UNIVERSITY
INSTITUTE
OF LISBON

Establishing Trust in e-Commerce Review Systems with Decentralized Solutions

João Afonso Ribeiro da Conceição Vilares Pereira

Master in Computer Engineering

Supervisor:
PhD Carlos José Corredoura Serrão, Associate Professor,
Iscte – Instituto Universitário de Lisboa

Supervisor:
PhD João Carlos Amaro Ferreira, Assistant Professor with Aggregation,
Iscte-Instituto Universitário de Lisboa

September, 2025

TECHNOLOGY
AND ARCHITECTURE

Department of Information Science and Technology

Establishing Trust in e-Commerce Review Systems with Decentralized Solutions

João Afonso Ribeiro da Conceição Vilares Pereira

Master in Computer Engineering

Supervisor:
PhD Carlos José Corredoura Serrão, Associate Professor,
Iscte – Instituto Universitário de Lisboa

Supervisor:
PhD João Carlos Amaro Ferreira, Assistant Professor with Aggregation,
Iscte-Instituto Universitário de Lisboa

September, 2025

Acknowledgment

I would like to express my sincere gratitude to my supervisor, Professor Carlos Serrão, for his unwavering support, guidance, and expertise throughout the development of this thesis. His invaluable insights, constructive criticism, and encouragement were instrumental in shaping this research. I also extend my deepest appreciation to my supervisor, Professor João C. Ferreira, for his guidance and contributions.

My thanks also go to the faculty and staff of the Department of Information Science and Technology at Iscte - Instituto Universitário de Lisboa. Their dedication to academic excellence has created a stimulating and inspiring environment for learning and research.

Finally, I am profoundly grateful to my family and friends for their constant encouragement and emotional support. In particular, I would like to thank Rodrigo Santos for his invaluable help with the front-end development, and Catarina Moreira and Afonso Caniço for their thorough review and insightful feedback on the thesis. Their belief in me has been a source of strength and motivation, without which this achievement would not have been possible.

Resumo

Os sistemas de críticas e avaliações em aplicações web de comércio electrónico enfrentam desafios recorrentes, como avaliações fraudulentas, centralização excessiva e falta de controlo do utilizador sobre os seus dados pessoais. Estes problemas comprometem a confiança pública e diminuem a fiabilidade das plataformas nas quais os consumidores confiam para tomar decisões informadas. Esta tese apresenta uma análise crítica e conceptual de como a tecnologia de Identidade Auto-Soberana (SSI) pode ser usada para superar estas limitações. Através da utilização de Identificadores Descentralizados (DIDs) e credenciais verificáveis, propomos um quadro que concede aos utilizadores a total propriedade e controlo da sua identidade e dos dados das suas avaliações. Esta abordagem não só atenua ameaças como ataques e avaliações falsas, mas também estabelece as bases para um sistema de avaliação mais transparente, seguro e fiável. O trabalho demonstra que as soluções descentralizadas podem restaurar a integridade e o poder do utilizador no ecossistema das avaliações online.

PALAVRAS-CHAVE: *Blockchain*, *Credenciais Verificáveis*, *Identificadores Descentralizados*, *Identidade Auto-Soberana*, *Sistema de Reputação*, *Rede de Confiança*

Abstract

Online e-commerce review and rating systems face recurrent challenges including fraudulent reviews, excessive centralization, and a lack of user control over personal data. These issues erode public trust and diminish the reliability of platforms that consumers rely on for informed decision-making. This thesis presents a critical and conceptual analysis of how Self-Sovereign Identity (SSI) technology can be leveraged to overcome these limitations. By utilizing Decentralized Identifiers (DIDs) and verifiable credentials(VCs), we propose a framework that empowers users with full ownership and control of their identity and review data. This approach not only mitigates threats like attacks and fake reviews but also establishes a foundation for a more transparent, secure, and trustworthy review system. The work demonstrates how decentralized solutions can re-establish integrity and user empowerment in the online review ecosystem.

KEYWORDS: *Blockchain*, *Verifiable Credentials*, *Decentralized Identifiers*, *Self-Sovereign Identity*, *Review System*, *Web of Trust*

Contents

Acknowledgment i

Resumo iii

Abstract v

List of Tables xi

List of Figures xiii

List of Acronyms xv

Chapter 1. Introduction 1
1.1. Background and Motivation 1
1.2. Research Questions 2
1.3. Objective 2
1.4. Methodology/Development Process 3
1.5. Thesis Structure 4

Chapter 2. Background 5
2.1. Background Concepts 5
2.1.1. Self-Sovereign Identity 5
2.1.2. Decentralized Identifiers 7
2.1.3. Verifiable Credentials (VCs) 8
2.1.4. Decentralized Ledger Technology 8
2.2. User Authentication Methods for Review Systems 9
2.2.1. Low-Assurance Authentication (No User Account) 9
2.2.2. Mid-Assurance Authentication (Simple User Account) 9
2.2.3. High-Assurance Authentication (Verified and Controlled) 9
2.3. Security and Privacy Considerations 10
2.3.1. Key Management and Compromise 10
2.3.2. Vulnerabilities in DID Methods and Infrastructure 10
2.3.3. Verifiable Credential Misuse and Abuse 11
2.3.4. Privacy Erosion and Correlation Risks 11
2.3.5. Social Engineering, Phishing, and User Error 12
2.3.6. Regulatory, Legal, and Interoperability Challenges 12
2.4. Conclusion 13

Chapter 3. Literature Review 15
3.1. Systematic Literature Review Methodology 15
3.1.1. Databases 15
3.1.2. Inclusion Criteria 16
3.1.3. Filters 17
3.1.4. Exclusion Criteria 17
3.1.5. Conclusion 18
3.2. Literature Review Analysis 18
3.2.1. SSI 18
3.2.2. SSI on Review Systems 20
3.2.3. Review Systems 21
3.2.4. Review Conclusion 22
3.3. Conclusion 26

Chapter 4. Review System Design 27
4.1. Review Systems 27
4.2. System Stakeholders and Roles 28
4.3. Non-Functional Requirements 28
4.4. Functional Requirements 28
4.4.1. Issuer Actions 29
4.4.2. User/Holder Actions 30
4.4.3. Verifier Actions 32
4.5. Solution Use Cases 34
4.6. System Architecture 35
4.7. System Processes 37
4.7.1. Issuer issues Credential to User 37
4.7.2. Credential Presentation and Verification 39
4.7.3. Concert Attendance Verification and Review Process Example 40
4.7.4. Conclusion 41

Chapter 5. System Prototype Implementation 43
5.1. Technology Stack and Tools 43
Central to Decentralized Identity: Privado ID 43
Blockchain Interaction and Development Tools: Alchemy 44
User Interface: HTML and JavaScript 44
Backend Logic and Data Handling: Node.js with Local JSON Files 44
Secure Localhost Exposure: ngrok 45
5.2. Authentication 46
5.3. Prototype Prerequisites 48
5.4. Credential Verification Flow for Service Interaction 49
5.4.1. Verifier Actions 49

5.4.2. User Actions 50
5.5. Conclusion 52

Chapter 6. A Technical Comparison: The SSI-Based Review System Vs Traditional Review System 55
6.1. Understanding the Two Review Systems 55
6.2. Core Principles and Use Cases 55
6.2.1. Control and Governance 56
6.2.2. Target Audience 56
6.2.3. Business Strategy 57
6.3. Use Cases and Limitations 57
6.4. Login Systems and User Identity 57
6.5. Security and Fraud Detection 58
6.6. Portability 58
6.7. Interoperability 59
6.8. Usability 59
6.9. Scalability 60
6.10. Conclusion 60

Chapter 7. Conclusion and Future Work 63
7.1. Conclusion 63
7.2. Future Work 63

Bibliography 65

List of Tables

3.1 Repository Queries 16
3.2 Repository Data 17
3.3 Comprehensive Summary of Analyzed Literature 23
3.3 Comprehensive Summary of Analyzed Literature (continued) 24
3.3 Comprehensive Summary of Analyzed Literature (continued) 25
3.3 Comprehensive Summary of Analyzed Literature (continued) 26

6.1 Comparison of E-commerce Review Systems 61
6.1 Comparison of E-commerce Review Systems (continued) 62

List of Figures

1.1 Applied DSR Methodology Process Model 3

2.1 Roles in the Self-Sovereign Identity Framework: Issuer, Holder, and Verifier [11] 6
2.2 Structure of a Decentralized Identifier (DID) [3] 7

4.1 Flowchart depicting issuer actions. 30
4.2 Flowchart depicting user actions. 32
4.3 Flowchart depicting verifier actions. 33
4.4 Use Case Diagram of the Credential Authentication System 34
4.5 System Architecture Design 36
4.6 Credential Issuance Sequence Diagram 38
4.7 Credentials issuance Sequence Diagram 39

5.1 Verification Flow using ngrok for Local Development 45
5.2 Homepage screen 47
5.3 Verifying screen 48
5.4 Credential Authentication Query Example 50
5.5 Unverified Form (Before Authentication) 52
5.6 Verified Form (After Successful Authentication) 52

List of Acronyms

BIM	Building Information Modeling
DIDs	Decentralized Identifiers
DLT	Decentralized Ledger Technology
DSMAC	Decentralized Self-Management of Access Control
DSRM	Design Science Research Methodology
DT-SSIM	Digital Twin Self-Sovereign Identity Management
EBSI	European Blockchain Services Infrastructure
ESSIF	European Self-Sovereign Identity framework
GDPR	General Data Protection Regulation
HIoMT	Healthcare Internet of Medical Things
HTML	Hypertext Markup Language
PpCT	Privacy-Preserving Contact Tracing
SLR	Systematic Literature Review
SSI	Self-Sovereign Identity
VCs	Verifiable Credentials
ZKP	Zero-Knowledge Proofs
RBAC	role-based access control
RDF	Resource Description Framework
SHACL	Shapes Constraint Language
SEER	Secure and Efficient sErvice Review System

CHAPTER 1

Introduction

In the digital era, online e-commerce review systems are fundamental, impacting both consumer choices and market dynamics. While these systems are intended to promote transparency and quality assessment, they often suffer from problems like unfair trading and fraudulent behavior, hindering their reliability [1]. To address these challenges, blockchain technology and Self-Sovereign Identity (SSI) offer innovative solutions that enhance security, authenticity, and user control over personal data [2].

This thesis explores the integration of blockchain technology with SSI principles to develop an e-commerce review system that leverages Decentralized Identifiers (DIDs) [3] and Verifiable Credentials (VCs) [4]. Blockchain, as a distributed ledger, ensures immutability and transparency, mitigating the risks of data manipulation and fraudulent activities. Meanwhile, SSI empowers users with complete ownership and control over their identities, reducing reliance on centralized authorities. By utilizing DIDs [3], individuals and entities can establish cryptographically verifiable identities, while VCs [4] allow for the issuance and verification of trusted attestations without exposing unnecessary personal information.

The proposed system aims to provide a trust-enhancing framework for online reviews, ensuring authenticity and verifiability while maintaining user privacy. This introduction outlines the core concepts, significance, and potential impact of integrating blockchain and SSI into review systems [5], setting the stage for a comprehensive analysis of its implementation, benefits, and challenges.

1.1. Background and Motivation

The rise of e-commerce and digital services has led to an increasing reliance on online review systems as a critical factor in consumer decision-making. Online reviews influence purchasing behavior, brand reputation, and market trends [6]. Platforms such as Amazon, Yelp, and TripAdvisor rely heavily on user-generated reviews to provide insights into products and services. However, despite their significance, these systems are often plagued by critical challenges that undermine their effectiveness and trustworthiness [6].

One of the primary concerns in current online review systems is the prevalence of fake reviews. Malicious actors, including businesses and competitors, can manipulate ratings by generating fraudulent positive or negative reviews. This phenomenon erodes consumer trust and distorts market competition [1]. Additionally, centralized control over these platforms grants substantial power to a few entities, raising concerns about bias, censorship, and the potential for data manipulation. Users also face privacy issues, as their

personal information and review histories are stored on centralized servers, making them vulnerable to data breaches and misuse [7]. Blockchain technology and Self-Sovereign Identity (SSI) present promising solutions to these challenges [5]. Blockchain, as a decentralized and immutable ledger, ensures transparency and accountability by making review data tamper-proof. SSI principles empower users by giving them full control over their digital identities, reducing the need for intermediaries and enhancing privacy protection. Through Decentralized Identifiers (DIDs) [3] and Verifiable Credentials (VCs) [4], individuals can establish verifiable, cryptographically secured identities, which contribute to the credibility and authenticity of online reviews.

The motivation behind this research stems from the pressing need to restore trust in online review systems while preserving user autonomy and data security. Addressing the flaws of traditional review mechanisms requires a paradigm shift towards decentralized and user-controlled identity frameworks. By integrating blockchain and SSI, a robust and transparent review system can be designed that mitigates fraud, enhances credibility, and fosters a more equitable digital marketplace [8]. The integration of DIDs and VCs ensures that only verified users can submit reviews, reducing the influence of bots and fraudulent actors. By eliminating reliance on central authorities, users can manage their own identities and interactions without fearing censorship or exploitation [2]. SSI enables selective disclosure of credentials, allowing users to prove their authenticity without exposing unnecessary personal data. A more reliable review system fosters fair competition, benefiting both consumers and businesses by providing accurate and verifiable information [1]. By addressing these challenges, this research aims to develop a trust-enhancing framework for online reviews that leverages blockchain and SSI principles.

1.2. Research Questions

This chapter outlines the core research question guiding this thesis. The goal is to address the trust and security issues within centralized review systems by exploring decentralized technology, investigating how Decentralized Identifiers (DIDs) and verifiable credentials can be applied to create a more transparent and secure environment for online reviews, ultimately enhancing user trust and data privacy.

The research question that will guide this work is the following: "How can blockchain technology and Self-Sovereign Identity be integrated, to develop a review system for e-commerce that enhances authenticity and reliability?"

