Blockchain-Backed SSI: Empowering Travelers With a Secure Platform for Digitalized Travel Information

by

Abdullah Al Anan
20301294
Mohammad Mahmudul Haque Siam
20301090
Sunjid Ibnul Anim
20301114
Sifat Jahan Sajin
20301322
Sazid Ahammed
20301155

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 and Engineering

Department of Computer Science and Engineering
Brac University
December 2024

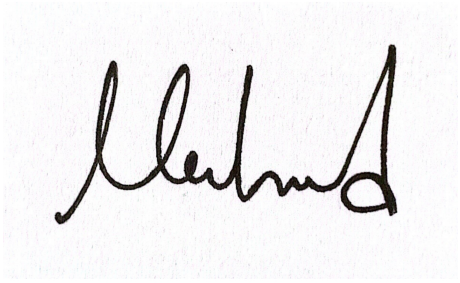
Declaration

It is hereby declared that

1. The thesis submitted is 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.

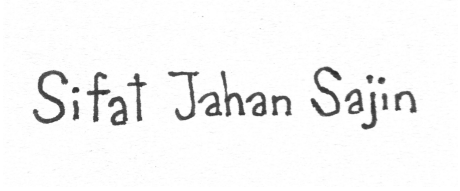
Student's Full Name & Signature:

Abdullah Al Anan
20301294

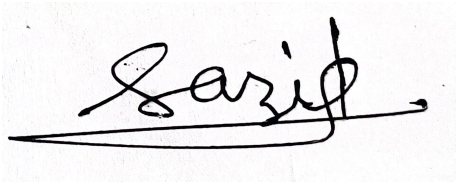


Mohammad Mahmudul Haque Siam
20301090

Sunjid Ibnul Anim
20301114



Sifat Jahan Sajin
20301322



Sazid Ahammed
20301155

Approval

The thesis titled "Blockchain-Backed SSI: Empowering Travelers With a Secure Platform for Digitalized Travel Information" submitted by

1. Abdullah Al Anan(20301294)
2. Mohammad Mahmudul Haque Siam(20301090)
3. Sunjid Ibnul Anim(20301114)
4. Sifat Jahan Sajin(20301322)
5. Sazid Ahammed(20301155)

Of Fall, 2024 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science and Engineering on December, 2024.

Examining Committee:

Supervisor:
(Member)

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

Thesis Coordinator:
(Member)

Md. Golam Rabiul Alam, 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

Document fraud poses significant security risks and can result in unauthorized entries into a country, as well as manual verification, a time-consuming process that raises concerns about the privacy of travelers as their data could be exposed during the verification process. Blockchain technology has advanced the concept of Self-sovereign identity (SSI), a user-controlled and secure identity management system made possible through distributed ledger technology. This study describes how blockchain-based SSI systems can be used where passengers can carry traveling information digitally and securely, which provides users with control over digitized personal information as per use. It is a user-consent and privacy-controlled platform where users share the least amount of information for verification. The adoption of this system, a digital travel pass credential wallet, will display traveler's ability to use digitized travel credentials that are valid on all conveyance systems. With this system, travelers won't need several cards or hard copies; rather, they will have it digitally and control their data. Overall, by eliminating the need for physical documents and relying on standardized digital credentials, the SSI framework simplifies the travel pass verification process and enhances efficiency for both individuals and verifiers.

Keywords: Blockchain, Self-Sovereign Identity (SSI), Passport, Visa, Travel Pass, Decentralized Identifier (DID), Digital Identity, Verifiable Credential (VC), Hyperledger Fabric, Hyperledger Indy, Hyperledger Aries, ACA-Py, Distributed Ledger Technology (DLT), Digital Credential Wallets.

Acknowledgement

Firstly, all praise to the Great Almighty for whom our thesis has been completed without any major interruption.

Secondly, to our supervisor, Dr. Md Sadek Ferdous sir, for his kind support and advice in our work.

And finally, to our parents, without their support, it may not be possible. With their kind support and prayer, we are now on the verge of our graduation.

Table of Contents

List of Figures

List of Tables

Chapter 1

Introduction

In the age of modern technology, our identity credentials are still paper-based. We still need to carry papers to identify ourselves on various platforms [9]. The process of verifying became very lengthy and tedious for both the holder (holding paper-based credentials) and the verifier (verifying credentials). However, the Self-sovereign Identity (SSI) has become the ground-breaking innovation for converting paper-based credentials to digital credentials. Self-sovereign Identity (SSI) solves the digital version of the paper and gives the individual full consent for these credentials [32]. One can share as much information as he wants; he can reduce the quantity of information as he has power over his identification credentials. In like manner, a passport and visa are vital identity credentials used in airports to travel to foreign countries. Every day, thousands of people travel around the world, and each must carry a notebook-sized passport and an A4 size visa to verify himself. People get stuck in a long queue because manual, paper-based verification kills time and strength [9]. For instance, when a person crosses from one country to another, the verification process is performed by different people in both countries whose manuals are the same, and they don't exchange information processes. After this, the data validation is duplicated, leading to the susceptibility to violation. Verifiers depend on the passport particulars provided by this individual [10]. However, such details might not give a full history of his previous traveling records, and this information is easily available to be faked for illegitimate purposes. The most concerning matter is when an individual loses a passport or a visa in a foreign country because a passport or a visa is the only credential to prove his identity in that country [9]. That individual will have to go through rigorous steps to regain his passport. In addition, several forms of modern technology and technical equipment are needed to create an e-passport. Although a passport is valid for five or ten years, it must be renewed after that duration, which is costly and time-consuming. The worldwide e-passport market is a massive industry, as seen by studying it. This market was valued at $23.9 billion in 2023 and is projected to grow to $81.5 billion by 2032 [10]. For instance, a passport in America costs around $130, while one in Germany costs over $140 and in our country, it is $45 etc [41]. This means that every user must pay a significant amount of money for a passport. Following the problem, this paper proposes a solution where the passport and visa will not be paper-based but will be initialized using the Self-sovereign Identity (SSI). In contrast to e-passports, which solely employ RFID cryptography, users' end devices will have several bio-

metric locks, including fingerprints and face locks. In this system, all the credentials regarding passport and visa will be stored in an SSI-based mobile wallet [32]. This will also incorporate the use of blockchain. It is also addressed as distributed ledger technology. Each ledger contains transactions for requests. Also, the system will not require any mandatory renewal process, so there will be no extra cost. Regarding visas, most countries rely on paper-based verification; people still need to borrow an A4 size paper and a passport to verify in the immigration center. There is a lack of centralized standards for visas, even though countries like Malaysia offer e-visas, which are just PDF versions of paper-based visas. Though e-visas are often convenient, they have drawbacks as well. Users may experience significant dissatisfaction if the e-visa application portal does not support it from the user end. This system will include the fundamental requirements that the majority of countries follow, as there is currently no fixed standard for visas. This system will be developed using the Self-sovereign Identity (SSI) framework, which is not centralized. However, Carrying all of the physical documents, including the passport, is inconvenient and time-consuming while trying to acquire a traditional or stamped e-visa. There is also the potential of losing physical papers, which causes great worry and concern to the user, but this system will not require any such physical documents because everything will be submitted online. Since Self-sovereign Identity (SSI) was used to construct the system, the user can only provide the required data. In other words, the user is in authority over their own data. Moreover, Blockchain is a secure platform to store credentials because it is distributed to everyone participating in the network [10]. So, it is transparent to everyone, which makes it more reliable. Blockchain is also immutable; once any data is inserted into any block, it will never be deleted, nor can it be altered [8].

1.1 Research Problem

This paper aims to build a Self-sovereign Identity (SSI) ecosystem where the paper-based passport and visa will be transformed into digitalized credentials. The users of the SSI ecosystem will be able to control their credentials [15]. Moreover, this system leverages user consent, which mitigates the threat model-9 (Lack of control). In an article [33], an RFID expert and a security consultant with DN-System explain how the data stored in the RFID passport chip can be cloned and have severe risks in terrorist activities. Also, the visa is still paper-based and does not use any chip to secure private data. However, this research will mitigate these problems by implementing a blockchain-backed SSI and a hyperledger fabric to maintain service access control from unauthorized users. Also, the proposed method builds trust using a blockchain ledger. All the entities (issuer, holder and verifier) of the SSI ecosystem will have Decentralized Identifiers (DIDs) saved in the blockchain ledger for security and verification purposes. Lastly, this study aims to create a user-friendly platform where users can quickly adopt the system.

1.2 Research Objectives

This study aims to develop and evaluate a blockchain-based SSI system designed for use in the travel sector. The objective of this system is to support and strengthen

travelers by providing a secure digital facility for managing all their traveling-related data. The key goals of this research include:

RO1. To analyze the benefits and challenges associated with Blockchain-based SSI for implementing the digitalized passport and visa.

RO2. To identify the drawbacks of ePassport and visa and propose solutions through the use of digital credentials functioning as verifiable credentials.

RO3. To initialize DID for every entity (issuer, holder and verifier) in the SSI ecosystem, which will be stored in the blockchain ledger for verification and existence proof.

RO4. To construct a second layer of Trusted Issuer List using Hyperledger Fabric.

RO5. To build a wallet that will hold all the verifiable credentials of the user and a medium for the user to get credentials from the issuer or share necessary credentials to the verifier.

1.3 Report Structure

Here, this section provides a brief structure of the report for each chapter. Chapter (1) highlights the motivation for the study and sets the stage for introducing a novel solution. Chapter (2) describes the research background involved in the concept of Self-sovereign Identity (SSI), how it is related to blockchain, and the current passport verification mechanisms that highlight problems and shortcomings that this study works to eliminate. Chapter (3) states a literature review, which will critically review the previous studies, emphasizing their strengths and weaknesses. Through careful comparative analysis, this study pinpoints the top practices and knowledge gaps that fuel our investigation by providing direction. Chapter (4) illustrates the proposed plan followed by the research methodology, threat model, and requirement analysis. After that, Chapter (5) discusses a detailed description of the system's architecture, protocol flow, and use cases. It also explains the cryptographic notations, data models, and how various system components interact. Chapter (6) explains various tools required for the implementation and development of the scheme and the steps to get credentials like passports and visas and check them. Next, Chapter (7) evaluates the system's performance, highlighting its advantages over traditional methods, limitations, and future improvement areas. Lastly, Chapter (8) concludes by summarizing the key findings and highlighting the potential of the proposed SSI-based solution to transform travel credential management, focusing on improved security, privacy, and efficiency. The report ends with a detailed bibliography of all referenced sources.

Chapter 2

Background

In this chapter, we will discuss different aspects of Blockchain in Section 2.1, then we will explore the working mechanism of Self-sovereign Identity (SSI) and also explore the mechanism of trust triangle in Section 2.2. Finally, in Section 2.3 and Section 2.4, we will describe different aspects, standards and threats of passport and visa.

2.1 Blockchain

Blockchain is a type of distributed ledger technology (DLT) that is decentralized, where the data is stored in a block and structured as a chain [20]. It is a distributed ledger technology that is based on transactions and also keeps track of transactions. Data recorded on a blockchain cannot be altered or changed once added [11], making this technology very secure and immutable. After the invention of blockchain, it has been used in several areas where anonymity, security, confidentiality and privacy were the main concerns. In [8], the author mentioned Since its founding, blockchain technology has found applications in a wide range of fields that prioritize user anonymity, security, confidentiality, and privacy [19]. In 2009 it was first introduced with the launching of Bitcoin, a cryptocurrency built on the principles of blockchain technology. Blockchain technology has seen significant advancements and is now being used in several other fields.

Decentralization: Blockchain technology is considered decentralized because all the data is not controlled nor stored in a single governing or central body [11]. It works through a chain of peers, which means all the peers have the same data stored on their end. So, there is no single point of failure. As a result, if any of the nodes is offline or unable, the system will function properly.

Security: To ensure security, this technology utilizes cryptographic methods such as hash function. Furthermore, data stored on the blockchain is up-to-date using transaction hashes. Also, the technology is decentralized and distributed, Therefore, it makes the system more secure and invulnerable to hacking.

Immutability: Data recorded on a blockchain cannot be altered or manipulated once added, making this technology very secure and immutable [6]. It is the non-reversible application of blockchain.

Transparency: Anyone in the network can see the transactions, which means every user is aware of all the transactions that take place in the blockchain [2], which makes this technology transparent.

Structure

In [11], Blockchain technology stores the data of transactions using blocks. Using many consensus algorithms, transactions are recorded in the blockchain. The hash used in this technology is known as cryptographic hash which connects the block. Moreover, authenticity, proof of ownership and sequence of transactions can be verified. To maintain the sequence of transactions a cryptographic hash joined in each block of the blockchain. This technology reduces the need for intermediaries, thereby streamlining and improving the transaction process. Each transaction has a size that is used to determine the maximum number of transactions that a block can contain within itself. The blockchain system uses proof of work (POW) and proof of authority (POA) as consensus rules [8].

Types

There are also several types of blockchains depending on the various use cases. The most common are public and private blockchains. Details of these two are given below:

- **Private blockchain:** This blockchain can only be accessed by a specific number of users or organizations who are authorized and trustworthy [14]. This blockchain is also known as permissioned blockchain. As it is a private blockchain, not everyone has access to participate in the ledger operations [9]. It is used only in some cases where important and sensitive data is transmitted.
- **Public blockchain:** This blockchain can be accessed by any user or organization. Therefore, no one needs to be authorized. This blockchain is also known as the uncommissioned blockchain. As it is a public blockchain, everyone has access to read, write or manipulate the blocks. In this blockchain, anyone in the network can see the transactions [9], which makes the system transparent. This system is not very safe in terms of privacy and confidentiality.

The difficulties that are facing nowadays are that this technology is not fast enough compared to the other technologies. Moreover, after the creation of a specific number of blocks, there will be no other solution till now. Energy consumption is also one of the most discussed challenges this technology should overcome.

2.2 Self-sovereign Identity (SSI)

Self-sovereign Identity (SSI) is progressively used in identity management, mostly with the expansion of online services [5]. Traditional Identity Management Systems (IMS) are mainly provider-centric, resulting in a complex and confusing pattern of identities for users [5]. These problems are sought to be resolved by SSI, which allows users greater control over their identity data, which is often lacking in current frameworks. In this regard, the continuous progression of SSI has led to different types of technological implementations and interpretations of that concept. But this also leads to a lack of harmonized understanding and sometimes inconsistent

definitions of SSI. SSI does not remove the need and significance of governments and other organizations to issue identity documents commonly used today. Indeed, SSI is intended to assist these organizations in a more effective and reliable manner while ensuring individual autonomy [31]. According to [27], Self-sovereign Identity (SSI) is the next generation of user-drivenness and originally revolved around locating users, and it all starts with putting the user at the heart of managing their identity. This implies that our identity must operate harmoniously in distinct places, but only with our approval. On top of that, an individual should have complete control over their digital identity, ensuring autonomous decision-making concerning it. In order to achieve this, a Self-sovereign Identity (SSI) should be portable, which means that it's not fixed at one particular location. In order to address these misperceptions, the community has been considering various names for SSI. One of those most commonly used as an alternative is a decentralized identity [31]. In [32], the seven building blocks of SSI are as follows:

i **Verifiable Credentials (VCs):** Operate as digitized versions of the credentials and documents we carry around to show our identity.

ii **Issuers, Holders, and Verifiers:** Credentials or digital certificates are issued by issuers. The holders store them in a digital wallet – which is like an online manifestation of our physical purse. Verifiers are those who validate these digital credentials whenever a holder presents them.

Figure 2.1 illustrates the "trust triangle" of the SSI ecosystem.

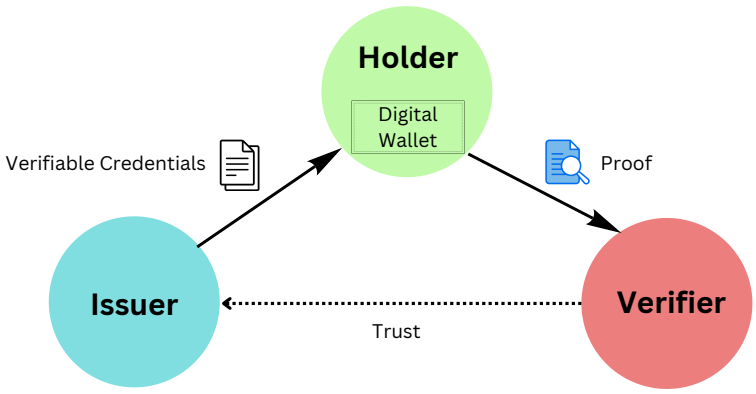


Figure 2.1: The Trust Triangle of SSI.

iii **Digital Wallets:** They are digital equivalents of our physical wallets. They store our verifiable credentials on devices.

iv **Digital Agents:** They are apps or software components that assist us in creating a practical digital wallet. They help with obtaining and presenting credentials, managing contacts, and securely passing these credentials to other digital agents.

v **Decentralized Identifiers (DIDs):** DIDs are a digital address innovation that uses cutting-edge cryptography, thus eliminating the centralized registration

authority. They simplify the creation and verification of digital identities.

vi **Blockchains and Verifiable Data Registries:** These are cryptographically secured, distributed databases. This is because they are a trusted source of truth for DIDs and public keys without relying on one-point failure or failing to ensure security.

vii **Governance Frameworks:** Whatever their form and size, various governance bodies publish sets of rules governing the use of SSI infrastructure. These guidelines encompass business, legal, and technical issues, providing a basis for trust within any sized digital ecosystem.

Next, several important features of a Self-sovereign Identity (SSI) have been outlined in [12], [27]. The author in [27] has presented ten essential properties, namely Existence, Control, Access, Transparency, Persistence, Portability, Interoperability, Consent, Minimalization and Protection. In 2005, Kim Cameron from Microsoft introduced the Laws of Identity [12]. The laws consist of seven principles: User Control and Consent, Minimal Disclosure for a Constrained Use, Justifiable Parties, Directed Identity, Pluralism of Operators and Technologies, Human Integration, and Consistent Experience Across Contexts. These laws offer recommendations for user identity management and disclosure, focusing on consent and minimally disclosing information to others regarding the individual's relationships with them based only on necessary identification demands. Christopher Allen's principles in [27] were written especially towards SSI consolidated at the center of user control.

2.3 Passport

The e-passport is a modern version of traditional passports built with an embedded RFID (Radio-frequency Identification) chip that holds an RFID tag [36]. It is a small device used for storing and transferring data. RFID tag uses a microchip and an antenna. The microchip contains security protocols, BAC (Basic Access Control) and EAC (Extended Access Control). Information like Passport number, Name, Nationality etc, is controlled by BAC [34]. Sensitive information like biometrics, fingerprints etc, is controlled by EAC. The antenna transfers data between the RFID tag and the RFID reader. An RFID reader is used to read information from the e-passport chip. At the bottom of the passport, there is a Machine Readable Zone (MRZ) [34], which holds a line of alphanumeric characters [36]. The RFID reader uses MRZ to unlock the chip data. Next, the core objective of the International Civil Aviation Organization's (ICAO) [34] traveler identification program is to establish secure, efficient, and timely verification of travelers' identities. This is where ePassport technology plays a major role. ICAO Document 9303 provides the international technical standards that govern ePassports. These passports have a contactless integrated circuit (chip), which securely holds the holder's biometric and biographic data. This technology automates a number of border management procedures. In light of the rising need for secure and simple travel, ICAO's New Technologies Working Group (NTWG) [34] is studying new trends in ePassport technology. These include compatibility enhancements with the current generation of ePassports. ePassport has some standards. To start, Logical Data Structure 2 (LDS2) [34] is a voluntary expansion of the ePassport chip that comes with extra ap-

plications for storing visas, travel endorsements, and biometrics post-issuance [34]. The applications of LDS2 include e-travel stamps, electronic visas, and secondary biometrics (such as iris and fingerprint) after issuance [34]. Later International Specifications (ICAO Doc 9303 -7 Edition) [34] This guide specifies specifications for the security characteristic authenticity design, manufacture, and issuance of Machine Readable Travel Document (MRTD) [34], along with the data scheme protocol in detail. Then LDS1 also includes data groups, of which machine-readable zones are included; biometrics-encoded (face-finger iris) portraits are displayed as signatures; and personal and document detail options for secondary biometric security. Besides, LDS2 adds functionality for visa records, travel records, and additional biometrics. It has many protocols, one of which is data authenticity/integrity (10), passive authentication, copy or clone protection, which includes active authentication and chip authentication, and access control, which uses PACE (password authenticated connection establishment) [34] for communications encryption. Besides, read/write authorization involves terminal authentication. Additionally, Public Key Infrastructure (PKI), a framework that includes various authorities and signers (like Country Signing Certification Authority (CSCA) and LDS2 CA) [34] responsible for the issuance and validation of digital certificates, ensures the security and integrity of data stored on ePassports [34]. In contrast, a digital passport, which is a verifiable credential (VC) can be compared with an ePassport while considering the aspects of digital identity verification. A passport, more conventionally, refers to an officially recognized proof of identity and citizenship, which is used for travel and identity confirmation. Similarly, a VC is a digital document (a passport in our case) that can be used to verify aspects of a person's identity or other personal credentials in an online or electronic environment. The VC is cryptographically signed by the issuer (passport office), validating the VC to be used for a particular user (citizen). The data from a Bangladeshi e-passport is displayed in Figure 2.2. The type of passport, country code, and unique passport number are shown here. Furthermore, this figure also shows the holder's name, nationality, passport number, location, DOB (date of birth), issuing authority, date of issuance, and expiration date. The bottom of the page for scanning is known as the Machine Readable Zone(MRZ). Besides that, the holder's signature and image UV reaction materials and watermarks are included as safety features.

