A Decentralized Framework for Government Issued NID using Self Sovereign Identity

by

Mirza Mahrab Hossain
21101048
Nihal Islam
22341054
Noshin Tabassum
21201530

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

Department of Computer Science and Engineering
Brac University
June 2025

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:

Mirza Meherab Hosen Rudra
21101048

Noshin Tabassum
21201530

Nihal Islam
22341054

Approval

The thesis titled "A Decentralized Framework for Government Issued NID using Self Sovereign Identity" submitted by

1. Mirza Mahrab Hossain (21101048)
2. Nihal Islam (22341054)
3. Noshin Tabassum (21201530)

Of Spring, 2025 has been accepted as satisfactory in partial fulfillment of the requirement for the degree of B.Sc. in Computer Science on June 20, 2025.

Examining Committee:

Supervisor:

Dr. Jannatun Noor Mukta

Associate Professor, CSE
Director, BSDS
United International University

Program Coordinator:
(Member)

Dr. Golam Rabiul Alam

Professor
Department of Computer Science and Engineering
School of Data and Sciences
Brac University

Head of Department:

Dr. Sadia Hamid Kazi

Associate Professor
Department of Computer Science and Engineering
School of Data and Sciences
Brac University

Abstract

As digital identity becomes increasingly essential for public services, national security, and individual autonomy, conventional centralized identity systems face critical challenges related to privacy, interoperability, and user control. Traditional identity systems have profound limitations in the control and management of personal data. These systems typically rely on centralized authorities, where users' personal information is stored in the hands of third parties and is often exposed to security risks. Incidents such as data breaches, identity theft, and unauthorized access to information occur regularly, posing challenges to protecting users' privacy. In addition, these systems lack interoperability, making identity verification processes across platforms or organizations complex and time-consuming. Since users lack control over their own data, they are often subject to opaque data management and misuse. These limitations are incompatible with the mobility and security demands of the digital age, which further highlights the need for a decentralized and user-controlled identity system. To address these limitations, this paper presents a decentralized identity framework that transforms government-issued National ID (NID) credentials into Verifiable Credentials (VCs), anchored to a public blockchain infrastructure following Self-Sovereign Identity (SSI) principles [25]. In this model, citizens generate Decentralized Identifiers (DIDs) and retain full control over their credentials via user-managed digital wallets. The system eliminates reliance on centralized identity providers by employing end-to-end encryption, digital signatures, and tamper-proof credential hashing mechanisms. A complete prototype is implemented using Ethereum smart contracts and evaluated across multiple wallet platforms, including MetaMask, SpruceID, and Bifold, as well as a custom-built wallet. Experimental results demonstrate enhanced usability, privacy, and scalability. Comparative analysis with OAuth 2.0, SAML-based federated systems, and decentralized social login solutions highlights superior user control and trust verifiability. By aligning with emerging digital identity standards such as the W3C Verifiable Credentials specification [26], this research offers a scalable, citizen-centric architecture suitable for national-level digital identity ecosystems. The framework achieves a balanced integration of governmental oversight and decentralized trust, paving the way for secure, interoperable, and privacy-preserving identity management.

Keywords: Self-Sovereign Identity (SSI), National ID (NID), Verifiable Credentials (VC), Decentralized Identifiers (DID), Blockchain, Digital Identity, Ethereum, Web3

Acknowledgement

Firstly, all praise to the Great Almighty for whom our thesis has been completed without any major interruption.
Secondly, to our supervisor, Dr. Jannatun Noor Mukta, for her 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

The rapid digitalization of public services, commerce, and daily interactions has made digital identity management a foundational pillar of modern societies. As governments and organizations expand their digital operations, the need for secure, scalable, and privacy-preserving identity management frameworks becomes increasingly urgent. Traditional Identity Management Systems (IMS), while enabling access control and regulatory compliance, often rely on centralized or federated architectures that leave individuals with limited control over their identity data, scattered credentials, and heightened exposure to privacy risks.

To address these limitations, Self-Sovereign Identity (SSI) has emerged as a decentralized identity model that repositions individuals as the primary custodians of their digital identities. Using blockchain and distributed ledger technologies, SSI enables citizens to securely store verifiable credentials in digital wallets, selectively disclose identity attributes to service providers, and interact with public and private sector systems without reliance on intermediary identity providers. This architecture offers a pathway for governments to continue serving as trusted credential issuers while returning ownership and control of personal identity data to citizens.

A particularly promising application of SSI lies in the context of government-issued National Identification (NID) systems. Current centralized or federated NID models introduce risks related to data breaches, surveillance, and limited cross-platform interoperability [65]. In contrast, SSI-based NIDs allow individuals to use their government-issued credentials across a wide range of services, including a potential replacement for platform-dependent login systems such as those provided by Facebook or Google, while maintaining data sovereignty and privacy. The public blockchain infrastructure can further enhance trust, transparency and global interoperability by providing tamper-resistant credential registries.

This thesis investigates the design of government-backed decentralized NID frameworks based on SSI principles. Through a comprehensive analysis of existing IMS models, technical architectures, governance challenges, and current SSI platforms, this study proposes a hybrid framework in which governments issue verifiable credentials anchored in public blockchain infrastructures, while citizens retain full control over credential management and disclosure via decentralized wallets.

1.1 Terminologies

In this section, we present key terminology and concepts that are frequently referenced throughout the thesis. Given the diversity and evolving nature of identity management literature, consistent definitions are essential to avoid semantic ambiguity. The following definitions reflect widely accepted interpretations as found in current literature, standards, and prior works.

- **Entity:** An entity refers to any physical or logical object that has a distinguishable existence and can be uniquely identified in a system [2]. Entities may include individuals, organizations, devices, or software agents.
- **Identity:** Identity represents a collection of attributes, characteristics, or claims associated with an entity that enable its recognition within a specific context [25]. An entity may hold multiple partial identities across different domains depending on the services involved.
- **Identifier:** An identifier is a unique value assigned to an entity to distinguish it from other entities within a given context [26]. Examples include usernames, digital IDs, or cryptographic keys.
- **Identity Management System (IMS):** A framework that enables the creation, management, verification, and use of digital identities across services and domains [10]. IMS encompasses policies, processes, and technologies for authentication, authorization, and credential management.
- **Identity Provider (IdP):** An organization or authority that creates, stores, and manages identity credentials for users, and issues identity assertions to relying parties or service providers [5].
- **Service Provider (SP):** An organization or system that offers services or resources to users, relying on identity claims issued by Identity Providers to authenticate users [5].
- **Federated Identity Management (FIM):** An identity model where multiple organizations share identity information based on mutual trust agreements, allowing users to access services across different domains with a single set of credentials [10].
- **User-Centric Identity:** A model that provides individuals greater control over their personal identity information by allowing selective disclosure of identity attributes to service providers while still relying on centralized authorities for credential issuance [4].
- **Self-Sovereign Identity (SSI):** A decentralized identity model where individuals have complete ownership and control over their digital identity data without relying on centralized intermediaries [25]. SSI enables users to manage credentials, selectively disclose information, and maintain privacy and autonomy.

- **Decentralized Identifier (DID):** A globally unique identifier managed on decentralized networks, typically anchored on blockchain systems, that allows entities to prove control over identity without reliance on centralized registries [26].
- **Verifiable Credential (VC):** A digitally signed assertion issued by trusted authorities containing specific claims about an entity, which can be independently verified without disclosing unnecessary information [26].
- **Blockchain:** A decentralized, immutable distributed ledger that records transactions in a verifiable and tamper-resistant manner [23]. In SSI, blockchains are often used to anchor DIDs and facilitate credential registries.
- **Governance Framework:** A set of policies, legal agreements, and operational rules that define roles, responsibilities, and compliance mechanisms for participants within decentralized identity ecosystems [36].
- **Key Management:** The processes and technologies involved in generating, protecting, rotating, and recovering cryptographic keys that secure identity credentials and digital signatures [25].
- **Credential Revocation:** The process of invalidating previously issued credentials to prevent further use, ensuring that outdated or compromised credentials are no longer trusted [19].

1.2 Motivation

The ability to securely identify individuals in digital environments is fundamental for both government services and private sector platforms. However, existing digital identity systems suffer from significant structural limitations. Centralized identity architectures create large, attractive targets for cyberattacks, increase risks of mass data breaches, and place full trust in single entities to manage and protect sensitive personal data. Federated identity systems offer limited interoperability improvements but still concentrate authority within identity providers, introducing privacy concerns, lack of user autonomy, and potential misuse of aggregated identity data.

Self-Sovereign Identity (SSI) presents a compelling alternative by decentralizing control of identity data and granting individuals full ownership over the storage, management, and disclosure of their credentials. This approach is particularly relevant for government-issued National ID (NID) systems, where existing models often fail to adequately balance state verification requirements with citizen privacy, data sovereignty, and cross-platform usability.

The primary motivation for this research was to establish a secure and fraud-free digital identity system for use across platforms, where the possibilities for creating fake identities would be eliminated. An SSI-based NID framework enables governments to retain their role as trusted credential issuers while allowing citizens to manage verified credentials using personal digital wallets. These credentials can be securely presented across multiple domains, including government services, financial

institutions, healthcare systems, and private platforms — even replacing current Single Sign-On (SSO) models offered by technology providers such as Facebook or Google. The use of public blockchain infrastructure further strengthens the system by ensuring tamper-resistance, transparency, and decentralized trust without relying on central databases.

By bridging the assurance requirements of governments with the privacy expectations of citizens, a decentralized NID framework grounded in SSI has the potential to establish a more secure, interoperable, and citizen-centric digital identity ecosystem.

1.3 Research Objectives

The primary objective of this thesis is to design and implement a decentralized identity framework that leverages Self-Sovereign Identity (SSI) principles and use Public blockchain technologies to have a transparent identity system which securely issue, manage, and verify government-issued National ID (NID) credentials. The study focuses on bridging citizen data sovereignty with institutional trust and interoperability.

The specific research objectives are:

- **Securely Verified Identity:** The main objective of our research was to introduce a highly secure digital identity system. As citizens, our only authentic identity is the National Identity Card (NID). A verifiable credential system issued by the government, where the National Identity Card is used as the basis, will be the most reliable. Since it is a government system, its verification process will be more secure and authentic.
- **Decentralized Identity System:** Our subsequent objective is to implement a decentralized identity system that will store user's Verifiable Credential (VC) using Public Blockchain (Ethereum) network.
- **User Centric Wallet:** Thirdly, we explore multiple digital wallets (e.g., MetaMask, SpruceID, Bifold, Custom) for users to demonstrate secure issuance, storage, and verification and compare the best suited for our SSI-based decentralized identity system.
- **Seamless Identity Verification:** Finally, a Service Provider (SP) will be able to authenticate user's Verifiable Credential (VC) by looking into public blockchain network without having the concent of issuer.

1.4 Research Contributions

This thesis makes the following key contributions:

- **Existing System Limitaions:** Analyze existing identity management models (centralized, federated, and user-centric) and identify their limitations in the context of national digital identity systems.

- **Theoretical Evaluation:** Evaluate the theoretical underpinnings and technical architecture of Self-Sovereign Identity (SSI), including its core standards such as Verifiable Credentials (VCs), Decentralized Identifiers (DIDs), cryptography and blockchain anchoring mechanisms.
- **System Experiments:** Design and develop a prototype SSI-based NID system using Ethereum, smart contracts, and verifiable credential wallets (e.g., MetaMask, SpruceID, Bifold, Custom) to demonstrate secure issuance, storage, and verification.
- **Comparative Analysis:** Conduct comparative and experimental evaluations of the proposed framework against traditional identity models and existing SSI platforms in terms of usability, security, and scalability.

1.5 Thesis Organization

This thesis is organized into nine chapters. Chapter 1 introduces the background, motivation, objectives and contributions of the research. Chapter 2 reviews relevant literature on identity management systems, SSI, blockchain, and government identity frameworks. Chapter 3 presents the proposed system architecture, design and protocol flow. Chapter 4 explains the research methodology and implementation steps. Chapter 5 discusses security and privacy considerations of the system. Chapter 6 provides a comparative analysis with existing identity models. Chapter 7 details the experimental setups and evaluation results. Chapter 8 outlines system limitations and future work. Finally, Chapter 9 concludes the thesis and summarizes key findings.

Chapter 2

Literature Review

2.1 Identity Management Systems

The evolution of Identity Management Systems (IMS) reflects the growing complexity of managing digital identities within increasingly interconnected digital ecosystems. Early identity management models were primarily silo-based shown in Figure 2.1, with each service provider maintaining independent identity databases. Users were forced to create and manage separate credentials for every service, leading to fragmented user experiences, limited interoperability, and significant security vulnerabilities. As Cameron observed, this fragmented "patchwork of identity one-offs" offered no consistent framework for users to assess the authenticity of the service provider or control personal information [2].

