (SSI). The functional requirements (FRs) outlined in Section 4.4.1 in Chapter 4 aims at enhancing identity verification while maintaining privacy and security. The proposed solution successfully met these requirements through the use of verifiable credentials (VCs), decentralized identifiers (DIDs), and cryptographic mechanisms.

FR1. We can see in the protocol flow from Table 5.3 that our proposed system satisfies this requirement. Multiple issuers (eg. NID office, Passport office) as SSI agents can be added to the system to provide VC and DID to the requested holder (user) which is shown in the figure 5.2 to 5.6.

FR2. Figure 5.5 satisfies that the system has a identity wallet (SSI Wallet) to store the VC and public DID for verification and maintain their digital identities.

FR3. Protocol flow from Table 5.4 satisfies this requirement. The verifier (third-

party organization) can verify users through VC using public DID which is shown in Figure 5.7 to 5.9.

FR4 and FR5. Our proposed model also satisfies this requirement from Table 5.5

6.1.2 Security Requirements (SR)

This section outlines the security requirements (SR) necessary to safeguard the system against various security threats (Section 4.4.2). These requirements are designed to ensure the integrity, authenticity, and confidentiality of data.

SR1. To address SR1, the system has cryptographic authentication mechanisms, such as decentralized identifiers (DIDs) and verifiable credentials (VC), and ensures that only the authorized user (holder) has control over their private keys (private DID) as shown in Table 5.3 and Table 5.4.

SR2. Regarding SR2, leverage the cryptographic properties of DLT (Distributed Ledger Technology) or decentralized consensus mechanisms to ensure data integrity as shown in Table 5.3 and Table 5.4.

SR3. Use smart contracts or digital signatures to provide non-repudiation evidence in Figure 5.3.

SR4. Regarding this, use selective disclosure mechanisms provided by verifiable credentials or permission mechanisms to share only the necessary information and use encryption techniques to protect sensitive data from Table 5.5.

SR5. To address SR5, multiple precautionary measures should be implemented because initiating a DoS (Denial of Service) attack does not necessarily rely on any vulnerabilities in the application or network. This type of attack can target any web service, so as a preventative measure, developers should employ various strategies during implementation. However, this is beyond the scope of our research.

SR6. Regarding SR6, it is essential to adopt and deploy an access control mechanism, especially when services are intended to be accessed by authorized users. Since our research does not focus on utilizing device features or services, this threat is not considered in our research.

SR7. Lastly, to mitigate SR7, nonces have been incorporated at all steps in each use case.

6.1.3 Privacy Requirements (PR)

This section details the privacy requirements (PR) necessary to protect user privacy within the proposed protocol (Section 4.4.3). These requirements focus on ensuring that personal information is handled securely and only shared with authorized parties.

PR1. In the proposed protocol, users must first send a claim request to the manufacturers before receiving a Verifiable Credential (VC). Additionally, legitimate owners are required to request a verifier for verification. This ensures compliance with PR1 as shown in Figure 5.4 and Figure 5.9.

6.2 Research Objectives Analysis

This study's objective is to investigate the conclusions drawn from the research, which have been carefully examined in order to ascertain whether a blockchain identity verification system is feasible and possible, as well as how it might enhance security, privacy, and trust in a decentralized approach.

The main focus was to test the theory of incorporating blockchain technology into identity management systems to eliminate problems like identity theft, data hacks, and privacy issues. This research has shown using a formal methodology that self-sovereign identity (SSI) frameworks allow individuals to have more control over their personal information and how it is used and compensates for the deficiencies in centralized systems (Section 1.3).

The first objective RO1, which aimed at enhancing identity verification and reducing fake identities, was successfully approached by employing blockchain's immutability and cryptographic features (Table 5.2). The introduction of the Issuer Trust Registry further solidified trust in the verification process, ensuring that credentials issued by trusted entities remain secure and verifiable without relying on centralized authorities which satisfies RO4 (Section 5.3.4).