Figure 2.2: ePassport.

Threats to ePassport Data Integrity

- Attackers are able to obtain sensitive data and personal information, including biometrics and personal information, if the authentication mechanism breaches or is executed improperly.
- Lack of control over unauthorized access further makes it easier for privacy to be violated and for several types of misuse, including fraud, scamming, identity theft, biometric spoofing, and many other illegal acts.
- Because LDS1 contains a variety of personal and sensitive data, it is an advantageous and selective target for attackers. As an example, attackers can simply obtain facial images by targeting DG2 (facial image) and using it for biometric spoofing [42].
- Another significant security issue is that if the counterfeit chip gets cloned, all of the data on the LDS1 could end up being duplicated. Cloning conveys a serious security risk to the e-passport even though it doesn't alter the integrity of the passport data.
- Passive authentication (PA) only validates digital signature data but plays no role in preventing cloning or spoofing. The security of LDS1 data is potentially vulnerable because Extended Access Control (EAC) and Supplementary Access Control (SAC) are not utilized in certain countries [42].
- LDS2 also raises security concerns and exposes potential threats due to the vast data sets, which include travel routines, visa information, and other sensitive information that may be exploited for illegal activities, surveillance, and profiling, making it an ideal target for attackers. The data structure of LDS2 is extremely complicated due to its hierarchical configuration and interrelated massive data sets. Data in LDS2 is dynamically upgraded in discrete chunks and stores rather than being stored in its whole. Inadequate protection of the update process makes it simple for hackers to obtain counterfeit data, including forged stamps and credentials [42].

2.4 Visa

A visa is an official approval document granted by a country's government to travel from one country to another. Since there are variations and various types of visas in different nations, there are no definitive standards for visas. However, most of the country's visas maintain a set of basic standards. The ICAO (International Civil Aviation Organization) has established several international standards that are applied to visas [34]. Standards unique to visas and other travel-related documents are included in ICAO (International Civil Aviation Organization) Document 9303: Machine Readable Travel Document (MRTDs) [37]. A fundamental component of MRVs (Machine-Readable Visas) is MRZ (Machine-Readable Zone), which uses the OCR (Optical Character Recognition) system to encode, organize, and structure the data [38]. OCR (Optical Character Recognition) system takes images, pre-processes them to transform them into text, and then converts them into a readable format. Biometric information is kept in a secure database. Biometric info such as Polar Coordinates for Irish data, CCF (Compact Card Format) format

for fingerprints, etc. Security is facilitated by the Public Key Directory (PKD), which verifies and validates data signatures for MRVs and e-Visa (ISO/IEC 27001) [37]. In order to ensure proper retrieval and cross-referencing of all Visa data, a relational database structure is employed. In the immigration system, all of those confidential visa details are exchanged. The immigration system uses SOAP (Simple Object Access Protocol) [38] or REST (Representational State Transfer) as APIs for data interchange in accordance with the ICAO(International Civil Aviation Organization) and ISO(International Organization for Standardization) criteria [37]. Physical visas are secured with a holographic coating in accordance with ICAO (International Civil Aviation Organization) regulations. Additionally, security inspections at border crossings utilize infrared and ultraviolet wavelengths. Besides, a watermark is used to add a unique identity [37]. Another kind of visa is called an e-visa. Although this type of visa is used in certain countries, the majority of nations still issue physical visas. Certain ICAO (International Civil Aviation Organization) standards also apply to e-visas. For biometric data, MRZ is utilized following "ICAO 9303" standards [38]. Identity verification is done using biometric information. There is a barcode and a QR code on the E-Visa. Basic visa information, including the visa number or reference ID, personal information, validity, URL, etc., are generally contained in this barcode. Bar codes only save reference IDs and other small amounts of data, but QR codes store many more data such as URLs, visa details etc. A PDF file with this barcode, QR code and all the details will be delivered when the e-visa is approved. This barcode's benefits include faster border verification, authenticity assurance, self-immigration, etc. While an e-visa does not require physical documents, an approval notice is necessary for the immigration officials to stamp the documents. Furthermore, IATA (International Air Transport Association) is another organization that provides guidelines governing visas and travel in real time for international air travel, although it does not have any involvement in visa regulations [39]. Visa legitimacy is confirmed and verified by Interpol using the SLTD (Stolen and Lost Travel Documents) database. WTTC (World Travel and Tourism Council) emphasizes the aspects and policies of visas in different countries [39].

Figure 2.3: Visa Variation.

Figure 2.3 shows three different kinds of visas for three countries, indicating that there is no fixed set standard for visas. The requirements vary depending on the country and the kind of visa. For instance, in the event of an e-visa, this Malaysian visa has all the information, including a barcode and a QR code, and it is not required to be carried physically. The Saudi visa we are seeing here is a tangible document that must be carried out for the duration of the trip. The Thailand visa is an example of a stamp visa, sometimes known as a visa sticker, as it is printed on a single page of the passport. Also, you must have this visa with you when you are in the country you are visiting.

Chapter 3

Literature Review

In this chapter, we will review the related works in section 3.1, and in section 3.2, we will discuss industrial applications.

3.1 Academic Literature

In [1], the authors have attempted to construct a public transport system that uses Self-sovereign Identity (SSI). A primitive model has been successfully developed to showcase the utilization of standardized travel details universally recognized by different transportation networks. Their proposed solution obviates the necessity for multiple travel cards. It allows individuals to exert greater authority over using their personal information by employing integrated ticketing services throughout the country. Furthermore, they introduced a rudimentary prototype of a decentralized identity control system for the public transportation sector, incorporating the essential elements of Self-sovereign Identity (SSI) and blockchain-based systems. Their system ensures the safety of transactions and stores the necessary data in the blockchain ledger. The authors have analyzed four methods for managing a Self-sovereign Identity (SSI) platform based on Blockchain technology: uPort, Sovrin, Namecoin, and Civic. In addition, they laid out both non-functional and functional requirements to define their system accurately. Nevertheless, they were unable to offer an appropriate consensus method for their research. Furthermore, the document lacks any cost-efficiency strategy to address the substantial transaction fee incurred during execution. Moreover, the text needs more elaboration of the mining procedure for the miners.

In [10], the authors discuss the limitations of traditional passport and visa management systems, which are time-consuming, especially when multiple visas are required for the same country. Then it proposes a solution using Hyperledger, a permissioned blockchain. The system aims to enhance efficiency, security, and reliability by creating a distributed ledger for passport data and visa records. It comprises four main components: passport issuing authority, visa office, third-party orderer, and user interface. This system's key advantage is the use of a permissioned blockchain that does not feature computationally demanding consensus since trust has been established as an invitation-only basis between involved organizations. The approach deals with several obstacles in permissionless blockchains, which makes it

relevant for non-financial applications such as passport and visa management. The system's architecture consists of organizational entities, orderers, channels, ledgers, and smart contracts. It provides algorithms for issuing and querying passports and visas, showing the possibility of achieving productivity gains in processes related to cashier handling procedures.

The authors in [13] discuss blockchain applications in the maintenance of government eIds. The research seeks to improve the security, efficiency, and trustworthiness of eIDs as they are utilized in identification processes and administrative documentation. Key benefits of incorporating blockchain into eIDs include more protection in the form of tamperproof records and enhanced verification, which plays an essential role in avoiding identity theft. It also facilitates effective eID information management by simplifying the administrative system and improving user comfort. In contrast, difficulties introduced in the paper include large-scale blockchain implementation complexity, such as privacy issues caused by immutable records and the need to make essential changes for infrastructure adjustments. However, the paper does not suggest a specific technology but provides an in-depth analysis of current blockchain and eID systems with case studies depicting potential applications and limitations.

Panchamia et al. [9] proposed a blockchain-based solution for the regulation of travel-related government documents such as passports, visas, and immigration. The authors have used Hyperledger Fabric, a permissioned blockchain platform, to execute this solution. The paper refers to smart contracts/chaincode in Hyperledger Fabric for the operation of business logic attached to a blockchain. These smart contracts are critical to certifying that data is correctly recorded into the ledger by the relevant agencies. A proof of concept (in Section V) is presented in the implementation section for their proposed system, which uses Hyperledger Composer, a tool useful for developing blockchain business networks. Hyperledger Composer supports the definition and deployment of business networks onto Hyperledger Fabric, including modeling components for assets, participants, and transaction management, along with access control rules and smart contracts. However, one of the main barriers they identified is getting several governing bodies on board since this refers to a transnational solution. The authors suggested defining the governance that will control such a system across the world. In addition, to boost additional security on the existing blockchain solution, intelligent biometrics could be used, which would validate the person before entry into the ledger data. In this case, Hyperledger Indy would be perfect, as it has been designed specifically for digital identity and can be employed as an authentication mechanism.

Goel et al. [21] attempted to show the immigration control issues and address the urgent problem of illegal immigration by suggesting a blockchain security model for managing records on immigrants. This system was developed to achieve a decentralized, secure, and scalable record-keeping method that facilitates the control and verification of migration records, thereby controlling illegal immigration. First, this system uses the Ethereum blockchain and Proof of Work for consensus, resulting in immutable uniques that improve integrity and prevent fraud. Nevertheless, the paper highlights several limitations of this system, including its dependence on primitive information and the risks involved if an administrator gets compromised. In particular, the paper does not confine itself to theoretical proposals but puts this

system into practice. It uses technologies like Ethereum for a blockchain framework, React to create interactive front-end web applications, Node.js server-side and networking application tools, Metamask for local testing, and various libraries such as Ganache Web3 or Express for development support. In this practical case study, blockchain technology shows its feasibility and efficiency in solving multi-dimensional problems such as the issue of immigration control. In Figure 3.1, we portray the flowchart to check for illegal immigration where, at first, it checks the blockchain records, and if found, then the immigrant follows the process; otherwise, it does not [21].

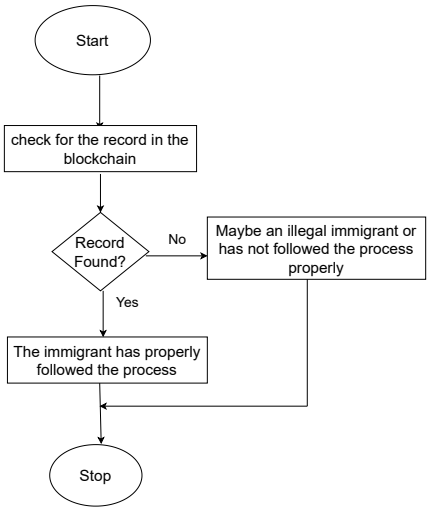


Figure 3.1: Flowchart to Check for Illegal Immigration [21].

Author Speelman [17] has mentioned SSI and its ability to give power back into the hands of users by allowing them to control their own digital identities, freeing them from centralized authorities, and promoting better privacy online. The paper provides a well-developed theoretical framework, improving the designs developed in SSI, and an examination of a collaborative design project with Kamer van Koophandel (KVK) aimed at meeting the need for 'authorization by legal entities', which is lacking in digital identities. It presents a new 'semantic layer' in SSI that adopts a smartphone app to enhance user control alongside interoperability. Yet, the paper considers some limitations, such as dependence on commercial organizations for data representation, which in turn may violate user privacy and a lack of a semantic layer within TrustChain infrastructure. Even with these limitations, this study has practical implications, as exemplified by the Android application designed for Dutch citizens, which was structured based on national identity attributes and facial inferences. The app is powered by TrustChain, incorporating technologies such as IPv8, an individualized distributed ledger, a REST API, and ZKPs privacy-preserving identity verification.

Swati v et al. [8] propose the utilization of Blockchain technology in the travel industry and highlight its benefits. The core components of blockchain where a cycle has been shown from cryptography to transaction to consensus, finally to blockchain in Figure 3.2. Furthermore, the paper imparted an essential understanding of blockchain technology. The article discusses the potential impact of Blockchain technology on the travel industry, namely in terms of enhancing data security, pre-

venting fraud, and facilitating fast credit transfers through various cryptocurrencies. This technology eliminates the need for intermediaries, thereby streamlining and improving the transaction process. The article aims to apply blockchain technology to facilitate hotel and airline reservations. Additionally, the study provides a valuable understanding of the limitations of blockchain technology. Nevertheless, their plan needs a description. The provided information needs more details regarding the utilization of the blockchain system in the travel sector, the visual representation of the system, and its practical functioning in real-world scenarios.

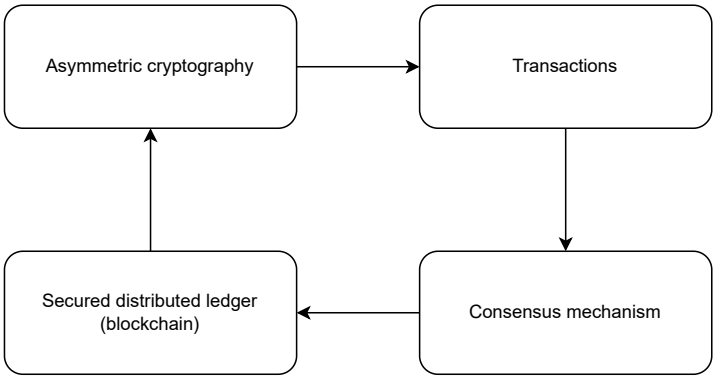


Figure 3.2: Core Components of Blockchain [8].

The authors in [6] have aimed to establish a safe, decentralized, and immutable system for seamless border control. The purpose is to facilitate governments in efficiently and effortlessly recording the movement of individuals entering and exiting their countries. Additionally, they demonstrated the secure storage of biometric data for the purpose of automatic passenger validation/verification. Hyperledger Fabric was utilized for the implementation. The text explains how the client initiates the transaction, the endorsing peers carry out the transaction, and the orderer peer manages the ordering service. Additionally, it offers a systematic process to demonstrate the functioning of departure and arrival systems. The author employs the pre-existing kiosks to integrate with the blockchain architecture in the backend, eliminating the need for passengers to acquaint themselves with an unfamiliar procedure. Nevertheless, there is still a worry regarding the confidentiality of the passengers' biometric data and the potential legal complications associated with its distribution.

Stokkink et al. [15] have proposed a digital identification solution that utilizes blockchain technology and does not rely on an external third party to establish a legally recognized digital identity. The study provides a basic introduction to Self-sovereign Identity (SSI) and illustrates the authors' 10 characteristics of Self-sovereign Identity (SSI) [25]. Furthermore, articles demonstrate how SSI gets integrated into their work by satisfying the essential verifiable assertions, including the timestamp, proof reference, proof structure, validity period, and name. The study demonstrates the utilization of timestamps for the detection of identity fraud. The author categorized the audit logs into three stages of escalation: passive, intent-based, and active models. In addition, they demonstrated that app8 utilizes QR codes to transmit attestations rather than relying on the internet. Their supporting

Non-Interactive verification is based on the process of iterative hashing, which is a secret key that is shared. Additionally, the platform utilizes a Trust-Chain key ed25519. Finally, they demonstrated that all of the systems successfully accomplish claim creation and claim verification in under 100 milliseconds. Finally, this paper aims to improve the user-friendliness of the technology for customers and make it easier for them to adopt the innovation.

In [19] the author describes a comprehensive examination of Self-sovereign Identity (SSI) alongside its implications for border governance and migrant supervision. The author examines SSI as a decentralized digital identification system tied to blockchain technology, which enables those who are less fortunate, such as refugees, to have greater control over their identities, hence facilitating their improvement. The analysis emphasizes the uncertainties and inconsistencies of Self-sovereign Identity (SSI). While discussions in nonprofit organizations often portray SSI as a potential tool for ensuring data security and helping refugees, the research reveals its inherent ambiguity. SSI functions as a means to strengthen both commercial and bureaucratic authority while also enabling flexibility. The paper contextualizes SSI within the historical framework of identity control systems and contends that it facilitates authorities and companies in exerting greater control over refugee groups.The writer states that this method enhances various aspects of the traditional and lengthy process, including data minimisation, cryptographic safeguards, and disclosure management. The paper analyzes the contrasting perspectives on Self-sovereign Identity (SSI) within this field and concludes that advanced technologies undermine and integrate conventional frameworks equally.

In [20], the author proposed a management system based on blockchain technology, utilizing Self-Sovereign Identity (SSI) to guarantee confidentiality and safety. This system ensures enhanced privacy and security. Reduce the quantity of documentation and expedite the procedure for processing. Minimize the absence of compatibility between administrative departments and other organizations. If resources are scarce, then the management system may not be optimal. The study describes a Self-sovereign Identity (SSI) management system utilizing Blockchain technology. Organizations strive to obtain access, while users grant specific information access and submit documents for authentication. This efficient approach eliminates the need to submit physical documents and provides companies with straightforward confirmation. Blockchain technology enhances the efficiency of identity verification procedures by safeguarding the privacy and security of users and enterprises. This study primarily examines the benefits and limitations of a Self-sovereign Identity (SSI).

Xu et al.[11] attempts to build a web-based identity authentication and verification management system for passports utilizing blockchain technology, studied in the context of blockchain applications. In addition, the Myanmar Immigration Office uses blockchain technology in conjunction with several thorough techniques to confirm and validate information. They used Geth (CLI), an implementation of the Ethereum node software, for their system. Based on a thorough strategy, this study proposes a management system that would guarantee data redundancy, duplication, security, and secrecy. This will simplify things as most transactions and operations use Geth (CLI). The immutability of the system discussed in the paper is guaranteed by employing this non-reversible application of blockchain and the used

hash function. This is because blockchain data cannot be changed or updated. In terms of precision, this method will efficiently keep all passport data stored on the blockchain up-to-date using transaction hashes. This system's development relies on the keccak-256 algorithm, which generates a unique address while guaranteeing security, privacy, and anonymity. Ethereum provides trustworthy and accurate data transmission by connecting all organizations in the system.

In [2], authors delve into the evolving realm of digital identity management. The paper analyzes Distributed Ledger Technology (DLT) and its impact on Self-sovereign digital power modification, transforming the progress of advancements and highlighting the significance of philosophical issues. The authors highlight the transformative potential of DLT by introducing the concept of "Self-sovereign Identity (SSI)" where individuals have complete control over their digital identity. Privacy, relationality, and data ownership are key considerations. Concerns about the backup process have been raised, particularly using Biotrex, calling for better reverse monitoring. The conclusion emphasizes the pressures of governance directives, cautions against decentralization-society problems, and political power in regulating advanced digital power.

The author in [4] explores the impact of blockchain technology on the hotel and tourism industry with a specific focus on hotel booking systems. Tepe aims to integrate blockchain technology into this system to benefit customers, emphasizing economic benefits and haste. The blockchain structure is shown where it shows how the list of transactions is converted into a Merkle root, which then gets hashed, shown in Figure 3.3. The study used qualitative research methods, including ethnography and document analysis, examining over 1600 user-generated content and 25 organizational documents. The results suggest that blockchain technology holds decentralization and improved economic benefits and satisfaction suggestions, but its end is currently limited. The study addresses the evolving hotel landscape, the role of online intermediaries, and blockchain's support for new authorizations for managerial systems. Foreign research questions focus on the impact of blockchain integration on consumers, the economic benefits of decentralization, and the impact of hazmat.