To address these challenges, federated identity management (FIM) models emerged, allowing organizations to share identity information across domains through mutual trust and standardized protocols. Federated systems introduced Single Sign-On (SSO), allowing users to authenticate once with a home Identity Provider (IdP) and access multiple Service Providers (SPs) within the federation [10][5]. Protocols such as SAML, WS-Federation, OpenID, and Liberty Alliance frameworks facilitated secure cross-organizational authentication exchanges [10][5], significantly improving usability while streamlining identity verification processes for organizations.

However, federated models introduced new concerns about privacy, trust, and control. Concentrating sensitive identity data within IdPs exposed users to identity theft, unauthorized data aggregation, and limited visibility over how personal information was shared and retained [5]. The reliance on trusted third parties to properly manage and protect identity attributes presented inherent risks that remained unresolved [5]. In response, user-centric identity models emerged, which allowed individuals more control over credentials and allowed selective disclosure of identity attributes [4]. Although these frameworks reduced data sharing and third-party dependencies, many still relied on centralized entities for credential issuance and verification, perpetuating core challenges related to trust and centralization [4].

These persistent limitations set the stage for a more radical paradigm: Self-Sovereign Identity (SSI). Building on lessons from earlier models, SSI proposes a decentralized architecture that fully restores control to individuals while addressing the long-

standing structural weaknesses of previous IMS frameworks shown in Figure 2.2. The subsequent sections will explore SSI's theoretical foundations, blockchain integration, government adoption potential, existing platforms, and remaining research gaps.

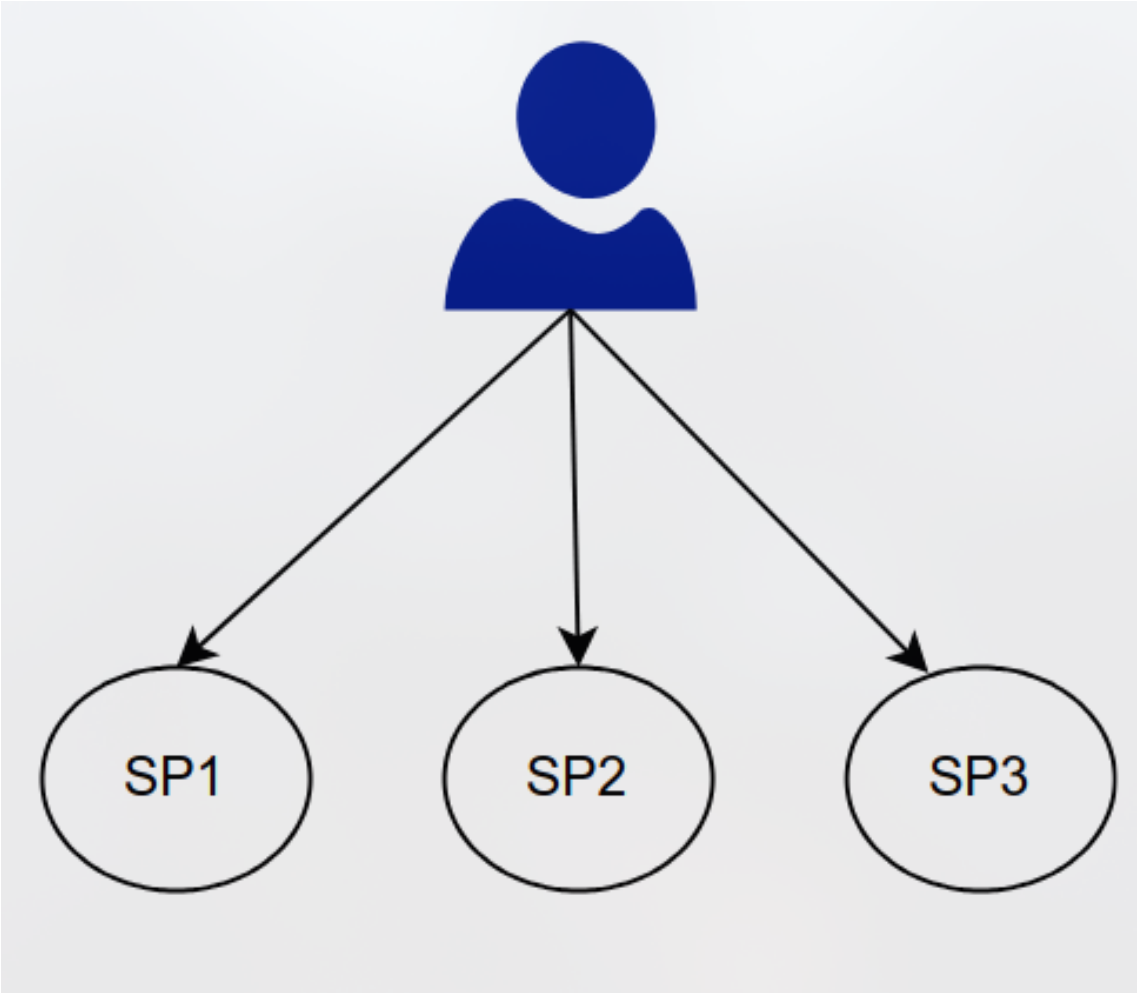

Figure 2.1: Silo Model

2.2 Self-Sovereign Identity

Self-Sovereign Identity (SSI) represents a significant shift in digital identity management, placing full ownership and control of identity data in the hands of individuals rather than centralized authorities. Unlike earlier centralized and federated models that create vendor lock-in and privacy concerns, SSI is grounded in principles emphasizing autonomy, consent, ownership, portability, and minimal disclosure [25][2][14], [16][40]. Allen's widely cited framework provides ten foundational principles that continue to inform SSI system design [14].

Mühle et al. outline a comprehensive SSI architecture comprising decentralized identifiers (DIDs), authentication mechanisms, verifiable credentials, and secure storage solutions [20]. DIDs, standardized by the W3C Verifiable Credentials framework

[26], pair cryptographic keys with decentralized registries to eliminate reliance on centralized identifier authorities. Verifiable credentials allow trusted third parties to issue attestations that users can present selectively, preserving both trust and privacy [20]. Soltani et al. provide a detailed survey of SSI ecosystems, highlighting how these core components, along with distributed ledger technologies, enable decentralized identity while still facing governance and regulatory challenges [43].

To formally characterize SSI systems, Ferdous et al. present a mathematical model that distinguishes between partial and complete identities across multiple domains [25]. Expanding on this, Grüner et al. introduce a quantifiable trust model that objectively evaluates trust relationships within decentralized identity networks—critical for ensuring interoperability and scalability, particularly in government and public-sector contexts [19]. These models support advanced system designs capable of managing multiple partial identities while facilitating cross-domain interoperability, a key advantage over traditional federated models [4][10].

SSI also introduces possibilities for cross-border identity continuity, enabling individuals to maintain consistent digital identities across national and organizational boundaries [16]. However, regulatory frameworks such as eIDAS 2.0 still face unresolved legal and interoperability challenges in adopting SSI principles for public sector use cases [42]. Zwitter and Hazenberg further emphasize that decentralized governance introduces new complexities in rule-making, accountability, and dispute resolution that must be addressed for wide-scale adoption [36].

This theoretical foundation supports the proposed decentralized government-issued NID framework explored in this study, where state authorities issue verifiable credentials while individuals retain full control over credential storage, management, and disclosure.

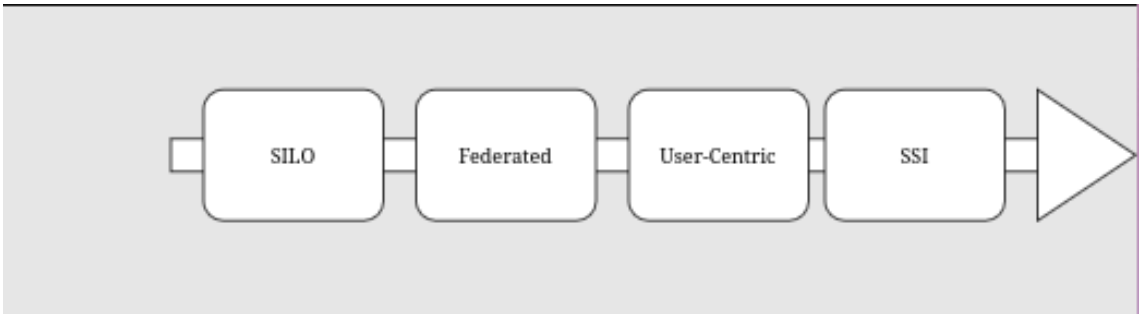

Figure 2.2: Evolution of Identity Models

2.3 Blockchain Technology for SSI

Blockchain plays a pivotal role in enabling Self-Sovereign Identity (SSI) by addressing long-standing shortcomings in traditional identity models—particularly around centralization, trust, and data ownership. While earlier identity systems—centralized IDM 1.0 and federated IDM 2.0—place control of identity data in the hands of third

parties, SSI leverages blockchain's decentralized architecture to enable users to independently own and manage their identity credentials [33][62]. Blockchain's immutability and distributed consensus mechanisms ensure tamper-resistance, transparency, and trust without reliance on centralized intermediaries [23].

In SSI architectures, blockchains primarily serve as decentralized anchors for identifiers, public keys, and credential registries [26]. Verifiable Credentials, defined by the W3C, allow trusted authorities to issue digitally signed attestations that are independently verifiable without exposing underlying personal data [26]. Grüner et al.'s trust model enables quantitative assessment of issuer-holder-verifier relationships within decentralized networks, which is critical for establishing cross-domain trust in blockchain-based identity ecosystems [19].

Various blockchain-based SSI platforms illustrate different design trade-offs. uPort, for example, utilizes public blockchains like Ethereum, deploying smart contracts for credential issuance, selective disclosure, and key recovery [33]. While uPort maximizes decentralization, it faces challenges related to scalability, transaction costs, and public data exposure [18]. Sovrin, in contrast, operates on Hyperledger Indy's permissioned ledger governed by a trust framework that balances decentralization with legal accountability, making it attractive for public-sector applications [33][40].

Despite blockchain's technical strengths, governance remains one of the most significant challenges for SSI, particularly in national identity contexts. As Zwitter and Hazenberg point out, decentralized systems require robust governance frameworks to address legal compliance, dispute resolution, regulatory oversight, and coordination among diverse stakeholders [36]. Preukschat and Reed further emphasize the importance of privacy-preserving cryptographic techniques such as zero-knowledge proofs and off-chain storage to ensure that sensitive identity data remains protected despite the transparency of blockchain ledgers [40].

Through careful architectural design, blockchain-based SSI enables governments to issue legally binding digital credentials while preserving citizen privacy, accountability, and auditability [23]. Public blockchain infrastructures also offer global interoperability, supporting the vision of transparent, inclusive, and sovereign digital identity systems [62].

2.4 SSI Protocols

To implement Self-Sovereign Identity in a practical and interoperable manner, several protocols have been introduced that formalize key components such as credential issuance, communication protocols, and identity data models. These protocols ensure that individuals, issuers, and verifiers can securely exchange identity data across diverse digital ecosystems, regardless of the underlying platform or blockchain. Rather than inventing entirely new mechanisms, many of these standard protocols extend existing web authentication technologies and cryptographic protocols to meet the specific requirements of decentralized identity.

2.4.1 OpenID4VCI (OpenID for Verifiable Credential Issuance)

OpenID for Verifiable Credential Issuance (OpenID4VCI) is an emerging protocol developed by the OpenID Foundation that extends the OAuth 2.0 authorization framework to support the secure and privacy-preserving delivery of Verifiable Credentials from issuers to user-controlled wallets. In contrast to traditional OpenID Connect flows used primarily for authentication, OpenID4VCI introduces a credential issuance process, where the user's digital wallet authenticates to an issuer (such as a government portal) and requests a signed credential in return.

This protocol ensures that credential exchange is consent-based, tokenized, and compatible with federated identity infrastructure while enabling decentralized storage and usage on the user's side. Because it builds on the well-established OAuth model, OpenID4VCI provides a pathway for integrating SSI principles into existing identity systems with minimal friction, particularly in government and enterprise contexts [54].

2.4.2 DIDComm (Decentralized Identifier Communication)

DIDComm is a secure messaging protocol standardized by the Decentralized Identity Foundation. It enables encrypted, peer-to-peer communication between participants in a decentralized identity ecosystem, such as issuers, holders, and verifiers. Using cryptographic keys associated with Decentralized Identifiers (DIDs), DIDComm facilitates confidential and authenticated message exchange without relying on centralized intermediaries.

The protocol supports a variety of transport layers, including HTTP, Bluetooth, WebSocket, and even QR code-based interactions, making it versatile across device types and network environments. It underpins advanced SSI workflows such as credential offers, requests for proof, and revocation notices. By embedding trust directly into communication flows, DIDComm helps ensure that sensitive identity data remains under the control of the user throughout its lifecycle [53].

2.4.3 W3C Verifiable Credentials (VC) Standard

The Verifiable Credentials data model, defined by the World Wide Web Consortium (W3C), provides the structural foundation for how identity information is formatted, signed, and verified in SSI systems. Each credential issued under this standard consists of subject claims (such as name, nationality, or date of birth), metadata about the issuer, and a cryptographic proof that binds the credential to both the subject and the issuer.