1.3. Objective

The primary objective of this work is to research, design and develop an online review system that leverages blockchain technology and Self-Sovereign Identity (SSI) to enhance trust, security, and user control. This research aims to establish a framework that ensures review authenticity and verifiability while maintaining user privacy. It seeks to analyze the feasibility and effectiveness of integrating Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs) within online review platforms. Additionally, this study intends to

evaluate the potential challenges and limitations associated with implementing a review systems that leverages blockchain-based decentralized technology and propose solutions to mitigate these obstacles. Ultimately, this research aspires to contribute to the advancement of transparent, fraud-resistant, and privacy-preserving online review mechanisms that can reshape digital trust and reputation management.

1.4. Methodology/Development Process

The research methodology applied in this study follows Design Science Research Methodology, which focuses on creating and evaluating artifacts to solve real-world problems [9]. The process is flexible and iterative, starting with identifying the research problem and motivating the need for a solution, followed by defining the solution objectives, designing and developing the artifact, demonstrating and evaluating its effectiveness, and communicating the findings. This research uses a Problem-centered initiation entry point, where the artifact development and evaluation evolve through iterative learning and feedback, as illustrated in Figure 1.1

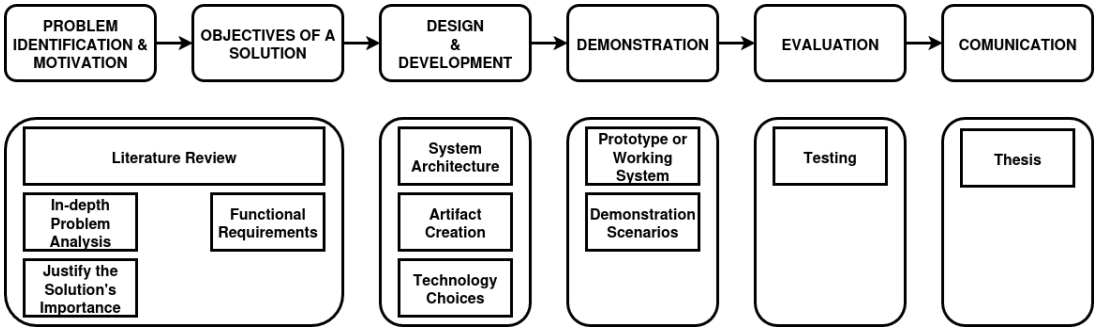


FIGURE 1.1. Applied DSR Methodology Process Model

(1) **Problem Identification and Motivation**: This phase involves identifying a research problem and motivating the need for a solution. A literature review helps to identify gaps to inform solution objectives. In this research, the problem is that online review systems are plagued by issues such as fake reviews, centralized control, and a lack of privacy. The motivation stems from the pressing need to restore trust in these systems.

(2) **Define the Objectives for a Solution**: Objectives for the proposed solution are defined, outlining the artifact's design, resources, success criteria, and technological constraints. For this study, the primary objective is to develop a E-Commerce review system that Self-Sovereign Identity (SSI) to enhance trust, security, and user control. The solution must ensure review authenticity, preserve user privacy, and maintain accountability without centralized gatekeepers.

(3) **Design and Development**: The artifact is created, with its functionality and implementation detailed based on theoretical foundations. This stage includes defining the system architecture, artifact creation, and making technology choices. A decentralized system architecture is proposed using Decentralized

Identifiers (DIDs) and Verifiable Credentials (VCs). The Review System is created, detailing its functionality and implementation.

(4) **Demonstration**: The artifact's functionality is demonstrated to validate its problem-solving effectiveness, and expert feedback on its utility is gathered. The system is applied in review-based scenarios such as restaurants or travel booking to validate its effectiveness.

(5) **Evaluation**: System performance is assessed via a validation consisting of a Detailed Technical Comparison between the proposed decentralized review system and traditional centralized systems. This comparison utilizes key criteria (including usability, security, scalability, portability, and interoperability) to extract conclusions on the developed artifact. The lack of end-user opinion is acknowledged as a limitation, which is deferred to future work.

(6) **Communication**: The final phase involved documenting and sharing the research findings and the artifact's utility. The results were disseminated through this thesis, with the intention of further future publications. The communication stage culminates in outputs such as a Thesis.

1.5. Thesis Structure

This thesis is structured into six chapters. Chapter 1 introduces the research, outlining the background and motivation for the study, defining the research questions, and detailing the methodology used. Chapter 3, the Literature Review, provides a comprehensive overview of foundational concepts such as Self-Sovereign Identity (SSI), Decentralized Identifiers (DIDs), and Verifiable Credentials (VCs). Chapter 4 focuses on the design of the proposed review system, including its architecture, functional requirements, and the roles of key stakeholders. The practical implementation of the system prototype is described in Chapter 5, which covers the technology stack and the credential verification process. Chapter 6 discusses the operating principles of the credential-based review system, comparing it to traditional centralized models and addressing security and privacy considerations. Finally, Chapter 7 summarizes the conclusions of the research and suggests directions for future work.

CHAPTER 2

Background

This chapter establishes the theoretical and technical foundation necessary to understand the decentralized solutions proposed in this thesis. It transitions from the general problem of trust in e-commerce identified in Chapter 1 to a detailed examination of the core technologies—specifically Self-Sovereign Identity (SSI) and Blockchain—that enable a shift away from centralized control. By defining key components such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), this chapter provides the technical context required to appreciate how user autonomy and data integrity can be restored in digital review ecosystems.

2.1. Background Concepts

This section establishes the foundational understanding necessary for the subsequent discussion of the proposed review system. It provides an overview of the core concepts that are central to the system's architecture and functionality. Specifically, it explains Self-Sovereign Identity (SSI) and its key components: Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). Additionally, it introduces Decentralized Ledger Technology (DLT), with a focus on blockchain, and its role in enabling secure and transparent data management. By elucidating these fundamental technologies, this section sets the stage for a detailed exploration of how they are integrated to address the challenges in current online E-commerce review systems.

2.1.1. Self-Sovereign Identity

Self-Sovereign Identity (SSI) is a decentralized identity model that enables individuals to have full control over their digital identities without relying on centralized authorities [10]. SSI leverages two core components: Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs).

DIDs are unique identifiers that are not controlled by any central authority, enabling individuals or entities to manage their own identities securely [8]. VCs, as will be detailed in section 2.1.3, are digital statements that validate specific claims about a subject [2]. By utilizing these technologies, the SSI framework ensures that users are the sole owners of their data and identity, reducing reliance on third-party gatekeepers.These roles and their interactions are illustrated in Figure 2.1.

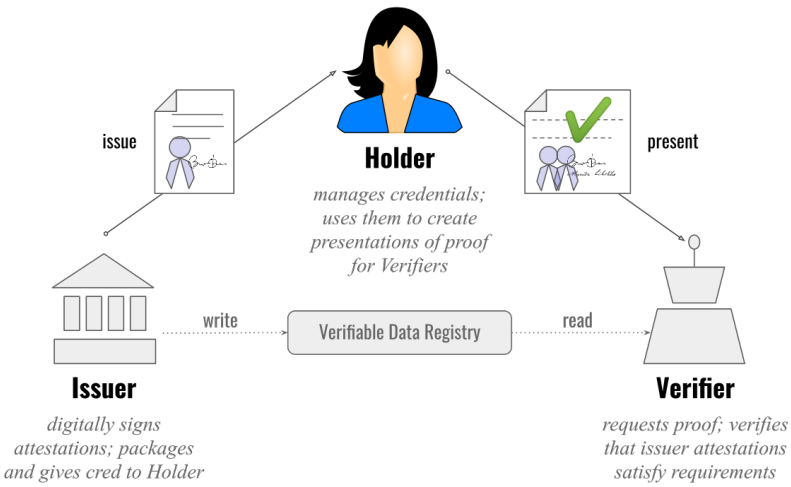


FIGURE 2.1. Roles in the Self-Sovereign Identity Framework: Issuer, Holder, and Verifier [11]

Cryptographic security in SSI is achieved using public-key infrastructure. A credential is a digitally signed data object that asserts a claim about a subject (the Holder). It is composed of three main parts:

- Subject: The entity the claim is about (e.g., a person, a device).
- Claim(s): The specific assertions being made (e.g., name, date of birth, a university degree).
- Issuer: The entity that issues and cryptographically signs the credential (e.g., a university, a government, a company).

The process of verification is as follows: The Issuer signs the credential with their unique private key. When a Verifier receives this credential, they use the Issuer's public key to check the signature. This public key is easily retrieved via the Issuer's Decentralized Identifier (DID), which acts as a global, verifiable address for the Issuer's public key. The cryptographic link between the DID and the public key ensures that the Verifier can confirm the credential's authenticity and that it truly belongs to the Issuer.

Here are some examples to illustrate how this works:

- University Degree: A university (the Issuer) issues a digital degree (the Credential) to a student (the Holder). The university signs it with its private key. An employer (the Verifier) can use the university's DID to get its public key and verify the signature, confirming the degree is authentic and came from that specific university.
- Proof of Age: A government (the Issuer) provides a digital credential to an individual (the Holder) that only states they are over 18. A business (the Verifier) can verify the government's signature using its public key without seeing the individual's birthdate, protecting their privacy.

Additionally, DIDs are often anchored on distributed ledgers or blockchains, which provide a tamper-evident trust layer. Techniques like selective disclosure and zero-knowledge proofs further enhance privacy by allowing Holders to reveal only the minimum required information [8].

2.1.2. Decentralized Identifiers

Decentralized Identifiers (DIDs) [3] are globally unique identifiers designed to enable verifiable, self-sovereign digital identities. Each DID represents a subject—such as a person, organization, or device—and is completely under the control of its designated owner, without reliance on centralized registries or authorities. This means that unlike traditional identifiers like usernames or email addresses, which are managed by companies or governments, the subject of a DID is the sole party who can manage it and prove ownership through cryptographic keys.

Unlike traditional identifiers that depend on external entities like certificate authorities or identity providers, DIDs are inherently decentralized. They are structured as Uniform Resource Identifiers (URIs), consisting of three components: the 'did' scheme, a method name, and a method-specific identifier. For example, in the DID 'did:example:123456789abcdefghi', the term 'did' designates the URI scheme, 'example' defines the DID method, and '123456789abcdefghi' serves as the unique identifier for the subject.

Figure 2.2 illustrates the typical structure of a DID and highlights its three essential components.



FIGURE 2.2. Structure of a Decentralized Identifier (DID) [3]

When a DID is resolved by the underlying decentralized network, it returns a corresponding DID Document—a JSON-based metadata file containing cryptographic material (e.g., public keys), service endpoints, and other relevant attributes. This process is governed by a DID method, which is a set of rules defining how the DID and its document are created, updated, and resolved on a specific network. The resolution process itself is not executed by a central server, but rather by a DID Resolver, which is a piece of software that understands the rules of the DID method. This allows the resolver to find and retrieve the DID Document from its designated network, such as a blockchain or a distributed file system, ensuring the process is decentralized and transparent.

The flexibility and extensibility of DID methods allow different implementations to interoperate across diverse platforms and ecosystems, making DIDs a foundational component in decentralized identity systems.

2.1.3. Verifiable Credentials (VCs)

Verifiable Credentials (VCs) [4] are a secure, privacy-respecting, and cryptographically verifiable method for expressing claims about a subject in digital environments. VCs enable an entity, referred to as the Issuer, to assert statements about another entity, the Holder, such as identity attributes, qualifications, or affiliations. These credentials can then be presented to a Verifier, who validates their authenticity and integrity without needing to contact the Issuer directly.

A typical VC consists of three core components:

- Credential Subject: The entity to whom the claims apply.
- Claims: Statements made by the Issuer about the subject (e.g., name, age, membership).
- Proof: Cryptographic evidence, usually a digital signature, that ensures the credential's authenticity.

Privacy and data minimization are central features of the VC framework. Techniques such as selective disclosure and zero-knowledge proofs allow the Holder to present only the necessary parts of a credential during verification. For instance, instead of revealing a full birthdate, a Holder may simply prove they are over 18.

As described in Section 2.1.1, the interaction among the Issuer, Holder, and Verifier forms the foundation of trust in the SSI framework. VCs serve as the tangible medium through which claims are exchanged and validated within this ecosystem, enabling a scalable and user-centric approach to identity verification.

2.1.4. Decentralized Ledger Technology

Decentralized Ledger Technology (DLT) is a distributed architecture that enables secure, transparent data management without relying on a central authority. While often used interchangeably with the term "blockchain," it is important to distinguish that DLT represents the broad category of shared ledgers, whereas blockchain is a specific implementation that organizes data into a linear, chronological chain of cryptographically linked blocks. While all blockchains are DLTs, other forms of DLT, such as Directed Acyclic Graphs (DAGs) or Hashgraphs, do not utilize a chain-based structure.

By utilizing a peer-to-peer network and consensus mechanisms to ensure data integrity, DLT provides a reliable foundation for decentralized applications. A primary use of this technology is in Self-Sovereign Identity (SSI), where an immutable and verifiable ledger replaces traditional registration authorities. This shift allows credentials to be authenticated based on the issuing entity's digital signature rather than through direct data verification, significantly enhancing privacy and reducing reliance on intermediaries [10].

Because the ledger is decentralized, a verifier no longer needs to contact a central authority to confirm a credential's authenticity. Instead, they can cryptographically verify that the data was issued and signed by a public key immutably linked to the issuer's identity on the ledger. This process is faster, more private, and removes the need for a third party to act as a trusted middleman. Furthermore, DLT networks support SSI by providing a censorship-resistant infrastructure for identity management. Unlike traditional databases, which often lack neutrality and are vulnerable to manipulation or privacy breaches [12], DLT offers a transparent and secure alternative that ensures users maintain full control over their own digital credentials.