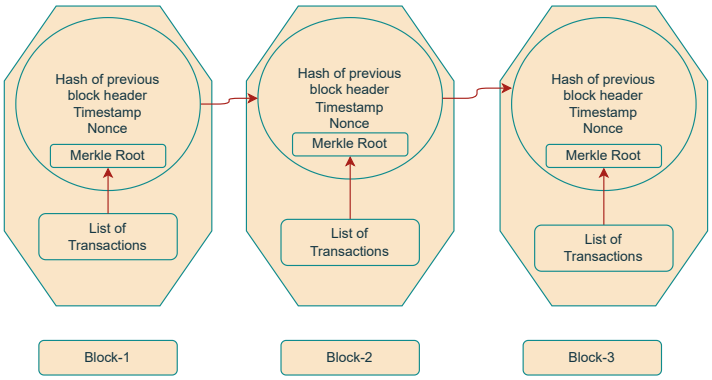


Figure 3.3: Bitcoin Block Structure as an Example for a Public Blockchain [4].

The author In [14] proposed a system based on the Hyperledger Indy private blockchain; the proposed Self-sovereign Identity (SSI) management system uses proof of work

(POW) and proof of authority (POA) as consensus rules in a test net environment. Theoretically, this system might be possible, but One of the difficulties is assessing effectiveness on a large scale because there aren't enough biometric samples or clients of applications for mobile devices. The benefits of the technology include the capacity to log every transaction on the blockchain, guaranteeing the confidentiality of both vehicle and individual ePassports, as well as the past records of border crossings. One area lacking improvement is creating a deeper relationship between official entities in a consortium system for effective user border-crossing legality authentication. The implementation of biometric encryption poses a significant challenge in the proposed system. One of the main challenges in the proposed system is implementing biometric encryption, which is a complex, time-consuming, and expensive process. The intricate procedure is integrated into the ePassport application, authorization, biometric identity verification, and Surveillant Information Reconciliation, among other system components. To ensure optimal effectiveness and confidentiality across all applications, it is imperative to address the challenges associated with biometric encryption. The intricate nature of this process emphasizes the importance of meticulously designing and implementing the incorporation of biometric characteristics into the proposed Self-sovereign Identity (SSI) management system.

Shih et al. [7] introduce an international change using hyper ledger Fabric for text-based COVID-19 vaccine boards, emphasizing pass-through passports' limitations and digit certificates' use. Federated Identity Management and a consortium blockchain are used for cross-border validation in the suggested solution. Affecting the global outcome of COVID-19, the study captures the key role of an international, federal identity management architect in ensuring. The goals prioritize verifiable proof of vaccination, privacy, and anti-tampering procedures. The study underscores the importance of hyper ledger fabric, proposes a decentralized application framework, recommends requests and suggests international discussions on the application of Covid-19.

The study [46] examines the use of Self-sovereign Identity (SSI) technology in the UK NHS to develop a digital staff passport that overcomes inefficiencies in credential verification during staff transfers. The system uses decentralized identities (DIDs), verifiable credentials, and the Sovrin Network as its trust registry, allowing employees to securely store and transfer credentials via digital wallets such as Evernym's Connect.Me. By replacing existing centralized processes with SSI's decentralized, peer-to-peer architecture, onboarding times were cut from days to minutes, lowering administrative costs and enhancing staff mobility at critical moments like the COVID-19 pandemic. The NHS used open standards, including W3C's Verifiable Credentials and OpenID Connect, to assure interoperability and scalability while emphasizing privacy by reducing dependency on public ledgers.

3.2 Industry Applications

Currently, some companies have developed some software focused on e-passport and identity solutions. This section provides information by evaluating the mechanisms, security concerns, and how all of these industrial software programs comply with the SSI standards.

VeriGo

The program "Veri Go" was created by a company named "Veridos." The user can use this application to transfer all of their e-passport data to their mobile device. They save all of the user's sensitive data on the smartphone through the app and retrieve it via NFC technology [44]. This app's wallet allows the user to save information from many passports. The security might be compromised if there is inadequate encryption and data transfer security since it is a mobile application that saves and exchanges private information that is confidential. Moreover, because of their dependency on a particular authority, their system does not entirely adhere to the Self-sovereign Identity (SSI) principle, which states that there should be no singular trusted authority. Therefore, their trust triangle is not justified. Additionally, mobile applications have a lot of security vulnerabilities that make them extremely dangerous for such private information. Third parties may occasionally misuse this information. Therefore, using this application is not very safe.

Idemia Mobile ID

A smartphone software called "Idemia Mobile ID" allows users to save information on genuine identification documents, such as passports and government-approved documents. All of this private data is kept in a digital wallet [43]. They collect and archive biometric data in a database. The user can utilize the Mobile ID system to access all of the data in the digital wallet. If all of the biometric information stored in this system has been compromised, it poses a serious security risk. In contrast to the SSI, their technology lacks DIDs (Decentralized Identifiers) and VCs (Verifiable credentials). The lack of VCs and DIDs prevents their system from properly identifying the Issuer, Verifier, and Holder. So their trust triangle is not proper according to SSI standards. As a result, employing this technology carries a high risk.

Yoti

This app, called "Yoti" stores sensitive user data using face recognition technology. This app uses encryption to store data. Blockchain technology is used to authenticate users [45]. The purpose of this program is to provide third parties with secured access to all of this confidential information. This system has several dangerous security flaws, such as data being shared with third parties; it might be used for illicit reasons if an unreliable third party manages to gain access to all of the data. Their system isn't entirely decentralized. Their trust triangle is invalid since they rely on the central infrastructure. Additionally, there is a significant chance of phishing. Since face recognition is the only technique that is employed, there is a chance that deepfake will be used to steal information. This method is extremely dangerous considering the significance of these factors.

Chapter 4

Proposal

This chapter portrays the proposed plan of our system. Firstly, Research Methodology describes our methodical approach to the system, including the data gathering and data analysis procedures we used. The system architecture is then covered in depth in the system proposal along with the overview. All possible security threats are covered by the Threat Model, along with ways to mitigate them. The functional requirements, security requirements, and privacy requirements are finally covered in the requirement analysis.

4.1 Research Methodology

The methodology in Figure 4.1 used in this study is organized systematically to fulfill the research objectives and to maintain a logical evolution of the work. The approach begins with identifying the problem in order to gain a comprehensive understanding of the current gaps and problems. Following that, the research objectives are created to help focus the study and highlight its expected contributions. A thorough assessment of relevant works is carried out to give context and strengthen the study's relevance. Based on this foundation, a proposal is created to present the framework. To ensure that the suggested solution is strong, a threat model is created to predict potential weaknesses and dangers. Rigorous requirement analysis is then carried out to identify the critical criteria for the solution's efficiency. The architecture design and protocol flow are developed next, ensuring the system's logical and functional integration. Afterwards, the tools required for development are identified, and the implementation phase is carried out according to the architectural design. Finally, performance testing is conducted to evaluate the solution's effectiveness, efficiency, and reliability based on predefined metrics criteria.

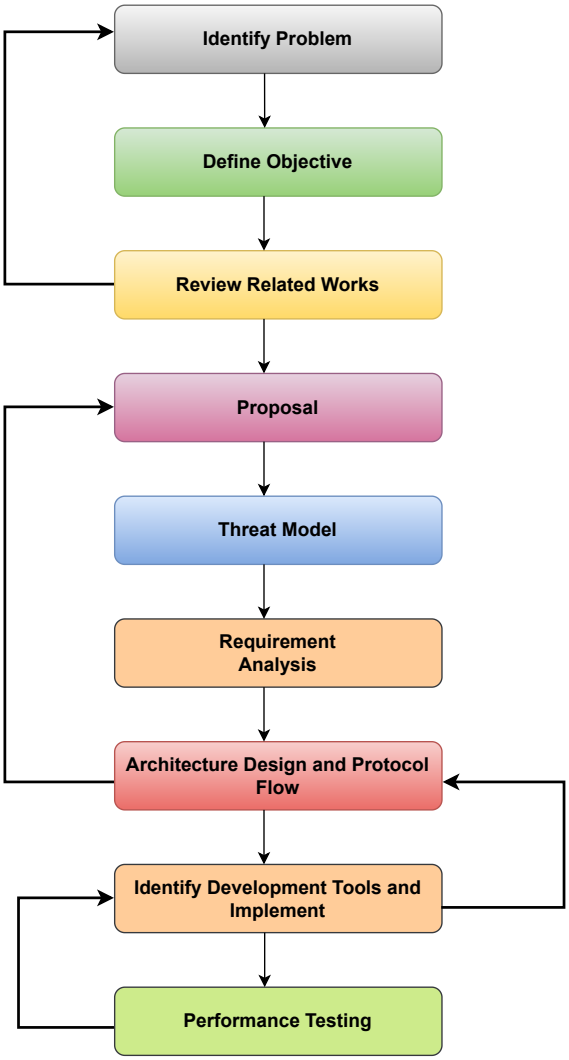


Figure 4.1: Research Methodology.

4.2 System Proposal

Proposal Existing systems lack digitized ePassports and visas using Self-sovereign Identity (SSI). While some papers propose using blockchain for digitized passports, they fail to provide adequate real-world application scenarios or adhere to ePassport standards. According to [8], It proposes the utilization of Blockchain technology in the travel industry but does not specify the digitalization of the passport or travel information, the system lacks a visual representation of the system and its practical functioning in real-world scenarios. Next, Centralized Public Key Infrastructure (PKI) has been brilliant in the environment of a scaled-down internet. Since our lives and corporation activities are becoming increasingly online, the centralized model is struggling to penetrate many areas of applications where entities want more control over their own certificate lifecycle, especially when only a few hundred

Certificate Authorities (CAs) worldwide can manage public keys as well as endpoints associated with them. However, if SSI is not used with blockchain, then travelers, specifically older citizens and children, have problems remembering or possessing public keys. For this purpose, we will use Aries bifold wallet. No need to memorize the DID. Hyperledger Indy is used to create and manage DID and corresponding DID Docs. DIDs are unique identifiers that do not arise from centrally managed registries whereby any entity can create a did for any cause. Given the fact that DIDs are huge random numbers, there is virtually no limit to the supply/namespace for these DIDs. As a single administrator is responsible for entering all the data, if a person or the system they use is compromised, then false data could be entered, and it would be difficult to distinguish it from actual data. This is a security risk that needs addressing [21]. In this case, the proven cryptographic systems are reinforced by Decentralized Identifiers. When a traveler carries out their identification, the digital wallet generates an identifier that is digitally signed using a private key known only to them. The asymmetrically matched public key is sent to a distributed ledger. Travelers may show the digital passport info to verifiers, and before giving a travel pass, the verifiers will verify that it is indeed issued by governments of citizens. In this context, blockchain is used as a verifiable registry for storing DIDs or DID Docs due to its features of immutability, resilience and decentralization [3]. Most importantly, however, these digital cards are confidential. This makes travelers masters of their own digital identities. They make the decisions for it. Next, Verifiable Credentials (VCs): These consist of credentials that are secured through cryptography, uphold privacy principles, and can be verified by machines. These are intended for utilization in Self-sovereign Identity (SSI) applications. Dependence on commercial organizations for data representation which can violate user privacy and lack of a semantic layer within TrustChain infrastructure [17]. Therefore, we wish to develop that when Verifiers receive the Verifiable Presentation, rather than contacting the original Issuer as they do in many existing systems. Now, Verifiers will be able to confirm that the attributes were issued by the indicated Issuer(s), ensuring they have not been tampered with and are still valid or if they are still valid by checking with the Verifiable Data Registry that contains the Issuers' Decentralized Identifiers, public keys, and revocation data. Now, Existing systems do not demonstrate a detailed framework for SSI or effective utilization of verifiable credentials, often leading to over-reliance on issuers and a lack of decentralized identifiers (DIDs). The authors of Paper [6] have tried to build a blockchain-based Border Control and Immigration system, for which they tried to utilize the preexisting kiosks to integrate with the blockchain architecture in the backend rather than transforming the credentials like passport or tickets into digital identity, which could make the system lot easier and efficient. Nonetheless, the movement of credentials between two locations is also significant since standard schemes for credential transfers will make it more straightforward to have VCs implemented. So, we are going to cover one of the major standard efforts 22 in progress for our system, such as Presentation Exchange, Verifiable Presentation Request, DIDComm Messaging, CHAPI - Credential Handler API [28]. However, no central location for wallet standardization exists despite the work that has been done in defining data models of representations within a wallet to avoid vendor lock-in. Various technical architectures and Wallet/Agent options are available. Therefore, we will utilize some of the biggest ones in our system, like Aries Agents, LER (Learning and Employment Records), and EDVs (Encrypted

Data Vaults) [29]. To advance further security on the existing blockchain, biometrics could be used which would legitimate the person before entry to the ledger data. In this case, Hyperledger Indy would be perfect, which has been anticipated for digital identity [9]. In addition, Hyperledger Fabric offers more flexibility and scalability, which is suitable for enterprise-level applications. The authors in [1] have attempted to construct a public transport system that uses Self-sovereign Identity (SSI), but they were unable to offer an appropriate consensus method for their research, which affects the transaction and mining process. Also, current systems primarily record basic travel information, such as origin and destination, without considering the traveler's history, which could pose significant security challenges. Accordingly, in our system, we will utilize ACA-Py (Aries Cloud Agent Python) and a mediator to facilitate communications in a peer-to-peer manner between decentralized entities in an SSI ecosystem. Due to the lack of opinionated components, the mediator facilitates effective asynchronous communication and delivers messages to the agents including the Aries Bifold Wallet, that might not necessarily have a public endpoint. The wallet receives messages safely through DIDComm protocols to communicate with the mediator. In a network backed by Hyperledger Fabric, agents such as government organizations or private entities can use ACA-Py to verify credentials and interact through a trusted framework. The mediator facilitates the interactions while at the same time keeping the system private and the control distributed, therefore playing a key role in the SSI architecture.

4.3 Threat Model

While working on an implementation-based thesis, we need to analyze all possible threats that we may face. Here, we talk about the potential threats our system might face.

T1 Spoofing Identity: As we aim to digitize passports using SSI, passport credentials can be spoofed through an individual's wallet. As the wallet holds a person's public and private keys and other credentials, if an attacker manages to get into one's wallet, then he can misuse the holder's credentials for illegal acts.

T2 Tampering with Data: As we are using blockchain-based SSI to store passport credentials, there remains the chance of data being tampered with. Because all the credentials are being stored in the blockchain ledger. And if an attacker manages to get control over 51% of the network, then he can temper any data from the ledger of any individuals. It can take place because of political pressure. Therefore, the risk remains.

T3 Repudiation: As all the verifiable credential (VC) gets issued by an issuer, a case might happen that the holder later sometimes denies that he requested any VC. If our system does not store all the VC requests and the consent history of the holder in the blockchain ledger, we might face a repudiation scenario.

T4 Information Disclosure: In our SSI system, Information disclosure can happen in many ways. Users can mistakenly share sensitive information or detailed information that was not required; once it is shared, now verifiers can use that information illegally if they want. Also, another way to disclose information is if the user unintentionally uses third-party apps or services. Third-party organiza-

tions usually do website phishing, which is creating fake websites, taking sensitive information from users, and then using their information illegally.

T5 Denial of Service (DoS): To utilize SSI one needs to use a wallet to request or share verifiable credentials. If a Denial of Service attack takes place, then the wallet will halt, and the user won't be able to access or control information. Also, if the underlying blockchain ledger gets a DoS attack, then all transactions will be disrupted; neither the issuer nor the verifier will be able to issue or verify for the user. A denial of service can heavily disrupt the ecosystem of the Self-sovereign Identity.

T6 Elevation of Privilege: If an attacker manages to take over one's wallet, then he can take privilege using user credentials. Attackers might use credentials for sensitive site verification which will affect the user record and won't affect the attacker in any way. Attackers may take control over everything that the user has, the attacker can sign with the private key of the user in any illegal service he wants to use. That is how an attacker can get an elevation of privilege.

T7 Replay Attack: This attack can take place while exchanging credentials from issuer to holder or holder to verifier. If the attacker captures the sensitive information later, he can request an illegal transaction. He can start a replay attack to use services even after the due date.

T8. Lack of Consent: A lack of consent can take place when a user mistakenly agrees to share sensitive information or does not have a proper idea about the service but agrees to use it. This will affect later on when the credentials will be used against him and will be used in illegitimate acts.

T9. Lack of Control: If our system does not utilize the user consent system, then it won't be able to give freedom to the user. A bug in the control system can cause a lack of control, and then it won't be decentralized anymore. A central authority will take control over an individual.

4.4 Requirement Analysis

In this section, we will explain the functional requirements, security requirements and privacy requirements that are needed for our system.

4.4.1 Functional Requirements (FR)

Here we will explain the functional requirements for our system.

FR1. The system needs to be able to securely handle user digital identities, the public and private keys storage or retrieval as well as any other personal credentials for such purposes.

FR2. Essentially, a SSI wallet should also be provided since it supports the system by allowing users to control their identities through such means.

FR3. Integration with the blockchain is required for storing passport credentials and other identity data. This ensures immutability and distributed validation.

FR4. The resulting system should have a mechanism that all VCs are issued by authorized issuers as well as the history of each verifiable credential request and its consent kept in the blockchain ledger.

FR5. Make sure that all credential releases need a user's explicit consent and allow them to obtain control over the individual claims released

FR6. Because the system deals with user data and identity information, it should comply with relevant privacy and security laws to ensure that stored data is protected.

FR7. Such a system needs to provide the user with an intuitive interface for managing digital identities and credentials, thus encompassing easy management of data by users.

4.4.2 Security Requirements (SR)

Here, we will explain the security requirements for our system.

SR1. Multifactor authentication of the wallet to gain access and prevent identity spoofing. In addition, the system should provide authentication via a VC-based SSI. This will avert the T1 peril.

SR2. To protect against the T2 threat, the system needs to implement advanced cryptographic measures that prevent data tampering and preserve ledger integrity.

SR3. The system should either maintain full logs (audit trails) of all VC requests and consents or use digital signatures in order to avoid the T3 threat.

SR4. The system needs to perform the heavy lifting of a strong encryption algorithm for data at rest and in transit so that only authorized parties are able to read it. This can prevent the T4.

SR5. The system should be able to withstand DoS attacks through network design resilience and redundant systems thus as to avoid the T5 threat.

SR6. To mitigate the impact of T6, stringent access control policies limiting unauthorized privilege elevation should be implemented.

SR7. To reduce the risk of T7, system safeguards against possible replay attacks must be introduced.

4.4.3 Privacy Requirements (PR)

Here we will explain the privacy requirements for our system.

PR1. T8 can be reduced by ensuring a user-centric consent management framework that guarantees the issuance of VCs with the concerned users' consent in the system.

PR2. In order to avoid T9, allow granular controllers on users' data sharing and claims release SPs.

Chapter 5

Architecture and Protocol Flow

This chapter elaborates on all the design details and operational processes of the system. First, it describes the system architecture and outlines the main components and the interaction between them. It proceeds by detailing the protocol flow necessary for depicting the system working in real life. Algorithms, with code snippets to show the technical implementation or core functionalities, are described toward the end.

5.1 System Architecture

Figure 5.1 depicts the architecture of the SSI-based secure travel pass system. The design of the architecture is set up to support the functionalities we discussed earlier. From Figure 5.1, the system has several key components: issuer (passport office, embassy), verifier (immigration center, embassy), user (citizen), mobile wallet, mediator, and blockchain (indy and fabric). The issuer and verifier are in charge of providing web services based on SSI features. Users use a wallet, along with a mediator, to interact with the issuer and verifier and to store the verifiable credentials (VCs) they receive [3]. The mediator connects the message between the wallet and issuer, as well as the verifier. It can also hold the messages sent to the wallet when it is offline and deliver them once online [3]. The verifier, issuer, and mobile wallet interact with the blockchain, which is used as a verifiable data registry. Our architecture incorporates the following functionalities.

i. **Setting up the connection:** A connection using Self-sovereign Identity (SSI) must be made between the user's wallet and both the issuer and the verifier.

ii. **Fetching DID from Trusted Issuer List:** The verifier, acting as an immigration center, needs to retrieve the passport and visa issuer's DID from the Fabric blockchain.

iii. **Checking the NID database:** Before issuing a verifiable credential (VC), the issuer, functioning as a passport office, must confirm the user's identity using the National ID database.

iv. **Issuing the VC:** Once requested by the user, the issuer can provide a Veri-

fiable Credential (VC) using the already established connection, similar to a user registration process in traditional passport systems.

v. **Storing the VC:** The VC that the user receives must be securely stored in their digital wallet.

vi. **Verifying the VC:** The verifier, such as an immigration center or embassy, uses the same connection to request proof of the VC from the user. This is the authentication process.