Credentials are expressed in JSON-LD format, enabling semantic interoperability across diverse platforms and jurisdictions. When users present a credential to a verifier, they may do so through a Verifiable Presentation that allows for selective disclosure and proof minimization. This approach balances privacy, authenticity, and interoperability, making it the cornerstone of most SSI implementations to date [26].

2.5 Government & National ID Systems in SSI Context

Many governments have adopted digital identity systems—such as eIDAS in Europe, Aadhaar in India, and Estonia's eID—to modernize public service access and citizen verification. However, these systems often rely on centralized or federated identity models, where state authorities or authorized providers control issuance, storage, and verification of identity credentials. This raises concerns around data privacy, surveillance, and lack of user control [39].

For instance, while eIDAS provides cross-border interoperability within the EU, its initial scope was limited to basic identity attributes and government services, restricting broader private-sector applications [56]. Schwalm and Alamillo-Domingo argue that despite eIDAS 2.0's efforts to integrate SSI principles, significant challenges persist regarding legal liability, interoperability, and trust framework complexities [42]. Estonia's highly advanced digital governance model offers seamless e-governance services but remains centralized, concentrating sensitive citizen data within state-controlled infrastructures [59]. Similarly, Aadhaar has expanded financial inclusion but attracted criticism for surveillance risks, privacy violations, and insufficient user consent mechanisms under its centralized architecture [8].

By contrast, SSI provides a decentralized alternative that empowers individuals to control their identity data through digital wallets while enabling selective disclosure of verifiable credentials without intermediary reliance [25], [47], [48]. Preukschat and Reed emphasize that governments can serve as trusted credential issuers within SSI ecosystems, issuing state-backed verifiable credentials that citizens control directly [40] [49]. Such hybrid models allow governments to meet legal and regulatory obligations while preserving individual data sovereignty through decentralized storage and management.

Emerging frameworks like eIDAS 2.0 reflect growing recognition of SSI's potential to enhance cross-border interoperability, transparency, and scalability for national identity infrastructures [56]. These developments form the foundation for the public blockchain-based SSI model proposed in this study, offering governments a path to issue legally valid, citizen-controlled digital national IDs that address the limitations of centralized eID architectures [37].

2.6 Existing SSI Platforms & Frameworks

A growing number of SSI platforms have implemented self-sovereign identity principles with varied architectures, an example shown in Figure 2.3, informing national ID system design. Sovrin stands among the most mature SSI ecosystems, operating on a public-permissioned ledger governed by the Sovrin Foundation's Trust Framework [22][32][45]. It employs DIDs, verifiable credentials, and zero-knowledge proofs to enable privacy-preserving selective disclosure, balancing decentralization with legal accountability suitable for national-scale deployments [22][40]. Sovrin's

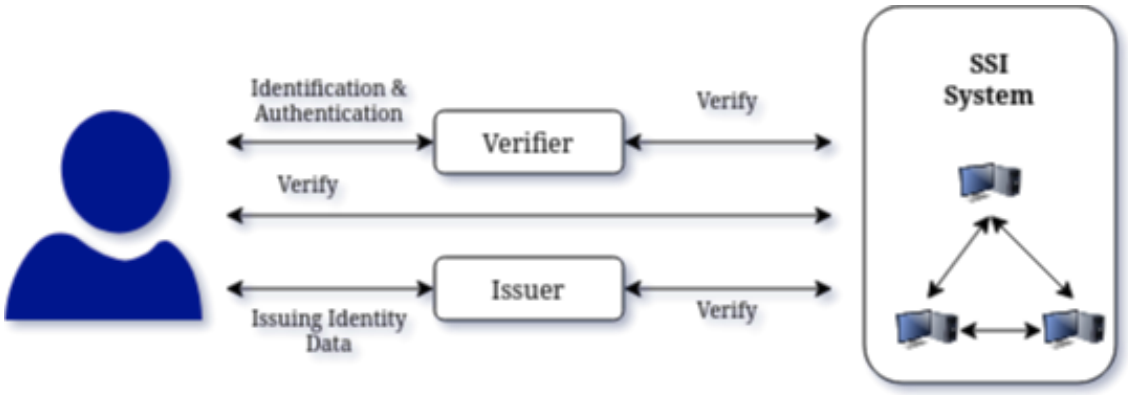

Figure 2.3: SSI Architecture

open-source foundation, Hyperledger Indy, provides cryptographic primitives, wallet services, and DID resolvers [30].

Alternatively, uPort utilizes public Ethereum networks, leveraging smart contracts for identity registration, credential issuance, and key recovery [15][18]. While maximizing decentralization, uPort faces scalability concerns, cost volatility, and public registry exposure [18]. Jolocom emphasizes interoperability across DID methods while offering software development kits for wallet deployment and credential management [31][35]. Blockcerts focuses specifically on educational and professional credential verification anchored on public blockchains, supporting auditability but offering limited general-purpose identity lifecycle management [27].

These platforms increasingly align with W3C standards for DIDs and verifiable credentials [26][34], promoting cross-jurisdictional interoperability. However, Preukschat and Reed caution that challenges remain around governance intermediaries, credential revocation, key recovery, and regulatory compliance [40]. Common limitations include ongoing dependencies on governance stewards, trade-offs between privacy and auditability, and scalability or usability barriers that complicate government-level adoption [29][25].

These limitations motivate this study's proposed framework, which leverages public blockchain infrastructure to preserve decentralization, regulatory accountability, and verifiable trust, while meeting government requirements for national ID issuance, interoperability, and citizen data sovereignty.

2.7 Research Gaps

Despite advancements in SSI technologies, significant research gaps remain that limit their application in government-issued national ID frameworks. Current government digital identity systems—such as eIDAS, Aadhaar, and Estonia's eID—retain centralized or federated control structures that restrict user autonomy and elevate privacy and surveillance risks [39][56][47][48].

While frameworks like eIDAS 2.0 attempt to integrate SSI principles, adoption re-

mains constrained by complex governance, legal liability concerns, interoperability gaps, and the absence of global trust standards [42][56]. Schwalm and Alamillo-Domingo highlight unresolved issues around legal responsibility, credential revocation, and cross-border enforcement when adapting SSI to existing legal frameworks [42].

Technically, platforms such as Sovrin, Hyperledger Indy, uPort, Jolocom, and Blockcerts offer strong cryptographic foundations [22][30][15][31][27], yet each presents trade-offs. Sovrin balances governance and privacy through permissioned ledgers but restricts full public accessibility [22][40], while uPort maximizes decentralization but struggles with scalability, cost, and privacy exposure [18]. Grüner et al.'s quantifiable trust model offers promising formalization but remains immature in practical adoption [19]. Usability challenges also persist around key management, credential revocation, and integration with government legal frameworks [25].

Governance, in particular, remains underdeveloped for decentralized public-sector identity systems. As Zwitter and Hazenberg argue, decentralized governance introduces new complexities in trust anchor designation, cross-border coordination, regulatory compliance, and dispute resolution that must be addressed for viable government-backed SSI adoption [36].

To address these limitations, this study proposes a new framework that fully utilizes public blockchain infrastructure while aligning with governmental regulatory requirements. This design enables issuance of legally recognized, citizen-owned national digital identities that maintain decentralization, ensure privacy, and support domestic and cross-border interoperability, balancing governmental accountability with true self-sovereignty.

2.8 Literature Summary Table

Topic	Key Concepts / Contributions	Limitations / Gaps	Key Sources
Identity Management Systems	Evolution from siloed to federated and user-centric identity; SSO, IdP-SP trust models	Centralization risks, privacy, lack of user control	[2][5][4]
Self-Sovereign Identity (SSI)	DIDs, VCs, cryptographic control, user autonomy	Governance complexity, interoperability, key recovery	[25][20][19][43]
Blockchain for SSI	Immutability, anchor for VCs/DIDs, public trust ledger	Cost, scalability, on-chain privacy	[33][62][18]
SSI Standards	OpenID4VCI, DIDComm, W3C VC for interoperability	Evolving specs, uneven adoption	[54][53][26]
Government eID Systems	eIDAS, Aadhaar, Estonia eID; centralized digital IDs	Surveillance risks, lack of user control, limited private sector use	[56][42][59]
Existing SSI Platforms	Sovrin, uPort, Jolocom, Blockcerts; use of ledgers, wallets	Trade-offs between decentralization and usability	[22][18][31]
Identified Research Gaps	Legal frameworks, trust anchor governance, adoption barriers	Lack of national-scale implementation, key revocation gaps	[36][19][40]

Table 2.1: Summary of Key Literature on Identity Systems and SSI

Chapter 3

System Design and Architecture

This chapter explains the overall architecture and design of our decentralized identity system. The system uses the information from the individual's National Identity Card (NID) to generate verifiable credentials (VC) and stores them in the user's wallet. A verifier (such as a service provider) can verify the authenticity of this VC if needed. The entire process is built on a combination of blockchain, encryption, and a web-based credential storage system.

3.1 Architecture

The decentralized identity system proposed in this study is built on an architecture shown in Figure 3.1 that uses modern Web 3.0 technologies to make personal identity management secure, autonomous, and out of centralized control. Decentralized identity is being considered as a future-proof solution to overcome the limitations of conventional centralized identity systems such as reliance on a single central authority, risk of data breaches, and low user control.

This system architecture is mainly based on Verifiable Credential (VC), Decentralized Identifier (DID), cryptography and blockchain technology. A key feature of the proposed architecture is its Self-Sovereign Identity (SSI) based design. In this, the user himself maintains full control over his identity and Credential. Credentials are stored in an encrypted state, which can only be decrypted by the user's private key. The system has adopted multiple approaches to storing credentials such as storing encrypted VC on the blockchain, using mobile-based wallet (SpruceKit) integration, Aries-based Bifold mobile wallet and Custom Wallet that uses Elliptic Curve Cryptography (ECC).

This architecture relies on four main roles: Issuer, Holder, Verifier and Blockchain Network. The Issuer, such as the government, issues a digitally signed Credential. The Holder, i.e. the user, accepts it and stores it securely in his wallet. Later, when a platform wants to verify its identity, the Verifier requests the Credential to be presented and verifies it against the hash stored on the blockchain network.

This system architecture is designed to maintain three important aspects security, transparency, and user control. Encryption at every stage, digital signatures, and the immutability features of the blockchain ensure that the user's identity information

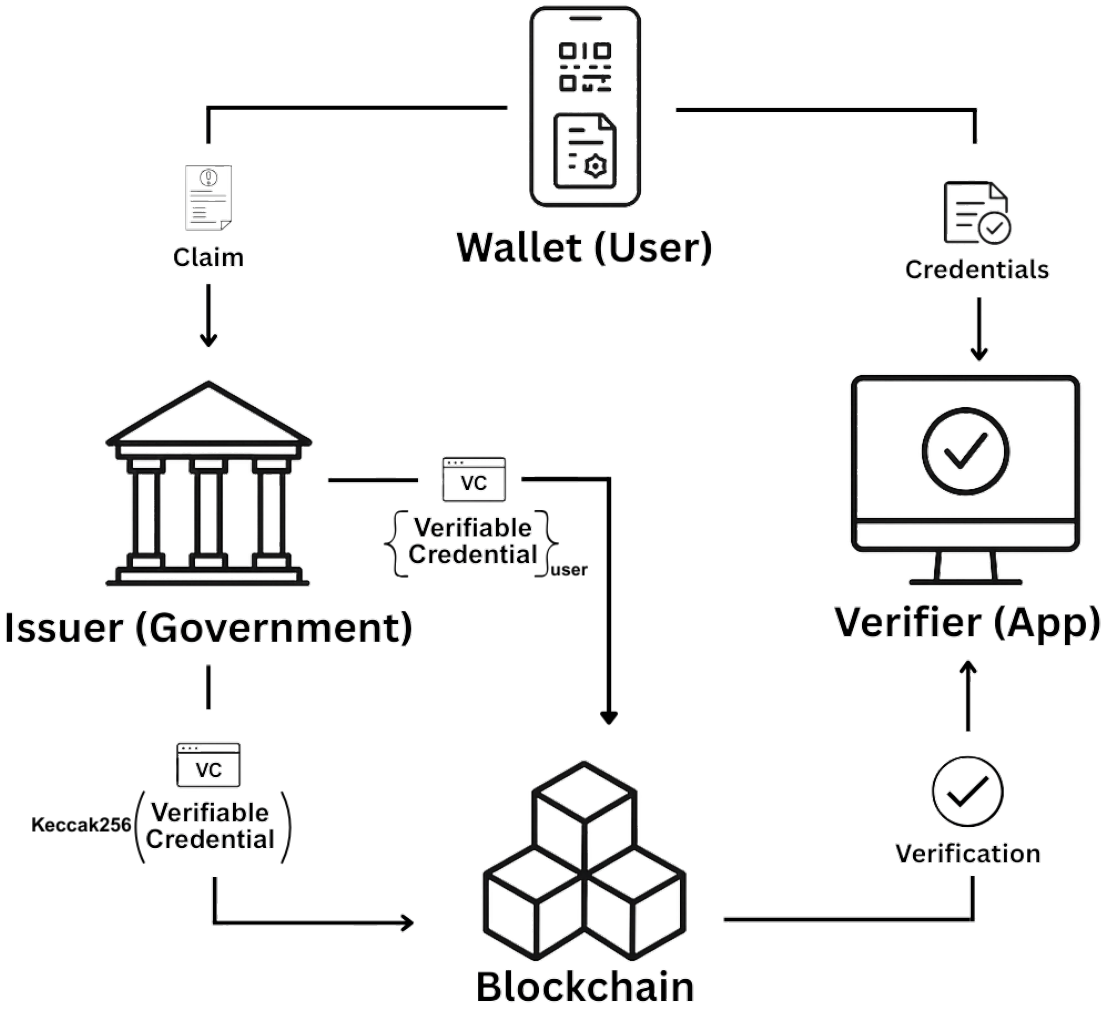

Figure 3.1: Government Issued VC using Self Sovereign Identity.

cannot be altered or forged by third parties in any way. At the same time, the user can decide when and where he presents his identity, which is the basis for a truly self-sovereign digital identity system.