The study also looked at how giving consumers more control over their data improves security and privacy. With the integration of consent-based access controls into the SSI infrastructure, users can now manage their personal information and define who can access it without authorization and under what conditions, effectively meeting RO3 (Figure 5.4 and Figure 5.9). Regarding privacy concerns and unauthorized access by third parties, that has been of great assistance.

Our model addresses the limitations of existing identity verification systems by leveraging the principles of Self-sovereign Identity (SSI) and decentralized technologies consistent with RO2. Traditional models often rely on centralized authorities for identity verification, which can result in single points of failure, data leakage, and privacy issues (Table 5.5). In contrast, our model provides more privacy, user control, and security by allowing users to manage and share their identities without intermediaries.

The last goal (RO5) of data being immutable and tamper-proof identity systems was also covered well. Using blockchain technology the research created a trustworthy and hacker-proof structure, so once the identity information is stored it cannot be changed or corrupted.

In conclusion, the research goals were achieved through the use of technical solutions

and the use of SSI ideals, which has led to a more secure, open, and user-friendly way of identity verification.

6.3 Advantages

The identity verification process using a Self-Sovereign Identity (SSI) with Issuer Trust Registry system offers several key advantages, as described in the following part:

User Autonomy: SSI grants individuals complete control over their digital identities, enabling them to create, manage, and share their identity data independently, without relying on central authorities or issuing organizations. This gives users greater control over their privacy and personal data.

Privacy: SSI's architecture is designed with privacy at its core. Users can selectively reveal only the necessary parts of their data during a specific interaction while withholding other personal information.

Security: SSI uses cryptographic methods to ensure the security and integrity of identity data. By employing public-private key pairs, it becomes highly resistant to tampering or fraud, thereby enhancing the security of digital identity verification processes.

Reduced Friction and Correlation: SSI allows individuals to use unique identifiers, like Decentralized Identifiers (DIDs), in different contexts, reducing the possibility of linking their activities across various platforms. This minimizes data correlation and improves the user experience by reducing friction.

Automated Verification Process: SSI facilitates an automated verification process through distributed identity systems, eliminating the need for manual checks, third-party intermediaries, or even issuer organizations. This enhances the system's security, privacy, efficiency, and overall user experience.

Issuer's Trust: In this identity verification system, an issuer trust registry plays a vital role in ensuring that only trusted entities issue verifiable credentials, further strengthening the system's integrity.

6.4 Challenges and Limitations

The current identity verification system faces several challenges, as outlined next:

1. The user's wallet plays a vital role, as it stores all Verifiable Credentials (VCs) and connections. Therefore, a secure backup mechanism is essential.

2. While Self-Sovereign Identity (SSI) systems aim to give users more control and autonomy over their data, many solutions can be complex or unclear, especially for non-technical users, leading to barriers to adoption.

3. The system relies on external Aries services and Fabric services, such as distributed ledgers or cloud agents, which may introduce potential points of failure or create dependency issues.

6.5 Comparison with Existing Relevant Research Studies

A remarkable property of our proposed approach is the adoption of the STRIDE model for threat analysis, which is unique among the works compared. The majority of the existing works, such as those by Belchior et al. [9], Htet et al. [11], and others, either do not specify the threat model or do not fully satisfy this aspect. The STRIDE model, mentioned in our work, addresses various threat categories systematically, providing a more comprehensive security analysis. In terms of security requirements, our proposed approach satisfies all the key security demands, similar to Belchior et al. [9], Htet et al. [11], and George et al. [32]. However, approaches like those from Naik et al. [12] and Jeyakumar et al. [20] fail to satisfy these requirements comprehensively. Our discussed security requirements make it more favorable for handling complex identity verification scenarios and make it strong against vulnerable security loopholes. Our proposal also ensures that functional and privacy requirements are fully met, similar to the majority of the existing approaches. It is found that Jeyakumar et al. [20] only partially satisfy these functional requirements. Our comprehensive focus on privacy requirements ensures minimal sensitive identity data exposure, thereby enhancing the safety of identity information compared to some previous works.