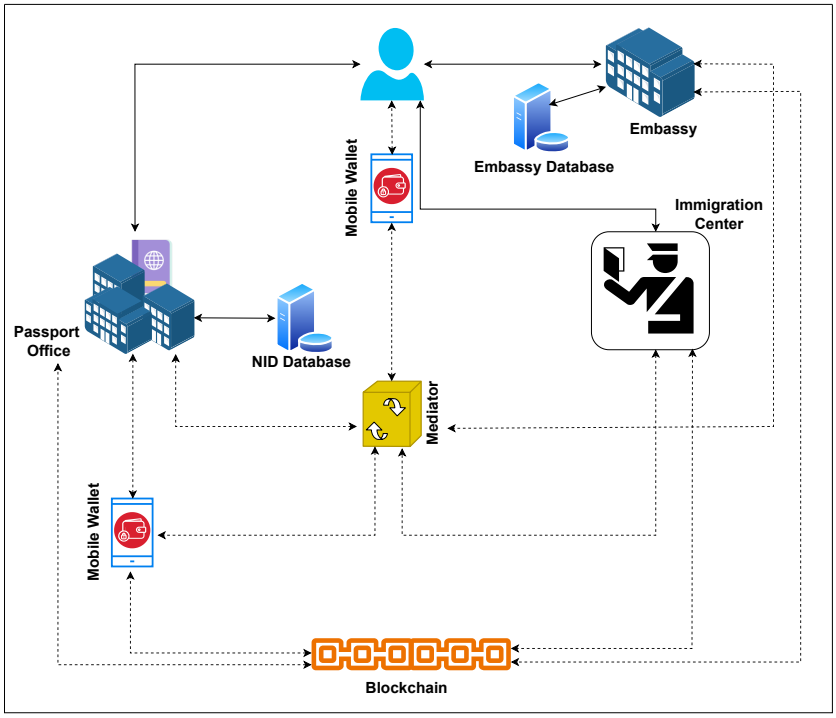


Figure 5.1: Architecture of SSI-Based Secure Travel Pass System.

5.2 Protocol Flow and Use-Case

We demonstrate some use-cases with protocol flows to show how SSI-based passports and visas can be used to access different countries. As a first step, we outline the cryptographic notations that will be applied in the Protocol. The function of each notation has been presented in Table 5.1.

Table 5.1: Cryptographic Notations.

Notations	Description
V	Acting as a Verifier
I	Acting as a Issuer
U	Acting as a User
K_I^U	Public key of I for U
$K_I^{-1\|U}$	Private key of I will used for U
K_U^I	Public key of U for I

Notations	Description
$K_U^{-1\|I}$	Private key of U will be used for I
K_V^U	Public key of V for U
$K_V^{-1\|U}$	Private key of V will be used for U
K_U^V	Public key of U for V
$K_U^{-1\|V}$	Private key of U to be used for V
DID_U^I	Decentralized identifier of U for I
DID_I^U	Decentralized identifier of I for U
DID_V^U	Decentralized identifier of V for U
DID_U^V	Decentralized identifier of U for V
DID_I^V	Decentralized identifier of I for V
DID_V^I	Decentralized identifier of V for I
VC_V^U	A verifiable credential issued by V to U
N_i	A fresh nonce
$\{...\}_K$	Encryption operation using a public key K
$\{...\}_{K^{-1}}$	Signature using a private key K^{-1}
H(M)	SHA-512 hashing operation of message M
B	Blockchain
nidDB	NID Database
$[...]_K$	Communication over a channel encrypted with key K
[...]	Communication over an unencrypted channel
[[...]]	Optional Data
X,Y	Country
CM	Consensus Mechanism
C_{all}	All Country
c_i	country 'i'
Req_{join}	Joining Request
$Data_Y$	Requested data from 'Y'
$Sign_Y$	Signature by 'Y'
$Vote_Y$	Voting for country 'Y' to join
$Result_{vote}$	Outcome of voting process from all the nodes
$Node_{join}$	Node Configuration
$Node_Y$	Node of 'Y'
$Cert_{CA}$	CA Certificate
$Config_Y$	Node Configuration of 'Y'
$Updated_{Ledger}$	Ledger update operation by Consensus Mechanism
$Sign_{CM}$	Signature by consensus Mechanism

Next, the data that is interacting between two entities is represented by a data model in an abstract manner, as shown in Table 5.2. The data model has been constructed along with request and response processes. Our protocol flow offers a request and a relevant response pattern consisting of four types of requests. Some of these are invite requests (inviteRequest), credential requests (credentialRequest), and service requests (serviceRequest), which indicate a request for a proof (proofRequest).

Table 5.2: Data Model.

request $\triangleq \langle \text{SSIOptionRequest}, \text{inviteRequest}, \text{credentialRequest}, \text{proofrequest} \rangle$
response $\triangleq \langle \text{SSIOptionResponse}, \text{inviteresponse}[1-2], \text{credentialResponse}, \text{proofResponse} \rangle$
SSIOptionRequest $\triangleq \langle \text{Url}_{Si}, [[\text{inviteCookie}, \text{serviceCookie}]] \rangle$
inviteRequest $\triangleq \langle \text{Url}_V, \text{Url}_I, N_i \rangle$
inviteResponse1 $\triangleq \langle N_i, \text{DID}_U^V, \text{DID}_I^V, \text{DID}_U^I \rangle$
inviteResponse2 $\triangleq \langle N_i, \text{DID}_V^U, \text{DID}_I^V, \text{DID}_I^U \rangle$
credentialRequest $\triangleq \langle$"Requesting Credential"$\rangle$
attributeRequest $\triangleq \langle a_1, a_2, \ldots, a_n \rangle$
attributeResponse $\triangleq \langle (a_1, a_V 1), (a_2, a_{V2}), \ldots, (a_n, a_{Vn}) \rangle$
fileRequest $\triangleq \langle$"Requesting Bank Statement, Work Statement, TIN , NOC "$\rangle$
fileRequest $\triangleq \langle$.pdf/.docx$\rangle$
credentialResponse $\triangleq \langle \text{VC}_I^U \rangle$
$\text{VC}_I^U \triangleq \langle \{(a_1, a_{V1}), (a_2, a_{V2}), \ldots, (a_n, a_{Vn})\}, H((a_1, a_{V1}), (a_2, a_{V2}), \ldots, (a_n, a_{Vn})) \rangle K_I^{-1\|U}$
initiateProofRequest $\triangleq \langle$"InitiatingProofRequest"$\rangle$
proofRequest $\triangleq \langle a_1, a_2, \ldots, a_n \rangle$
proofResponse $\triangleq \langle \text{VC}_V^U \rangle$
TrustedIssuerListInsert $\triangleq \langle DID_I^V \rangle$
retrieveTrustedIssuerList $\triangleq \langle DID_I^V \rangle$
NidRequestApi $\triangleq \langle a_1, a_2, \ldots, a_n \rangle$
NidResApi $\triangleq \langle$Verification Status$\rangle$

The inviteRequest takes place first between entities. For each inviteRequest, there are two invite responses. An inviteRequest contains the URL of any SSI agent (such as government or embassy) and a fresh nonce. An inviteResponse1 contains the nonce used for the inviteRequest and the user's DID to be used for the issuer or verifier. inviteResponse2 holds the nonce and a DID of the issuer or verifier to be used by the user. Likewise, attributeRequest and attributeResponse are used as prerequisites for credentialRequest. The attributeRequest holds the list of attributes, and the attributeResponse contains the value alongside attributes. A credentialResponse is sent to the user containing a verifiable credential (VC) addressing a specific credentialRequest. A verifiable credential includes a list of attributes. To represent a passport as VC, the attributes will hold information related to a citizen (user), for example; name, birth date, gender, passport number etc, denoting a specific user's passport. The VC will be cryptographically signed by the issuer (passport office) for a particular user, maintaining the integrity and validity of the VC for the user. Moreover, an initiateProofRequest is sent to the verifier, and in response, the verifier asks for proofRequest, which contains the attributes. The user then sends a proofResponse, which holds a verifiable credential issued earlier to the user. A general database is used to store Nid-related attributes; it returns true or false after verification. TrustedIssuerListInsert (trust issuer list) and RetrieveTrustedIssuerList are used to store the "DID" Docs of specific country issuers in a fabric blockchain, ensuring a standard passport protocol.

Next, we describe the protocol flow in four use cases. The flow is illustrated from

Table 5.3 to Table 5.6 and then explained.

5.2.1 Building Trusted Issuer List

This use-case depicts the protocol flow by which a country becomes part of the consortium and participates in maintaining the Trusted Issuer List depicted in Table 5.3.

Table 5.3: Use-case 1.

Message	Flow
M1	$Y \rightarrow X : [Req_{join}, Data_Y, Sign_Y]_{\text{https}}$
M2	$X \rightarrow CM : [Req_{join}, Data_Y, Sign_Y]_{\text{https}}$
M3	$CM \rightarrow C_{all} : [Vote_Y, Req_{join}, Data_Y, Sign_Y]_{\text{https}}$
M4	$C_i \rightarrow CM : [Vote_{approve/reject}, Sign_Y]_{\text{https}}$
M5	$CM \rightarrow Y : [Approval/Rejection, Result_{vote}, Sign_{CM}]_{\text{https}}$
M6	$Y \rightarrow CM : [Node_{join}, Cert_{CA}, Config_Y, Sign_Y]_{\text{https}}$
M7	$CM \rightarrow C_{all} : [Node_Y, Updated_{Ledger}, Sign_{CM}]_{\text{https}}$

M1: Country 'Y' sends a request to join the consortium body along with the required data to Country 'X'.

M2: Country 'X' forwards the request from Y to the consensus mechanism (CM) for processing. The consensus mechanism distributes this request to all nodes in the consortium.

M3: The consensus mechanism broadcasts the join request to all countries (C_{all}) in the consortium for voting.

M4: Each country C_i in the consortium evaluates the request and sends its vote (approve/reject) back to the consensus mechanism.

M5: Consensus Mechanism (CM) communicates the final decision (approval or rejection) to country Y along with the majority vote result.

M6: Country 'Y' submits its node configuration, CA certificate, and other required configurations to join the consortium.

M7: The consensus mechanism updates the ledger to include country 'Y' as part of the consortium and broadcasts this update to all member nodes.

Figure 5.2 shows how a country can join the consortium through the consensus mechanism and contribute towards updating the Trusted Issuer List.

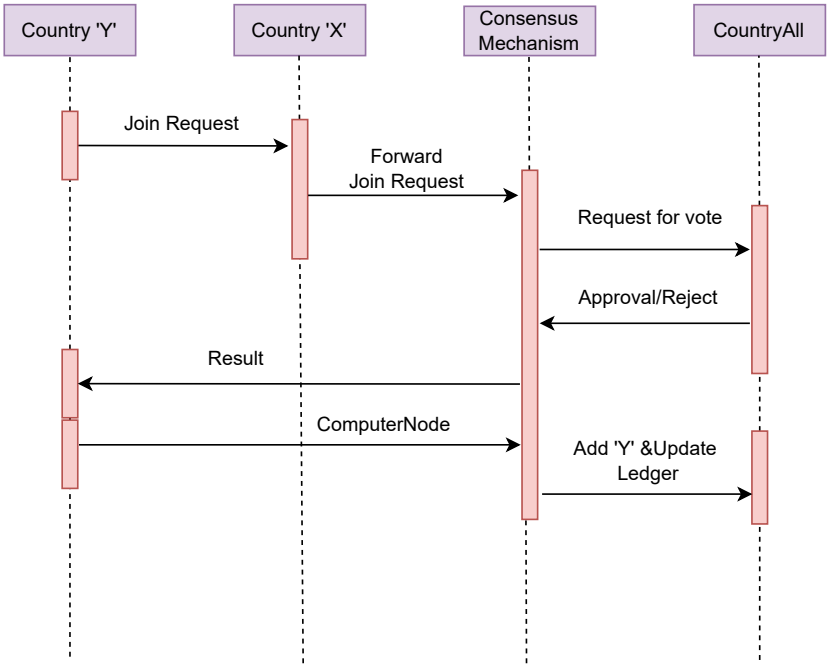


Figure 5.2: Building up the Trusted Issuer List.

5.2.2 Receiving a Passport

Here, 5.4 displays the protocol flow between the issuer (Passport Office) and user (Citizen of country X). In this process, a citizen submits the required information to apply for a passport and receives it as a verifiable credential (VC), as shown in Table 5.4.

Table 5.4: Use-case 2.

Message	Flow
M1	$U \rightarrow I : [N_1, \text{passportServicePageRequest}]_{\text{https}}$
M2	$I \rightarrow U : [N_2, \text{nidSubmissioResponse}]_{\text{https}}$
M3	$U \rightarrow I : [N_2, \text{nidResponse}]_{\text{https}}$
M4	$I \rightarrow NidDb : [N_3, \text{nidResponse}]_{\text{https}}$
M5	$NidDb \rightarrow I : [I, N_3, \text{verificationStatus}]_{\text{https}}$
M6	$I \rightarrow U : [N_3, \text{ssiConnectionPage}]_{\text{https}}$
M7	$U \rightarrow M : [I, N_3, \text{connectionResponse1}(DID_U^I)]$
M8	$M \rightarrow I : [N_3, \text{connectionResponse1}(DID_U^I)]$
M9	$I \rightarrow M : [U, N_3, \text{connectionResponse2}(DID_I^U)]$
M10	$M \rightarrow U : [N_3, \text{connectionResponse2}(DID_I^U)]$
M11	$I \rightarrow U : [N_5, \text{fileRequest}]_{\text{https}}$
M12	$U \rightarrow I : [N_5, \text{fileResponse, credentialRequest}]_{\text{https}}$
M13	$I \rightarrow M : [U, \{N_5, \text{credentialResponse}\}K_U^I]_{\text{http}}$
M14	$M \rightarrow U : [\{N_5, \text{credentialResponse,offer}\}K_U^I]_{\text{http}}$
M15	$M \rightarrow I : [N_5, \text{confirmationOfAcceptance}]_{\text{https}}$

M1: The user (Citizen) looks for the passport service page from the issuer (Passport office) website.

M2, M3, M4 and M5: Here, firstly, the issuer sends the Nid login page, where the user provides his nid number, which then gets checked by the issuer nid database and receives a verification status from the database.

M6: The issuer creates a new connection and displays a QR code for the user to scan.

M7 and M8: Upon scanning a QR code with their mobile wallet, the user initiates the creation of a public key and private key pair ($K_U^I$and $K_U^{-1|I}$) and a decentralized identifier (DID) denoted as (DID_U^I). A corresponding DID Document is then constructed using this key pair and subsequently uploaded to the Indy blockchain. Following this, the wallet generates an inviteResponse1 message, incorporating (DID_U^I), and transmits it to the issuer (passport office) through an intermediary referred to as Mediator M.

M9 and M10: The issuer accesses the required DID Document from the Indy blockchain by referencing DID_U^I and retrieves the associated public key K_U^I. Utilizing this key, the issuer produces a new public and private key pair (K_I^U and $K_I^{-1|U}$) and assembles a new DID Document. This updated document is then published to the blockchain. Finally, the issuer formulates an inviteResponse2 message using K_I^U and forwards it to the user for further interaction.

M11 and M12: Now the issuer sends a file upload page for offline verification and accepts files like Noc, Tin and other necessary documents. In response, the user sends those files by initializing a credential request.

M13 and M14: After offline verification, the Issuer generates and returns a new VC (VC_I^U via mediator) by retrieving necessary attributes using the nid number of the user.

M15: The mediator then passes the VC_I^U to the user.

Use-case 2 is illustrated in Figure 5.3, where we portrayed how a user could acquire a passport as VC.

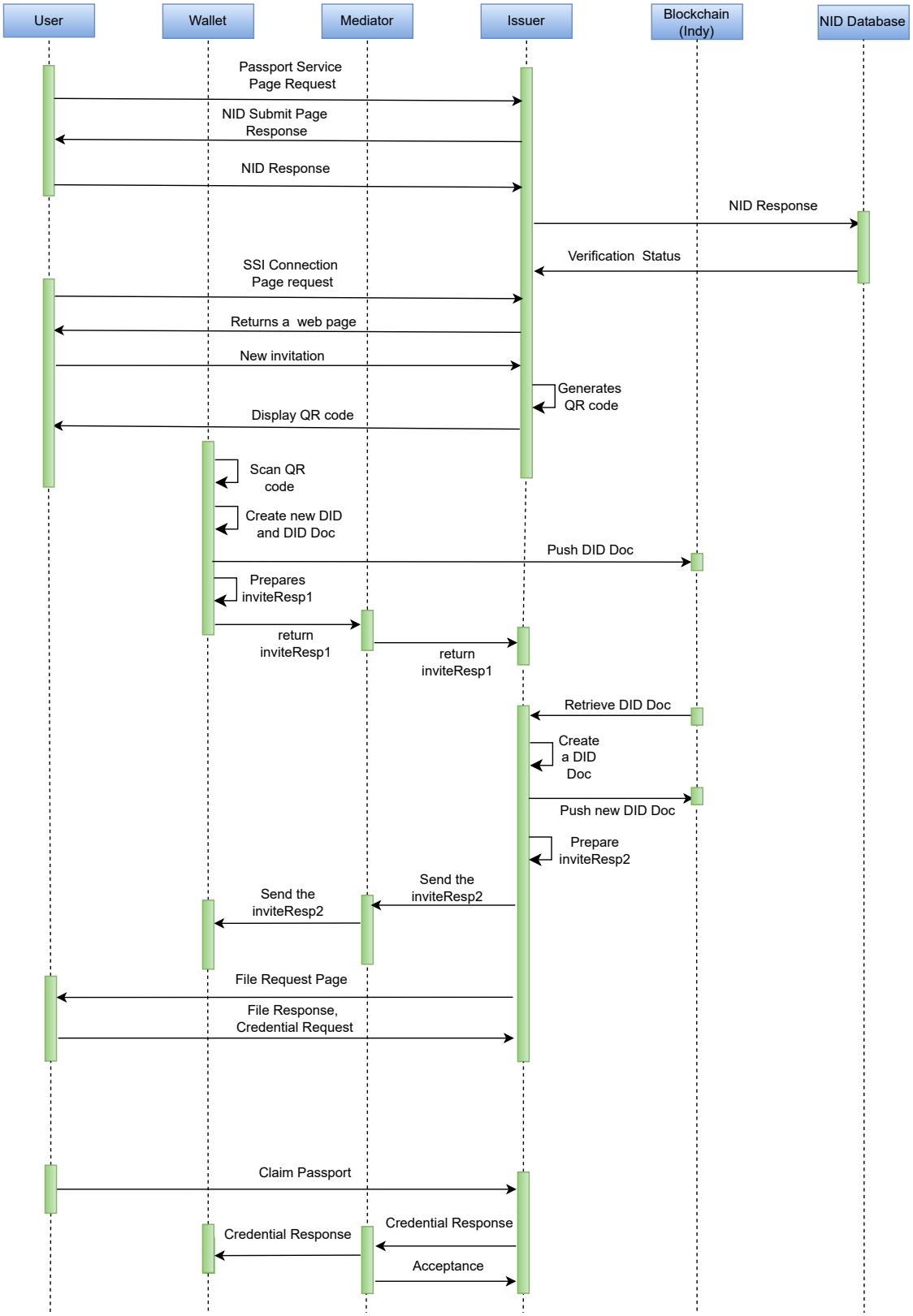


Figure 5.3: Receiving Passport as a Verifiable Credential.

5.2.3 Receiving a Visa

Following, Use-case 3 demonstrates the protocol flow between the embassy and the user (Citizen) acquiring a visa as a verifiable credential in Table 5.5. In use case 3, the embassy will act as both the verifier and issuer. They will first verify the passport from the Trusted Issuer List, which is available at both the immigration center and the embassy within the country.

Table 5.5: Use-case 3.