3.2 Key Components

The effectiveness of a decentralized identity system depends on the coordination of its various key components. In this project, four key components work together to represent and verify a user's identity in a secure and verifiable manner. Each component is discussed in detail below.

3.2.1 Issuer

Definition: Issuer is the organization or authority that creates a Verifiable Credential and issues it to the user. The government acts as the issuer in this system.

Importance: Our motivation is to create a trustworthy, secured identity system that can verify a user properly. As government-issued identities undergo a more rigorous and secure verification process, they serve as a highly trusted foundation for digital identity systems. Furthermore, issuers play a key role in establishing trust in the system. They add a digital signature to the VC, which proves to the verifier that it was actually issued by the government.

3.2.2 Holder

Definition: The holder is the person upon whom the VC is issued and who owns and controls that VC. Ordinary users (e.g., citizens), who are known by their Ethereum address and use a wallet to hold and manage credentials.

User Control: The holder has complete control over when, how, and to whom to present the VC. As the Verifiable Credential (VC) of the holder is hashed and encrypted before storing in the blockchain, no one else can retrieve the original VC.

3.2.3 Verifier

Definition: A verifier is an organization or platform that seeks to verify a user's identity. Any third-party service provider (e.g., a bank, online service, or university) is a verifier that wants to verify the user's identity.

Transparancy: Verifiers can verify information directly from the blockchain, not relying on any central server. This makes the process more transparent and reliable. Existing digital identities, depending on their underlying protocols, may be vulnerable to forgery or manipulation, leading to potential identity fraud. In contrast, a Verifiable Credential (VC) issued by a government authority is anchored in official, legally recognized identity verification processes. As a result, when such a government-issued VC is presented, verifiers can confidently authenticate the legitimacy and identity of the user, significantly reducing the risk of impersonation or false claims.

3.2.4 Blockchain Network

Definition: Ethereum is a public, decentralized blockchain platform that provides the ability to store and verify information through smart contracts.

Importance: Blockchain's Distributed Ledger Technology (DLT) ensures immutable and tamper-proof storage of a user's Verifiable Credential (VC) hash. This public and transparent infrastructure allows any authorized party to independently verify the authenticity of a user's credential without compromising sensitive personal data, thereby enhancing trust and accountability in the identity verification process. Public blockchain network ensures the verification process seamless for every Service Providers (SP).

The combined activities of these four components create a complete, secure, and user-centric decentralized identity ecosystem. In this, the issuance, storage, and verification of user identities is completely user-controlled, privacy-enhanced, and blockchain-based, which is much more advanced and secure than traditional centralized methods.

3.3 Protocol Flow

The Verifiable Credential (VC) mechanism in a decentralized identity system follows a consistent protocol flow through which a user's identity can be verified, stored, and later retrieved and verified. This section explains each step in detail, from VC issuance to verification.

3.3.1 Digital Wallet Creation

In the first step, a user enters the government portal to issue their Verifiable Credential (VC). Before registering for VC, a user needs to create a digital Wallet. In our system we propose a Custom Wallet system the government portal offers. It follows the HD Wallet key derivation using BIP standards, for wallet creation. First user will provide a new password to continute to the next step. In the following step, A series of Mnemonic keys similar to Figure 3.2 are generated using 'ethers'[13] library. User securely stores the 12 key phrase values so that later they can recover their wallet. If forgotten, not possible to retrieve user's wallet. After confirming, it generates a seed using PBKDF2 from the Mnemonic keys.

Finally a private key is generated that generates a public key and user's ethereum public address. The raw public key and Ethereum address is stored in user's local storage. Additionally, the private key is encrypted using Symmentric Key algorithm (AES) with the wallet password as key and stored in user's local storage. The key pair follows Elliptic Curve Cryptography (ECC) algorithm to later encrypt and decrypt credentials.

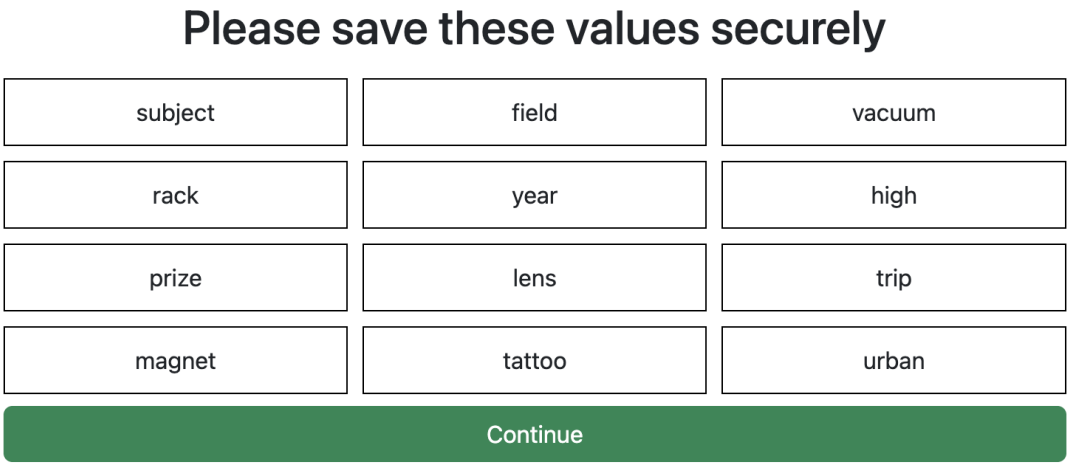

Figure 3.2: Mnemonic-based hierarchical deterministic key derivation

3.3.2 VC Issuance

After successfully wallet creation, a user registers with a government service or platform providing their information along with their National Identity Card (NID) according to Figure 3.3. To verify this information, the government or a designated authority matches the information provided by the user with the information stored in the national database. The system automatically retrieves user's public Ethereum address from their digital wallet. Once the information is verified, the authority generates a Verifiable Credential (VC) using 'did-jwt-vc'[28], which includes the user's name, date of birth, national identity number (NID), and a DID (Decentralized Identifier). This DID is actually based on the user's Ethereum Address that was retrieved earlier from user's wallet, such as: did:ethr:0x1234abcd.... The format of the VC is created in JSON-LD format according to the W3C Verifiable Credentials standard and the government digitally signs the VC, which is later verifiable by verifiers.

3.3.3 Storing VC

In the third step, the government-issued Verifiable Credential (VC) is store in the the Distributed Ledger Technology (DLT) using Smart Contract. However, this Credential is not sent directly or in its unaltered form. Rather, the VC is both encrypted and hashed to ensure the user's privacy and security. The encryption process uses the Elliptic Curve Cryptography (ECC) with user's public encryption key, which is obtained from user's wallet. This ensures that only the user, who owns the private key, will be able to decrypt the Credential.

Once the VC is encrypted, it is converted into a secure Base64 encoded string. This encrypted string is then stored on the blockchain via a specific Ethereum smart contract. This keeps the Credential in a permanent and immutable state on the blockchain. At the same time, a SHA-256 hash of the VC is also generated and

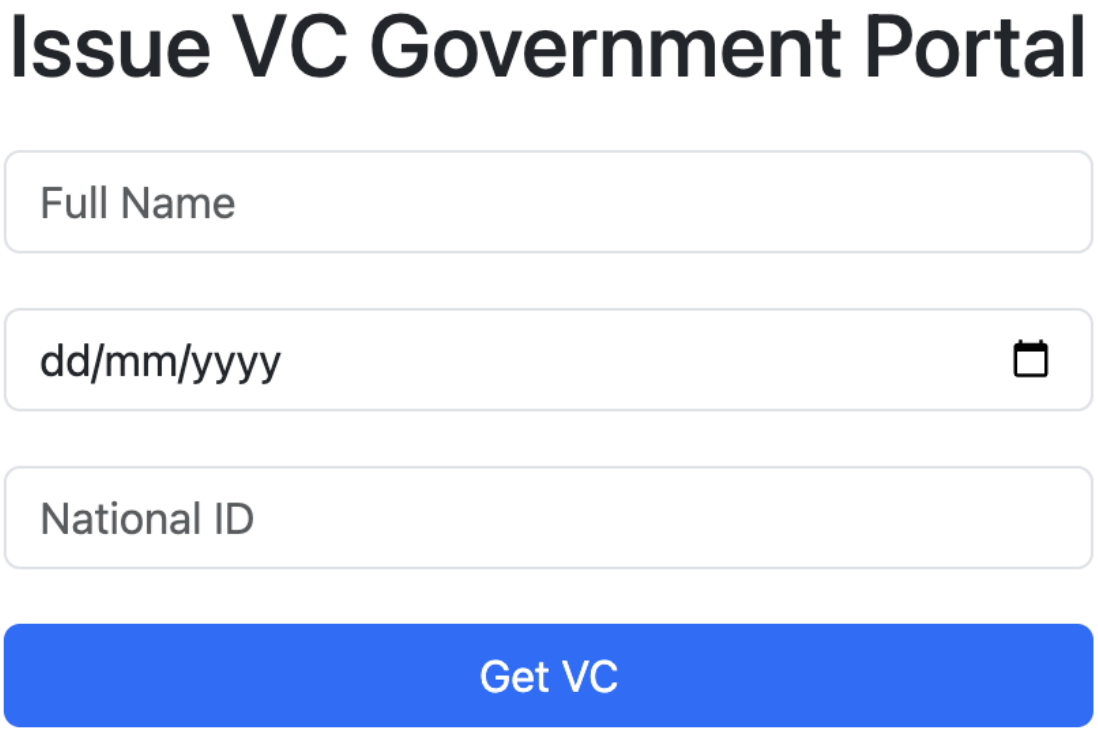

Figure 3.3: VC Issuance Government Portal

stored separately on the blockchain. This hash function allows the credential to be later verified to ensure that it has not been altered or tampered with in any way since its issuance.

3.3.4 Retrieving VC

Next, when a user wants to avail a specific service such as opening a new account at a bank, applying for admission to an educational institution, or applying for a government grant, user needs to recover their digital wallet or retrieve public Ethereum address if wallet existed. In this step, the verifier first collects the user's Ethereum-based Public Address to search for the encrypted VC on DLT.

This VC is initially stored in encrypted form in such a way that the verifier or any third party cannot read it directly. In the next step, user retrieves the encrypted Verifiable Credential. Then user provides the wallet password in Figure 3.4 to decrypt the encrypted private key that was stored in the local storage. Later with the private key user decrypts the Verifiable Credential and passes it to the Verifier.

3.3.5 Verifying VC

In the final step, the verifier (e.g., a bank, educational institution, or government agency) verifies the Verifiable Credential (VC) presented by the user and confirms its authenticity. At the beginning of the verification process, the verifier analyzes the digital signature attached to the VC to ensure that it is from a trusted and authentic source that is, issued by the government or a designated issuing authority.

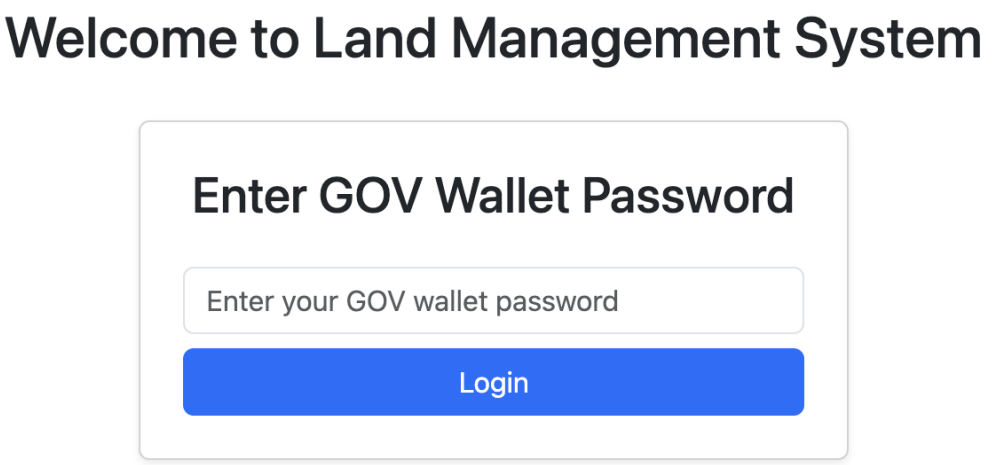

Figure 3.4: Services Verifying VC

Digital signature verification proves that the VC has not been altered or tampered with in any way since issuance.