Another unique feature of our proposed approach is its implementation of the Issuer Trust Registry. While Jeyekumar et al. [20] and Chadwick et al. [27] also incorporate this aspect, many of the other approaches leave it unspecified. This trust registry strengthens the SSI identity verification system by creating a list of authentic and trusted issuers. Minimal data disclosure is another property where our proposed approach presents a clear advantage to prevent privacy violations and sensitive data leaking. Unlike some earlier studies, which either do not specify for example, Chalaemwongwan et al. [4] or do not fully satisfy this area, our proposed model ensures that only the necessary information is disclosed during the verification process. This contributes to enhanced user privacy. Lastly, in terms of use cases, our proposed approach supports a broader range of applications in the real world, including personal identity verification with different types of identity documents like NID, Passports, etc., and authentic issuer trust, combining the strengths of previous research while addressing their limitations.

In the following Table 6.1 provides a more clear analytical comparison of existing research papers on identity verification, focusing on some attributes such as the threat model, security requirements, privacy concerns, and core technologies needed. The table also shows specific use cases, allowing a clear understanding of the differences between methodologies and their applications. This comparison presents both the similarities and contributions of our proposed approach with other existing

research. Inside the Table 6.1, the '●' symbol is used to signify that a certain property is satisfied by the respective research, the '◐' signifies that a certain property is partially satisfied by the respective work, the '○' symbol signifies that the research does not satisfy the property and lastly '-' symbol signifies unspecified.

Table 6.1 illustrates that our thesis proposes a more reliable and secure identity verification mechanism using the Issuers Trust Registry with a detailed protocol flow. The proper integration of SSI ensures that this approach is user-centric, with users having ultimate control over their sensitive identity data that can be securely managed and verified.

Now in another Table 6.2, we will analyze the system architecture in detail with the papers that align with our proposed approach. Htet et al. [11], Naik et al. [12] and Chadwick et al. [27] did not provide any specific system architecture diagram in their paper. So, we are analyzing the rest of the paper's system architecture in the presented Table 6.2 which serves as a comparative analysis taking into concern key components, trust models, data handling, and storage, core technology requirements, blockchain integration, and privacy mechanisms. This analysis evaluates the approaches of different studies alongside our proposed architecture, focusing on both similarities and distinctions.

In terms of key components, existing proposed architectures emphasize some discrete features, such as the Access Control Engine, Trust List, and Digital Wallet. Our proposed architecture distinguishes itself by incorporating both the Issuer Trust Registry and the Identity Wallet, suggesting a more comprehensive system for managing digital identities. This integration proposes a clear understanding of identity management and verification where users gain control over their personal identity information while facilitating trusted identity verification.

All existing architectures adopt a Self-Sovereign Identity (SSI) framework regarding the trust model. However, variations exist concerning access control mechanisms and external dependencies, such as the inclusion of DNSSEC. Our proposed architecture aligns with the SSI model and introduces the Issuer Trust Registry, which enhances trust through a structured decentralized ledger system. This addition aims to enhance user confidence by providing a transparent and reliable framework for identity verification maintaining the issuers' trust.

When examining data handling and storage, the architectures show different approaches. Some architectures utilize distributed systems and public ledgers, while others focus on user-controlled data. Our proposed architecture emphasizes a user-centric approach by recommending system data storage within a decentralized ledger while simultaneously maintaining identity data within the Identity Wallet. This duality ensures both transparency and user control, addressing critical concerns surrounding data privacy and ownership.

The analysis of blockchain integration reveals that some architectures incorporate blockchain technology, while others do not. Our proposed architecture asserts its use of blockchain, ensuring decentralization and data immutability which is one of

the main goals of our research. This commitment to blockchain technology not only enhances security but also aligns with up-to-date trends in digital identity management.