Message	**Flow**
M1	$U \rightarrow I : [N_1, \text{visaServicePageRequest}]_{\text{https}}$
M2	$I \rightarrow U : [N_2, \text{nidSubmitPageResponse}]_{\text{https}}$
M3	$U \rightarrow I : [N_2, \text{nidResponse}]_{\text{https}}$
M4	$I \rightarrow NidDb : [N_3, \text{nidResponse}]_{\text{https}}$
M5	$NidDb \rightarrow I : [N_3, \text{verificationStatus}]_{\text{https}}$
M6	$I \rightarrow U : [N_3, \text{ssiConnectionPage}]_{\text{https}}$
M7	$U \rightarrow M : [I, N_3, \text{connectionResponse1}(DID_U^I)]$
M8	$M \rightarrow I : [N_3, \text{connectionResponse1}(DID_U^I)]$
M9	$I \rightarrow M : [U, N_3, \text{connectionResponse2}(DID_I^U)]$
M10	$M \rightarrow U : [N_3, \text{connectionResponse2}(DID_I^U)]$
M11	$U \rightarrow I : [N_6, \text{initiateProofRequest}]_{\text{https}}$
M12	$I \rightarrow M : [U, \{N_6, \text{presentPassportRequest}\}K_U^I]$
M13	$M \rightarrow U : [\{N_6, \text{presentPassportRequest}\}K_U^I]$
M14	$U \rightarrow M : [I, \{N_6, \text{presentPassportResponse}\}K_I^U]$
M15	$M \rightarrow I : [\{N_6, \text{presentPassportResponse}\}K_I^U]$
M16	$I \rightarrow B : [\{N_6, \text{readRequest}\}K_I^U]$
M17	$B \rightarrow I : [N_6, \text{retrieveTrustIssuerList}(DID_I^V)]$
M18	$I \rightarrow U : [N_7, \text{fileRequest}]_{\text{https}}$
M19	$U \rightarrow I : [N_7, \text{fileResponse,credentialRequest}]_{\text{https}}$
M20	$I \rightarrow M : [U, \{N_5, \text{credentialResponse}\}K_U^I]$
M21	$M \rightarrow U : [\{N_5, \text{credentialResponse, offer}\}K_U^I]$
M22	$M \rightarrow I : [N_5, \text{confirmationOfAcceptance}]_{\text{https}}$

M1: The user(Citizen) looks for the visa service page from the issuer (Embassy) website.

M2, M3, M4 and M5: Here, firstly, the issuer sends the Nid login page, where the user provides his nid number, which then gets checked by the issuer nid database and receives a verification status from the database

M6: The issuer creates a new connection and displays a QR code for the user to scan.

M7, M8, M9 and M10: Similar to M7-M10 from Use-case 2. Here, the issuer is the embassy.

M11: The user is redirected to the SSI options page and selects the passport present request option.

M12 and M13: The visa issuer creates a proof request and sends it to the user's wallet through the mediator.

M14 and M15: Initially, the user's verifiable credential (VC_I^U) is retrieved and cross-checked against the previously issued credential presented to them. The corresponding credential is then shown to the user for confirmation. Upon receiving the user's approval, the mobile wallet generates a proofResponse containing the validated credential, such as passport information, and transmits it to the issuer via the mediator.

M16 and M17: The Issuer(playing the role of verifier) will retrieve the Trusted Issuer List from the fabric blockchain and compare it with the user's VC to verify if the DID of the issuer who issued the VC to the user is included in the trusted issuer list (usecase1 M7). If the DID matches then the issuer (ambassador) will proceed to issue the visa.

M18 and M19: The issuer (Embassy) requests necessary documents such as a bank statement, work statement, TIN, and NOC. The user (Citizen) then responds by submitting these files in .pdf or .docx format. Also, the user sends a credential request to the issuer.

M20 and M21: After offline verification, the Issuer generates and returns a new VC (VC_I^U via mediator) by retrieving necessary attributes using the nid number of the user. The mediator then passes the VC_I^U to the user.

M22: Here, the mediator passes acceptance confirmation to the issuer.

Use-case 3 is depicted in Figure 5.4, where we portrayed how a user could acquire a visa as VC.

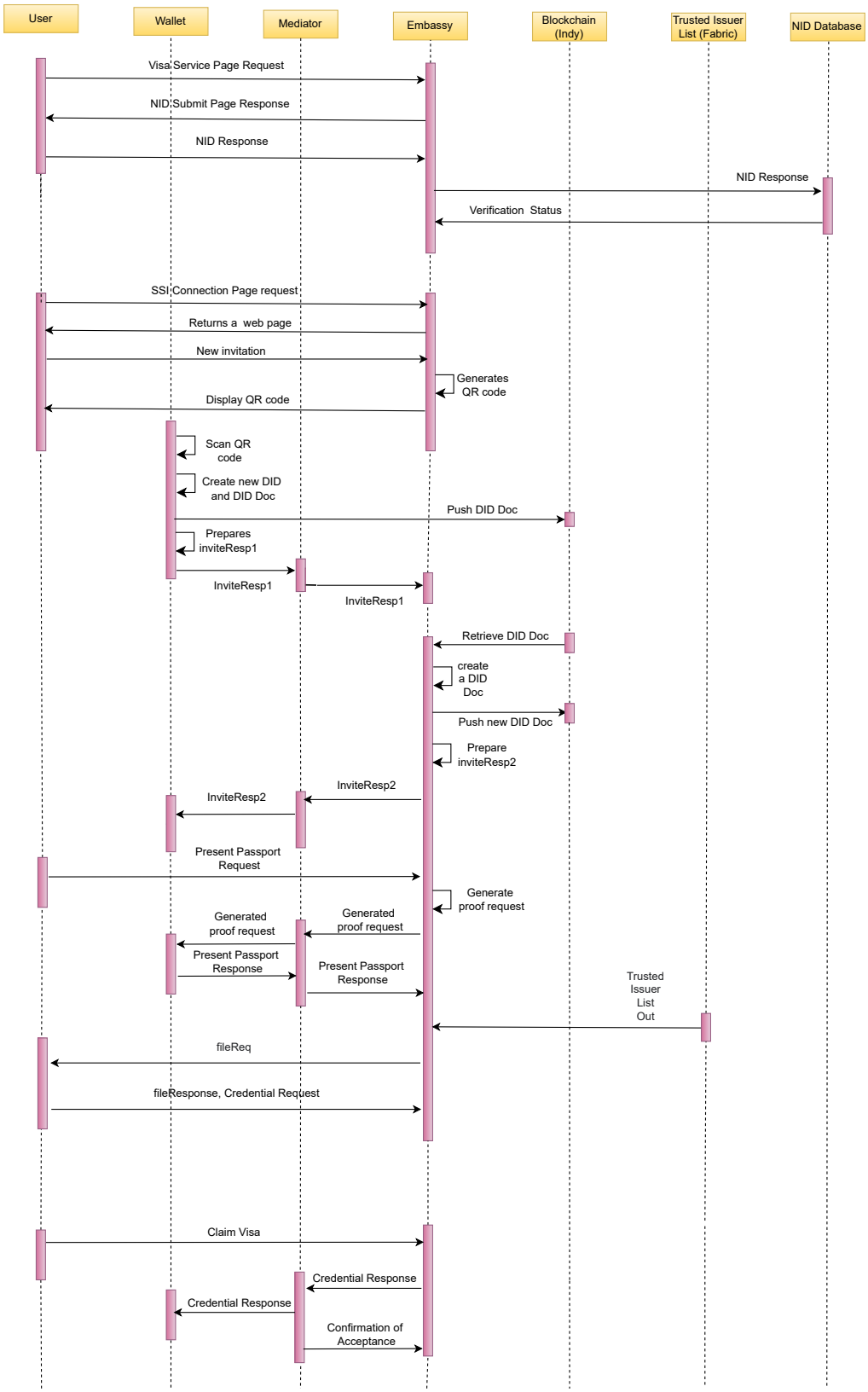


Figure 5.4: Receiving Visa as a Verifiable Credential.

5.2.4 Passport and Visa Verification during Immigration

Likewise, Use-case 4 portrays the protocol flow between the user (Citizen) and the verifier (Immigration center) while crossing the border or immigration in Table 5.6. In this use-case, the user provides the passport and visa as variable credentials (VC) to the immigration officer, which then gets verified for passing the immigration or the border.

Table 5.6: Use-case 4

Message	**Flow**
M1	$U \rightarrow V : [N_1, \text{immigrationServicePage}]_{\text{https}}$
M2	$V \rightarrow U : [N_2, \text{connectionPage}]_{\text{https}}$
M3	$U \rightarrow M : [V, N_3, \text{connectionResponse1}(DID_U^V)]$
M4	$M \rightarrow V : [N_3, \text{connectionResponse1}(DID_U^V)]$
M5	$V \rightarrow M : [U, N_3, \text{connectionResponse2}(DID_V^U)]$
M6	$M \rightarrow U : [N_3, \text{connectionResponse2}(DID_V^U)]$
M7	$U \rightarrow V : [N_6, \text{initiateProofRequest}]_{\text{https}}$
M8	$V \rightarrow M : [U, \{N_6, \text{presentPassportRequest}\}K_U^V]$
M9	$M \rightarrow U : [\{N_6, \text{presentPassportRequest}\}K_U^V]$
M10	$U \rightarrow M : [I, \{N_6, \text{presentPassportResponse}\}K_V^U]$
M11	$M \rightarrow V : [\{N_6, \text{presentPassportResponse}\}K_V^U]$
M12	$V \rightarrow B : [\{N_6, \text{readRequest}\}K_V^U]$
M13	$B \rightarrow V : [N_6, \text{retrieveTrustedIssuerList}(DID_I^V)]$
M14	$V \rightarrow M : [U, \{N_6, \text{presentVisaRequest}\}K_U^V]$
M15	$M \rightarrow U : [\{N_6, \text{presentVisaRequest}\}K_U^V]$
M16	$U \rightarrow M : [I, \{N_6, \text{presentVisaResponse}\}K_V^U]$
M17	$M \rightarrow V : [\{N_6, \text{presentVisaResponse}\}K_I^U]$
M18	$V \rightarrow B : [\{N_6, \text{readRequest}\}K_V^U]$
M19	$B \rightarrow V : [N_6, \text{retrieveTrustedIssuerList}(DID_U^I)]$
M20	$V \rightarrow U : [\text{Allowed to cross the border}]_{\text{https}}$

M1: The user(Citizen) looks for the Immigration service page from the verifier (Immigration Center) website.

M2: The verifier creates a new connection and displays a QR code for the user to scan.

M3, M4, M5 and M6: Similar to M7-M10 from Use-case 2. Here, the verifier is the immigration center.

M7: The user (citizen) is switched to the SSI options page of the immigration center, where they choose the initiate proof request option so that they can prove their valid passport.

M8 and M9: The verifier (immigration center) constructs a present passport (proof request) for the passport as a verifiable credential (VC) and sends it to the user's wallet through the mediator.

M10 and M11: Upon receiving the proof request, the wallet reviews the requested attributes and conditions specified by the verifier. The corresponding VC is then

presented to the user for validation. Once the user grants approval, the wallet generates a proofResponse containing the verified passport credentials and forwards it to the immigration center via the mediator.

M12 and M13: After receiving the first proofResponse, the verifier checks the Trust Issuer list Blockchain with RetrieveTrustedIssuerList (DID_I^V). If the responded VCs (passport) issuer is found in the Trust Issuer list blockchain, then the passport is acceptable.

M14 and M15: Again, the verifier generates a proofRequest for the visa as VC, which is then sent to the user's wallet via the mediator.

M16 and M17:Similar to M10 and M11.

M18 and M19: After receiving the 2nd proofResponse, the verifier checks the Visa Blockchain with TrustedIssuerList (DID_U^I) to check whether the specific user's DID doc has been issued with a visa. If the DID doc matches the TrustedIssuerList, the responded VC (visa) is valid.

M20: After verifying both the passport and visa, the verifier confirms the immigration, sending a message to the user, 'Proof Success, Access Granted'.

Use-case 4 is illustrated in Figure 5.5, where we portrayed the passport and visa verification process during immigration. Additionally, the verifier will collect the user's (holder's) fingerprint for real-time verification.

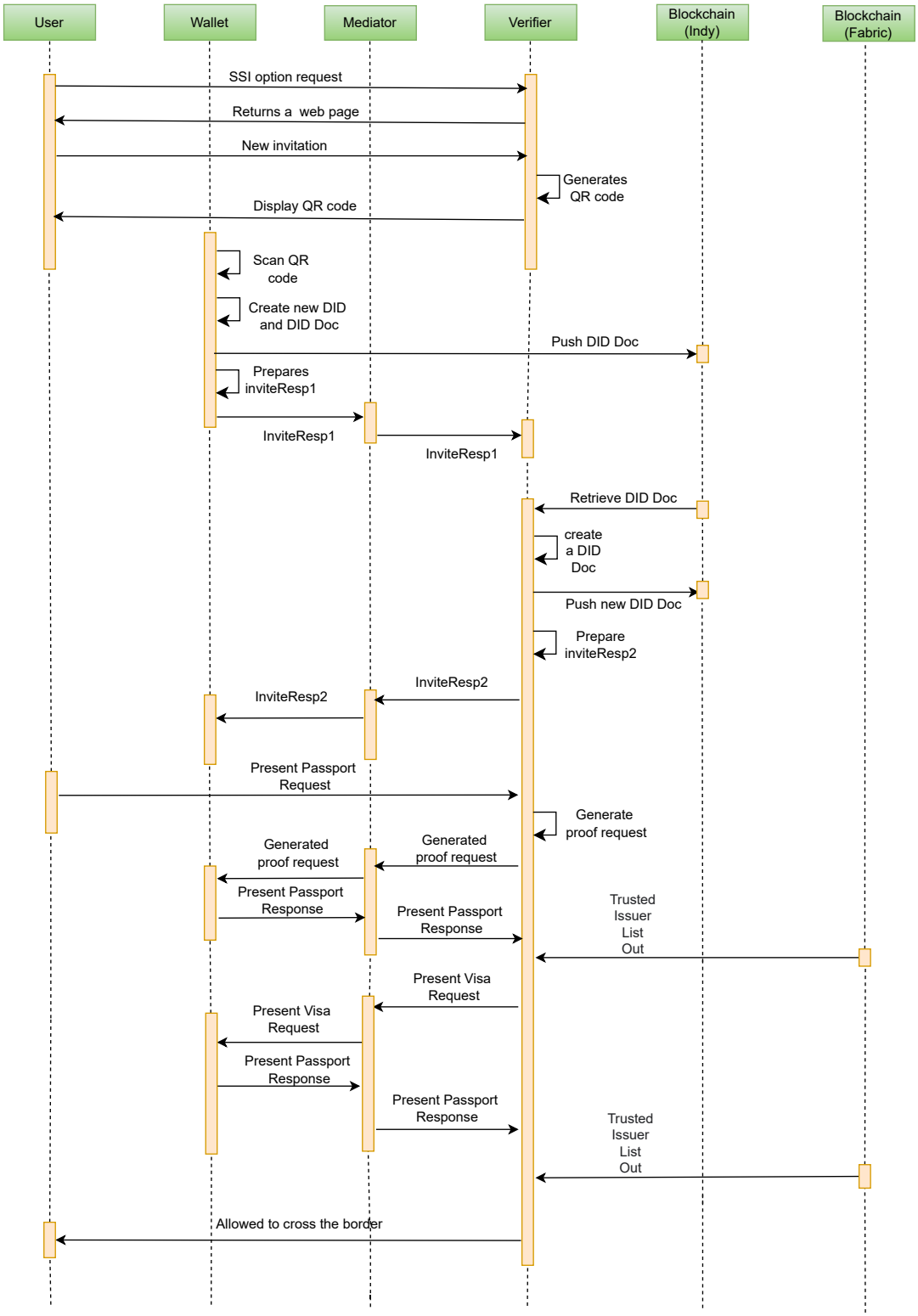


Figure 5.5: Passport and Visa Verification During Immigration.

5.3 Algorithom

Algorithm 1: Verifying from Trusted Issuer List.

```
Function checkIssuerList(decrypt(issueDID)):
    response = GET method call for fabric "ngrok-url";
    fabricDID = retrieve username;
    fabricOrg = retrieve organization name;
    if issueDID matches fabricDID then
        Display "Listed in trusted issuer list";
        if presentation received then
            return "Proof successful";
        else
            return "Presentation required";
    else
        return "Proof Rejection";
```

This function checks the issuer DID from the consortium blockchain Trusted Issuer list. It retrieves the DID and checks if the DID from the proof request and from the trusted issuer list matches or not. If it matches and the presentation is received from proof response, then it returns "proof successful" or else failure to prove.

Algorithm 2: ProofReq Function.

```
Function ProofReq(res):
    revokeCheck = Db.Find(encrypt(res));
    if decrypt(revokeCheck) == true then
        return "Revoked";
    else
        VC_p^c := ProofResponse.VC;
        DID_p^c := ProofResponse.DID_p^c;
        auth = checkSign(VC_p^c, DID_p^c);
        Send DID_p^c to the Trusted Issuer List and retrieve response;
        TIL = response;
        if TIL then
            return "Access Granted";
        else
            return "Not Allowed";
```

Algorithm 2 illustrates that the verifier first checks the revocation list to see if the passport is revoked or not. Then, after getting a proof response from citizens, verifiers will check the issuers' DID from the Trusted Issuer List to verify and allow access.

Chapter 6

Development

This chapter describes the development process, focusing on how ACA-Py manages DIDs and VCs on a blockchain network. It covers the deployment of a controller web server, integration with the BCovrin Test network for SSI workflows, and the use of Ngrok for secure and seamless communication with Hyperledger Fabric. Key tools like bifold and Rust libraries are also discussed to enhance interoperability and increase functionality.

6.1 Deployment Tools

In the blockchain context, ACA-Py stands for an Aries Cloud Agent Python application utilized to create, manage, and interact with DID and VC on a decentralized basis. It allows for secure communication and proving of identity or ownership in a blockchain network. This is an open-source tool that has been created as part of the Hyperledger Aries project, and it makes communication between different entities within a blockchain network to be secure and interoperable. This is the core of Aca- py which is simply a service we refer to as an agent. Once it is initiated, it also comes up with some API for us as well. Thus, ACA-Py is equipped with a connection, Issuing VC, and Proofing VC features that are all-inclusive. Next, To use those APIs, we need a web server from which to call them; this web server is referred to as the controller. We can think of it as a backend server that works with and invokes the APIs of ACA-Py. Hence, we developed a web server from which we run connection, VC, and proof APIs using ACA-Py. In addition, for the purpose of moving data in different situations, ACA-Py uses a webhook. In our instance, we used the URL for our controller by defining a route path that ends with /webhooks. For the project, we have used Bifold, an easy-to-use mobile app based on Aries Mobile Agent React Native that provides a secure way of exchanging verifiable credentials between agents. It has been developed in React Native and Aries Framework JavaScript (AFJ). It connects to the Indy ledgers using the ZMQ protocol [40]. In addition, our Proof of Concept utilizes the Hyperledger Indy-based blockchain network BCovrin Test (accessible at http://dev.greenlight.bcovrin.vonx.io/), which is a development instance. It is a verifiable data registry for testing and developing in an ecosystem of Self-sovereign identity (SSI). This network is part of the Verifiable Organizations Network (VON) development environment and is a registry and

resolution of DIDs, schemas, credential definitions, and other components of the SSI workflows. It is a test designed for developers and organizations that want to experiment with SSI technologies because it provides a safe, not production, environment to test how identity frameworks interact with SSI. To run our agent and communicate with Hyperledger Fabric, we used Ngrok (https://ngrok.com/). Still, Ngrok is a great tool that makes it possible to run local services (for example, an Aries Cloud Agent - ACA - based on Python) and allow these to be accessed in front of the public internet through safe (encrypted) tunnels. When we run an agent locally and want to interact with a Hyperledger Fabric network running on a different machine, we have a gap that needs to be bridged across our communications. Ngrok provides a public URL that points to the agent's local port. This setup suits the agent to send requests as well as the transactions and queries to the Fabric network and get back the response or callback. While testing a webhook or creating one can be done over HTTP, nothing aside from the HTTP method is secure, Ngrok achieves this by creating an encrypted HTTPS tunnel. It also has real-time traffic monitoring features to help it debug and inspect the interaction between the agent and Fabric.

6.2 System Overview

This section introduces the second layer of trust in the Hyperledger Fabric network, whereby countries come into a consortium to manage a Trusted Issuer List for passports and visas. It explains consensus and voting for adding new members, chaincode for revocation and sovereignty, and the multi-tier structure that allows secure international data sharing and building trust.

6.2.1 Trusted Issuer List

Figure 6.1 illustrates the second layer of trust introduced in our research, where multiple countries act as organizations within a Hyperledger Fabric blockchain network to make a consortium body. Each country operates its own peer nodes, representing entities like banks, passport offices, and customs or immigration departments. There is a consensus mechanism that acts as a gatekeeper, ensuring that any country wishing to join the blockchain adheres to its standards. It operates through predefined policies and voting mechanisms. New countries must communicate with any country within the consortium body and submit the required data to join. For instance, if a country 'Y' wants to join the consortium body, then it should send a request to country 'X' with the required data. Next, country 'X' will pass the request to the consensus mechanism. The consensus mechanism will pass this request to all the nodes (countries) in the consortium body. After that, there will be a voting mechanism in which every country has a vote concerning the request. If the consensus gets the majority vote then it will add the new country 'Y' into the consortium body.