In the next step, the verifier recalculates the hash from the VC presented by the user and compares it with the hash previously stored in the blockchain. If this comparison is successful—that is, both hashes match and the digital signature is proven valid then verification is considered successful. As a result, the user is allowed to receive the specified service.

This entire verification process is completed in an environment controlled by the user, where no information is shared without his consent. There is no reliance on a central server or authority, but rather all authentication processes are performed through blockchain and cryptographic methodologies. It is a modern and decentralized identity verification system designed to follow the principles of the Self-Sovereign Identity (SSI) model full user control, transparency, and security.

This flow ensures that all user identity information is under their own control, that information is stored encrypted on the blockchain, and that the third-party verification process is fully trusted and transparent. The protocol outlines an advanced, decentralized, and secure identity system while maintaining user privacy.

Chapter 4

Research Methodology

This chapter outlines the methodological approach undertaken to design, develop, and evaluate a decentralized, secure, and user-centric identity verification system grounded in Self-Sovereign Identity (SSI) principles. The research aimed to build a functioning prototype that uses Verifiable Credentials (VCs), Decentralized Identifiers (DIDs), and blockchain technology to replace centralized identity verification mechanisms. The methodology combines iterative system development, technical experimentation, and standards-based integration.

4.1 Research Design

The research follows an applied, prototype-driven design methodology. Given the focus on addressing real-world limitations of centralized identity systems, a practice-oriented approach was adopted. The project targeted the design and implementation of a complete decentralized identity lifecycle — including issuance, encryption, on-chain storage, and selective presentation of Verifiable Credentials.

To achieve this, the research employed a blend of technical review, solution benchmarking, and rapid prototyping. Each core functionality (such as DID generation, VC signing, or smart contract deployment) was first developed in isolation, validated through testing, and then integrated into the broader system pipeline. Comparative analysis was conducted to evaluate different SSI tools, frameworks, and digital wallet providers.

4.2 Development Method

The system was developed using an Iterative Development Model. This approach allowed for gradual construction of the decentralized identity framework, where feedback from each stage was used to refine the next. The initial milestone involved establishing a basic flow for Verifiable Credential issuance. This was incrementally extended by adding Ethereum-based Decentralized Identifiers (did:ethr), credential signing using JWT, encryption using public keys, on-chain storage via smart contracts, and user-controlled credential presentation and verification.

At each iteration, small-scale prototypes were created to validate assumptions, confirm compatibility with SSI standards, and measure functional performance. These prototypes included credential generation scripts, different wallet such as MetaMask, Spruce ID, Bifold-integrated interfaces, and Ethereum smart contracts on test networks.

4.3 Data Collection and Analysis

Rather than using a dataset in the traditional sense, this research involved an in-depth evaluation of existing SSI tools and frameworks. Technologies such as W3C Verifiable Credentials, the did:ethr method, and decentralized wallets (SpruceID Credible Wallet, Bifold, Custom) were selected based on documentation review, compatibility testing, and practical experimentation.

Testing was conducted on Ethereum's Ganache testnet environment to simulate real blockchain interactions without incurring transaction fees. MetaMask was used to interact with the Ethereum network for signing, encryption, and VC decryption workflows. Each implementation decision—such as choice of encryption scheme or storage method—was made based on observed behavior, interoperability with other SSI components, and alignment with published standards.

4.4 Technical Tools and Environment

The following tools, libraries, and platforms were employed in the development and testing of the proposed framework:

- **Ethereum (Ganache):** Used to simulate a blockchain environment for deploying and testing smart contracts.
- **Solidity:** Used to write the smart contract responsible for storing encrypted VCs and their hashes on the blockchain.
- **Node.js (Express):** Backend APIs were developed for credential issuance, encryption, and interaction with Ethereum smart contracts.
- **React.js:** The frontend interface was built using React to facilitate user registration, VC requests, and VC presentation workflows.
- **MetaMask:** Used as a browser-based wallet for key management, digital signatures, public key encryption, and VC decryption during presentation.
- **SpruceKit, Bifold:** These mobile digital wallets were tested to validate compatibility with VC formats and DID methods, enabling storage, retrieval, and presentation of credentials.

4.5 Implementation Steps

The development of the system was broken down into the following sequential steps and a visual representation is shown in Figure 4.1:

- **DID Generation:** A Decentralized Identifier was generated using the ‘did:ethr‘ method, derived from the user’s Ethereum address with the help of the `ethr-did` library.
- **Credential Issuance:** After verifying user identity via National ID (NID), a Verifiable Credential was created in JSON-LD format. The credential was signed using `did-jwt-vc`, binding the credential to the user’s DID.
- **Credential Encryption:** The VC was encrypted using the user’s Ethereum public key. The encrypted credential was then Base64-encoded for blockchain compatibility.
- **Blockchain Storage:** A smart contract was developed in Solidity to store the Base64-encoded encrypted VC and its corresponding SHA-256 hash. This ensured both immutability and integrity verification.
- **Decryption and Verification:** When a verifier requested identity proof, the system retrieved the encrypted VC, and the user decrypted it locally using wallet’s private key. The decrypted VC was then validated by checking the issuer’s digital signature and matching the recomputed hash with the blockchain-stored value.
- **Wallet Testing:** Additional testing was conducted with SpruceKit, and Bifold wallets to ensure cross-platform credential interoperability, storage, and selective presentation.

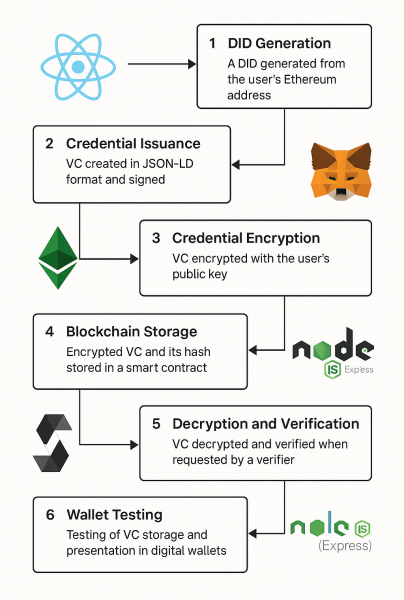

Figure 4.1: Steps

4.6 Methodological Rationale

The chosen methodology reflects the inherent complexity of decentralized identity systems. Unlike centralized IAM solutions, SSI requires coordination across multiple cryptographic, blockchain, and wallet-based components. A waterfall or static

research model would not have supported this complexity. Therefore, iterative prototyping was necessary to isolate and solve interoperability, cryptographic signing, and encryption challenges incrementally.

Real-time testing on Ethereum testnets, compatibility checks with W3C standards, and end-to-end encryption via MetaMask were critical to ensuring that the solution not only adhered to SSI principles but also worked reliably in practice. Emphasis was placed on adherence to international standards such as OpenID4VCI, DIDComm, and the W3C VC Data Model to future-proof the implementation and ensure compliance with the broader SSI ecosystem.

Chapter 5

Security and Privacy Considerations

Security and privacy were given top priority when creating this decentralized identity system. Since the project is based on personal identity information, it was of utmost importance that the user's information be protected from unauthorized access, modification, or manipulation. At the same time, the user's identity data should always be under his own control and he can decide when, where, and with whom to share it.

5.1 Data Encryption

The project provides for the storage of Credentials through encryption. After the Verifiable Credential (VC) is issued, it is directly encrypted using the user's Ethereum public key. As a result, the Credential can only be read or decrypted by the user whose private key is associated with that public key. The Elliptic Curve Cryptography (ECC) used for encryption, which is currently supported by multiple ventures and wallets and is considered secure. As a result, the Credential cannot be read or copied by anyone else, even if it is stored on the blockchain or anywhere else.

5.2 Digital Signature

Digital signatures are used to verify the authenticity of the Credential. The issuer (government) attaches a digital signature to the Credential, which is cryptographically verifiable. The verifier can then verify this signature to ensure that the Credential was issued by the issuer and has not been altered. This provides effective defense against Man-in-Middle (MIM) attacks, Credential forgery, and Replay Attacks.

5.3 Data Integrity

Integrity and Immutability are ensured by storing the hash of the Credential on the blockchain. A SHA-256 hash of the Credential is generated and stored in a smart contract on the Ethereum blockchain. When a Credential is presented for verification, its hash is recomputed and compared with the hash stored on the blockchain.

As a result, if any change occurs to the Credential, it can be immediately detected and verification fails. This process is effective in preventing Credential Tampering.

5.4 User Control

The credential presentation process is completely under the user's control. The user can decide which verifier to present the credential to. For this, multiple wallet support has been exproled such as MetaMask, SpruceKit, and Bifold Aries Wallet including a Custom Wallet. Each of which does not allow sharing of credentials without user consent. This is consistent with important privacy principles such as Data Minimization and Consent-Based Access.

5.5 Data Privacy

The system does not rely on centralized data storage, which helps to avoid centralized database breach or single point of failure issues. All credentials are stored in encrypted form on the client-side or on the blockchain, and no Personally Identifiable Information (PII) is stored on the backend server. This significantly reduces the possibility of data leakage.

5.6 Consensus

We use the Proof of Stake (PoS) consensus mechanism, which is currently the main consensus method of the Ethereum blockchain. Since we are storing hashes and encrypted data of Verifiable Credential (VC) on the blockchain using Ethereum smart contracts, PoS is the natural foundation of our system. One of the reasons for choosing PoS is its speed, low cost, environmental friendliness, and strong security. PoS selects validators according to stake without heavy computation like PoW, thus maintaining scalability and efficiency. PoS creates a reliable foundation for our SSI-based identity system, where trustless and decentralized verification is important. It holds validators accountable and ensures the immutability of the blockchain, which is essential for sensitive systems like VC verification.

Overall, the security and privacy architecture of this project is designed according to current SSI and DID standards OpenID4VCI, DIDComm and W3C VC, where the user's information remains under his own control, and cannot be modified, collected, or used by any unauthorized third party. This system design protects user rights, opens up new doors for secure identity systems, and lays the foundation for future trusted digital systems.

Chapter 6

Comparative Analysis

In the current technological context, the importance of digital identity systems is rapidly increasing. A reliable and secure identity process has become essential across various domains such as e-governance, online services, digital banking, and cross-border data access. Currently, most identity verification systems are built on centralized or federated architectures like OAuth and SAML, which have served well for interoperability but raise significant concerns over user autonomy, third-party dependency, and long-term trust viability.

OAuth and SAML-based systems, while standardized and widely deployed, give limited control to the user over their personal data and introduce a high degree of dependence on third-party Identity Providers (IdPs). These models also expose identity systems to vulnerabilities such as token leakage, single-point failures, and metadata surveillance [11][9].

In contrast, the Self-Sovereign Identity (SSI) model shifts the paradigm toward decentralization. It enables users to create their own Decentralized Identifiers (DIDs), receive Verifiable Credentials (VCs) from trusted issuers (e.g., governments), and independently prove their identity using cryptographic proofs anchored in blockchain. The SSI-based system proposed in this research is designed to be secure, tamper-resistant, and privacy-respecting, relying on open standards such as Ethereum DID, W3C VC, and decentralized ledger technology (DLT).

This chapter presents a detailed comparative analysis between the proposed SSI system and conventional identity systems, focusing on aspects such as architecture, trust model, user control, interoperability, and practical applicability.

6.1 Comparative Analysis of our proposed system with existing works

Below is the comparative analysis shown in Table 6.1, between different blockchain networks, standards, and storage methods with our proposed system. The purpose of this analysis is to evaluate the technical aspects of different SSI applications—such as the blockchains used, standards, data storage methods, and limitations in a structured manner.