2.2. User Authentication Methods for Review Systems

Choosing an user authentication method for a review system is a crucial decision that balances security, user anonymity, and control. Here are three common approaches to consider, each using SSI for its underlying service but with different levels of implementation and verification.

2.2.1. Low-Assurance Authentication (No User Account)

In this model, users are not required to create a formal account or verify their identity to leave a review. This approach offers the highest degree of anonymity for reviewers, which can be beneficial for encouraging participation and simplifying the process. It also requires minimal development effort. However, because a reviewer's identity is not linked to a persistent credential, they cannot update or delete a review after it has been made. This method is highly susceptible to spam and fraudulent reviews from bots, as the lack of a verified identity makes it easy for a single entity to submit multiple reviews.

2.2.2. Mid-Assurance Authentication (Simple User Account)

This method involves a simple mail/password login, leveraging SSI in the backend for service without external authentication providers. The primary advantage here is that users can manage their reviews—updating or deleting them—since the reviews are tied to a specific account. This provides a level of accountability that helps to reduce bot spam compared to the low-assurance system. A key consideration, however, is that a user would need to re-authenticate their credentials to modify or delete a review, which could be an inconvenience. While a step up in security, this method is still relatively easy for malicious actors to exploit for spamming, and it offers less anonymity than the first option.

2.2.3. High-Assurance Authentication (Verified and Controlled)

This advanced approach uses modern decentralized identity technologies, offering a higher degree of control and trust. As the provided document notes, traditional systems often struggle with fraud, excessive centralization, and a lack of user control over their data, all of which a decentralized solution can mitigate. This method uses technologies such as Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). These tools

empower users to control their digital identities and data, allowing them to prove their identity and legitimacy without revealing unnecessary personal information. This verifiable process ensures that only legitimate users can submit reviews, which helps to reduce the influence of bots and fraudulent accounts. The result is a system with a high level of control for the site owner, while also giving the user more privacy and data control. While the system can be designed to be fraud-resistant and to mitigate issues like Sybil attacks, it is more complex to implement and reduces user anonymity, as a verified identity is required to post a review.

2.3. Security and Privacy Considerations

Self-Sovereign Identity (SSI) systems, while offering enhanced security and privacy, are not immune to potential risks and threats. A comprehensive understanding of these vulnerabilities is crucial for designing robust and resilient SSI implementations.

2.3.1. Key Management and Compromise

The foundation of SSI security lies in cryptographic keys. However, the compromise or loss of private keys poses a significant threat. If a private key associated with a Decentralized Identifier (DID) is stolen, an attacker could impersonate the DID controller, sign malicious transactions, or tamper with DID documents. This can lead to unauthorized actions, fraudulent credential issuance, or denial of legitimate actions.

While SSI supports verification method rotation and revocation as reactive measures, their effectiveness relies on timely detection of a compromise and prompt action by the DID controller. If a compromise goes unnoticed for a period, significant damage can occur. Therefore, proactive key management is essential, including:

- Secure storage mechanisms.
- Multi-factor authentication (MFA)for key access.
- Robust backup and recovery mechanisms.

The secure storage and management of private keys, particularly for individuals, remains a critical challenge, with risks stemming from insecure digital wallets, malware, and phishing attacks targeting key material. DID recovery mechanisms, often involving a combination of rotation and revocation, are critical, but their effectiveness depends on pre-configured recovery methods and the timeliness of the controller's response to a compromise.

2.3.2. Vulnerabilities in DID Methods and Infrastructure

The security of an SSI system is inherently linked to its underlying DID method and the broader infrastructure components.

2.3.2.1. *DID Method Vulnerabilities* A poorly designed or implemented DID method can introduce vulnerabilities. For example, a method that does not adequately ensure the integrity of DID document updates, or one that is susceptible to replay attacks, could be exploited. Furthermore, reliance on specific verifiable data registries (e.g., blockchains) introduces dependencies on the security, liveness, and immutability of those registries.

Any centralization points within a DID method, even if seemingly minor, could become targets for attack.

2.3.2.2. *Attack Vectors on Infrastructure Components* SSI relies on various infrastructure components, including DID resolvers, verifiable data registries, and credential repositories. These components, while often decentralized, can still be targets for attacks.

- **Denial-of-Service (DoS) and Resource Exhaustion Attacks:** An attacker could flood DID resolvers with requests or attempt to overload verifiable data registries, hindering legitimate operations. While proof-of-work or rate-limiting can mitigate some of these, a determined attacker with sufficient resources could still impact system performance and availability. Pollution of public credential registries with spam or garbage data could also lead to resource exhaustion for verifiers attempting to process and filter information.
- **Exploits and Data Manipulation:** Vulnerabilities in the software implementations of these components could lead to data manipulation, unauthorized access, or service outages, undermining the reliability and integrity of the SSI ecosystem.

2.3.3. Verifiable Credential Misuse and Abuse

While Verifiable Credentials (VCs) enhance data minimization and control, they are still susceptible to misuse and abuse:

- **Credential Over-Issuance:** A malicious issuer could flood the system with invalid or misleading credentials, diminishing the trustworthiness of legitimate credentials. Similarly, a malicious or compromised issuer could issue fraudulent credentials, potentially leading to identity spoofing or unauthorized access to services. Although trust frameworks and reputation systems can help identify and mitigate such risks, the decentralized nature means a single point of failure might not be evident, and the propagation of untrustworthy credentials could be challenging to contain.
- **Credential Forgery/Tampering:** Although cryptographic signatures aim to prevent this, vulnerabilities in signature schemes or improper implementation could lead to forged or tampered credentials.
- **Replay Attacks:** If not properly protected (e.g., through nonces or timestamps), a legitimate VC proof could be replayed in a different context or at a later time, leading to unauthorized access or actions.

2.3.4. Privacy Erosion and Correlation Risks

While SSI aims for privacy-preserving interactions, the potential for correlation still exists:

- **Cross-Context Correlation:** If pairwise DIDs are not consistently used, or if ancillary data (e.g., IP addresses, browser fingerprints) is collected across different interactions, a sophisticated adversary could link various pseudonymous identities to a single individual.

- **Metadata Exposure:** The public nature of some verifiable data registries could expose metadata that, while not directly personally identifiable, could contribute to deanonymization when combined with other data.
- **Misconfigurations and Over-sharing:** Misconfigurations or improper usage of SSI systems can still lead to privacy leaks. For instance, if users consistently use the same pairwise DID for unrelated interactions or if attributes are disclosed in a way that allows for re-identification, the benefits of privacy-preserving features can be negated. Poorly designed user interfaces or applications that encourage over-sharing of information could also inadvertently compromise user privacy.

2.3.5. Social Engineering, Phishing, and User Error

Even with strong cryptographic foundations, SSI systems are susceptible to human vulnerabilities:

- **Social Engineering and Phishing Attacks:** Malicious actors may trick users into signing transactions they don't intend, disclosing sensitive information, or granting unauthorized access to their DIDs or credentials. The decentralized nature of SSI means there's no central authority to warn users about such scams, placing a greater burden on individual users to exercise caution and develop a critical understanding of the interactions they engage in.
- **Usability and User Error:** The complexity of managing cryptographic keys and understanding SSI concepts can lead to user errors. Users might lose their keys, fall victim to phishing attacks, or inadvertently approve malicious operations if user interfaces are not intuitive and secure. The burden of security often shifts to the individual, requiring a higher level of digital literacy and responsibility.

2.3.6. Regulatory, Legal, and Interoperability Challenges

The nascent nature of SSI systems introduces broader challenges:

- **Lack of Legal Clarity and Regulatory Compliance:** Legal and regulatory frameworks are still evolving. This can lead to uncertainties regarding liability, data protection responsibilities, and the legal enforceability of cryptographic proofs in different jurisdictions. Non-compliance with regulations like GDPR could result in significant penalties and loss of trust. The decentralized and global nature of SSI particularly presents challenges regarding regulatory and legal compliance across different jurisdictions with varying laws concerning data privacy, digital signatures, and identity management.
- **Interoperability Challenges:** While standards like DIDs and VCs promote interoperability, the fragmented ecosystem of different DID methods, credential formats, and trust frameworks can create silos. This can hinder seamless interactions between different SSI implementations and potentially introduce vulnerabilities at the integration points.

Addressing these risks requires a multi-faceted approach, combining robust cryptographic engineering, careful DID method design, adherence to privacy-by-design principles, user education, and ongoing vigilance against emerging threats.

2.4. Conclusion

In summary, this chapter has detailed the foundational pillars of decentralized identity and the cryptographic mechanisms that underpin the proposed system. We have explored the "trust triangle" of Issuers, Holders, and Verifiers, and analyzed various authentication methods ranging from low to high assurance. Furthermore, the discussion of security and privacy risks—such as key management and regulatory challenges—highlights the complexities of implementing these technologies in a real-world environment. These technical foundations provide the necessary lens through which the existing research and industry trends will be evaluated in the following chapter.

CHAPTER 3

Literature Review

Building upon the technical foundations laid in Chapter 2, this chapter provides a systematic and critical evaluation of the current state of research regarding trust, reputation, and decentralized identity. The objective is to identify how academic and industry efforts have addressed the limitations of traditional, centralized review systems and to pinpoint remaining gaps in the literature. This review is structured in two parts: first, a detailed explanation of the systematic methodology used to select and filter relevant scholarly works; and second, an analysis of the findings across various domains, including healthcare, finance, and e-commerce.

3.1. Systematic Literature Review Methodology

A literature review was conducted to understand the current state of the art in the chosen research area. This review is presented in two parts. Firstly, the methodology used to select relevant papers is defined. This involved crafting specific search queries for selected databases, defining inclusion and exclusion criteria to determine which articles would be included or removed, and establishing a series of sequential filters to structure the literature review process. Secondly, the review presents conclusions drawn from the final set of papers. It also includes an in-depth analysis of key findings and trends identified across the selected articles.

3.1.1. Databases

The selection of databases and the formulation of the corresponding queries Table 3.1 were guided by the principles of efficiency and relevance. The chosen repositories were selected for their extensive collections of academic articles and their ability to automatically enforce inclusion criteria, thus streamlining and optimizing the search process.

The databases used in this research include:

- Scopus: A comprehensive database for peer-reviewed literature, including articles, books, and conference proceedings.
- ACM Digital Library: A dedicated repository for computing and information technology research.
- IEEE Xplore Digital Library: A key resource for engineering and computer science papers.
- Web of Science: Valuable for its citation indexing, which helps identify influential articles.

- B-On: The Portuguese national library of online scientific knowledge, providing access to a wide range of academic resources.

TABLE 3.1. Repository Queries

Repository	**Query**
Scopus	`(TITLE-ABS-KEY("Blockchain") AND TITLE-ABS-KEY("Verifiable Credentials" OR "decentralized identifiers") AND TITLE-ABS-KEY("Self-sovereign identity")) OR (TITLE-ABS-KEY("review system" OR "web of trust") AND TITLE-ABS-KEY("customer feedback" OR "user feedback") AND NOT TITLE-ABS-KEY("AI" OR "Machine Learning")) AND (LIMIT-TO(SUBJAREA, "COMP")) AND (LIMIT-TO(DOCTYPE, "ar")) AND (LIMIT-TO(LANGUAGE, "English"))`
ACM Digital Library	`([Abstract: blockchain] AND ([Abstract: "verifiable credentials"] OR [Abstract: "decentralized identifiers"]) AND [Abstract: "self-sovereign identity"]) OR (([Abstract: "review system"] OR [Abstract: "web of trust"]) AND ([Abstract: "customer feedback"] OR [Abstract: "user feedback"]) AND NOT ([Abstract: "ai"] OR [Abstract: "machine learning"]))`
IEEE Xplore Digital Library	`(("Abstract":"Blockchain") AND ("Abstract":"Verifiable Credentials" OR "Abstract":"decentralized identifiers") AND ("Abstract":"Self-sovereign identity")) OR (("Abstract":"review system" OR "Abstract":"web of trust") AND ("Abstract":"customer feedback" OR "Abstract":"User feedback") AND NOT ("Abstract":"AI" OR "Abstract":"Machine Learning"))`
Web Of Science	`(((AB=("Blockchain")) AND AB=("Verifiable Credentials" OR "decentralized identifiers") AND AB=("Self-sovereign identity")) OR ((AB=("review system" OR "web of trust")) AND AB=("customer feedback" OR "User feedback") AND NOT AB=("AI" OR "Machine Learning")))`
B-On	`(AB blockchain AND AB ("Verifiable Credentials" OR "decentralized identifiers") AND AB ("Self-sovereign identity")) OR (AB ("review system" OR "web of trust") AND AB ("customer feedback" OR "User feedback") NOT AB ("AI" OR "Machine Learning"))`

3.1.2. Inclusion Criteria

The inclusion criteria define the essential properties that articles must present to be included in the final selection:

- **IC1**: The publication must include the defined keywords either in the title OR abstract.
- **IC2**: The publication must be accessible for free or through ISCTE's scientific license.
- **IC3**: The publication is written in English.
- **IC4**: the publication type should be: article (excluding other document types such as reviews,editorials, etc.).
- **IC5**: The article should be downloadable and accessible for personal reading and verification.
- **IC6**: The article must not be a duplicate.
- **IC7**: The article must not be out-of-scope

3.1.3. Filters

Table 3.2 presents the results obtained during the selection process, following the sequential application of the filters described below:

- **No filter**: IC1 AND IC2
- **Filter 1**: IC3
- **Filter 2**: IC4
- **Filter 3**: IC5
- **Filter 4**: IC6 AND IC7

TABLE 3.2. Repository Data

Repository	**No filter**	**Filter 1**	**Filter 2**	**Filter 3**	**Filter 4**
Scopus	95	94	30	9	9
ACM Digital Library	3	3	3	3	3
IEEE Xplore Digital Library	20	20	20	1	1
Web Of Science	15	15	12	12	5
B-On	124	55	24	24	8
Total	**257**	**187**	**89**	**49**	**26**

3.1.4. Exclusion Criteria

The exclusion criteria are applied to remove publications that do not meet the required standards.