In addition, the countries interact through channels in the blockchain, which enable them to access the ledger and data like the Trusted Issuer List and the chaincode. This Trusted Issuer List is an international registry of sorts and is maintained by all the countries in the network. It contains each country code as well as a decentralized identifier (DID) of all the passport Issuer and visa issuer. The registry

functions in accordance with the ICAO requirements when granting passports and visas. However, the recognition of such credentials still remains at the sovereign discretion of particular countries. For instance, country "A" can decline passports or visas of country "B" using a personal chaincode. This chaincode also maintains a Revocation List, which records any revoked passports or credentials.

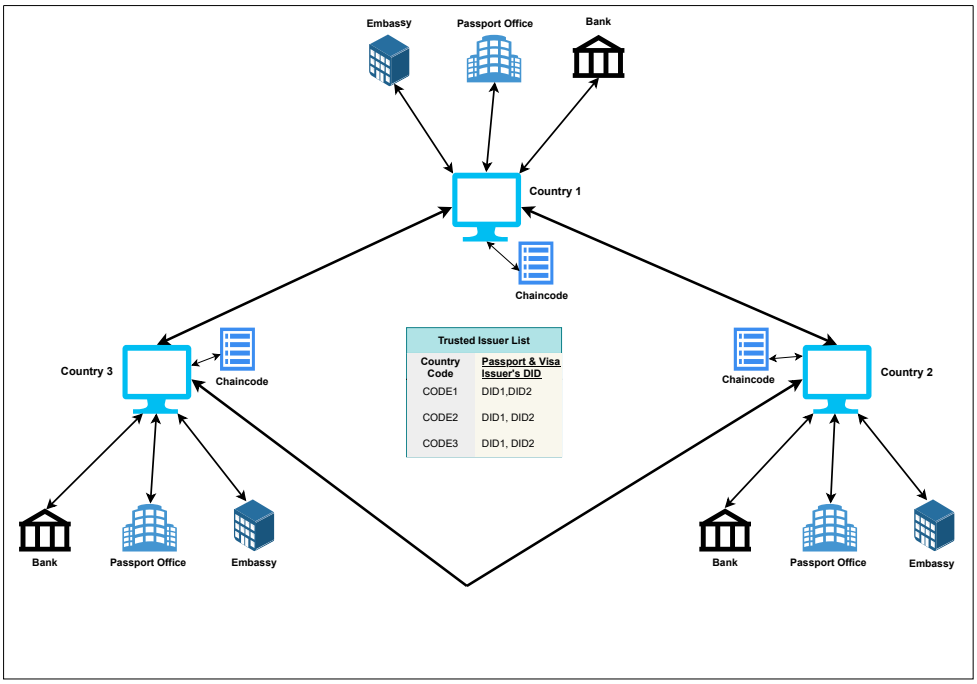


Figure 6.1: Second Layer of Trust.

For example, a scenario where Israel requests to join the Hyperledger Fabric network. After providing all the necessary data, Israel acquires authorization through a majority vote within the body of the consortium and becomes part of the network. Still, Bangladesh may decide not to recognize and accept passports to be issued by Israel. When an Israeli citizen presents their proof through SSI communication, the Bangladeshi immigration center follows a three-step verification process:

- **Verify the Trusted Issuer List:** Check whether Israel's passport office DID is present in the list.
- **Check Israel's Revocation List:** Access Israel's personal chaincode to determine if the citizen's DID has been revoked by Israel's government.
- **Consult the Rejected Country List:** Check Bangladesh's own chaincode to confirm whether Israel is listed among the rejected countries.

If the DID is revoked or if the country Israel is listed in the rejected country list in Bangladesh, the proof request will be denied. Other countries in the Hyperledger Fabric network can also see the chaincode of a certain country, but they can not modify it. This immutability is enforced through Hyperledger Fabric's role-based access control (RBAC) policies and its consensus mechanism. Also, the endorsement

policies of Fabric let countries disseminate and authenticate vital data with no compromising on data or policy sovereignty. It sets an optimal and protected multi-party and multi-tier structure of international data sharing and trust establishment.

6.2.2 Acquire Passport

In this use case, we have shown how a citizen of a country can issue a passport digitally using an SSI wallet. At first, a user will have to look for a Google passport page. It will take him to the Department of Passport page Figure 6.2, where he will be asked to provide the nid number. The nid number will be checked from the database. All the data in the NID database has been encrypted. After checking, if the NID matches, the page will auto-render to the SSI connection page Figure 6.3.

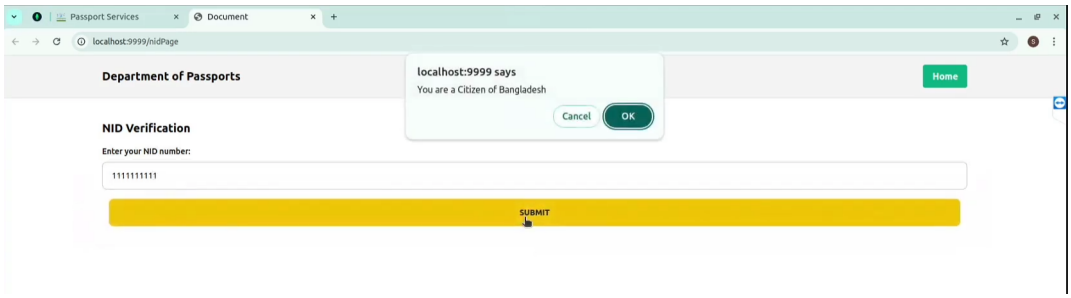


Figure 6.2: NID Verification.

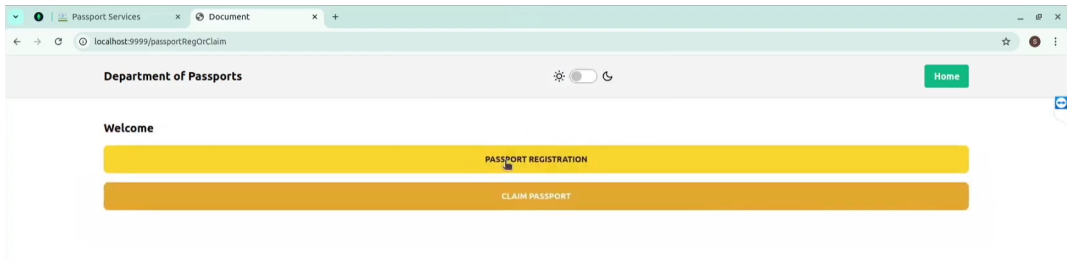


Figure 6.3: Passport Registration.

Figure 6.4: Connection to Passport Office.

They must connect to the passport office by clicking on passport registration. It will be rendered on the connection page in Figure 6.4.

Here with the SSI wallet, they will have to scan to get connected to the passport agent. After connecting, the page will render Figure 6.5.

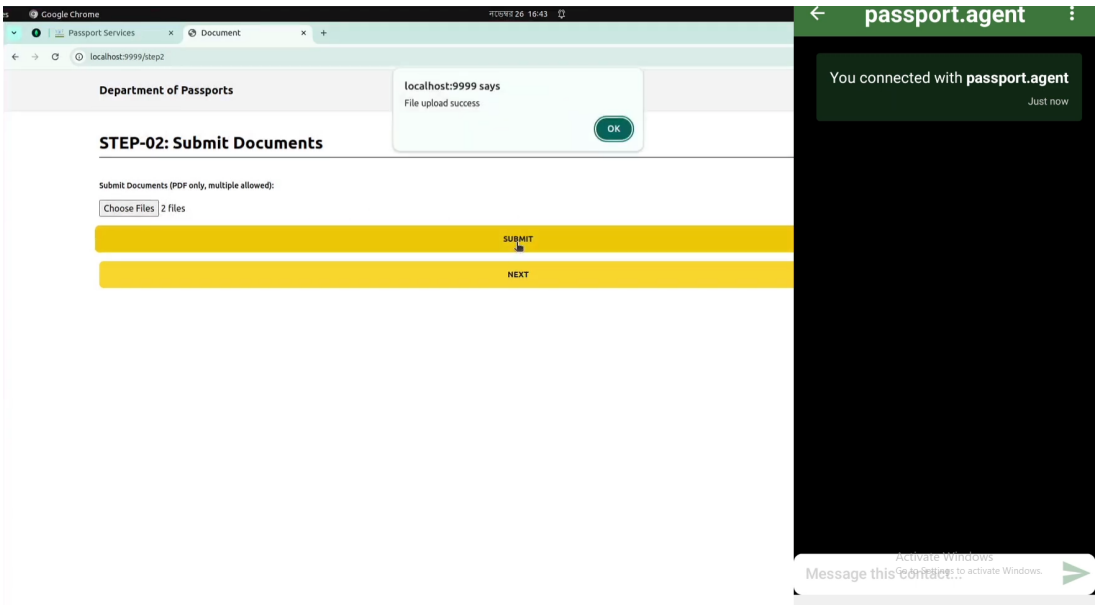


Figure 6.5: Passport Documents Submission.

They will submit the necessary files for offline verification here. After submission, the page will rendered to the waiting phase. Where they will be told to wait or recheck to claim. Now, when the verification is done, they will be able to claim their passport.

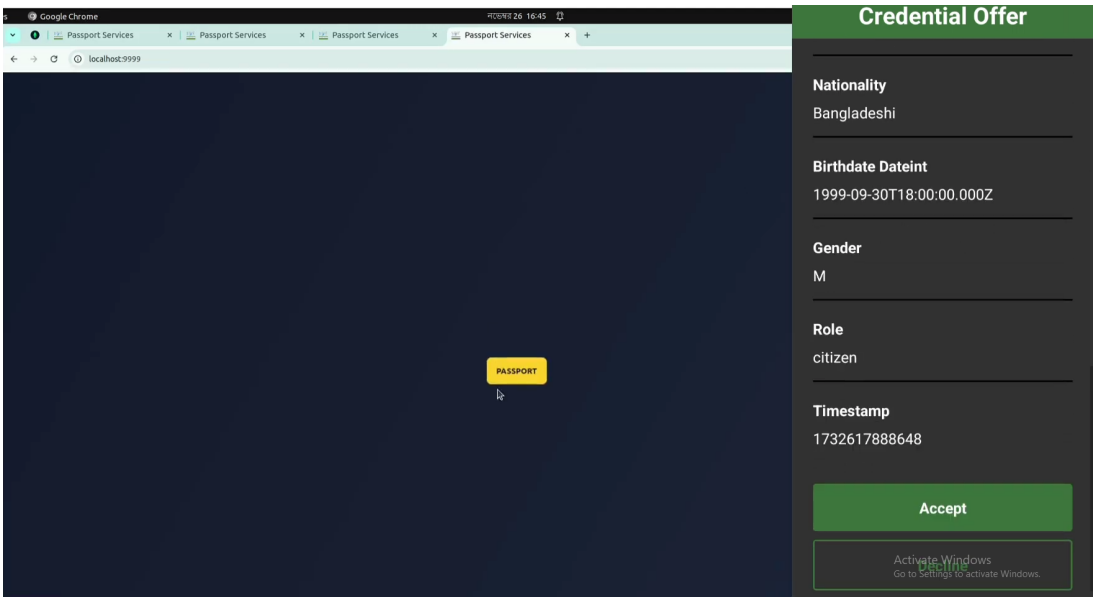


Figure 6.6: Passport Credential.

The passport will be issued and sent to the wallet, which the user will have to accept Figure 6.6. After acceptance, the passport credentials will be stored in the wallet. In this use case, we have handled various corner cases, such as a citizen holding a passport not being able to issue another passport.

6.2.3 Acquire Visa

Here, we have shown how to get a visa as a verifiable credential by providing the passport credential. The first few steps are the same as acquiring a passport. When the user provides the NID number. After checking, they will have to create a connection with the visa agent. After a successful connection, the page will auto-render to Figure 6.7.

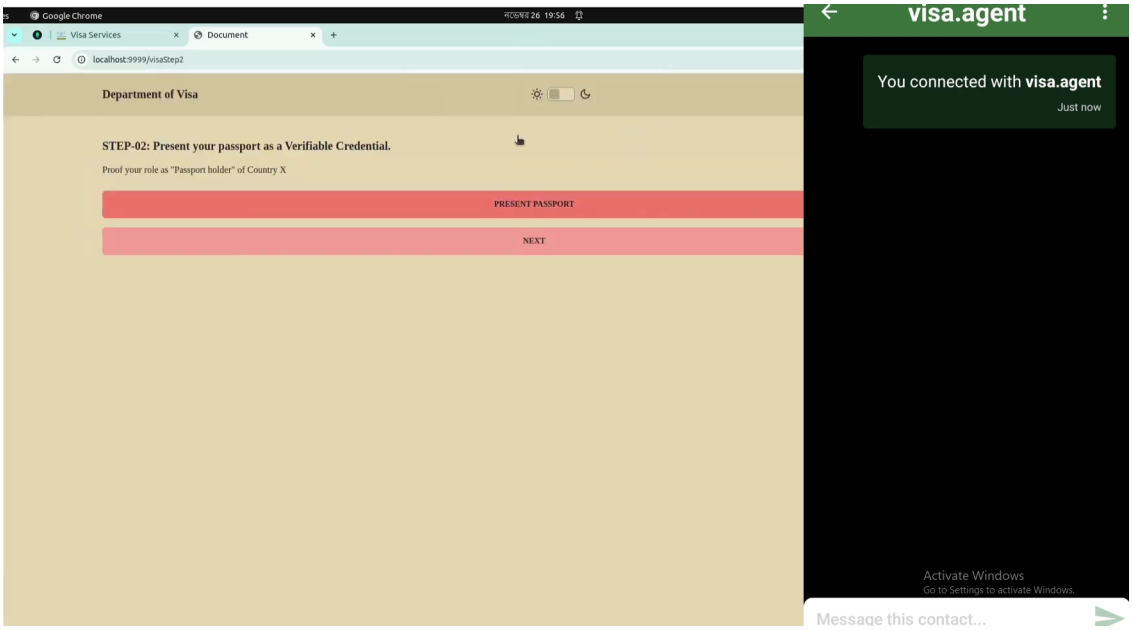


Figure 6.7: Present Passport.

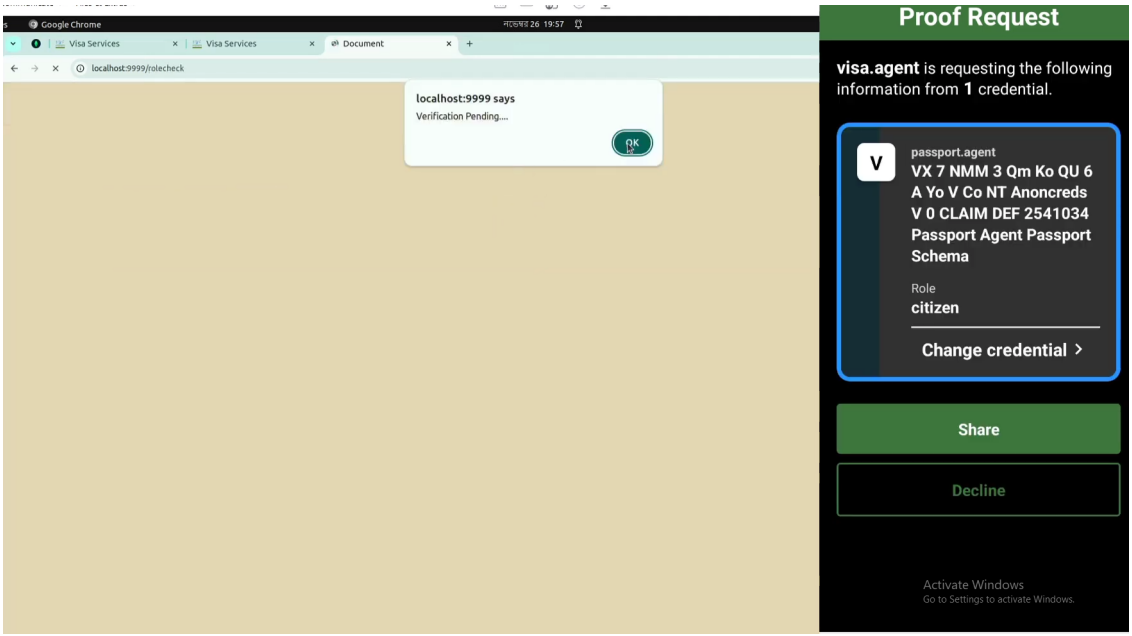


Figure 6.8: Passport Proof Request.

Now, they will have to click the present passport. Here, in the backend, a schema has been created for the passport. The schema will be checked, and the user wallet

will be asked to present the passport credentials, as shown in Figure 6.8.

After sharing the passport credential as proof, the verifier will check the authenticity of the proof by checking the Indy blockchain as well as the Trust Issuer List, which we have maintained through Hyperledger fabric. The verifier will retrieve the issuer DID from the Trusted Issuer List and will check if the issuer DID is available or not. If it is not available, then the proof for the passport will not work. But if it works, then the page will auto-render to Figure 6.9.

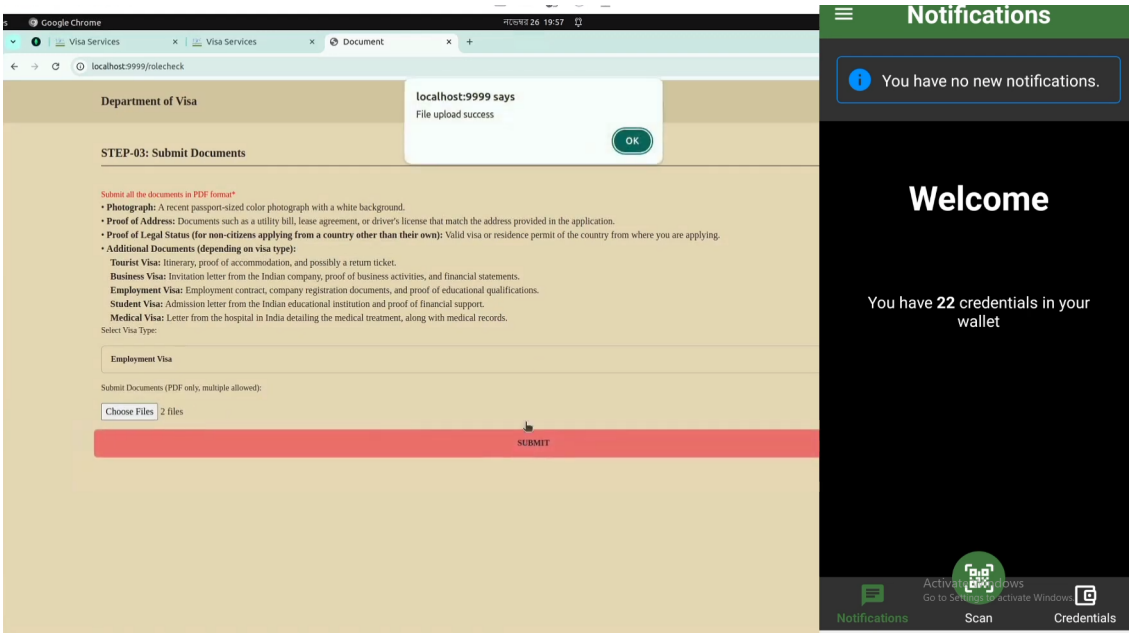


Figure 6.9: Visa Document Submission.