Authors	Blockchain	Storage	Standard	Security	Limitations
Shuaib et al., 2023 [62]	Hyperledger Indy/Aries	Off-chain IPFS	W3C VC	Solid	Limited public deployment
Pärni, 2023 [60]	Bitcoin (ION)	Cloud/Custom wallet	OpenID4VC	Solid	Relies on centralized cloud storage
Mühle et al., 2018 [20]	Hyperledger Indy	DLT + IPFS	Hyperledger Aries	Solid	Complex key management
Ding & Sato, 2022 [44]	General DLT (SSIaaS)	Wallet + Registry	W3C VC, DID	Notable	Early prototype; usability challenges
Schanzenbach et al., 2018 [21]	GNS (name system)	ABE-encrypted namespace	DID, OIDC	High	Potential namespace scalability issues
Naghmouchi et al., 2022 [46]	Ethereum + Indy	Device Wallets + Smart Contracts	W3C DID, Aries	Solid	IoT constraints (latency, device limits)
Ghirmai et al., 2023 [55]	Ethereum/Web3	SSI Wallet	Custom/Web3	Moderate	Conceptual stage; early development
Babel & Sedlmeir, 2023 [52]	zk-Blockchain	Wallet + ZKP proofs	ZK / W3C-compatible	Solid	Prototype complexity and performance trade-offs
Satybaldy et al., 2023 [61]	Mixed (Indy, Ethereum, ION)	IPFS, Wallet, Cloud	W3C, Aries, OpenID4VC	Varies	Integration issues; no unified model
Naik et al., 2021 [38]	General DLT	Wallet-based	W3C VC, DID	Moderate	General-purpose; lacks deployment evidence
Our Proposed System	Ethereum	DLT + Custom Wallet	W3C VC	Solid	Presentation tied to wallet compatibility

Table 6.1: Comparative Analysis of SSI Systems

This paper presents an in-depth comparative evaluation of digital identity systems proposed by different authors. Both Shuaib et al., (2023) [62] and Mühle et al., (2018) [20] proposed an off-chain storage (IPFS) solution using Hyperledger Indy/Eris, while following the W3C VC standard. Although the security framework of their system is robust, Shuaib et al.'s model has faced limited public deployment, while the complex key management in Mulay et al.'s approach remains a major challenge. Pärni, (2023) [60] proposed a solution based on Bitcoin (ION), which uses the OpenID4VC standard, but it relies on centralized cloud storage, which weakens the core principle of decentralization.

On the other hand, Ghirmai et al., (2023) [55] and Naik et al., (2021) [38] proposed their model using Ethereum/Web3 and general DLT, respectively. Although Ghirmai et al.'s approach follows the custom/web3 standard, it is still conceptual and limited to early development. Naik et al.'s model is general-purpose but lacks practical deployment.

Our proposed system is a fully decentralized solution based on Ethereum, where a custom wallet is used, and this wallet uses the HD wallet key derivation method according to the BIP standard protocol. Here, encryption and decryption are done through public-private key pairs using ECC (Elliptic Curve Cryptography), and

only encrypted and hashed values are stored in the DLT. It does not use any central database, making the system completely decentralized and privacy-preserving. In this respect, our approach is ahead of the model of Satybaldy et al., (2023) [61], where mixed (Indy, Ethereum, ION) blockchains are used, but the lack of a unified model and integration issues remain.

Babel & Sedlmeir, (2023) [52] proposed a secure model based on zk-blockchain, which uses ZKP proof. Although the security of their system is strong, there are still trade-offs in the complexity of the prototype and performance. Our system overcomes these limitations by providing a simple and user-friendly interface, which is more convenient for users.

Overall, this comparative analysis shows that our proposed system overcomes many limitations of existing methods. It not only follows the W3C VC standard, but also provides a robust and complete decentralized identity system, which is able to advance the current research trend.

6.2 Similar Identity Management Systems

Technological advancements in identity management have led to the use of a variety of systems, including centralized authentication methods such as OAuth, SAML, and decentralized modern approaches such as Self-Sovereign Identity (SSI). Our proposed system follows a Decentralized Identity Framework, where users have full control over their own identities and do not have to rely on any central authority. From this perspective, a comparative analysis with OAuth, SAML, and other decentralized login systems is presented below to understand the uniqueness and effectiveness of our approach compared to conventional Identity Management Systems.

6.2.1 Centralized OAuth Framework

OAuth 2.0 is the most dominant framework for centralized identity authorization today, widely used by platforms like Google, Facebook, and GitHub. In this model, a user authenticates through a third-party IdP, which provides an access token to the relying application. This token is used to grant limited access to the user's data without revealing credentials.

Despite its flexibility, OAuth suffers from key limitations. The identity process remains dependent on a central server that stores and manages access tokens. Studies show that OAuth implementations are frequently flawed, with issues such as insecure token storage, token interception, and improper redirect URI handling, which can lead to session hijacking and data breaches [11].

In the proposed SSI system, user credentials are issued as cryptographically signed VCs by a trusted issuer (e.g., a government agency). Once issued, these credentials are stored in the user's wallet, allowing the user to present them to any verifier without calling back to the issuer. This eliminates third-party dependency, supports selective disclosure, and strengthens privacy.

6.2.2 SAML-Based Federated Identity System

Security Assertion Markup Language (SAML) is an XML-based standard for exchanging authentication and authorization data between identity providers and service providers. It has been widely adopted in government and enterprise environments, particularly in Europe where eID frameworks often rely on SAML-based architectures [7].

SAML enables federated login through assertions sent by IdPs to service providers, which trust the IdP to have correctly verified the user. However, this requires a tight trust relationship and prior configuration between IdP and SP. The user has little visibility into what is shared and when.

In contrast, our SSI system provides cryptographically verifiable credentials in a decentralized way. The user generates a DID and receives a VC from a government issuer, which can then be shared directly with verifiers. Assertions are JSON-LD based and support selective disclosure. Unlike SAML, no centralized session or API call is needed after issuance, and trust is established through digital signatures and blockchain-anchored hashes.

6.2.3 Decentralized Social Login Systems

New decentralized identity projects such as Web5 (TBD), uPort, and Ceramic Network have introduced user-controlled identifiers and decentralized storage solutions. These systems typically allow users to generate their own DIDs and store claims on peer networks or content-addressed storage systems like IPFS or Gaia [50]. While this removes centralized control, it raises issues of trustworthiness and formal verification.

Most decentralized social login systems rely on self-asserted claims or peer endorsement, which lack the institutional trust required for sensitive use cases like national identity, healthcare, or voting. Furthermore, many systems lack built-in revocation, version control, and formal credential schemas.

In contrast, our proposed system merges decentralized architecture with government-backed trust. Even though the user self-generates their DID, the Verifiable Credential is issued by an authorized entity, signed using secure keys, and its hash is stored on a blockchain. This allows any verifier to check the authenticity of the credential without trusting a centralized intermediary.

The systems discussed in Web5, uPort, and Ceramic are designed to provide users with self-defined identities and data ownership **“cite –muhle2018survey”**. Users create their own DIDs and store their data using various Decentralized Data Stores or Streams. However, a major challenge in these systems is credibility. This is because identity verification is usually based on their own claims, and no government or authorized organization issues these VCs.

On the other hand, in the SSI-based identity system that we have built, even though the user creates the digital wallet themselves, the government or a trusted authority

verifies the identity and issues the credential. The credential is created according to the W3C VC standard, and its hash is stored on the blockchain, which is cryptographically verifiable to anyone who verifies it. As a result, it is not limited to developers or encryption ecosystems, but is also useful in real-world applications such as citizen services.

6.3 Comparative Analysis on Consensus Algorithms

One of the fundamental foundations of blockchain technology is the consensus algorithm, which helps maintain a uniform and trustworthy state among all participants in the network. Different consensus mechanisms bring differences in efficiency, security, scalability, and decentralization in different contexts. Our proposed system uses Ethereum's Proof of Stake (PoS)-based framework, but a comparative analysis between different conventional consensus algorithms is necessary to justify why it is suitable. Below, the differences between PoS and consensus algorithms such as Proof of Work (PoW), Ethereum Layer 2 (Optimistic Rollups, zk-Rollups), Practical Byzantine Fault Tolerance (PBFT) are analyzed to clarify the rationale for our chosen consensus model.

6.3.1 Proof of Work (PoW)

Proof of Work was accounted for more that 90% of the total market capitalization of existing digital cryptocurrencies in 2016 [12]. It is a traditional consensus algorithm where "miners" have to solve a complex cryptographic problem (called a "hash puzzle") to add new blocks to the network. In this method, thousands of mining machines compete to solve the same problem, which consumes a lot of computing power and electricity. The miner who finds the correct solution first through this competition gets to add the block to the network and receives some amount of cryptocurrency (such as ETH) as a reward. A major advantage of this method is that it is very secure and able to maintain the integrity of the blockchain, because if someone wants to cheat the network, they would have to control most of the computing power of the entire network, which is almost impossible [3]. However, its main problem is that it takes a long time to create blocks, it is highly energy-intensive and harmful to the environment.

The PoS Ethereum system provides us with a fast, stable, and environmentally friendly platform for storing VC hashes and encrypted data. PoW would have cost a lot more gas fees, time, and energy to perform the same operations. Moreover, Ethereum 2.0's PoS is now more mature in terms of decentralization and attacker resistance, as bad actors can be suppressed using random validator selection and slashing mechanisms [58].

6.3.2 Proof of Stake (PoS)

The Ethereum network itself has seen a real transition between Proof of Stake and Proof of Work, Ethereum switched from PoW to PoS in the 2022 "Merge" event [58]. Proof of Stake is a new generation consensus method that Ethereum is currently using (after Ethereum 2.0 or "The Merge"). This method does not require any

mining or solving cryptographic puzzles to create blocks. Instead, users who stake (lock) a certain amount of ETH are selected as "validators". For each block, a validator is randomly selected to propose a block, and other validators verify that block. If the validator works correctly, they receive a reward and if they try to cheat, some or all of their staked ETH can be lost (slashing) . This method consumes much less energy, can create blocks faster, and is also much more suitable in terms of scalability. It is environmentally friendly, making blockchain technology more sustainable and future-proof [41].

6.3.3 Ethereum Layer 2 (Optimistic Rollups, zk-Rollups)

To address Ethereum's high transaction fees and limited scalability, these issues, various Layer 2 solutions have been developed that work on top of the main Ethereum network and make transactions more scalable and faster. Among the Layer 2 solutions, Optimistic Rollups (e.g. Optimism, Arbitrum) and zk-Rollups (e.g. zkSync, Scroll) are the most widely used.

- The Optimistic Rollup method assumes that every transaction is valid (i.e., "optimistic assumption") and is directly reflected on the Ethereum mainnet if no one objects to it [51]. However, if someone expresses doubt or challenges, it is possible to prove the error by submitting a fraud proof. This challenge window may have some latency (usually from a few hours to a day), but it greatly reduces the gas fee per transaction and greatly increases throughput.
- On the other hand, zk-Rollup uses Zero-Knowledge Proofs which summarize each batch of transactions with a cryptographic proof and submit it to the Ethereum mainnet [66]. This method has low latency, very strong security, and instant finality, but is technically much more complex and computationally intensive.

However, one important aspect is that all Layer 2 solutions ultimately rely on Ethereum's underlying Layer 1 PoS consensus [51]. That is, no matter what happens in Rollup, the ultimate security and block finality is with the Ethereum mainnet's PoS.

In the our system we designed, hashes of verifiable credentials (VC) and encrypted data are stored on the blockchain. These transactions are generally infrequent and do not rely on real-time finality. As a result, there is no need for very high throughput or ultra-low latency. For this reason, Ethereum's core Layer 1 network and its Proof of Stake consensus are quite efficient and secure for us. Although it is possible to reduce gas fees and further increase scalability by using Rollup, its necessity is limited in our case. Because in the SSI system we are not doing volume-based high-speed transactions. In addition, the final consensus is always done with Ethereum's PoS, which keeps our system robust, decentralized, and tamper-proof.

6.3.4 Practical Byzantine Fault Tolerance (PBFT)

In contrast, Practical Byzantine Fault Tolerance (PBFT) is a consensus-based consensus algorithm that is commonly used in permissioned blockchain networks or

enterprise Ethereum implementations, such as Hyperledger Besu, Quorum, or Pantheon [6]. The validator nodes participating in this consensus are predetermined. Only authorized and known nodes can participate in the consensus. PBFT finalizes blocks through trust and communication between a set number of nodes [1]. This makes it relatively fast, low latency, and less resource-intensive, which is useful for private networks.

However, its main limitations are, low decentralization and central trust model. Since validators are specifically assigned, and consensus depends on the consent of specific parties, it establishes a kind of central control. Using a private network based on PBFT would centralize consensus power in the hands of only certain validators, potentially re-establishing a central trust authority [1]. It is inconsistent with the decentralization philosophy of our system. As a result, citizens or users may lose trust in the Verifiable Credentials stored in a private consensus, as they do not know who is actually conducting the consensus process.

6.4 Other Components

We analyzed some of the other components that we used in our system and why they are best fit to our system. The comparison's are given below:

6.4.1 Elliptic Curve Cryptography vs RSA

Both Elliptic Curve Cryptography (ECC) and RSA are widely used methods in modern cryptography, mainly for public key cryptography. However, there are fundamental differences between the two technologies that determine which method is more suitable for which purpose.

RSA is a very old and has been a cryptographic algorithm used around the world for many years. It basically uses the product of two large prime numbers to generate a public and private key. The private key is generated using the inverse modulo operation. Its security depends on the integer factorization problem, which is very time-consuming to calculate for large numbers. For example, if you use a 2048-bit RSA key, it could take millions of years to break it with current computer technology, this is the basis of its security [57].

On the other hand, ECC is a relatively modern method that is based on the elliptic curve mathematical structure. Its security depends on the complexity of the elliptic curve discrete logarithm problem (ECDLP), which is computationally much harder and more difficult to solve. Because of this, ECC can provide security similar to RSA even with a much smaller key size.