- **EC1**: The publication exhibits poor linguistic quality.
- **EC2**: The publication does not fall within subject areas such as Computer Science or Engineering.
- **EC3**: The publication is too narrowly focused on a topic that is not directly relevant to the thesis.

These criteria identify characteristics that make a publication unsuitable for inclusion, beyond simply failing to meet the inclusion criteria. The application of these criteria resulted in the exclusion of three articles from the final selection.

3.1.5. Conclusion

As shown in Table 3.2, a total of 26 papers were initially selected: 9 from Scopus, 3 from the ACM Digital Library, 1 from IEEE Xplore, 5 from Web of Science, and 8 from B-On. Of these, 3 articles were excluded for being out of scope based on the established exclusion criteria. Additionally, 4 relevant papers were identified through the reference lists of previously selected articles. This resulted in a final dataset of 27 papers for analysis.

3.2. Literature Review Analysis

This section reviews existing research and systems that utilize Verifiable Credentials (VCs), Decentralized Identifiers (DIDs), and Self-Sovereign Identity (SSI) across various applications. The articles are grouped by their main focus areas to provide a structured overview of the relevant literature.

3.2.1. SSI

At its core, SSI gives individuals complete control and ownership over their digital identity, allowing them to manage their personal data and credentials independently, without relying on a central authority. This paradigm shift from traditional, centralized identity systems has significant implications for a wide range of applications, from enhanced security and access control to the secure verification of documents and personal information. The following sections delve into the foundational architectures of SSI and its various applications across different sectors.

3.2.1.1. *Core SSI Architecture and Web3 Infrastructure*

The foundation of decentralized identity management lies in robust architectures that support the SSI principles. Yuki YASUNO et al. [10] introduces a trustworthy architecture for Web3 service, leveraging DIDs and trust scores to establish self-sovereign services. This work calculates trust scores by analyzing social networks derived from users' past transaction history stored on the blockchain, using measures of centrality and similarity to quantify trust, which are then used to generate policies for role-based access control (RBAC). The architecture facilitates interactions between service providers and users through smart contracts, showcasing the potential of SSI to build trust in decentralized environments. Complementing this,Christoph H.-J.Braun et al. [13] presents an architecture for semantic interoperable SSI-based access control on the Web. This research addresses the need for interoperability across different SSI approaches by using RDF, SHACL, and extending the Hyperledger Aries Present Proof protocol to enable flexible and interoperable access control. These works lay the groundwork for building SSI systems and ensuring their effective integration.

3.2.1.2. *SSI for Access Control and Security*

Moving beyond core architectural considerations, SSI offers significant advantages in enhancing access control and security across various applications. Dr. Padma Adane et al.[8] presents a software module for granting verifiable credentials for access to restricted areas. This system utilizes Hyperledger Indy and Aries for the creation and verification of VCs, demonstrating how SSI can be applied to control entry into secure locations without relying on centralized authorities. In a different context, Francesco Buccafurri et al. [14] explores an SSI-based solution to support lawful interception, focusing on secure interactions between law enforcement agencies (LEAs) and law enforcement monitoring facilities (LEMFs). The proposed solution uses verifiable credentials and DIDs to strengthen security and standardize interactions, ensuring privacy-preserving identity management in a sensitive domain. Furthermore, Denver Naicker and Mackaylan Moodley [15] details a credential management system for public building access rights using SSI. This system automates the verification process, integrating business rule validations and addressing privacy and health and safety concerns. These studies highlight the versatility of SSI in providing secure and user-centric access control solutions.

3.2.1.3. *SSI for Document and Identity Verification*

Building on the security and access control features, the ability of SSI to provide secure and verifiable digital documents and identities is a key area of research. Abylay Satybaldy et al. [2] proposes a framework for online document verification using SSI. This research addresses the complexity and interoperability issues in current systems, aiming to improve the authenticity and privacy of digital credentials. This is particularly relevant in scenarios requiring high trust. Similarly, Joâo Luís et al. [16] proposes a solution to streamline and secure person and document authentication in the real estate sector. This work leverages Polygon ID(now Privado ID), a blockchain-based identity management solution, to offer enhanced security, trust, and efficiency compared to traditional methods. These works showcase SSI's potential to revolutionize document and identity verification processes.

3.2.1.4. *SSI in Healthcare*

Extending the scope of SSI's applications, the healthcare sector is a prominent area of SSI application, with research focusing on improving data security, privacy, and patient empowerment. Luisanna Cocco and Roberto Tonelli [12] proposes an SSI and blockchain-based model for deep digital transformation in healthcare. This model aims to give individuals control over their medical information and ensure secure communication between stakeholders by treating all medical reports as verifiable credentials. Addressing access control within healthcare systems, HAFIDA SAIDI et al.[17] proposes a Decentralized Self-Management of Access Control (DSMAC) scheme for the Healthcare Internet of Medical Things (HIoMT). This scheme aims to provide secure, fine-grained access control and

protect patient privacy by leveraging blockchain technology and attribute-based encryption. Expanding on this, Efat Samir et al. [18] introduces a Digital Twin Self-Sovereign Identity Management (DT-SSIM) framework for smart healthcare systems. This framework combines digital twin technology with SSI and blockchain to enhance data security, privacy, and interoperability. Finally, Marie Tcholakian et al. [19] proposes an SSI architecture for consented and content-based access to medical records using blockchain. This architecture aims to provide secure and privacy-preserving access to medical data, addressing the vulnerabilities of centralized systems. These studies collectively demonstrate the transformative potential of SSI in the healthcare domain.

3.2.1.5. *SSI for Specific Applications*

Beyond specific applications like healthcare, SSI is also being tailored for various other unique contexts. Wenting Song et al. [20] introduces a Privacy-Preserving Contact Tracing (PpCT) application that leverages SSI and blockchain. This application aims to trace contacts of individuals who tested positive for COVID-19 while ensuring user privacy. In the financial sector, Kang Woo CHO et al. [21] proposes a new model for credit scoring data collection using Verifiable Credentials with double zero-knowledge proof (ZKP). This model aims to enhance the reliability and security of credit scoring data while ensuring user sovereignty. These examples illustrate the adaptability of SSI to address unique challenges in different contexts.

3.2.1.6. *SSI Infrastructure and Implementation*

The practical implementation of SSI requires attention to infrastructure and integration. Luisanna Cocco and Roberto Tonelli [22] presents a model for deep digitalization in the construction sector, integrating Building Information Modeling (BIM) with SSI and blockchain to achieve greater transparency and verifiability. This work addresses challenges such as counterfeiting, waste, and lack of trust in the industry. Finally, Evrim Tan et al. [23] provides an assessment of the implementation challenges of the European Blockchain Services Infrastructure (EBSI) and the European Self-Sovereign Identity framework (ESSIF) through action research. This research identifies obstacles and potential solutions for the transformation of digital credential frameworks towards decentralized systems compatible with SSI.

3.2.2. SSI on Review Systems

While the foundational concepts and varied applications of SSI are well-established, a critical area of research focuses on addressing the inherent trust challenges within decentralized identity ecosystems. Andrea De Salve et al. [5] introduces a multi-layer trust framework designed to enhance the reliability of SSI by leveraging the Web of Trust (WoT) concept. They argue that while SSI provides mechanisms for verifying the authenticity and integrity of VCs, it does not inherently guarantee the trustworthiness of

the credential issuers, particularly in scenarios where multiple issuers may provide similar credentials. The authors propose a framework that utilizes blockchain technology to manage and propagate trust relationships between issuers and verifiers, enabling contextualized trust assessments. Their work highlights the importance of incorporating trust mechanisms into SSI architectures to ensure the credibility and usability of decentralized identity systems, exemplified by their application of the framework to mitigate the spread of fake news. This research is particularly relevant to the development of review systems, where trust mechanisms proposed for SSI can be effectively adapted to address inherent trust issues.

3.2.3. Review Systems

Review systems have become integral to online platforms, influencing user decisions and shaping the reputation of services and products. Several studies have explored various aspects of these systems, focusing on trust, security, and the analysis of user-generated content.

3.2.3.1. *Trust and Reputation*

The establishment of trust and reputation systems has become increasingly important in the 21st century, as these systems play a vital role in online environments by providing quality assessment and ensuring customer satisfaction. These systems contribute to business intelligence in various ways, such as fostering customer relationships, providing insights into consumer behavior, and enabling the dissemination of feedback. Beyond these benefits, they also help to identify and mitigate dishonest practices, unfair trading, and fraudulent activities.

Elizabeth Chang et al. [1] introduce the CCCI methodology, which offers a structured approach to measuring trustworthiness in e-service environments. This methodology evaluates the correlation between promised and delivered services, providing a quantifiable measure of the reliability of the service provider. The authors define a metric for the trust level or trustworthiness value of a Trusted Agent after a service interaction, adding a quantifiable dimension to trust assessment.

Farookh Khadeer et al. [24] addresses the need for a more structured understanding of reputation systems by proposing a defined ontology. This work emphasizes the ability of reputation systems to offer recommendations across various entities, from businesses to individual agents, highlighting the broad applicability of reputation in decision-making processes.

Judit POÓR and Gergely HORVÁTH [7] also contributes to the discourse on trust and reputation within online platforms, specifically focusing on the context of online travel agencies. This study likely explores how electronic word-of-mouth and guest review systems influence trust and shape consumer choices in the travel sector.

The importance of trust and reputation systems is further emphasized in [1], [6], [7], which collectively highlight their growing development and significant impact on business entities, emphasizing their crucial role in facilitating transparent and reliable online interactions.

3.2.3.2. *Security in Review Systems*

The security of review systems is paramount , Xiaohui Liang et al. [25] tackles security issues within service-oriented mobile social networks. This research identifies vulnerabilities, including review linkability, rejection, and modification attacks, and proposes the SEER system to enable secure user feedback. The proposed system employs techniques designed to counter these attacks and ensure the integrity of review data

3.2.3.3. *Content Analysis*

Analyzing the content of user reviews is essential for businesses to gain valuable insights, Akshada Y. Doifode et al. [6] focuses on aspect extraction in sentiment analysis. This work highlights the importance of analyzing user feedback to improve products and services. It addresses the challenges of accurately interpreting emotions from general reviews and suggests using NLP and ML algorithms to identify user interest in specific product features.

Changyong Niu et al.[26] introduces a novel technique for measuring feedback similarity to enhance trust generation within the web of trust systems. The authors argue that considering similarities among user feedback can mitigate the sparseness problem in these systems and allow for more personalized and accurate trust evaluations.

3.2.3.4. *Web Site Trust Evaluation*

Understanding how users evaluate the trustworthiness of websites is crucial and Chunsik Lee and Jisu Huh [27] investigates this process. This study applies the Development Likelihood Model (ELM) to examine the cognitive processes involved in the evaluation of website trust. It differentiates between central arguments and peripheral cues in website elements and analyzes how user involvement and knowledge influence trust assessment.

Young Ae Kim and Rasik Phalak [28] also explores the trust of websites, focusing on developing a framework to predict trust in online networks and contributing to a better understanding of the establishment and maintenance of trust.

3.2.4. Review Conclusion

The systematic literature review conducted in this chapter provides a granular perspective on the intersection of decentralized technologies and trust management within review systems. By applying the PRISMA [29] guidelines and the Design Science Research methodology [9], this study has identified a diverse array of frameworks and applications.

Table 3.3: Comprehensive Summary of Analyzed Literature

Article Title	**Domain**	**Key Contribution / Focus**
A multi-layer trust framework for Self Sovereign Identity on blockchain [5]	SSI / Web of Trust	Proposes a review system leveraging Self-Sovereign Identity (SSI) and decentralized identifiers.
A trustworthy architecture for Web3 service [10]	SSI / Web3	General SSI architecture with strong visual representations of the framework.
Integration of Self Sovereign Identity in Security Systems [8]	SSI Security	Basic integration of SSI within broader security infrastructures.
A Framework for Online Document Verification Using SSI Technology [2]	Banking / Identity	Detailed use case for banking involving interesting evaluation systems.
An SSI-Based Solution to Support Lawful Interception [14]	Communications	Specific focus on law enforcement communications and SSI.
SSI-Blockchain-Based Model for Transformation in Healthcare [12]	Healthcare	Digital transformation through SSI in the medical sector.
Privacy challenges in SSI for autonomous building access (COVID-19) [15]	Infrastructure	Analysis of user data privacy and verifiable credentials for building access.
Digital Transformation in the Construction Sector: Blockchain, BIM and SSI [22]	Construction	Exploration of on-chain and off-chain solutions for sustainable construction.

Table 3.3: Comprehensive Summary of Analyzed Literature (continued)

Article Title	**Domain**	**Key Contribution / Focus**
DSMAC: Privacy-Aware Decentralized Self-Management of Data Access [17]	Healthcare	Focuses on security and health data management with visual architectures.
DT-SSIM: A Decentralized Trustworthy SSI Management Framework [18]	Cybersecurity	Methods for secure DID storage and general cybersecurity enhancements.
Real Estate Documentation Authentication with Blockchain and SSI [16]	Real Estate	Application of SSI for document authentication in the Portuguese real estate market.
SSI and User Control for Privacy-Preserving Contact Tracing [20]	Public Health	Enhancing security for COVID-19 contact tracing applications.
SSI for Consented and Content-Based Access to Medical Records [19]	Healthcare	Management of medical records through blockchain-based SSI.
SISSI: Semantic Interoperable SSI-based Access Control on the Web [13]	Web / Interoperability	Addresses interoperability challenges for SSI access control on the web.
VC Proof Generation and Verification Model for SSI Credit Scoring [21]	Finance	SSI application for decentralized credit scoring data.