	Chalaemwongwan et al. [4]	Belchior et al. [9]	Htet et al. [11]	Naik et al. [12]	Jeyakumar et al. [20]	Chadwick et al. [27]	George et al. [32]	Our Proposed Approach
Threat Model	○	◐	○	○	○	○	○	STRIDE (●)
Security Requirements	●	●	●	○	○	○	●	●
Functional Requirements	●	●	●	○	◐	●	●	●
Privacy Requirements	○	●	●	●	●	○	●	●
Protocol Flow Design	●	○	○	○	○	●	○	●
Issuer Trust Registry	○	○	○	○	●	●	○	●
Minimal Data Disclosure	○	●	○	-	●	●	●	●
SSI	○	●	○	●	●	●	●	●
Core Technology Needed	NIDBC [4]	Hyperledger Indy	Ethereum	-	TRAIN [20]	TRAIN [27]	Hyperledger Indy	Hyperledger Aries, Hyperledger Fabric
Use Cases	National Digital ID System	Cross Organizational Access Control	Passport Verification	Digital Wallet	Credential Trust Management	Verifier Trust Management	Health Verification System	Personal Identity Verification, Authentic Issuer Trust

Table 6.1: Comparison with the Existing Research on Identity Verification

	Chalaemwongwan et al. [4]	Belchior et al. [9]	Jeyakumar et al. [20]	George et al. [32]	Our Proposed Architecture
Key Components	-	• Access Control Engine	• Trust List	• Digital Wallet	• Issuer Trust Registry • Identity Wallet
Trust Model	-	• SSI • Access Control Engine	• SSI • DNS with DNSSEC	• SSI	• SSI • Issuer Trust Registry
Data Handling and Storage	-	• DID Stored in Public Ledger • User Controlled Data	• Distributed via Web • JSON Schemas • No Blockchain	• Server outside of SSI Framework	• DID Stored in Public Ledger • Identity Data in Identity Wallet
Core Technology Needed	• NIDBC [4]	• Hyperledger Indy	• TRAIN [20]	• Hyperledger Indy	• Hyperledger Aries • Hyperledger Fabric
Blockchain	Yes	Yes	No	Yes	Yes
Privacy Mechanisms	Same as Our Architecture	Same as Our Architecture	Verification Through DNSSEC with Less Emphasis on Cryptography	Same as Our Architecture	Cryptographic Verification with Public-Private Key Encryption

Table 6.2: Comparison with the Existing System Architectures

Therefore, our proposed architecture represents a strong system architecture that effectively integrates advanced features, such as the Issuer Trust Registry and Identity Wallet, combined with blockchain technology and strong privacy mechanisms. This complete approach not only aligns with modern identity management practices but also addresses the limitations observed in existing architectures. As a result, it represents an optimistic solution for future implementations within digital identity ecosystems.

6.6 Future Work

The following outlines potential future enhancements aimed at improving the functionality, security, and scalability of the proposed system. The planned developments address existing limitations, expand the system's capabilities, and explore new use cases. Key areas for future work include:

1. At present, our proposed system supports verifying only one credential at a time. However, as the need for simultaneous verification of multiple Verifiable Credentials (VCs) grows, the concept of Verifiable Presentations (VPs) offers an effective solution [40]. VPs enable secure, efficient verification of multiple credentials in a single interaction. In the future, we plan to integrate VPs into our wallet, allowing users to verify multiple identity credentials with a single click, enhancing both the verification process and data security through user-controlled, privacy-preserving mechanisms.

2. Currently, if a user's wallet is lost, the Verifiable Credentials (VCs) stored within it are also lost. Therefore, it is crucial to implement a secure backup and recovery process for VCs, ensuring that they can be restored even if the wallet is lost. We plan to integrate this feature into our wallet in the future.

3. In the current approach, we assume that authentic issuers will be whitelisted within the consortium through an offline verification process. In the future, a detailed onboarding policy for the consortium will be introduced.

4. The system can be confusing for non-technical users, it can be researched further for a better understanding of user experience.

Chapter 7

Conclusion

This research has proposed a blockchain-based system architecture for decentralized identity verification based on the Self-Sovereign Identity principles integrated with an Issuer Trust Registry. Using blockchain technology, our presented system is able to mitigate the traditional identity management systems' deficits in data breach risk, identity theft, and centralized control of sensitive personal data.