Where RSA requires a 2048-bit key in a secure configuration, ECC can achieve that level of security using only 256-bit keys [17]. As a result, ECC-based systems are much lighter and faster. It reduces processing time, consumes less bandwidth, and is very suitable for small devices like mobile or embedded systems.

Now if we consider the matter in the context of Self-Sovereign Identity (SSI), it can be seen that in SSI each user has a cryptographic identity (such as DID) and with that identity, Verifiable Credential creation, signing, verification, etc. have to be done. If larger keys and signatures were used for all these tasks, like RSA, then the entire system would become slow and would not be able to work effectively on underdeveloped devices. This is why ECC is considered ideal for such decentralized identity systems.
Using ECC:

- Verifiable Credentials take up less space
- Signature verification is faster
- Low bandwidth usage
- And can be effectively used in client apps like MetaMask or mobile wallets

Many modern DID methods (such as did:ethr) and systems (such as Ethereum, SpruceID, Bifold Wallet) in the world already use ECC-based key pairs (especially secp256k1 curves).

Chapter 7

Experimental Evaluation

In this chapter, we implement and analyze various experimental setups on our proposed SSI-based identity verification system. The system is built and tested in four different configurations, where each step of identity verification is compared in terms of time, security, and usability.

7.1 Experiments

7.1.1 Storing VC Manually

In this method, the user provides his/her name, NID number, and Ethereum Public Address manually. The government creates the VC stores the hash on the DLT and passes the VC to the user. After receiving the VC, users could download and store it themselves—on their computer, browser storage (like IndexedDB), or even an encrypted USB drive. When needed, they would upload the VC manually to a verifier. While this method offers full control and keeps data completely offline, it depends heavily on the user's technical comfort. We found it simple but not ideal for frequent use or non-technical users.

7.1.2 Automatic Encrypted Verification using MetaMask

In this model, we tested a more automated system using Ethereum smart contracts. In this method, we encrypted the VC using the user's MetaMask public key and stored it directly on the blockchain. The system could later fetch and decrypt the VC using the user's private key through MetaMask, once the user gave consent [64]. This approach offered strong security and automation while ensuring the user remained in control.

Limitation: The decryption with private key using the 'eth_decrypt' method is prohibited by MetaMask, so alternative key management is required in the future [64].

7.1.3 Storing VC in SpruceKit Wallet

In this setup initially, the user provides their information, National Identity Number (NID), and Ethereum Public Address. This Ethereum address is automatically

collected from the user's MetaMask wallet. The government generates a VC and stores in DLT. This VC is then encoded and generated as a QR code. Scanning the QR automatically stores the vc to the SpruceKit Wallet.
SpruceKit is a mobile-based verifiable credential wallet service, where a unique Wallet ID is generated for each user. The wallet supports modern standards like OpenID4VCI and allows users to share credentials with just a click.

Limitation: VC stored locally encrypted. Not persistent across different devices. We faced credential format issue while storing VC through QR code.

7.1.4 Storing VC in Bifold Wallet

This setup creates a mobile-centric, decentralized, and user-controlled verifiable credential management system. The entire process is similar to SpruceKit, but here the user's VC is stored in the Bifold Wallet app installed on the user's own mobile device rather than in the cloud.

The user first installs a mobile app, where a DID and key pair are generated for them. Later, when the user provides their identity, NID, and Ethereum address to the government, the government verifies that information and issues a Verifiable Credential.

This VC is then sent directly to the user's Bifold Wallet via the DIDComm protocol. This is a peer-to-peer encrypted messaging method that securely delivers VC to the user's mobile wallet. The user can share VC with any verifier by one-click. However, we were unable to match the credential format to this wallet. [63].

The main advantage of this method is that the user completely owns their credentials. It is accessible offline and does not rely on any third party.

Limitation: It only works as a mobile app. This means that users who use a desktop or laptop cannot access this wallet directly.

7.1.5 DLT + Custom Wallet

We Implemented a Custom Wallet that helps user create digital wallet by following the MetaMask like Mnemonic-based hierarchical deterministic key derivation. Using the generated Public key the VC is encrypted and stored in the Ethereum Network via Smart Contract. Later fetched the encrypted VC and decrypts using user's private key. It follows the Elliptic Curve Cryptography (ECC) algorithm using 'eth-crypto' [24] library for encryption and decryption. Keys are controlled by user and credentials are stored securely by encryption.

Limitation: Elliptic Curve Cryptography (ECC) libraries are limited to backend (nodejs) environment.

7.2 Evaluation

Table 7.1 compares the performance of different methods for issuing and verifying verifiable credentials (VCs). The average time for each method was calculated based on the results of 10 tests. The manual method requires the user to manually input their name, date of birth, Ethereum address, and national ID number, resulting in an average issuance time of 27.7 seconds. During verification, the user again has to manually provide the Ethereum address and VC, which requires an average of 10.1 seconds. The main limitations of this method are its complexity and difficulty in scaling, as human intervention is required at each step.

Experiment	**Avg Issuance Time**	**Blockchain Hashing Time**	**Avg VC Verification Time**	**Storage Method (User End)**	**Limitation**
Manually Stored	27.7 sec	4.2 sec	10.1 sec	Manually Saved	Tedious, non-scalable, error-prone
Metamask	19.0 sec	4.5 sec	N/A	DLT	MetaMask can't decrypt anymore (deprecated method)
SpruceKit Wallet	20.7 sec	4.3 sec	N/A	SpruceKit Wallet	
Bifold Wallet	20.7 sec	4.3 sec	N/A	Bifold Wallet	Mobile-only access, no desktop integration
Custom Wallet	17.3 sec	4.5 sec	5.6 sec	DLT	Browser Based ec-ccrypto library depricated

Table 7.1: Experimental Evaluations

The issuance process is somewhat automated using MetaMask, where the user's Ethereum address is automatically collected and the rest of the information is passed through input field. It takes an average of 19.0 seconds to issue, which is faster than the manual method. However, this method requires two blockchain transactions, one to store the hash of the VC and the other to encrypt the VC using the user's MetaMask public address. Unfortunately, the verification process could not be evaluated because MetaMask's decryption method is not currently supported.

The issuance process is almost identical for the Sprucekit wallet and Bifold wallet methods. In both cases, the user's Ethereum address is taken from MetaMask and a QR code is generated after inputting other information. These methods take an average of 20.7 seconds to issue and only one blockchain transaction occurs, which is used to store the hash of the VC. However, the verification process could not be tested in these methods because the format of the generated VC was not acceptable.

In the custom wallet method, the user first creates a wallet, through which his Ethereum address is automatically saved. The issuance process requires the user to input other information and takes an average of 17.3 seconds, which is the fastest of all the other methods. This method performs two blockchain transactions—one to store the hash of the VC and the other to encrypt the VC with the public key of the user's custom wallet. During verification, the user is required to provide their wallet password, which is used to decrypt the private key from local storage. The VC obtained from the DLT is decrypted using this private key, and takes an average of 5.6 seconds. However, the 'eth-crypto' [24] library is not browser compatible. As a result we had decrypt the VC on the nodejs backend.

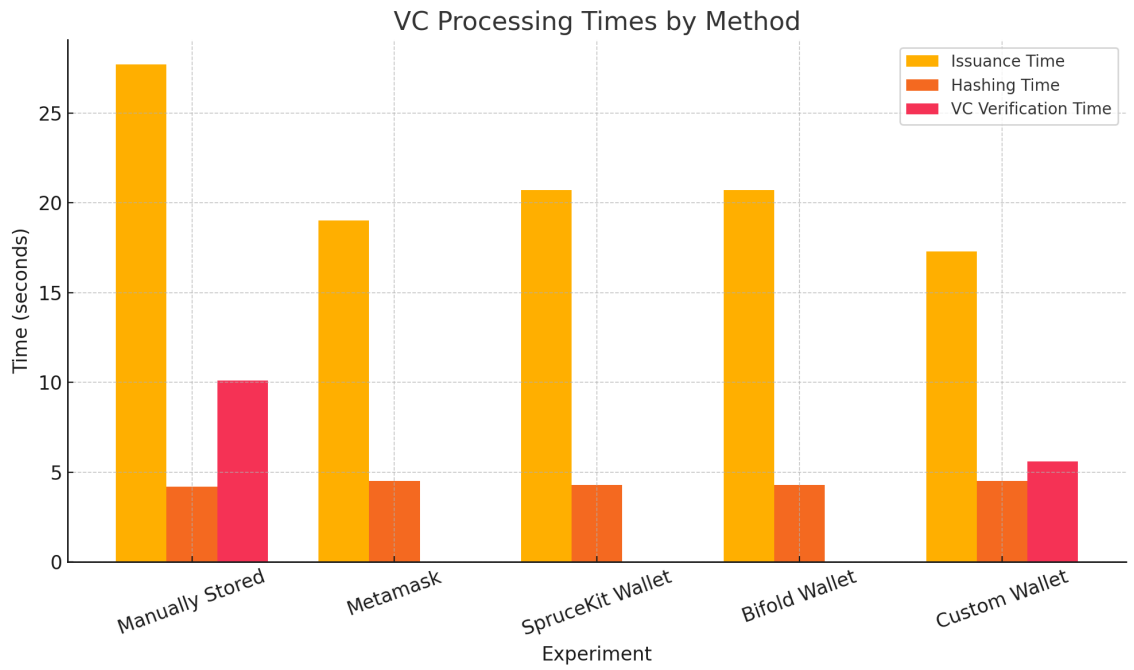

Figure 7.1: Comparison of VC Processing times

The blockchain hashing time is almost the same across all methods, averaging between 4.2 and 4.5 seconds, indicating that there is no significant difference in the time it takes to store data on the blockchain. Manual saves, DLTs, and various wallets have been used as storage methods, each with its own advantages and disadvantages. Overall, the custom wallet method provides the fastest issuance and verification times, but its effectiveness depends on the specific library and the security of the user's wallet. We've shared a visual of the comparsion of VC processing times in Figure 7.1

Chapter 8

Limitation and Future Work

8.1 Dependence on Ethereum Blockchain

Although the proposed SSI-based National ID framework offers a promising approach to decentralized digital identity, it is not without limitations. One major technical concern is the reliance on the Ethereum blockchain. While Ethereum provides a secure and mature platform, it presents challenges in terms of scalability, transaction speed, and gas fees. These issues could become significant barriers when deploying the system at a national level, especially in countries with limited technological infrastructure.

8.2 Key Management and Usability Issues

In addition, secure key management and credential recovery continue to be major usability concerns. Non-technical users may struggle to manage private keys or understand wallet operations, which could result in data loss or access issues. Addressing this gap requires further research into user-friendly key recovery mechanisms and educational tools that reduce the learning curve for everyday users.

8.3 Institutional and Infrastructural Readiness

A broader challenge lies in institutional and infrastructural readiness. Implementing a decentralized identity system at a national scale demands significant government support, technical capacity, and inter-agency coordination. Legacy systems would need to be upgraded or integrated, policies and legal frameworks must be adapted, and secure infrastructure must be maintained. This transformation could incur high costs and logistical complexity, particularly in developing regions.

8.4 Social Adoption and Public Awareness

Moreover, successful adoption depends heavily on social factors. Citizens must be educated on how to manage their digital identities, store their credentials securely, and consent to verifications confidently. This will require comprehensive public awareness campaigns, inclusive onboarding strategies, and potentially new regulatory bodies to oversee training, outreach, and ethical safeguards.

8.5 Future Directions

In future work, we aim to address these challenges by exploring more scalable blockchain platforms, integrating privacy-preserving technologies such as zero-knowledge proofs, and building legal frameworks for public trust. Most importantly, we emphasize the need for a coordinated effort between technology developers, governments, and civil society to ensure that the system is not only technically sound but also equitable, inclusive, and practically implementable.

Chapter 9

Discussion and Conclusion

This thesis explored the design and implementation of a decentralized digital identity framework leveraging Self-Sovereign Identity (SSI) principles and blockchain technology for government-issued National ID (NID) systems. Through detailed architectural planning and experimental prototyping, we demonstrated how verifiable credentials can be securely issued by government authorities, encrypted and stored using decentralized identifiers (DIDs), and selectively disclosed by citizens via digital wallets, entirely under user control. Compared to traditional centralized and federated models, our approach significantly enhances data privacy, system transparency, and user autonomy, while minimizing reliance on third-party identity providers.

The integration of Ethereum-based smart contracts, DID standards, and verifiable credential protocols not only ensures integrity and authenticity but also positions the system for future interoperability across national and sectoral boundaries. By aligning with emerging standards such as W3C VC, OpenID4VCI, and DIDComm, the proposed framework contributes a robust, scalable, and future-proof model for secure digital identity in public-sector use cases.

Ultimately, our work reinforces the viability of government-backed decentralized identity systems as a secure and citizen-centric alternative to conventional identity architectures. This offers a path toward greater trust, accountability, and sovereignty in digital identity ecosystems.