Table 3.3: Comprehensive Summary of Analyzed Literature (continued)

Article Title	**Domain**	**Key Contribution / Focus**
Verification of Education Credentials on EBSI (Belgium/Italy) [23]	Education	Cross-border transfer of diplomas using European Blockchain Services Infrastructure.
CCCI Metrics for the Measurement of Quality of e-Service [1]	E-Services	Analysis of review evaluation levels and service quality metrics.
E-WOM on Online Booking Interfaces: Travel Guest Review Systems [7]	Tourism	Comparative analysis suggesting 1-5 rating scales for online travel agencies.
On Feedback Similarity Measurement in Web of Trust [26]	Trust Management	Mathematical approach to measuring feedback similarity in trust networks.
Online Reviews System using Aspect Based Sentimental Analysis [6]	AI / NLP	Focuses on opinion mining and sentiment analysis for review systems.
SEER: A Secure and Efficient Service Review System for Mobile Networks [25]	Mobile / Security	Security-focused review system using tokenization for mobile social networks.
Towards Defining an Ontology for Reputation [24]	Reputation Systems	Basic definitions and ontology structures for reputation management.
Web Site Trust Evaluation as Cognitive Information Processing [27]	Cognitive Science	Evaluates website trust through the lens of user knowledge and involvement.

Table 3.3: Comprehensive Summary of Analyzed Literature (continued)

Article Title	Domain	Key Contribution / Focus
A trust prediction framework in social networks without a Web of Trust [28]	Social Networks	Large-scale framework for local trust prediction in rating-based networks.

The analysis of the literature yields several significant findings that inform the development of decentralized review systems:

- **The Trust Gap:** While blockchain ensures data integrity, it does not inherently guarantee the honesty of the human actors. Research by [26] and [5] emphasizes that a "Web of Trust" or reputation ontology [24] is necessary to evaluate the credibility of issuers.
- **Privacy-Security Paradox:** There is a recurring tension between complete user anonymity and the need for accountability. Frameworks like SEER [25] demonstrate that it is possible to achieve "unlinkable" reviews that are still verifiable and resistant to manipulation.
- **Sectoral Versatility:** The utility of SSI extends far beyond e-commerce. The transition from medical records [19] to education credentials [23] and real estate [16] suggests that a unified decentralized identity model is becoming a cross-industry standard.
- **User-Centric Empowerment:** The shift from centralized databases to User-Controlled models [20] is the most significant architectural change, allowing users to provide "consented access" to their data without third-party intermediaries.

3.3. Conclusion

The literature review has demonstrated a clear trend toward the adoption of SSI and blockchain across diverse sectors to solve problems of privacy and verification. While research in fields like healthcare has matured significantly, the application of these technologies specifically to e-commerce review systems remains an emerging area with substantial potential for innovation. The 27 articles selected and analyzed confirm that while the technical building blocks exist, a comprehensive framework that balances user friction with high-assurance verification is still lacking. These findings validate the research questions of this thesis and serve as the direct justification for the system design presented in Chapter 4

CHAPTER 4

Review System Design

This chapter provides a detailed blueprint for a decentralized review system. This chapter outlines the system's architecture, including key stakeholders, functional requirements, and core processes. It also analyzes different user authentication methods and illustrates the system's functionality through various use cases.

4.1. Review Systems

Review systems are essential components of digital platforms that enable users to share feedback about products, services, or experiences. These systems operate in markets where individuals or organizations provide assessments that influence purchasing decisions and platform reputation. Users write reviews based on their personal experiences, while platforms seek to ensure the credibility and authenticity of those reviews. Within this ecosystem, review verification plays a crucial role in maintaining trust and fairness.

The verification process involves evaluating various data points or documents associated with the reviewer and the transaction, often issued or confirmed by different entities, such as platforms, service providers, or third-party validators (the Issuers). Because this information originates from multiple sources, gathering and validating it can become a complex and time-consuming process.

Verifiers, in the context of review systems, are entities or mechanisms capable of confirming the legitimacy of user reviews. This includes ensuring that the reviewer is a real user, that a transaction occurred, and that the review content aligns with platform standards. Unfortunately, fake reviews, bots, and misrepresentations are persistent problems. Another challenge is the lack of automated trust between issuers and verifiers. Currently, trust mechanisms often depend on manual checks or direct platform contact, which limits scalability and efficiency.

The emergence of blockchain and other decentralized technologies provides a foundation for this solution. This approach leverages decentralized tools, such as Decentralized Identifiers (DID) and Verifiable Credentials (VC), to simplify and secure the process of validating reviews. By using Privado ID services, which employs Zero-Knowledge Proofs (ZKP), the system allows users to prove their identity or meeting certain criteria without revealing any personal information. This is a key component for ensuring privacy and security in the review system. By issuing VCs as proof of real transactions or user identity, the system reduces the dependency on physical or traditional verification processes, thereby enhancing review system integrity while making the process more seamless for both users and platforms.

4.2. System Stakeholders and Roles

The system operates within the SSI trust triangle: **Issuer**, **Holder**, and **Verifier**. The main stakeholders are:

- **Issuers:** Businesses or platforms (e.g., restaurants, hotels, e-commerce sites) that issue credentials confirming user interactions or purchases.
- **Holders:** Customers who receive verifiable credentials too submit reviews.
- **Verifiers:** Review platforms verifying the authenticity of a review without knowing the real identity of the reviewer.

Additional roles:

- **Administrators:** Platform moderators who can flag or restrict abusive DIDs.
- **Credential Registries:** Blockchain/DLT networks that anchor DIDs and credential schemas.

4.3. Non-Functional Requirements

Non-Functional requirements define the system's overall quality attributes and are a direct reflection of the design goals of a decentralized solution. The system must be Privacy-Preserving where the user has control over their data, ensuring the system's design minimizes data collection and exposure. By default, personal information is not shared, giving users a higher degree of privacy than with centralized platforms. The core principle of the system's architecture eliminates the single point of failure and control that exists in centralized systems. No central authority can censor reviews, revoke credentials arbitrarily, or control user identities, making the system more resilient and censorship-resistant. Furthermore, the use of cryptographic methods to link credentials to a decentralized ledger makes the system highly resistant to tampering. Once a credential is issued, it cannot be altered or forged, ensuring the integrity and trustworthiness of all data within the system.

4.4. Functional Requirements

The functional requirements are essential for the system to perform its core tasks. They are directly related to how the decentralized architecture solves problems found in traditional, centralized review systems. The system must permit users to submit reviews linked to their credentials, which is crucial for ensuring the authenticity of reviews by confirming the reviewer is a genuine customer. This mechanism is the foundation of the system's ability to combat fake reviews without relying on a centralized database of user information. A key privacy-enhancing feature is the support for selective disclosure using Zero-Knowledge Proofs (ZKP). Instead of revealing sensitive personal information to prove a review's legitimacy, ZKPs allow users to prove they meet certain criteria without disclosing any other data. This is fundamental to a privacy-preserving system.

4.4.1. Issuer Actions

In this system, the **Issuer** represents a trusted entity, specifically an e-commerce platform, service provider, or vendor, that is responsible for issuing credentials to verify the purchase of products or experiences. The steps, illustrated in Figure 4.1, that the Issuer must follow are:

(1) **Register Identity and Declare Credential Types:**
The Issuer begins by registering its identity on the platform, establishing its legitimacy within the decentralized ecosystem. It must also define the types of credentials it can issue—for example, product purchase receipts, booking confirmations, or service completion verifications, all within the context of e-commerce.

(2) **Fill the Credential Schema:**
After a customer completes a purchase, the Issuer generates a verifiable credential by populating a defined schema with transaction details. The specific fields filled depend on the nature of the purchase. For an activity, the credential would include the activity name/ID, the activity location, and the date of activity. If a product was purchased, the credential would be populated with the product name/ID, date of purchase, and the delivery status, along with any other relevant metadata.

(3) **Issue the Credential:**
Once the transaction information is verified and formatted, the Issuer generates a *Verifiable Credential (VC)* and issues it to the buyer. This VC serves as cryptographic proof that the user legitimately purchased a product or participated in a service or experience.

(4) **Revoke or Update Credentials:**
If the transaction is later refunded, canceled, or found to have errors, the Issuer has the authority to revoke the original credential. A corrected or updated version can then be reissued to maintain accurate and trustworthy records.

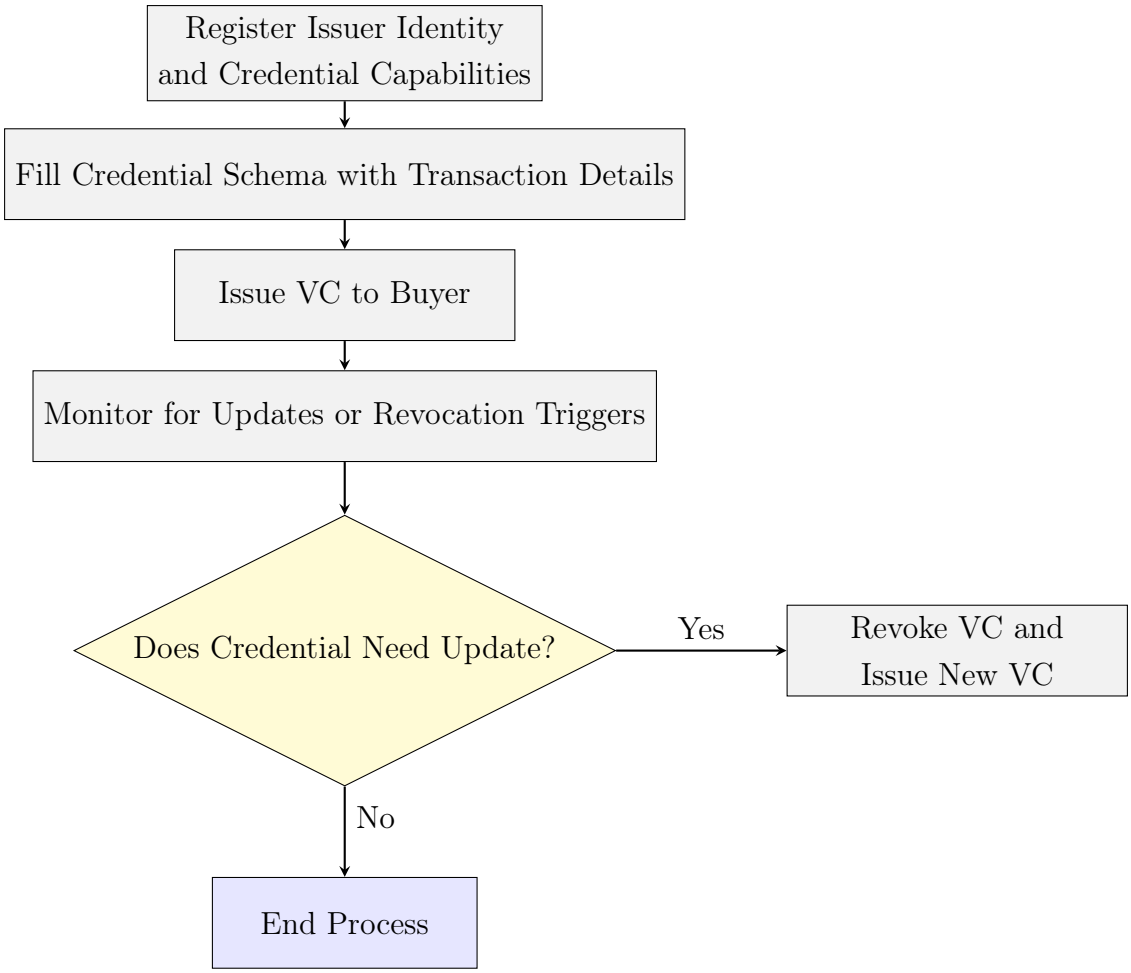


FIGURE 4.1. Flowchart depicting issuer actions.

The flowchart in Figure 4.1 visualizes the Issuer's role in the verifiable credential lifecycle. From establishing their identity and declaring credential types, to issuing, monitoring, and potentially revoking credentials, each step contributes to a secure and trustworthy credential ecosystem. This structured process ensures that every issued VC is backed by verified data and remains current even in the face of transaction changes. By following this flow, Issuers lay the groundwork for downstream use cases such as verified reviews, loyalty rewards, and fraud-resistant resale environments.

4.4.2. User/Holder Actions

In this system, the **User** represents the buyer or participant—typically an individual who receives a Verifiable Credential (VC) after completing a transaction. These credentials can later be presented to prove ownership, claim benefits, or enable secondary interactions. The steps, illustrated in Figure 4.2, that the User must follow are:

(1) **Purchase Item or Experience:**
The User initiates the process by purchasing a product, booking a service, or participating in an experience. This transaction forms the basis for the credential that will later be issued.

(2) **Obtain and Store Credential:**
After the transaction is confirmed, the User receives a Verifiable Credential from the Issuer. The credential is stored in a secure digital wallet or identity management application that supports verifiable credentials.

(3) **Present Credential for Verification:**
When required—for returns, warranty claims, loyalty benefits, or entry to events—the User can selectively disclose the VC or specific attributes of it to a trusted Verifier.

(4) **Monitor Credential Status:**
The User should remain aware of the status of their credential. If the credential is revoked or updated (e.g., due to a cancellation or refund), the change will be reflected in the user's wallet.

(5) **Use Credential in External Services:**
The User can leverage the VC in external services such as resale platforms, loyalty programs, or access-control systems to prove purchase authenticity without revealing excess personal information.

(6) **Make Verified Review:**
Using the VC as cryptographic proof of purchase, the User can submit a verified review on platforms that support authenticated feedback. This helps increase trust and credibility in digital review systems.