Our system will ensure the following security and privacy features; decentralization, crypto protections, and the ability to store Decentralized Identifiers (DIDs) on a tamper-proof ledger. Based on the combined use of different cryptographic mechanisms, such as verifiable credentials and secure channel protocols, we have presented how more control can be given to the user in SSI systems over his identity data. Furthermore, thanks to the presence of the Issuer Trust Registry, we ensure that only checked and qualified entities grant credentials, thus allowing an enhancement in the trustworthiness of an identity assurance process.

Despite all of the prior advantages, some of the challenges and limitations include it might isolate non-technical users through the underlying system's complexity, being dependent on third-party services like Aries and Hyperledger Fabric, and requiring secure backup mechanisms for identity wallets. These challenges merely point out the need for further research and development in terms of use and the reduction of technical barriers.

In conclusion, this study reinforces the potential of blockchain technology to transform identity verification by enhancing security, reducing fraud, and protecting privacy. Our proposed system sets the stage for future research on usability and broader adoption in various sectors, such as healthcare, banking, and government services. As the field of digital identity management continues to evolve, blockchain-based SSI systems stand out as a promising solution to address both current and upcoming challenges in identity security.

Bibliography

[1] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "A design science research methodology for information systems research," *Journal of management information systems*, vol. 24, no. 3, pp. 45–77, 2007.

[2] A. Shostack, *Threat modeling: Designing for security*. John Wiley & Sons, 2014.

[3] Oct. 2016. [Online]. Available: https://www.bbc.com/news/world-asia-india-37725187.

[4] N. Chalaemwongwan and W. Kurutach, "A practical national digital id framework on blockchain (nidbc)," in *2018 15th International Conference on Electrical Engineering/Electronics, Computer, Telecommunications and Information Technology (ECTI-CON)*, 2018, pp. 497–500. DOI: 10.1109/ECTICon.2018.8620003.

[5] T. T. A. Dinh, R. Liu, M. Zhang, G. Chen, B. C. Ooi, and J. Wang, "Untangling blockchain: A data processing view of blockchain systems," *IEEE transactions on knowledge and data engineering*, vol. 30, no. 7, pp. 1366–1385, 2018.

[6] Z. Zheng, S. Xie, H.-N. Dai, X. Chen, and H. Wang, "Blockchain challenges and opportunities: A survey," *International journal of web and grid services*, vol. 14, no. 4, pp. 352–375, 2018.

[7] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, "Dns-idm: A blockchain identity management system to secure personal data sharing in a network," *Applied Sciences*, vol. 9, no. 15, p. 2953, 2019.

[8] N. Alilwit, "Authentication based on blockchain," in *2020 IEEE 39th International Performance Computing and Communications Conference (IPCCC)*, 2020, pp. 1–6. DOI: 10.1109/IPCCC50635.2020.9391553.

[9] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, "Ssibac: Self-sovereign identity based access control," in *2020 IEEE 19th International Conference on Trust, Security and Privacy in Computing and Communications (TrustCom)*, 2020, pp. 1935–1943. DOI: 10.1109/TrustCom50675.2020.00264.

[10] P. Datta, A. Bhowmik, A. Shome, and M. Biswas, "A secured smart national identity card management design using blockchain," in *2020 2nd International Conference on Advanced Information and Communication Technology (ICAICT)*, 2020, pp. 291–296. DOI: 10.1109/ICAICT51780.2020.9333487.

[11] M. Htet, P. T. Yee, and J. R. Rajasekera, "Blockchain based digital identity management system: A case study of myanmar," in *2020 International Conference on Advanced Information Technologies (ICAIT)*, IEEE, 2020, pp. 42–47.

[12] N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in *2020 8th IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (MobileCloud)*, 2020, pp. 90–95. DOI: 10.1109/MobileCloud48802.2020.00021.