Bibliography

[1] M. Castro and B. Liskov, "Practical byzantine fault tolerance," in *OSDI*, USENIX Association, vol. 99, 1999, pp. 173–186.

[2] K. Cameron, *The laws of identity*, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf, Microsoft Corporation, Whitepaper, 2005.

[3] S. Nakamoto, *Bitcoin: A peer-to-peer electronic cash system*, https://bitcoin.org/bitcoin.pdf, 2008.

[4] Y. Cao and L. Yang, "A survey of identity management technology," in *2010 IEEE International Conference on Information Theory and Information Security*, 2010, pp. 287–293. DOI: 10.1109/ICITIS.2010.5689468.

[5] Z. A. Khattak, S. Sulaiman, and J.-L. A. Manan, "A study on threat model for federated identities in federated identity management system," in *2010 International Symposium on Information Technology*, vol. 2, 2010, pp. 618–623. DOI: 10.1109/ITSIM.2010.5561611.

[6] R. Kotla, L. Alvisi, M. Dahlin, A. Clement, and E. Wong, "Zyzzyva: Speculative byzantine fault tolerance," *ACM Trans. Comput. Syst.*, vol. 27, no. 4, Jan. 2010, ISSN: 0734-2071. DOI: 10.1145/1658357.1658358. [Online]. Available: https://doi.org/10.1145/1658357.1658358.

[7] B. Zwattendorfer, T. Zefferer, and A. Tauber, "The prevalence of saml within the european union," in *8th International Conference on Web Information Systems and Technologies (WEBIST)*, 2012, pp. 571–576.

[8] A. Gelb and J. Clark, "Identification for development: The biometrics revolution," *Center for Global Development Working Paper*, no. 315, 2013.

[9] K. Gibbons, J. O. Raw, and K. Curran, "Security evaluation of the oauth 2.0 framework," *Information Management and Computer Security*, vol. 22, no. 3, pp. 01–23, 2014.

[10] D. Hühnlein, T. Wich, J. Schmölz, and H.-M. Haase, "The evolution of identity management using the example of web-based applications," *it-Information Technology*, vol. 56, no. 3, pp. 134–140, 2014.

[11] E. Ferry, J. O Raw, and K. Curran, "Security evaluation of the oauth 2.0 framework," *Information & Computer Security*, vol. 23, no. 1, pp. 73–101, 2015.

[12] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, ser. CCS '16, Vienna, Austria: Association for Computing Machinery, 2016, pp. 3–16, ISBN: 9781450341394. DOI: 10.1145/2976749.2978341. [Online]. Available: https://doi.org/10.1145/2976749.2978341.

[13] R. Moore, *Etherjs*, https://github.com/ethers-io/ethers.js, 2016.

[14] A. Tobin and D. Reed, "The inevitable rise of self-sovereign identity," *The Sovrin Foundation*, vol. 29, no. 2016, p. 18, 2016.

[15] uPort Project, "Uport: A platform for self-sovereign identity," Consensys, Tech. Rep., 2016. [Online]. Available: https://blockchainlab.com/pdf/uPort_whitepaper_DRAFT20161020.pdf.

[16] U. Der, S. Jähnichen, and J. Sürmeli, "Self-sovereign identity – opportunities and challenges for the digital revolution," *arXiv preprint arXiv:1712.01767*, 2017.

[17] D. Mahto and D. YADAV, "Rsa and ecc: A comparative analysis," *International Journal of Applied Engineering Research*, vol. 12, pp. 9053–9061, Jan. 2017.

[18] P. Dunphy and F. A. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE security & privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[19] A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, "A quantifiable trust model for blockchain-based identity management," in *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)*, Ieee, 2018, pp. 1475–1482.

[20] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, "A survey on essential components of a self-sovereign identity," *Computer Science Review*, vol. 30, pp. 80–86, 2018.

[21] M. Schanzenbach, G. Bramm, and J. Schütte, *Reclaimid: Secure, self-sovereign identities using name systems and attribute-based encryption*, arXiv preprint arXiv:1805.06253, 2018.

[22] Sovrin Foundation, "Sovrin: A protocol and token for self-sovereign identity and decentralized trust," Sovrin Foundation, Tech. Rep., 2018. [Online]. Available: https://sovrin.org/library/sovrin-protocol-and-token-white-paper/.

[23] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *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)*, IEEE, 2018, pp. 1336–1342.

[24] R. Wenzel, *Ethcrypto*, https://github.com/pubkey/eth-crypto, 2018.

[25] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103 059–103 079, 2019. DOI: 10.1109/ACCESS.2019.2931173.

[26] M. Sporny, D. Longley, and D. Chadwick, "Verifiable credentials data model 1.0," *W3C recommendation*, vol. 19, 2019.

[27] Blockcerts Project, *Blockcerts documentation guide*, Accessed: 2025-06-17, 2020. [Online]. Available: https://www.blockcerts.org/guide/.

[28] D. I. Foundation, *Did-jwt-vc*, https://github.com/decentralized-identity/did-jwt-vc, 2020.

[29] V. Gatteschi, F. Lamberti, C. Demartini, C. Pranteda, and V. Santamaria, "Governing principles of self-sovereign identity applied to blockchain-enabled privacy preserving identity management systems," *ResearchGate Preprint*, 2020. [Online]. Available: https://www.researchgate.net/publication/347377303_Governing_Principles_of_Self-Sovereign_Identity_Applied_to_Blockchain_Enabled_Privacy_Preserving_Identity_Management_Systems.

[30] Hyperledger Foundation, *Hyperledger indy documentation*, Accessed: 2025-06-17, 2020. [Online]. Available: https://hyperledger-indy.readthedocs.io/en/latest/.

[31] Jolocom, *Jolocom library documentation*, Accessed: 2025-06-17, 2020. [Online]. Available: https://jolocom-lib.readthedocs.io/en/latest/.

[32] D. Kuperberg, A. Küpper, and M. Hübner, *Decentralized identity: The good, the bad and the ugly*, arXiv preprint arXiv:2006.04048, 2020.

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

[34] D. Reed, M. Sporny, C. Longley, M. Sabadello, and K. Jordan, *Decentralized identifiers (dids) v1.0: Core architecture, data model, and representations*, W3C Working Draft, https://www.w3.org/TR/did-core/, 2020.

[35] C. Toth and B. Anderson-Priddy, *Self-sovereign identity: A position paper*, arXiv preprint arXiv:2003.11781, 2020.

[36] A. Zwitter and J. Hazenberg, "Decentralized network governance: Blockchain technology and the future of regulation," *Frontiers in Blockchain*, vol. 3, p. 12, 2020.

[37] A. Jagers, B. van Wingerde, and W. Witsenburg, *Self-sovereign identity adoption: A domain analysis*, arXiv preprint arXiv:2104.09332, 2021.

[38] N. Naik, P. Jenkins, and C. Perera, "Blockchain-based self-sovereign identity: Current trends and research challenges," *Computer Science Review*, vol. 40, p. 100 424, 2021. DOI: 10.1016/j.cosrev.2021.100424.

[39] D. Pöhn, M. Grabatin, and W. Hommel, "Eid and self-sovereign identity usage: An overview," *Electronics*, vol. 10, no. 22, p. 2811, 2021.

[40] A. Preukschat and D. Reed, *Self-sovereign identity*. Manning Publications, 2021.

[41] F. Saleh, "Blockchain without waste: Proof-of-stake," *The Review of Financial Studies*, vol. 34, no. 3, pp. 1156–1190, 2021. DOI: 10.1093/rfs/hhaa075.

[42] S. Schwalm and I. Alamillo-Domingo, "Self-sovereign-identity & eidas: A contradiction? challenges and chances of eidas 2.0," *Wirtschaftsinformatik*, vol. 58, pp. 247–270, 2021.

[43] R. Soltani, U. T. Nguyen, and A. An, "A survey of self-sovereign identity ecosystem," *Security and Communication Networks*, vol. 2021, no. 1, p. 8 873 429, 2021.

[44] Y. Ding and H. Sato, "Self-sovereign identity as a service: Architecture in practice," in *IEEE 46th Annual Computers, Software, and Applications Conference (SAPSE) Workshops*, 2022.

[45] I. Leung, N. Tapas, G. David, and B. Mihaljevic, *Towards standardizing trust in self-sovereign identity ecosystems*, arXiv preprint arXiv:2206.08937, 2022.

[46] M. Naghmouchi, H. Kaffel, and M. Laurent, *An automatized identity and access management system for iot combining self-sovereign identity and smart contracts*, arXiv preprint arXiv:2201.00231, 2022.

[47] A. Satybaldy, A. Subedi, and M. Nowostawski, "A framework for online document verification using self-sovereign identity technology," *Sensors*, vol. 22, no. 21, p. 8408, 2022.

[48] M. Shuaib, N. H. Hassan, S. Usman, *et al.*, "Land registry framework based on self-sovereign identity (ssi) for environmental sustainability," *Sustainability*, vol. 14, no. 9, p. 5400, 2022.

[49] M. Soleymani, F. Asgari, R. Mahmod, and M. Z. Zamani, *A lightweight self-sovereign identity model for iot networks*, arXiv preprint arXiv:2207.04512, 2022.

[50] TBD - A Block Company, *Web5: Decentralized web platform by tbd*, https://decentralized-id.com/projects/tbd/web5/, Accessed: 2025-06-22, 2022.

[51] L. T. Thibault, T. Sarry, and A. S. Hafid, "Blockchain scaling using rollups: A comprehensive survey," *IEEE Access*, vol. 10, pp. 93 039–93 054, 2022. DOI: 10.1109/ACCESS.2022.3200051.

[52] M. Babel and J. Sedlmeir, "Bringing data minimization to digital wallets at scale with general-purpose zero-knowledge proofs," *arXiv preprint arXiv:2301.00823*, 2023.

[53] D. I. Foundation, *Didcomm messaging specification v2.0*, https://identity.foundation/didcomm-messaging/spec/, DIF Specification, 2023.

[54] O. Foundation, *OpenID for Verifiable Credential Issuance 1.0*, https://openid.net/specs/openid-4-verifiable-credential-issuance-1_0.html, OpenID Specification Draft, 2023.

[55] S. Ghirmai, D. Mebrahtom, M. Aloqaily, M. Guizani, and M. Debbah, "Self-sovereign identity for trust and interoperability in the metaverse," *arXiv preprint arXiv:2303.00422*, 2023.

[56] T. Guggenberger, D. Kühne, V. Schlatt, and N. Urbach, "Designing a cross-organizational identity management system: Utilizing ssi for the certification of retailer attributes," *Electronic Markets*, vol. 33, no. 1, p. 3, 2023.

[57] E. Jintcharadze and M. Abashidze, "Performance and comparative analysis of elliptic curve cryptography and rsa," in *2023 IEEE East-West Design Test Symposium (EWDTS)*, 2023, pp. 1–4. DOI: 10.1109/EWDTS59469.2023.10297088.

[58] E. Kapengut and B. Mizrach, "An event study of the ethereum transition to proof-of-stake," *Commodities*, vol. 2, no. 2, pp. 96–110, 2023, ISSN: 2813-2432. DOI: 10.3390/commodities2020006. [Online]. Available: https://www.mdpi.com/2813-2432/2/2/6.

[59] P. Lillemets, "E-estonia—a digital government in digital transformation," Ph.D. dissertation, Tallinn University of Technology Tallinn, Estonia, 2023.

[60] M. Parni, *On self-sovereign identity: Verifiable credentials and presentations with openid connect*, https://helda.helsinki.fi/server/api/core/bitstreams/94f45ddf-e25b-4627-9deb-614626f56a4b/content, 2023.

[61] A. Satybaldy, M. S. Ferdous, and M. Nowostawski, "A taxonomy of challenges for self-sovereign identity systems," *IEEE Access*, 2023. DOI: 10.1109/ACCESS.2024.3357940.

[62] M. Shuaib, S. Alam, M. S. Alam, and M. S. Nasir, "Self-sovereign identity for healthcare using blockchain," *Materials Today: Proceedings*, vol. 81, pp. 203–207, 2023.

[63] H. Aries, *Bifold wallet github repository*, Accessed: 2025-06-17, 2024.

[64] M. Developers, *Metamask developer documentation*, https://docs.metamask.io/, Accessed: 2025-06-17, 2024.

[65] F. M. Tiham, A. R. Fahim, G. M. Julcarnine, and H. M. Usman, "Decentralized identity verification: A blockchain-based framework for self-sovereign identity (ssi) with issuer trust registry," *BRAC University DSpace*, 2024. DOI: http://hdl.handle.net/10361/25158.

[66] K. M. Gogol, S. Gurgul, F. N. Siddiqui, D. Branes, and C. J. Tessone, "Scaling defi with zk rollups: Design, deployment, and evaluation of a real-time proof-of-concept," *arXiv preprint arXiv:2506.00500*, 2025, Submitted May 31, 2025. DOI: 10.48550/arXiv.2506.00500. [Online]. Available: https://arxiv.org/abs/2506.00500.