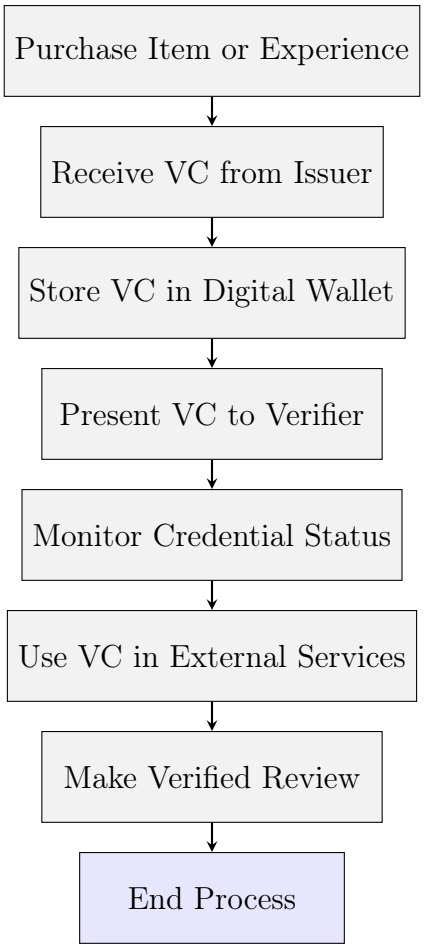


FIGURE 4.2. Flowchart depicting user actions.

The flowchart in Figure 4.2 illustrates the complete lifecycle of user interactions within the credential ecosystem. Starting from the initial purchase, each step—from receiving and storing the credential to presenting it and monitoring its status—builds toward secure and privacy-preserving participation. The final stages demonstrate how users can actively benefit from their credentials by using them in external services and contributing *verified reviews*, reinforcing trust in digital platforms. This process empowers users with control over their digital proof of ownership while enhancing transparency and accountability across the ecosystem.

4.4.3. Verifier Actions

In this system, the **Verifier** represents a third-party platform—such as a review site, resale marketplace, or loyalty program—that needs to confirm whether a user's claim of purchase or participation is genuine. By verifying the cryptographic authenticity of presented credentials, the Verifier ensures only legitimate interactions are accepted. The steps, illustrated in Figure 3.4, that the Verifier must follow are:

(1) **Receive Verifiable Credential from User:**
The Verifier begins the process by accepting a Verifiable Credential (VC) presented by the user. This could be for writing a verified review, accessing a loyalty benefit, or proving eligibility for a service.

(2) **Validate Credential Structure and Signature:**
The Verifier checks that the VC conforms to the expected schema and that its digital signature is cryptographically valid. This ensures the credential has not been altered since issuance.

(3) **Check if Issuer is Trusted:**
The Verifier verifies that the VC was issued by a trusted entity. This typically involves consulting a trusted Issuer registry or allowlist defined within the ecosystem.

(4) **Check Credential Status and Expiry:**
The Verifier checks if the credential has been revoked, is expired, or remains valid, by referencing revocation registries or expiry fields.

(5) **Authorize Action Based on Credential:**
If the credential passes all prior checks, the Verifier authorizes the requested action—for example, accepting a verified review or activating a loyalty reward. Otherwise, the request is denied or flagged for further inspection.

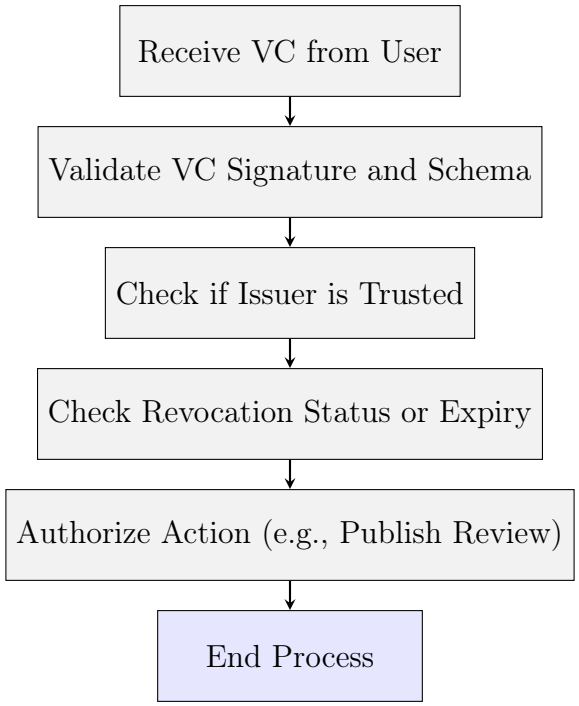


FIGURE 4.3. Flowchart depicting verifier actions.

The flowchart in Figure 4.3 outlines how Verifiers systematically validate credentials before accepting user actions. In addition to checking the VC's structure and status, the Verifier ensures it originates from a recognized and trusted Issuer—an essential defense

against spoofed or unauthorized credentials. This layered verification model reinforces platform integrity, discourages fraud, and enables users to engage in verified actions such as posting authentic reviews or claiming legitimate rewards.

4.5. Solution Use Cases

This system involves three user roles: **an issuer**, **a user**, and **a verifier**. The use cases of each role are outlined below and are visually represented in Figure 4.4, which summarizes the main interactions within the Credential Authentication System.

Issuer:
- Register Identity: The issuer, a legal entity, registers its identity publicly, ensuring its legitimacy is recognized within the system.
- Issue Credential: The issuer provides a Verifiable Credential (VC) to the user, enabling the user to prove the authenticity of the credential.

User:
- Receive and Store Credential: A user receives a credential from an issuer. They then store this credential as a verifiable credential (VC) in their digital wallet, which serves as proof.
- Present Credential: When required, the user presents the credential and relevant data fields to a verifier.

Verifier:
- Verify Credential: The verifier, in this case, a review platform, needs to validate a set of credentials. With the user's permission, the verifier receives a Verifiable Presentation, which is then checked to confirm its authenticity, integrity, and ownership.

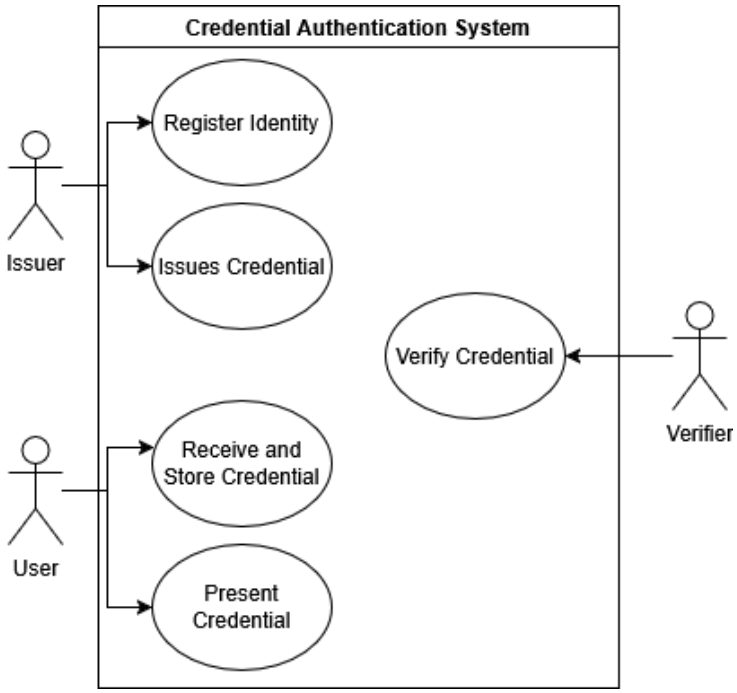


FIGURE 4.4. Use Case Diagram of the Credential Authentication System

Figure 4.4 illustrates the interactions among the issuer, user, and verifier within the credential authentication system. Each actor has distinct responsibilities, forming a clear

and secure flow: issuers create and release credentials, users manage and present them, and verifiers assess their validity. This model supports trust and efficiency in real estate and other sensitive transactions where identity and credential authenticity are essential.

4.6. System Architecture

The review verification system leverages decentralized identity technologies to ensure the trustworthy and verifiable management of user-generated reviews and credentials. Various components and business actors work together to maintain system integrity, as illustrated in Figure 4.5.

The system architecture includes all essential components to guarantee full functionality. A review platform or organization acts as the issuer, registering its identity within a Self-Sovereign Identity (SSI) framework. This allows it to generate and issue Verifiable Credentials (VCs) related to user reviews, ratings, or qualifications.

Users store these credentials securely in their private digital wallets, alongside their Decentralized Identifiers (DIDs), which are used for secure authentication during both issuance and presentation of VCs. Both users and review verifiers access the platform through an application that authenticates them using DIDs provided by the SSI infrastructure.

The verifier, such as a third-party service, employer, or platform moderator, accesses an application that lists registered users involved in the review process. This includes the credentials they hold and shared metadata from those credentials (e.g., rating categories, reviewer identity attributes, or content categories). The verifier checks the authenticity of the VC presented by the user, including verifying the identity of the original issuer.

The verifier also assesses whether the credentials match the claimed qualifications or review history, and confirms that the credentials have not been revoked or expired, ensuring they are still valid and trustworthy. The following components make up the decentralized purchaser verification system based on Self-Sovereign Identity (SSI) technologies:

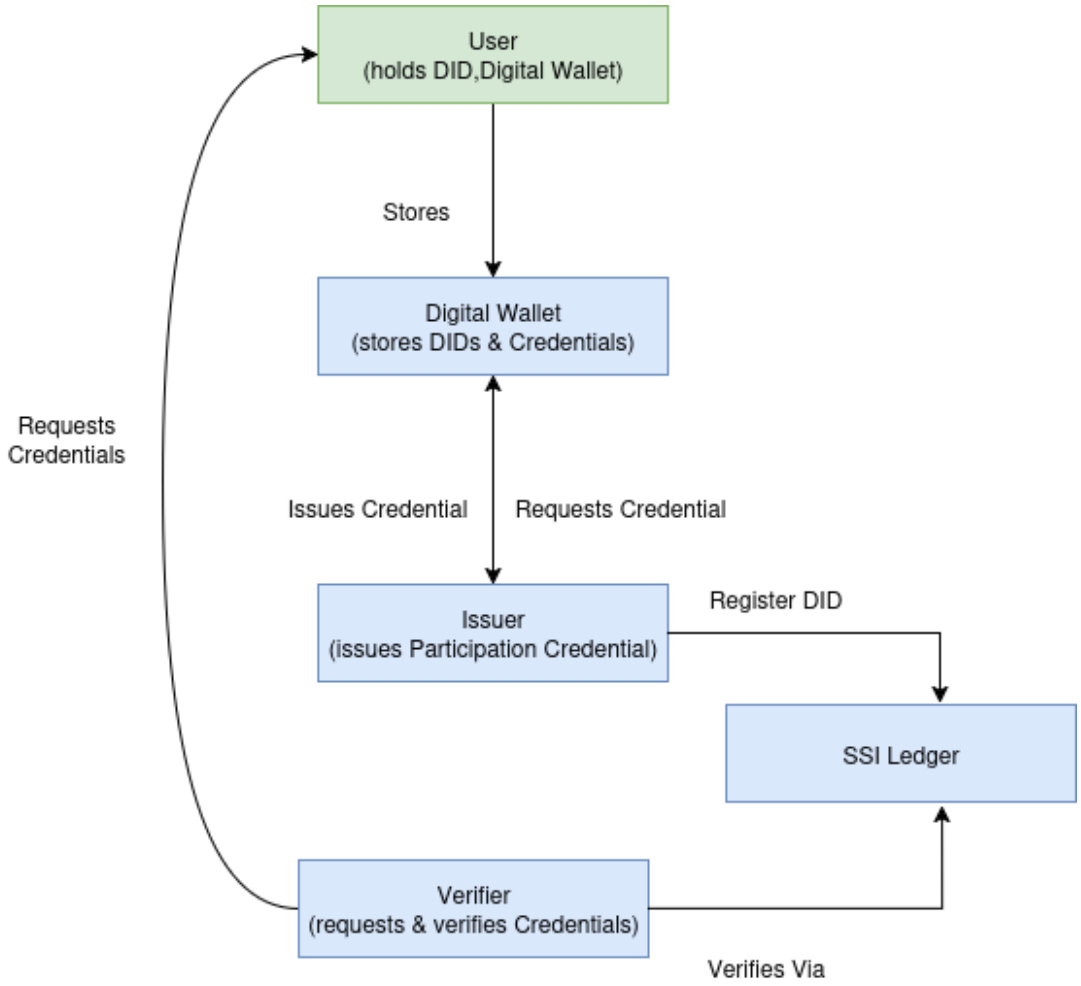


FIGURE 4.5. System Architecture Design

- **SSI Ledger:** The backbone of the system is the SSI ledger, which facilitates decentralized authentication and credential management. It enables identity verification for users and verifiers through Decentralized Identifiers (DIDs), supports cryptographic validation of Verifiable Credentials (VCs), and allows selective disclosure to preserve user privacy.
- **Issuer:** The Issuer is the entity responsible for registering its Decentralized Identifier (DID) on the Self-Sovereign Identity (SSI) ledger. Its primary role is to issue standardized Participation Credentials (Verifiable Credentials, or VCs) based on a user's verified activities on a third-party platform (e.g., attending an event, joining a service, or making a purchase). These VCs serve as verifiable proof of participation, regardless of payment status, and include essential metadata such as the platform name, activity type, timestamp, and any optional contextual details necessary for the review system.

- **Digital Wallet:** Users store their DIDs and participation credentials in a digital wallet compatible with SSI protocols, such as Polygon ID. The wallet enables secure storage, selective disclosure of credential attributes, and seamless interaction with verifiers.
- **Credential Verification Services:** Verifiers—such as platforms requiring proof of prior engagement (e.g., event hosts or review systems)—can request participation credentials from users. Users respond by presenting the relevant VC, which the system verifies cryptographically, including checks for issuer validity, expiration, and revocation status.
- **Verifiable Credential Schema:** A standardized schema for participation credentials will be developed to ensure trust, interoperability, and extensibility across a wide range of platforms and activity types.