[13] R. Páez, M. Pérez, G. Ramírez, J. Montes, and L. Bouvarel, "An architecture for biometric electronic identification document system based on blockchain," *Future Internet*, vol. 12, no. 1, p. 10, 2020. DOI: 10.3390/fi12010010. [Online]. Available: http://dx.doi.org/10.3390/fi12010010.

[14] E. Bandara, X. Liang, S. Shetty, and K. De Zoysa, "A blockchain and self-sovereign identity empowered digital identity platform," in *2021 30th International Conference on Computer Communications and Networks (ICCCN)*, IEEE, Jul. 2021, pp. 1–9.

[15] M. Kubach and H. Roßnagel, "A lightweight trust management infrastructure for self-sovereign identity," 2021.

[16] S. Mahula, E. Tan, and J. Crompvoets, "With blockchain or not? opportunities and challenges of self-sovereign identity implementation in public administration," *DG.O2021: The 22nd Annual International Conference on Digital Government Research [Preprint]*, 2021. DOI: 10.1145/3463677.3463705.

[17] A. Preukschat and D. Reed, *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Manning Publications, 2021.

[18] *Welcome to Hyperledger fabric's documentation — fabricdocs 1.0 documentation*, [Online; accessed 17. Oct. 2024], Jan. 2021. [Online]. Available: https://fabrictestdocs.readthedocs.io/en/latest.

[19] R. Z. Fathiyana, S. N. Yutia, and D. J. Hidayat, "Prototype of integrated national identity storage security system in indonesia using blockchain technology," *JOIV: International Journal on Informatics Visualization*, vol. 6, no. 1, pp. 109–116, 2022.

[20] I. H. Johnson Jeyakumar, D. W. Chadwick, and M. Kubach, "A novel approach to establish trust in verifiable credential issuers in self-sovereign identity ecosystems using train," in *Open Identity Summit 2022*, Bonn: Gesellschaft für Informatik e.V., 2022, pp. 27–38, ISBN: 978-3-88579-719-7. DOI: 10.18420/OID2022_02.

[21] C.-H. Liao, X.-Q. Guan, J.-H. Cheng, and S.-M. Yuan, "Blockchain-based identity management and access control framework for open banking ecosystem," *Future Generation Computer Systems*, vol. 135, pp. 450–466, 2022.

[22] R. Mukta, H.-Y. Paik, Q. Lu, and S. S. Kanhere, "Credtrust: Credential based issuer management for trust in self-sovereign identity," in *2022 IEEE International Conference on Blockchain (Blockchain)*, IEEE, 2022, pp. 334–339.

[23] R. Mukta, H.-Y. Paik, Q. Lu, and S. S. Kanhere, "Credtrust: Credential based issuer management for trust in self-sovereign identity," in *2022 IEEE International Conference on Blockchain (Blockchain)*, 2022, pp. 334–339. DOI: 10.1109/Blockchain55522.2022.00053.

[24] B. Podgorelec, L. Alber, and T. Zefferer, "What is a (digital) identity wallet? a systematic literature review," in *2022 IEEE 46th Annual Computers, Software, and Applications Conference (COMPSAC)*, IEEE, 2022, pp. 809–818.

[25] M. Shuaib, N. H. Hassan, S. Usman, *et al.*, "Self-sovereign identity solution for blockchain-based land registry system: A comparison," *Mobile Information Systems*, vol. 2022, pp. 1–17, 2022.

[26] L. Arbona, *Protecting children online: Power of age verification*, Jun. 2023. [Online]. Available: https://veridas.com/en/protecting-children-online-the-power-of-age-verification-and-regulatory-measures/.

[27] D. W. Chadwick, M. Kubach, I. Sette, and I. H. Johnson Jeyakumar, "Establishing trust in ssi verifiers," in *Open Identity Summit 2023*, Bonn: Gesellschaft für Informatik e.V., 2023, pp. 15–26, ISBN: 978-3-88579-729-6. DOI: 10.18420/OID2023_01.