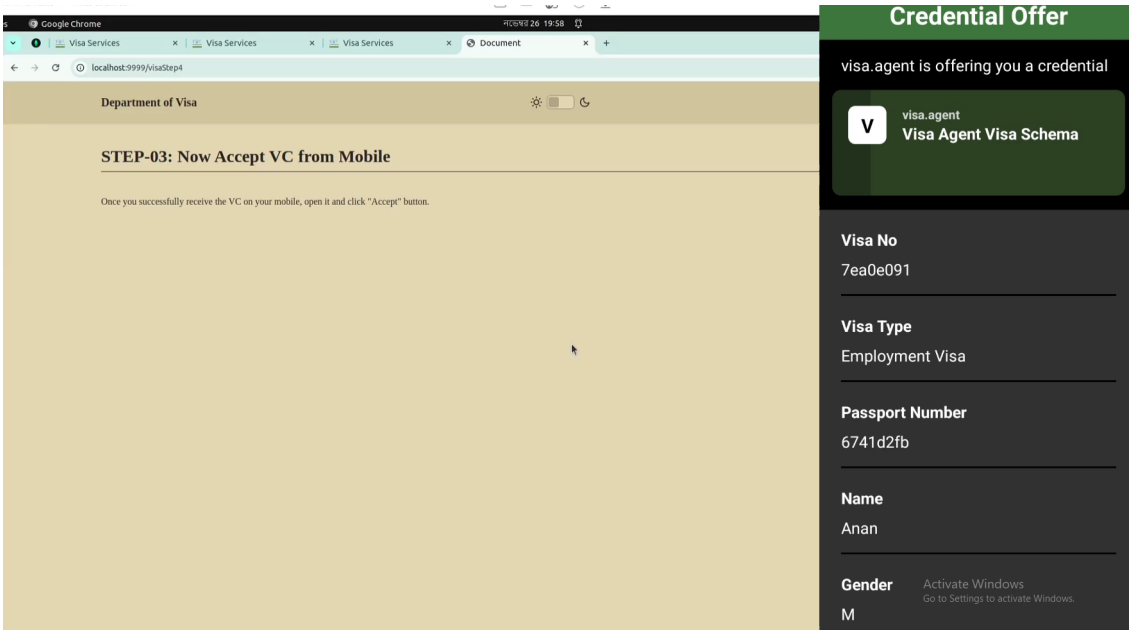


Figure 6.10: Visa Credential.

Here, they will have to submit the necessary files for offline verification. After

submission, the page will auto-render to the wait phase. When the verification is done, only then will the user be able to claim their respective visa credential.

In Figure 6.10, the visa credential has been sent to the mobile wallet, and the user will have to accept the credential. After that, the credential will be saved in the wallet. So, from acquiring a passport, the user acquired a passport credential, and from acquiring a visa, the user acquired the visa credential.

6.2.4 Verifying Passport and Visa for Immigration

i On the screen shown in Figure 6.11, citizens will establish a new connection by scanning a QR code using the Aries Bifold app.

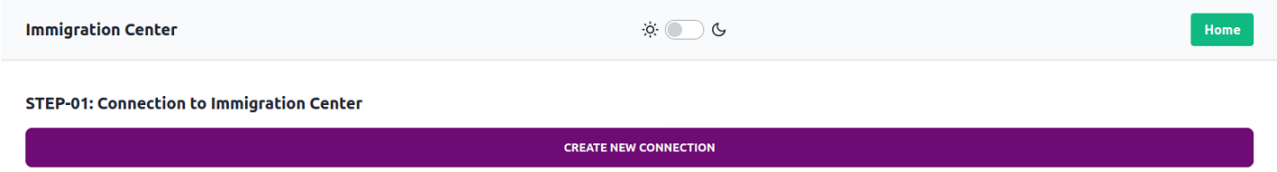


Figure 6.11: Establishing Connection by Providing QR Code.

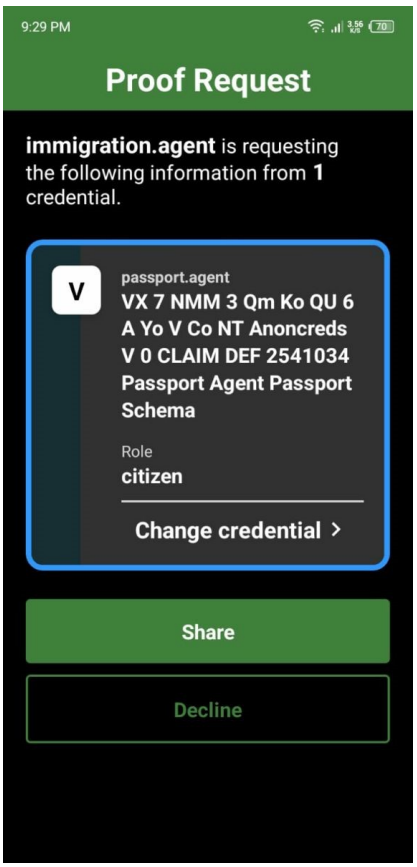


Figure 6.12: Proof Request (passport) Waiting Screen.

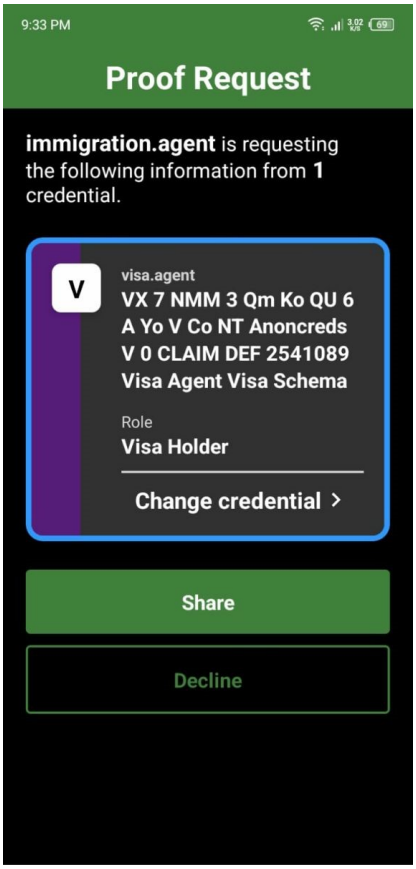


Figure 6.13: Proof Request (visa) Waiting Screen.

ii Next, the immigration center will request the citizen to present their passport as part of a proof request. The citizen will then share their passport credential in response. The immigration center will extract the passport issuer's DID from the credential and verify it against their list of trusted issuers. If the issuer is listed, the process will continue to the next step shown in Figure 6.12.

iii Following this, the immigration center will request the citizen to present their visa through another proof request as shown in Figure 6.13. The citizen will share their visa credential in response. The immigration center will once again verify the issuer's DID against the trusted issuer list. If the issuer is verified, the citizen will be granted permission to depart.

Chapter 7

Discussion

This section describes the performance evaluation and points out the advantages and limitations of this system. After that, comparative analysis has been shown. Finally, the last subsection describes the future work.

7.1 Performance Evaluation

The performance of the 'NID check' API was tested using JMeter with 500 concurrent requests at first. We have chosen 15 second time window for testing. The API was completed entirely without errors, and the average response time was 58 ms, while the Throughput was recorded as 33.27 req/sec, as shown in Figure 7.1. The latency graph in Figure 7.1 depicted stable and harmonic clogging signal fluctuations, proving the API stability and performance under load circumstances.

Label	Samples	Average	Median	Error	Throughput
HTTP Request	500	58	58	0	33.26679973
TOTAL	500	58	58	0	33.26679973

Table 7.1: Performance Result for 500 Users.

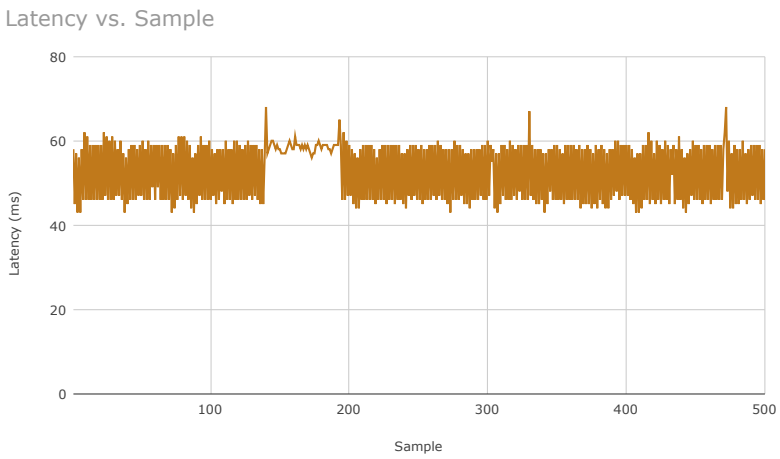


Figure 7.1: Latency Graph for 500 Users.

Next, for 1000 users, the API successfully processed all requests without errors, achieving an average and median response time of 58 milliseconds. The throughput increased to 66.48 requests per second, showcasing improved handling of a larger load as reflected in Figure 7.2. The latency graph in Figure 7.2 displayed consistent response times, with minimal spikes, indicating that the API maintained stability and efficiency under increased user traffic.

Label	Samples	Average	Median	Error	Throughput
HTTP Request	1000	58	58	0	66.47610184
TOTAL	1000	58	58	0	66.47610184

Table 7.2: Performance Result for 1000 Users

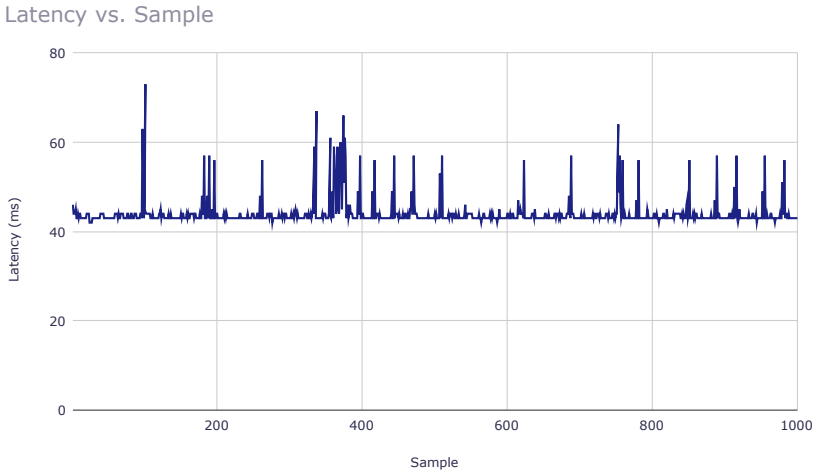


Figure 7.2: Latency Graph for 1000 Users.

Moreover, this API was tested with stress with 1,500 and 2,000 concurrent users. For 1500 users, the results in Figure 7.3 demonstrate the API kept a relatively constant average and median response time of 58ms and achieved 99.69 requests per second through low latency variance. As seen in Figure 7.3, The latency remained stable, with minor variations as shown in the latency graph. When tested with 2,000 users, the latency spikes observed in Figure 7.4 aligned with the average response time was higher at 127 milliseconds and the throughput higher at 124.42 request/sec as shown in Figure 7.4. But even with a higher load, the API remained rather stable and served all incoming requests without failure. These results support the API's effectiveness in driving more users to the application. Thus, These results prove it for high traffic and its ability to quickly validate NID.

Label	Samples	Average	Median	Error	Throughput
HTTP Request	1500	58	58	0	99.68764538
TOTAL	1500	58	58	0	99.68764538

Table 7.3: Performance Result for 1500 Users.

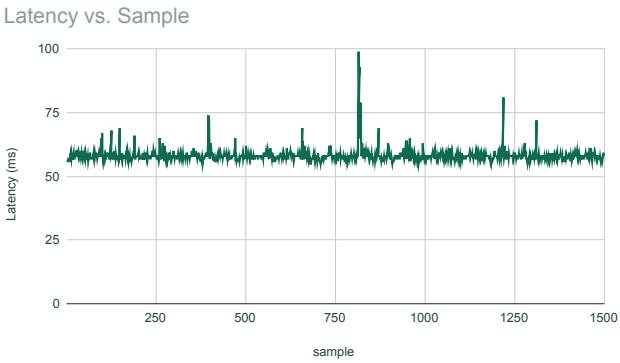


Figure 7.3: Latency Graph for 1500 Users.

Label	Samples	Average	Median	Error	Throughput
HTTP Request	2000	127	58	0	124.4245365
TOTAL	2000	127	58	0	124.4245365

Table 7.4: Performance Result for 2000 Users.

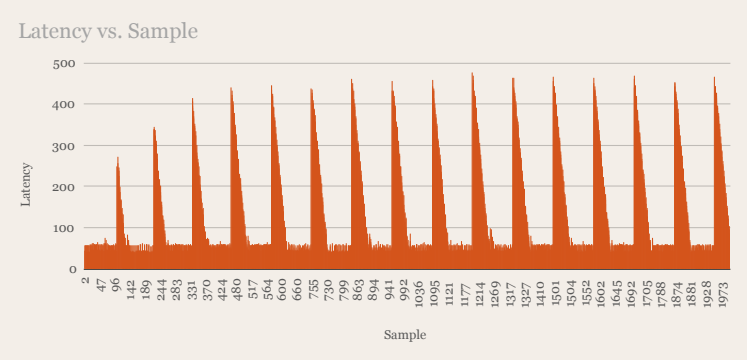


Figure 7.4: Latency Graph for 2000 Users

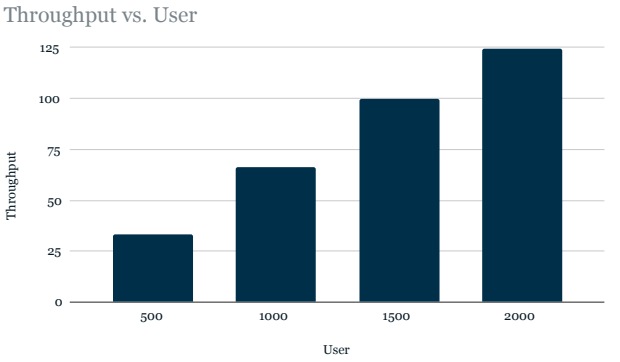


Figure 7.5: Throughput Graph for 500, 1000, 1500 and 2000 Users.

Figure 7.5 depicts the throughput for 500, 1000, 1500 and 2000 users. The testing period takes only 15 seconds, and it is the key to efficient assessment of the system's

performance, its reliability and, gradually, its scalability. This helps to get necessary recommendations on how effectively the system works under certain user loads for further improvements.

The 'DID fetching' API to retrieve the username and issuers DID from Hyperledger Fabric was tested on 500, 1000, 1500 and 2000 requests using JMeter. The performance testing was conducted to check the number of hits and API requests in a given time period in addition to studying the impact of high load on API.

From Figure 7.5, it is evident that the average response for the API was 4 ms, and the median response for API was 3 ms for the 500 concurrent users. The throughput was measured at around 33 requests per second. Figure **??** highlights that the majority of samples have low latency, meaning that the API proved rather effective at the identified load level.

Label	**Samples**	**Average**	**Median**	**Error**	**Throughput**
HTTP Request	500	4	3	0	33
TOTAL	500	4	3	0	33

Table 7.5: Performance Result for 500 Users.

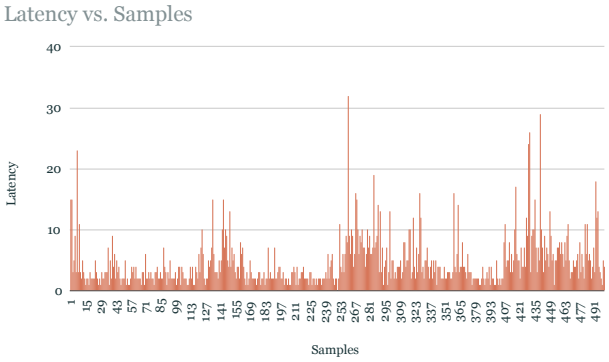


Figure 7.6: Latency Graph for 500 Users.

It showed that with 1000 concurrent users, the average response time was 12ms, and the throughput increased to 67 requests per second, as per the inspection of Figure 7.6. The latency graph showcased a fairly high at start but constant response time, which confirms API has proven scalable when the user traffic doubles, shown in Figure 7.7. The API neither returned any errors nor failed to respond to any of the requests made to it.

Label	**Samples**	**Average**	**Median**	**Error**	**Throughput**
HTTP Request	1000	12	4	0	67
TOTAL	1000	12	4	0	67

Table 7.6: Performance Result for 1000 Users.

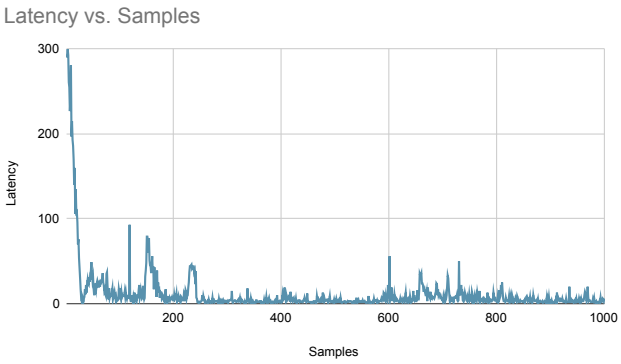


Figure 7.7: Latency Graph for 1000 Users.

When there were 1500 concurrent users, the results in Figure 7.7 demonstrate the average response time was 22 ms with throughput being again improved to 99.96 requests per second. Figure 7.8 shows The latency graph displayed periodic spikes but the API maintained stability overall, but there were no issues requiring output for API increased loading times with any errors. This shows that the API is still fast and continues to perform quite well as traffic increases.

Label	**Samples**	**Average**	**Median**	**Error**	**Throughput**
HTTP Request	1500	22	7	0	99.96001599
TOTAL	1500	22	7	0	99.96001599

Table 7.7: Performance Result for 1500 Users.

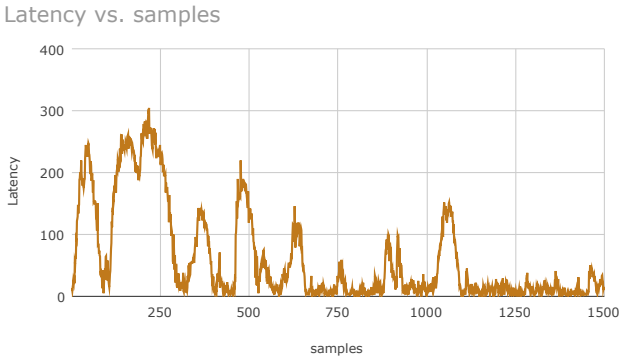


Figure 7.8: Latency Graph for 1500 Users.

At the concurrency level of 2000 users, as reflected in Figure **??**, the API response rate was higher, with an average of 27 ms and a median of 10 ms. Nevertheless, the rate of the throughput was 125.1 requests per second, which proved that many requests may be processed within a short period using the API. According to Figure 7.9, the latency graph showed more frequent and higher spikes due to the consequences of enhanced traffic on response time, which is in contrast to users' activity. Nevertheless, the API kept the error rate to zero percent as it was able to process all the requests.

Label	Samples	Average	Median	Error	Throughput
HTTP Request	2000	27	10	0	125
TOTAL	2000	27	10	0	125

Table 7.8: Performance Result for 2000 Users.

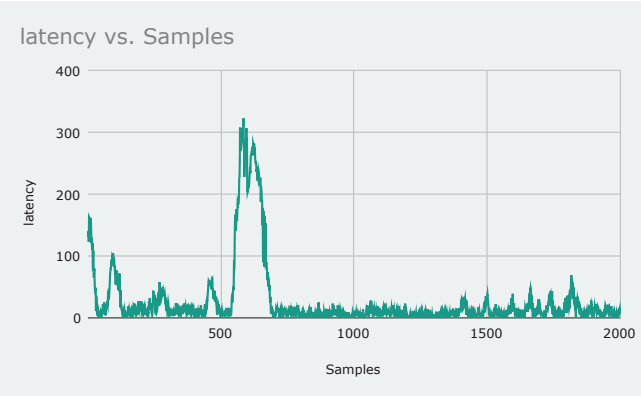


Figure 7.9: Latency Graph for 2000 Users.

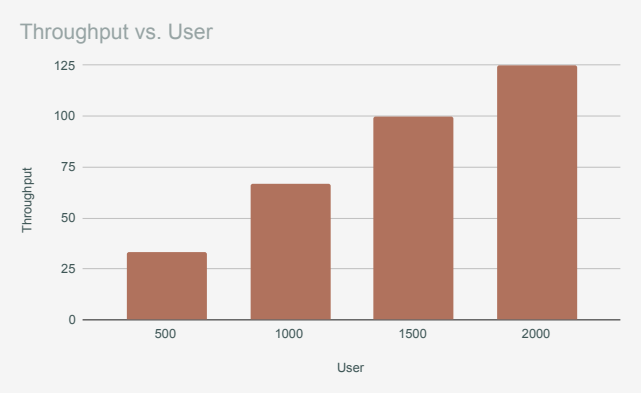


Figure 7.10: Throughput Graph for 500, 1000, 1500 and 2000 Users.

Figure 7.10 shows the throughput for 500, 1000, 1500 and 2000 users for /users API.

7.2 Advantages & Limitations

Advantages

The SSI-based passport and visa have many advantages over the current system.