4.7. System Processes

This section illustrates the core services involved in credential issuance (represented as Verifiable Credentials), authentication, and verification, along with the various interactions between the user, issuer, and verifier.

4.7.1. Issuer issues Credential to User

Figure 4.6 depicts the process where an issuer, acting as a Trusted Issuer (TI), provides a user with a Verifiable Credential (VC). The issuer offers a service or product that the user has engaged with and registers its Decentralized Identifier (DID) on the Polygon blockchain. This registration allows both users and verifiers to reliably recognize the issuer. Additionally, the issuer publishes the credential schema to guarantee consistent and standardized issuance of credentials.

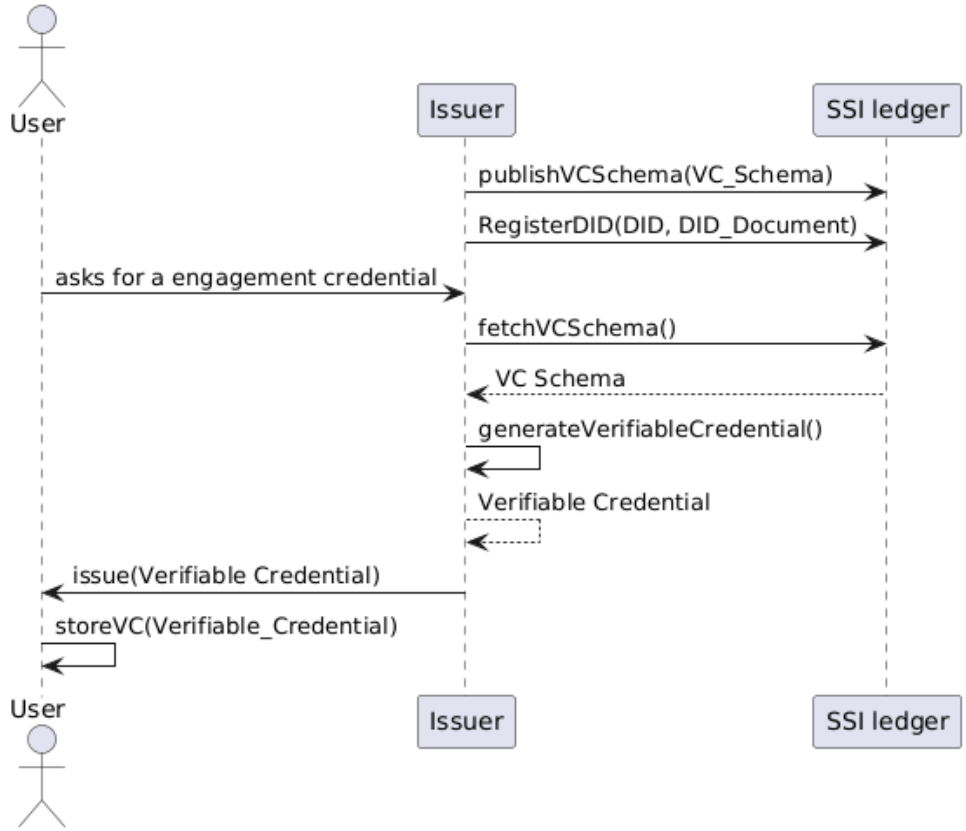


FIGURE 4.6. Credential Issuance Sequence Diagram

When a user requests proof of their interaction, the issuer generates a VC based on the predefined trust schema, which includes specific data fields such as the issuance date, expiration date, and relevant DIDs. The VC is then issued to the user, who securely stores it in a personal digital wallet compliant with Self-Sovereign Identity (SSI) technology.

The Credential Issuance process is depicted in Figure 4.6 and follows the sequence:

(1) **Preliminary Issuer Actions:** The **Issuer** first registers its Decentralized Identifier (DID) and publishes the Verifiable Credential (VC) schema on the **SSI ledger**. This establishes the Issuer's identity and the standardized format for the credentials it will issue.
(2) **Request for Engagement Credential:** The **User** then initiates a request to the **Issuer**, asking for an engagement credential.
(3) **Schema Retrieval:** The **Issuer** retrieves the relevant VC schema from the **SSI ledger** to ensure the credential adheres to the standardized format.
(4) **Credential Generation:** Using the fetched schema, the **Issuer** generates a Verifiable Credential specifically tailored to the user's engagement data. This credential includes critical information such as the issuance and expiration dates, as well as associated DIDs.
(5) **Credential Issuance:** The **Issuer** then issues the newly generated Verifiable Credential to the **User**.

(6) **Secure Storage:** Upon receipt, the **User** securely stores the credential in their personal digital wallet, which follows the principles of **Self-Sovereign Identity (SSI)**, ensuring privacy and user control over their credentials.

This process guarantees trust and interoperability by leveraging the blockchain-backed SSI ledger as a source of truth for credential schemas and issuer identities, enabling reliable verification by third parties when the user presents the credential.

4.7.2. Credential Presentation and Verification

After the Verifiable Credential (VC) is issued and securely stored in the user's digital wallet, the next phase involves presenting this credential for verification as needed. The verification process is illustrated in Figure 4.7 and outlines the steps a verifier follows to authenticate a presented document.

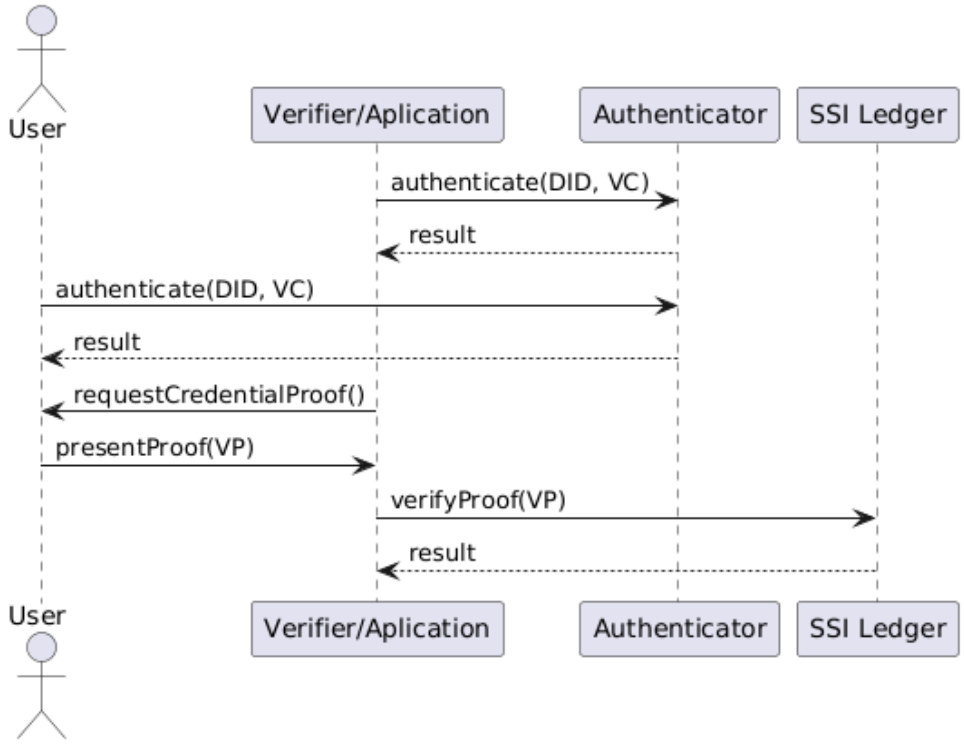


FIGURE 4.7. Credentials issuance Sequence Diagram

The presentation and verification process is depicted in Figure 4.7 and follows the sequence:

(1) **Authentication:** The process begins with both the **User** and the **Verifier** authenticating with the platform.
(2) **Request for Credential Proof:** After authentication, the **Verifier** requests a verifiable proof of the user's engagement.
(3) **Presentation Generation:** The **User**'s digital wallet generates a **Verifiable Presentation (VP)**, which contains the VC. This presentation can selectively

disclose only the required information, leveraging technologies like **Zero-Knowledge Proofs (ZKPs)** to preserve user privacy.

(4) **Presentation to Verifier:** The **User** securely sends the generated **Verifiable Presentation** to the **Verifier**.

(5) **Proof Verification:** The **Verifier** verifies the authenticity and integrity of the **Verifiable Presentation** by checking it against the **SSI Ledger**.

(6) **Verification Result:** The **Verifier**'s application then displays the result of the verification, confirming that the user's review is backed by a genuine engagement.

This process guarantees that reviews are trustworthy and tied to real interactions without compromising user privacy. By leveraging a blockchain-backed SSI Ledger, the system acts as a single source of truth for all credential schemas and issuer identities, enabling reliable and transparent verification by third parties, as long as the verifier trusts the issuer.

4.7.3. Concert Attendance Verification and Review Process Example

This section presents a real-world application of Verifiable Credentials (VCs) in the context of concert attendance and post-event reviews. It demonstrates how digital credentials and decentralized identity systems can ensure that only genuine attendees are able to leave verified feedback. The participants in this process are Alice (a concertgoer), LiveMusic Events (the concert organizer and credential issuer), and SoundRate (a third-party review platform acting as verifier).

Initially, Alice purchases a ticket for a concert organized by **LiveMusic Events**, identified by the decentralized identifier (DID) `did:example:livetickets`. As part of the purchase process, Alice—identified by `did:example:alice456`—receives a VC in her digital wallet. This VC contains metadata such as: `ticketId`, `eventName`, `eventDate`, `seatInfo`, and `attendanceStatus`.

To establish trust, LiveMusic Events must be recognized as a Trusted Issuer by the review platform that will later verify the credential, SoundRate in this case. This is a straightforward registration process in which LiveMusic Events applies to be listed as a trusted source of concert ticket credentials. The goal is simply to ensure that verifiers can confirm the credential comes from an authorized event organizer.

At issuance, the VC's `attendanceStatus` is marked as `pending`. After the concert concludes, LiveTickets updates the VC to reflect an `attended` status, based on venue check-in data (e.g., QR code scans at the entrance). This update confirms that Alice actually attended the event.

Once the VC is updated, Alice receives a notification allowing her to leave a review on **SoundRate**, a decentralized concert review platform, identified by `did:example:soundrate789`. To post a review, Alice first authenticates on the platform via Web3 using her digital wallet. At the same time, SoundRate authenticates itself by presenting its own VC, issued by a known review authority.

SoundRate then verifies Alice's credential by performing the following checks:

- Confirms the issuer's DID (`did:example:livetickets`) is a recognized and trusted authority.
- Verifies that Alice is the subject of the credential (`did:example:alice456`).
- Ensures the VC's `attendanceStatus` is set to `attended`.
- Checks the credential's integrity and signature.
- Confirms the VC has not expired or been revoked.

Upon successful verification, Alice is permitted to post a review, and SoundRate displays a badge indicating that the review originates from a verified concert attendee. To preserve privacy, Alice only discloses the required VC fields (e.g., event name and attendance status) through selective disclosure, omitting sensitive or unrelated personal data.

This approach helps ensure that reviews are trustworthy, bot-free, and written by real participants, thereby enhancing the credibility and reliability of feedback on concerts and live performances.

4.7.4. Conclusion

Chapter 5 establishes a robust framework for a review system designed to enhance trust and combat fraud in online review environments through decentralized solutions. By meticulously defining the roles and interactions of Issuers, Holders, and Verifiers within the SSI paradigm, the system ensures that reviews are authentic and verifiable while prioritizing user privacy and control over personal data. The proposed design, leveraging VCs and DIDs, sets the foundation for a transparent and secure review ecosystem, addressing critical challenges prevalent in traditional centralized systems.

CHAPTER 5

System Prototype Implementation

This chapter details the practical realization of the proposed decentralized review system prototype. Unlike a full-fledged application encompassing all aspects of a review platform, this prototype is focused on demonstrating the verification of credentials to prove service interaction. Other broader system functionalities, such as extensive credential issuance or comprehensive data management, are intentionally left open for third-party implementations, as they fall outside the core scope of this thesis. This chapter outlines the selected technology stack, the tools used, and the methodologies employed, showcasing the feasibility and functionality of the architectural design (as presented in Chapter 4) specifically concerning the robust and secure verification of Self-Sovereign Identity (SSI) credentials. The objective is to provide a tangible and focused demonstration of how SSI can be leveraged to establish and enhance trust through verifiable proofs of service interactions within decentralized environments.

5.1. Technology Stack and Tools

Developing a decentralized review system prototype required a specific set of technologies. Our choices were driven by the need to support Self-Sovereign Identity (SSI) principles, enable critical interactions, and provide an intuitive user interface for verification processes. We prioritized technologies that would directly facilitate decentralized identity solutions, with a strong focus on the verification aspect, aligning with common implementation strategies for verifiable processes in similar projects.

Our core technology stack and tools include the elements that will be presented and described next.

Central to Decentralized Identity: Privado ID

Privado ID [30] formed the backbone of our SSI implementation. Privado ID provides a middleware infrastructure and tools for applications that implement privacy-preserving digital identity, empowering users to own their data and share it only with their consent [30]. It was crucial for both the issuance (where necessary for demonstration) and, most importantly, the verification of credentials. Privado ID provided the necessary infrastructure to manage Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs), which are fundamental to proving service interactions within the system. While underlying Distributed Ledger Technology (DLT) like Hyperledger supports Privado ID's operations, our prototype interacted directly with the Privado ID ecosystem.

We leveraged Privado ID for:

- Credential Issuance (as a prerequisite for verification demonstrations).
- Robust verification of service interaction-related credentials (e.g., proof of transaction, confirmed service delivery, event participation).
- Management of DIDs and facilitating secure, private interactions between users and verifiers.

This directly enabled the core verification processes, fostering trusted assertions of service interaction.