[28] A. De Salve, D. Di Francesco Maesa, P. Mori, L. Ricci, and A. Puccia, "A multi-layer trust framework for self sovereign identity on blockchain," *Online Social Networks and Media*, vol. 37-38, p. 100 265, 2023, ISSN: 2468-6964. DOI: https://doi.org/10.1016/j.osnem.2023.100265. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2468696423000241.

[29] K. J. Eer, J. Diaz, and M. Kohlweiss, "Bottom-up trust registry in self sovereign identity," in *Blockchain and Applications, 4th International Congress*, J. Prieto, F. L. Benítez Martínez, S. Ferretti, D. Arroyo Guardeño, and P. Tomás Nevado-Batalla, Eds., Cham: Springer International Publishing, 2023, pp. 423–433, ISBN: 978-3-031-21229-1.

[30] M. S. Ferdous, A. Ionita, and W. Prinz, "Ssi4web: A self-sovereign identity (ssi) framework for the web," in *Blockchain and Applications, 4th International Congress*, J. Prieto, F. L. Benítez Martínez, S. Ferretti, D. Arroyo Guardeño, and P. Tomás Nevado-Batalla, Eds., Cham: Springer International Publishing, 2023, pp. 366–379, ISBN: 978-3-031-21229-1.

[31] L. Franceschi-Bicchierai, *Bangladesh government website leaks citizens' personal data*, Jul. 2023. [Online]. Available: https://techcrunch.com/2023/07/07/bangladesh-government-website-leaks-citizens-personal-data/.

[32] M. George and A. M. Chacko, "Health passport: A blockchain-based phr-integrated self-sovereign identity system," *Frontiers in Blockchain*, vol. 6, 2023. DOI: 10.3389/fbloc.2023.1075083.

[33] BCdiploma, *What is a Decentralized IDdentifier (DID) and what can it be used for?* [Online; accessed 17. Oct. 2024], Oct. 2024. [Online]. Available: https://www.bcdiploma.com/en/blog/what-is-a-did-definition-and-uses.

[34] *education/LFS171x/docs/introduction-to-hyperledger-indy.md at master · hyperledger-archives/education*, [Online; accessed 17. Oct. 2024], Oct. 2024. [Online]. Available: https://github.com/hyperledger-archives/education/blob/master/LFS171x/docs/introduction-to-hyperledger-indy.md.

[35] *Hyperledger Fabric | Read the Docs*, [Online; accessed 17. Oct. 2024], Oct. 2024. [Online]. Available: https://readthedocs.org/projects/hlf.

[36] *Hyperledger Indy Basics - ACA-Py Docs*, [Online; accessed 17. Oct. 2024], Oct. 2024. [Online]. Available: https://aca-py.org/latest/gettingStarted/IndyBasics.

[37] *NID data leak: Case filed against 19, including Joy, Palak*, [Online; accessed 17. Oct. 2024], Oct. 2024. [Online]. Available: https://www.dhakatribune.com/bangladesh/361276/nid-data-leak-case-filed-against-19-including.

[38] R. A. Pava-Díaz, J. Gil-Ruiz, and D. A. López-Sarmiento, "Self-sovereign identity on the blockchain: Contextual analysis and quantification of ssi principles implementation," *Frontiers in Blockchain*, vol. 7, p. 1 443 362, 2024.

[39] N. Sakib, M. Y. Ali, N. M. Momo, *et al.*, "Secure ownership management and transfer of consumer internet of things devices with self-sovereign identity," *arXiv preprint arXiv:2408.17184*, 2024.

[40] O. Terbu, T. Lodderstedt, K. Yasuda, and T. Looker, *OpenID for Verifiable Presentations - draft 21*, [Online; accessed 17. Oct. 2024], Aug. 2024. [Online]. Available: https://openid.net/specs/openid-4-verifiable-presentations-1_0.html.

[41] *What is Blockchain?* [Online; accessed 17. Oct. 2024], Oct. 2024. [Online]. Available: https://www.oracle.com/middleeast/blockchain/what-is-blockchain.