- **User-centric:** The SSI passport and visa give individuals the authority to hold private data to themselves and use their data for any verification. The private data of the user is kept secure in their wallet. User does not need to memorize their DID for verification. Citizens no longer need to borrow physical passports or visas; they can just carry their wallets.
- **Time Management:** Manual verification takes a lot of time and creates a long queue of people. Whereas our wallet-based verification takes a few

seconds. Also, to issue passports, people have to come to the passport office and submit paper-based documentation. Whereas our system provides an online portal for submission.

- **Secure System:** We have secured our system using blockchain, SSI, and hyperledger fabric, ensuring that the data is cryptographically secured and saved in the wallet. As the wallet is controlled by the user only so, there is no intervention from third parties; they can just connect to the verifier agent and prove their verifiable credential.

Limitations

Although our system is efficient and secure, it also has some limitations.

- **Network Connection:** Our system suggests using a wallet; to do that, we need an internet connection to verify our verifiable credentials. If the network is down for some reason, then we won't be able to use our wallet, also, if the mobile gets switched off for low battery, the user won't be able to verify their credential.
- **Effect of New Technology:** Our system requires a smartphone and a mobile wallet, so it will be difficult for older citizens who are not well-trained to use smartphone functionalities. They will need to be trained before using a wallet.

7.3 Comparative Analysis

In this section, firstly we will compare our system with other existing papers, then we will compare our system with industrial applications, and after that, we will analyze the existing ePassport with our digitalized passport, finally we will compare the existing visa system with our digitalized visa.

7.3.1 Comparative Analysis of the System with Existing Works

In Table 7.9, we present the comparative analysis among the reviewed works. As per the table, we have used different notations.

Here, ✓= satisfied, ✗= not satisfied

We are performing this comparative analysis based on some criteria and properties, which are

- Proposal/Implementation: Proposed or Implemented.
- Threat Model: We have selected a well-known threat model called STRIDE [35].
- Requirement Analysis: Functional requirements represent the essential functionalities to be provided by the system, while security and privacy concerns ensure that they do address threats [3].
- Performance Analysis

- Security Evaluation: To address the classified security threats.
- SSI Framework: Framework for Integrating Self-sovereign Identity (SSI).
- Blockchain
- ePassport: ePassport standards [34].

Author	Proposal/ Implement	Threat Model	Requirement Analysis	Performance Analysis	Security Evaluation	SSI Framework	Blockchain	ePassport Standards
Panchamia et al.,2017 [9]	✓ Both	×	×	×	×	×	✓ Hyperledger Fabric	×
Kuperberg et al.,2019 [13]	Survey	×	×	×	×	×	✓	×
Chandra et al.,2021 [10]	✓ Proposal	×	×	×	×	×	✓ Hyperledger Fabric	×
Goela et al.,2020 [21]	✓ Proposal (web application)	×	×	×	×	×	✓ Ethereum	×
Speelman, 2020 [17]	✓ Both	×	×	✓	×	×	✓ TrustChain	×
Stockburger et al,. 2021 [1]	✓ Proposal	×	✓	×	×	×	✓ hyperledger Indy	×
Patel et al. ,2018 [6]	✓ Both	✓	×	×	×	×	✓ Hyperledger Faric	×
Cheesman et al.,2020 [19]	✓ Proposal	×	×	×	×	×	✓	×
Swati V et al.,2018 [8]	✓ Proposal	×	×	×	×	×	✓	×
Shety et al. ,2022 [16]	✓ Proposal	×	×	×	×	×	✓ Ethereum	×
Xu et al., 2022 [14]	✓ Proposal	×	×	×	×	×	✓ Hyperledger Indy	×
Zwitter et al., 2020 [2]	✓ Proposal	×	×	×	✓	×	✓ Ethereum	×
Stokkink et al.,2018 [15]	✓ Both	×	×	✓	×	×	TrustChain	×
Htet et al. ,2020 [11]	✓ Proposal	×	×	×	×	×	✓ Open Source Ethereum Infrastructure	×
Tepe, 2022 [4]	✓ Both	×	×	×	×	×	✓ Hyperledger Fabric	×
Shih et al., 2022 [7]	✓ Proposal	×	✓	×	✓	×	✓ Hyperledger Fabric	×
Lacity et al., 2022 [46]	✓ Both	×	×	×	×	✓ Sovrin	✓	×
Our Work	✓ Both	✓	✓	✓	×	✓ Aca-Py	✓ Hyperledger Fabric, Hyperledger Aries, Hyperledger Indy	✓

Table 7.9: Comparative Analysis Table.

We compared each reviewed paper with these criteria to determine whether it satisfied them. Out of 16 papers, five present both proposal and implementation, but the remaining 10 papers are only proposal-type, and one is survey-type. If we focus on the threat model criteria, we can see that only one paper (Patel et al.,2018) follows the threat model structure. We also looked at requirements analysis and performance analysis aspects to consider the standard of the paper. In this case, two papers have shown requirements analysis in their work, namely (Stockburger et al., 2021) and (Shih et al., 2022). On the other hand, performance analysis has shown this aspect in two papers, namely (Speelman, 2020) and (Stokkink et al., 2018). Among the 16 papers mentioned, only two focused on security evolution, namely (Zwitter et al., 2020) and (Shih et al., 2022). If we defend the SSI framework on these criteria, we will observe the operation of the SSI principle only in one paper (Speelman, 2020). We have also worked on the type of blockchain used in these 16 papers. Four types of work have been done here: Hyper Ledger Fabrics, Ethereum, Trust Chain, and Open Source Ethereum Infrastructure. None of the 16 papers mentioned followed the e-passport standard. According to the table of the

selected parameters, no paper could satisfy all the parameters. The primary issue is that no one followed the ePassport standards. We had a research gap here. In our paper, we have applied almost all the factors except the security evaluation, which we intend to include in our future work.

7.3.2 Comparative Analysis of the System with Industry Applications

We examine the many characteristics of the three industrial software applications available and discover that none of them comply with all of the SSI's criteria. Their trust triangle is also not certified. First of all, "VeriGo" relies on a particular authority; "Idemia-Mobile Id" lacks VC and DIDs, which shows a lack of proper entity identification; and lastly, the "Yoti" program is not entirely decentralized. Our system will fully adhere to the SSI principles, which will also create a legitimate trust triangle. Our system will be more secure as well.

7.3.3 Comparative Analysis between ePassport and Digital Passport

ePassport

Greater privacy risks: In [33], Grunwald, in his experiment, showed that RFID (Radio-frequency Identification) chips won't make the documents safe as the data can be cloned. Gathering more biometric identity data such as iris and fingerprint scans in addition to photographs is an infringement on people's rights to privacy. The more biometric data is being stored, the more likely the information will be abused or accessed by unauthorized persons, possibly leading to identification theft or clumsy surveillance.

Need for Strong Privacy Rules: Biometric data collection and storage over long periods create high privacy risks and thus require improved privacy frameworks. Such frameworks are designed so that the changes can only be made securely, and there is a clear policy on who can view the data, how it can be used, and for how long it can be stored. These issues must be addressed by drafting or amending the privacy laws section, which takes time and effort in the countries.

Cost of Biometric Systems: The procurement and installation of systems that have the capability and capacity for capturing and processing biometric data entails a great deal of capital expenditure. Such features may include the expense incurred in placing the biometrics technology for capturing the data, the secure databases where the biometrics data is to be stored and the continuing expense incurred in maintaining as well as updating the security of the biometrics data.

Modifications: Changes, adjustments, and modifications to an e-passport require a lot of effort and many different types of physical documents. Paper documents must also be reissued, meaning it requires money as well as time. Apart from that, it is burdensome for travelers to have to complete all of these documentation and procedures in person.

Digital Passport

User Control and Privacy: VCs can be structured to empower the holder with control over their personal information, allowing them to share only what is necessary in a given situation. This is akin to showing a passport only when required at border control or hotel check-ins or creating a bank account in country X. This selective disclosure enhances privacy and user control.

Using Privacy-Safe Technologies: VCs can be built with the use of customers' anonymity-preserving technologies such as zero-knowledge proofs. These technologies provide the means for data assurance without offering the actual data. For instance, the zero-knowledge proof can certify that a certain person is eligible for voting, but we cannot tell his/her date of birth or any other value.

Less Need for Large Databases: Since fingerprints, etc., can be validated with cryptography techniques, and there is no need to access the central database, the biometric databases can be minimized. This minimizes the probability of network breaches affecting vast quantities of data and also decreases the expense of investing in data architectures.

Modifications: It's very simple and quick to modify and revoke a digital passport. The digital passport saves a significant amount of time and trouble because it can be remotely updated, canceled, and modified with the assistance of the secured server. On top of that, it provides the government the ability to regulate any passport's functionality from anywhere at any time.

7.3.4 Comparative Analysis on Current Visa System with Digitalized Visa

Our current visa system is still paper or pdf-based. As it is paper-based, it can get lost. People will need to wait in a long queue to submit their necessary files and documents. Most concerning is that all the data is centralized, and people are not in control of their own data. The problem we face with these systems needs to be solved. Our proposed solution suggests a digitalized visa where all the data will be secure using blockchain technology. With blockchain technology, we have used Self Sovereign Identity, and to control access, we have implemented hyperledger fabric. It gives citizens the leverage to hold their own data in their wallets. Moreover, they will not need to carry a pdf or paper for verification. Also, centralized systems are always a target for hackers as they can manipulate sensitive data from the database. But our wallet is protected with cryptography and no private data is saved in hyperledger indy, only the DID doc is saved and the schema of credentials is. So, data is only stored in the user's wallet. So, implementing our system will give users the power to use their data securely.

7.4 Future Work

In the future, we would like to make our system more secure and dynamic by following the points:

- We would like to add a consensus protocol in our hyperledger fabric system, which we briefly showed in our use case 1, which will maintain the addition of an organization to our consortium.

- As our system requires the usage of a mobile wallet, to make it easier for all classes of people, we want to add a dummy tutorial in the wallet. In which the user will go through the exact process of creating a connection and issuing and proofing credentials.
- We would like to upgrade our verification process so that we won't need any offline verification.
- We would like to work on security evaluation in the future.

Chapter 8

Conclusion

Almost everywhere, the immigration process is still paper-based. The citizens have to carry a passport, a visa, and other necessary documents. Because of paper-based verification, the process is too slow, which kills a lot of time for both users and officers and creates a long queue of immigrants. Our proposed system has mitigated all the difficulties that the traditional procedure faces. This paper proposes through various studies, a comprehensive framework for a blockchain-based Self-sovereign Identity system aimed at digitizing travel documents while improving the security, efficiency and privacy of international travel. By leveraging blockchain technology and decentralized identifiers (DIDs), the proposed system transforms traditional paper-based passports and visas into verifiable digital credentials stored in a secure mobile wallet which will ease the process for both citizen and immigrant officers. We have shown in our literature review how their proposed methods and implementation lack functional requirements, detailed descriptions of use cases in real-life scenarios, and other limitations. Also, we described the architecture of the proposed system based on a threat model and the requirement analysis, detailed its implementation, and demonstrated four implementation works to show its feasibility. We are confident that these contributions will open new avenues for research in this field.

Bibliography

[1] Stockburger, L., Kokosioulis, G., Mukkamala, A., Mukkamala, R. R., & Avital, M. (2021, June 1). Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation. Blockchain: Research and Applications. [Online]. Available: https://doi.org/10.1016/j.bcra.2021.100014

[2] Zwitter, A., Gstrein, O. J., & Yap, E. (2020, May 28). Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual. Frontiers in Blockchain. [Online]. Available: https://doi.org/10.3389/fbloc.2020.00026

[3] Ferdous, Md.S., Ionita, A. & Prinz, W., 2022, SSI4Web: A Self-sovereign Identity (SSI) Framework for the Web, ResearchGate.

[4] Tepe, Y. (2022). Decentralisation of Hotel and Tourism Industry: Effects of Blockchain Technology in Hotel Booking Systems. [Online]. Available: https://openrepository.aut.ac.nz/items/425f9e46-f4a9-4086-ab55-73ca136638ec

[5] M. S. Ferdous, F. Chowdhury and M. O. Alassafi, "In Search of Self-Sovereign Identity Leveraging Blockchain Technology," in IEEE Access, vol. 7, pp. 103059-103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[6] Patel, D., B., & Mistry, V. (2018, January 1). Border Control and Immigration on Blockchain. Lecture Notes in Computer Science. [Online]. Available: https://doi.org/10.1007/978-3-319-94478-4_12.

[7] Shih, D.-H.; Shih, P.-L.; Wu, T.-W.; Liang, S.-H.; Shih, M.-H. An International Federal Hyperledger Fabric Verification Framework for Digital COVID-19 Vaccine Passport. Healthcare 2022, 10, 1950. [Online]. Available: https://doi.org/10.3390/healthcare10101950

[8] S. V. and A. S. Prasad, "Application of Blockchain Technology in Travel Industry," 2018 International Conference on Circuits and Systems in Digital Enterprise Technology (ICCSDET), Kottayam, India, 2018, pp. 1-5, doi: 10.1109/ICCSDET.2018.8821095.

[9] S. Panchamia and D. K. Byrappa, "Passport, VISA and Immigration Management Using Blockchain," 2017 23RD Annual International Conference in Advanced Computing and Communications (ADCOM), Bangalore, India, 2017, pp. 8-17, doi: 10.1109/ADCOM.2017.00009.

[10] Chandra, K. (2021). Digital Passport and Visa Asset Management Using Private and Permissioned Blockchain. [Online]. Available: https://www.semanticscholar.org/paper/Digital-Passport-and-Visa-Asset-Management-Using-Chandra-Mushtaq/e89b0e6f4d0d83691aedc6b5993a5e1162441b4f

[11] M. Htet, P. T. Yee and J. R. Rajasekera, "Blockchain based Digital Identity Management System: A Case Study of Myanmar," 2020 International Conference on Advanced Information Technologies (ICAIT), Yangon, Myanmar, 2020, pp. 42-47, doi: 10.1109/ICAIT51105.2020.9261785.

[12] K. Cameron. Microsoft Corporation. (Nov. 5, 2005). The Laws of Identity. Accessed: Mar. 20, 2019. [Online]. Available: http://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf

[13] Kuperberg, M., Kemper, S., & Durak, C. (2019, January 1). Blockchain Usage for Government-Issued Electronic IDs: A Survey. Lecture Notes in Business Information Processing. [Online]. Available: https://doi.org/10.1007/978-3-030-20948-3_14

[14] Xu, B., Niu, Q., Jiang, R., Bouridane, A., & Li, C. T. (2022, January 1). Biometric Blockchain (BBC) Based e-Passports for Smart Border Control. Springer eBooks. [Online]. Available: https://doi.org/10.1007/978-3-031-04424-3_13

[15] Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 2018, pp. 1336-1342, doi: 10.1109/Cybermatics_2018.2018.00230.

[16] Satybaldy, A.; Subedi, A.; Nowostawski, M. A Framework for Online Document Verification Using Self-Sovereign Identity Technology. Sensors 2022, 22, 8408. [Online]. Available: https://doi.org/10.3390/s22218408

[17] Tim, Speelman. (2020). Self-Sovereign Identity: Proving Power over Legal Entities. [Online]. Available: https://repository.tudelft.nl/islandora/object/uuid:aab1f3ff-da54-47f7-8998-847cb78322c8/datastream/OBJ/download

[18] Pekka, Koskela., Anni, Karinsalo., Jori, Paananen., Laura, Salmela. (2022). Streamline Border Control with Blockchain Towards Self-Sovereign Identity. doi: 10.5121/csit.2022.122207

[19] Margie Cheesman (2020): Self-Sovereignty for Refugees? The Contested Horizons of Digital Identity, Geopolitics, DOI: 10.1080/14650045.2020.1823836

[20] Gauri, S., Shetye., Nandini, Sonar., Dhanamma, Jagli. (2022). Blockchain-based Self-sovereign Identity Management System. International Journal For Science Technology And Engineering, 10(6):2128-2131. doi: 10.22214/ijraset.2022.44335

[21] Goel, A., Sharma, A., Gupta, D., & Khanna, A. (2020, January 1). Immigration Control and Management System Using Blockchain. Social Science Research Network. https://doi.org/10.2139/ssrn.3564189

[22] E. Zeydan, J. Mangues, S. Arslan and Y. Turk, "Blockchain-based Self-Sovereign Identity Solution for Vehicular Networks," 2023 19th International Conference on the Design of Reliable Communication Networks (DRCN), Vilanova i la Geltru, Spain, 2023, pp. 1-7, doi: 10.1109/DRCN57075.2023.10108183.

[23] K. Binjola, K. Joshi, R. Bondale, A. Sakhapara and D. Pawade, "Fake Passport Detection Using Blockchain," 2022 5th International Conference on Advances in Science and Technology (ICAST), Mumbai, India, 2022, pp. 243-246, doi: 10.1109/ICAST55766.2022.10039603.

[24] Zeren, S. K., & Demirel, E. (2019, November 10). Blockchain Based Smart Contract Applications in Tourism Industry. Contributions to Management Science. [Online]. Available: https://doi.org/10.1007/978-3-030-29739-8_28

[25] Miraç Yücel Başer, Tuba Büyükbeşe & Murat Kizildag (2023) What if we could travel without passport? First sight to blockchain-based identity management in tourism, Asia Pacific Journal of Tourism Research, 28:4, 341-363, DOI: 10.1080/10941665.2023.2229922

[26] 5th EMAN Conference Proceedings (part of EMAN conference collection). (2021, January 1). International Scientific Conference EMAN. Economics & Management: How to Cope With Disrupted Times. [Online]. Available: https://doi.org/10.31410/eman.2021

[27] C. Allen. (Apr. 25, 2016). The Path to Self-Sovereign Identity. Accessed: Mar. 23, 2019. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[28] DIF - Decentralized Identity Foundation. (n.d.). https://identity.foundation/

[29] Encrypted Data Vaults v0.1. (n.d.). https://identity.foundation/edv-spec/

[30] Verifiable Credentials Data Model v1.1. https://www.w3.org/TR/vc-data-model/

[31] Young, K. (2021, March 2). Domains of Identity - Identity Woman. Identity Woman. http://identitywoman.net/domains-of-identity/

[32] PPreukschat, A., & Reed, D. (2021, June 8). Self-Sovereign Identity. Simon and Schuster. https://shorturl.at/ETYZ0

[33] Zetter, K. (2006, August 3). Hackers Clone E-Passports. WIRED. https://www.wired.com/2006/08/hackers-clone-e-passports/

[34] Ikura, J., & Kinneging, T. (Year). The ePassport: What's Next? [PowerPoint slides]. International Organization for Standardization (ISO). [Online]. Available: https://www.icao.int/Meetings/TRIP-Symposium-2016/Documents/Ikura%20Kinneging2.pdf

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

[36] Lekkas, D., Gritzalis, D. (2007, August 13). E-Passports as a Means Towards the First World-Wide Public Key Infrastructure. Lecture Notes in Computer Science. https://doi.org/10.1007/978-3-540-73408-6_3

[37] Milde, M. (2008). International air law and ICAO (Vol. 4). Eleven International Publishing.

[38] Abuadhmah, N. A., Naser, M., Samsudin, A. (2010). E-Visas Verification Schemes Based on Public-Key Infrastructure and Identity Based Encryption. Journal of Computer Science, 6(7), 723.

[39] Duerrmeier Rizzi, M. (2014). Travel visa impacts on destination choice and perception. Worldwide Hospitality and Tourism Themes, 6(4), 305-316.

[40] Hyperledger. (n.d.). GitHub. https://github.com/hyperledger/

[41] T T. (2024, October 23). Global Passport Fees 2024: Massive Update! | by Tom Topol. Passport-Collector.com. https://www.passport-collector.com/global-passport-fees/

[42] Marksteiner, S., Sirjani, M., Sjödin, M. (2024, July). Automated Passport Control: Mining and Checking Models of Machine Readable Travel Documents. In Proceedings of the 19th International Conference on Availability, Reliability and Security (pp. 1-8).

[43] Lopez-Solano, J., Castañeda, J. D. (2024). 'A promising playground': IDEMIA and the digital ID infrastructuring in Colombia. Information, Communication Society, 1-17.

[44] The Digital and Secure Future of Travel. (2023). Mobileidworld.com. https://mobileidworld.com/the-digital-and-secure-future-of-travel/

[45] Yoti Reworks ID System for Government Use with Blockchain Technology. (2018). Idtechwire.com. https://idtechwire.com/yoti-government-blockchain-501253/

[46] Lacity, M., Carmel, E. (2022). Implementing Self-Sovereign Identity (SSI) for a digital staff passport at UK NHS. University of Arkansas.