Blockchain Interaction and Development Tools: Alchemy

To support our blockchain interactions, we leveraged Alchemy [31]. Alchemy is a complete Web3 development platform that provides the infrastructure, tools, and APIs for developers to build and scale blockchain-based applications, often called dApps. This was a crucial addition to our tech stack, as it provided the robust infrastructure needed for a seamless and reliable connection to the underlying blockchain. Alchemy offered a suite of developer tools, including a powerful API, to handle the complexities of blockchain communication, such as retrieving data and managing transactions. By using Alchemy, we could focus on the prototype's core logic—credential verification—without having to build and maintain our own blockchain nodes. This integration was essential for ensuring that our system's interactions with the decentralized ledger were efficient and dependable.

User Interface: HTML and JavaScript

For the prototype's front-end, we chose HTML [32] and JavaScript [33] to create the user interface. Our goal was to build an intuitive and responsive user experience for both users (presenting proofs) and verifiers (requesting and validating proofs). This combination of technologies allowed us to create the necessary structure and add the dynamic functionality required for the prototype.

The use of standard web technologies like HTML and JavaScript aligns with common practices for developing user interfaces, especially for showcasing credential interaction flows clearly.

Key uses of HTML and JavaScript in this system included:

- Creating the user interfaces for managing identity and credentials.
- Enabling the initiation and response to verification requests (e.g., displaying QR codes for proof requests, showing verification results).
- Establishing the primary interface for user and verifier interaction within the prototype's verification scope.

Backend Logic and Data Handling: Node.js with Local JSON Files

For the prototype's backend logic and data handling, we used a Node.js [34] environment for server-side scripting. The prototype's main focus was on credential verification rather than extensive data management, which allowed for a lightweight and flexible approach to data persistence.

Local JSON files were utilized for non-sensitive or temporary data. This included:

- Orchestrating verification request flows with Privado ID.
- Receiving and processing verification proofs from user wallets.
- Managing temporary session IDs and logs of completed verifications.

This method simulated basic data persistence without the need for a complex database server or containerization. It was a pragmatic and sufficient choice for demonstrating the core functionalities and interactions with Privado ID, making the implementation faster and easier for this proof of concept. Although a tool like MongoDB would be a more robust solution for a production application, JSON files were ideal for the scope of this prototype.

Secure Localhost Exposure: ngrok

Ngrok [35] for development and demonstration, exposing our locally running Node.js backend to the internet was critical. This allowed Privado ID, an external service, to send callbacks and communicate with our local server for verification flows. ngrok provided a secure and straightforward method to create public URLs that tunnel traffic to our local development environment. This bypassed common network complexities like firewalls, enabling seamless integration and testing of the prototype's interaction with the external Privado ID platform without a full deployment as show in figure 5.1. We used it to create secure HTTPS tunnels, generate public URLs for webhook callbacks, and facilitate remote access for demonstrations.

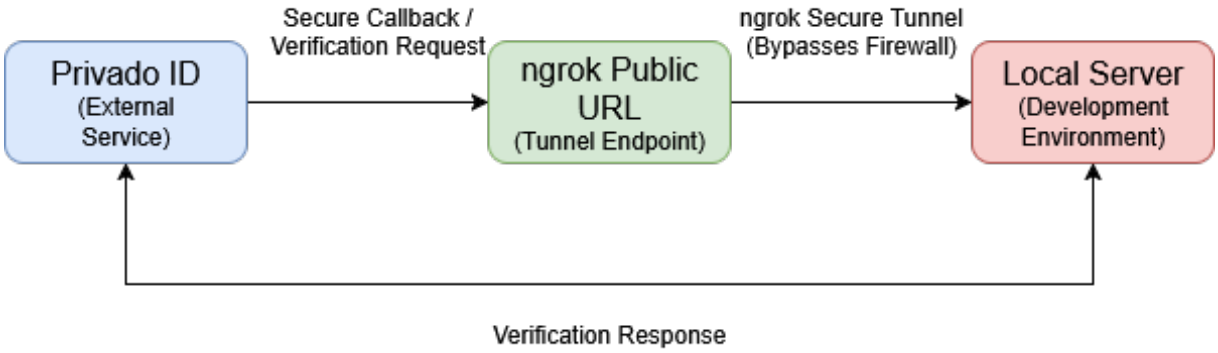


FIGURE 5.1. Verification Flow using ngrok for Local Development

This carefully chosen, streamlined selection of technologies provided a practical and focused foundation for developing a functional prototype dedicated to demonstrating verifiable service interactions. It effectively showcases the potential of decentralized identity solutions, centered around Privado ID, in establishing trust through credential verification within online review ecosystems.

5.2. Authentication

In the context of Web3 authentication using Privado ID, our decentralized review prototype implements a fundamental authentication method involving Decentralized Identifiers (DIDs) and Verifiable Credentials (VCs). This authentication is not a general login to a broad application but serves as the crucial initial step for users to connect their Privado ID wallet and assert their identity, thereby enabling them to present verifiable credentials for proving service interaction. This process ensures secure and verifiable user identity within the system, establishing a foundational layer of trust for subsequent credential verification flows.

The implemented authentication method is a Basic Authentication Request, which facilitates secure interaction with a user's wallet and authenticates the user based on their DID. This process involves creating a minimal DID request and verifying proof of ownership of the DID. This authentication is essential for a user to establish their digital presence and participate in the credential verification mechanisms of the prototype.

This method is implemented via the application's backend logic, which interacts directly with the Privado ID ecosystem. The process begins when a user accesses the frontend and initiates the authentication process,by clicking on "Verify" as shown in 5.2. The frontend sends a request to the backend, which, in turn, constructs an authentication query to be processed by Privado ID. This query typically includes:

- The reason for authentication (e.g., "Authenticate Identity for Credential Presentation").
- The requester's DID (our prototype's DID, if acting as a verifier).
- A randomly generated challenge message that will be cryptographically signed by the user's wallet.
- A callback URL where the wallet will later send the proof for verification back to our application's backend.

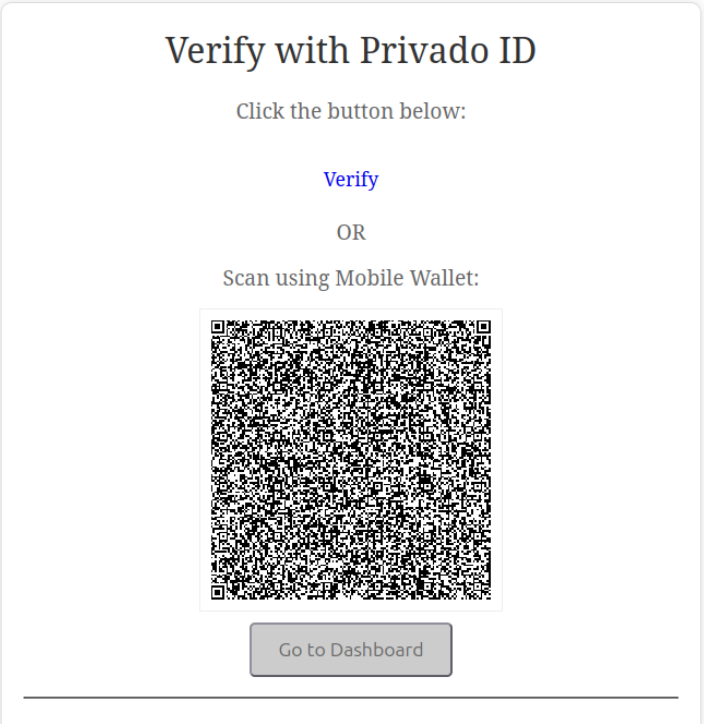


FIGURE 5.2. Homepage screen

The authentication request flows from our backend to your frontend, presenting you with two ways to interact. You can either scan a QR code, which works if you have the Privado ID wallet installed on your device, or use a deep link has shown in figure 5.2. The deep link is a versatile option that works for both the Privado ID wallet and other compatible cryptocurrency wallets you might have, such as Trust Wallet or MetaMask, and it directly opens your chosen wallet application. Once your wallet receives the request, it processes it and generates a cryptographic proof of your DID ownership by signing a challenge. This proof is then securely sent to our application's backend, which acts as the verifier, via a specified callback URL has shown in figure 5.3.

Once the proof is received by the backend of the application, it initiates a call to the Privado ID verifier to process and validate the proof. During this verification process, the Privado ID verifier unpacks the proof, verifies its cryptographic validity against the criteria set in the initial request, and confirms that the proof satisfies all required conditions, thereby authenticating the user's DID ownership and establishing a trusted connection for further interactions.

Upon successful authentication by a user, the application generates a JSON Web Token (JWT). This token serves as an authorization mechanism, granting the authenticated user access to perform subsequent actions within the prototype strictly related to credential presentation and verification flows.

The authentication phase is crucial in ensuring the security and integrity of the decentralized review prototype's core functionality: verifiable service interaction. By leveraging Privado ID's DID and VC mechanisms, the system securely manages and verifies user

identities, enabling them to participate in the credential verification processes for proving service interaction. These processes are vital for maintaining the confidentiality of user data and the integrity of interactions within the prototype, thereby providing a robust foundation for trust in a decentralized review environment.

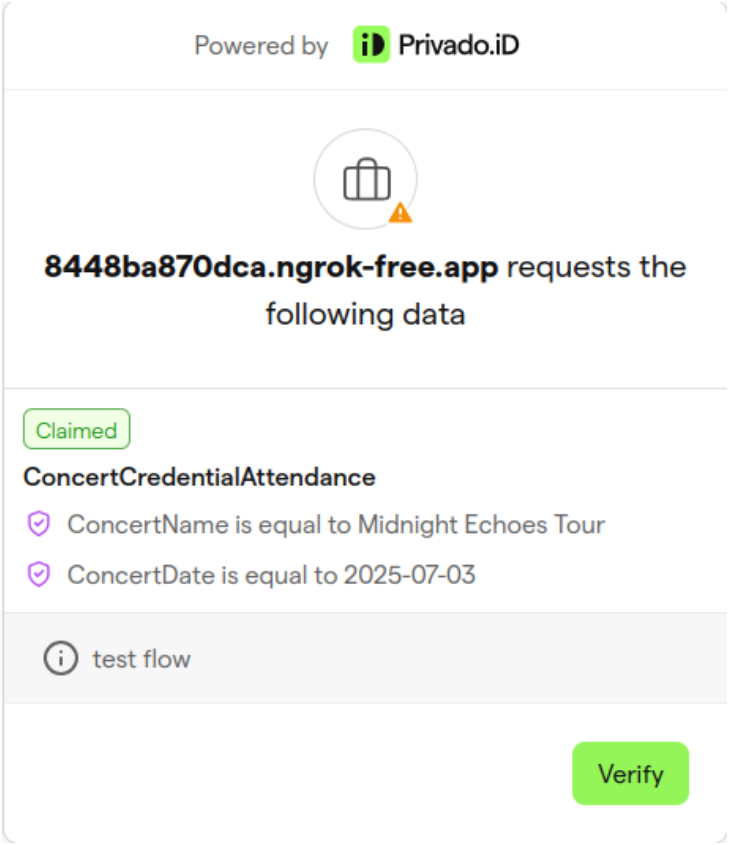


FIGURE 5.3. Verifying screen

5.3. Prototype Prerequisites

This prototype's functionality is contingent on a few key prerequisites related to the issuance and claiming of a Verifiable Credential (VC). The Issuer of the credential has two options: they can either create a new, dedicated credential for this purpose or reuse an existing one.

To enable the user to claim this credential, the Issuer must provide a method for distribution, such as a QR code or a direct link. The timing of this claim process is flexible and can be determined by the Issuer, taking place either at the beginning or the end of the user's experience.

For example, this could function as a digital receipt, or in a ticketing application where scanning a ticket to enter a venue automatically sends the user a credential link. The user must possess this credential to access and use the prototype. It's important to note that this method is only viable if the Verifier (in this case, the review platform) explicitly trusts the Issuer.

5.4. Credential Verification Flow for Service Interaction

This section will detail the core contribution of this prototype: the mechanism for verifying credentials that assert a service interaction. It outlines the process through which a service interaction is cryptographically proven and verified using SSI principles, specifically adapted from the general document verification model to fit the context of verifiable service reviews.

5.4.1. Verifier Actions

After an entity (acting as a verifier, e.g., a review platform) is authenticated. The verifier's primary action is to verify a proof of a specific service interaction.

- **Make Request:** If the verifier requires proof of a service interaction from a user, they can select the desired attributes related to that service (e.g., service type, date, amount, service provider DID) via the frontend. The frontend then transmits these attributes to the backend. The backend forwards this request to the Privado ID API to generate a verifiable presentation request. The Privado ID API, based on the provided information, constructs this request as shown in 5.4. A conceptual request would include attributes such as:
  - **From:** Represents the verifier's DID, establishing their identity and ensuring the request originates from a legitimate source.
  - **To:** The user's DID, optional but recommended to confirm user ownership and prevent forgery.
  - **Type:** Refers to the type of communication or request being made (e.g., a verifiable presentation request for a specific credential type).
  - **Body:** Contains the fields requested from the service interaction credential. This includes the reason for the verification (e.g., "Verify service completion for review"), a challenge message for proof of DID ownership, and the callback URL for proof submission. The scope within the body defines the specific fields requested, using selective disclosure to reveal only the necessary details. Each scope request would specify:
    - **Credential Type:** The specific type of Verifiable Credential representing the service interaction (e.g., "ServiceCompletionCredential").
    - **Allowed Issuers:** Specifies the DIDs of authorized issuers allowed to issue the VC representing the desired service interaction (e.g., the DID of the service provider). This prevents unauthorized entities from issuing fake credentials.
    - **Context (if applicable):** A link to where the VC schema is published (often handled implicitly by Privado ID).
    - **Credential Subject (specific attributes):** Details the specific attributes within the credential subject that are requested for disclosure (e.g., ‘serviceID‘, ‘completionDate‘, ‘serviceProviderDID‘).

Following this process, the request is designed to reveal only the necessary attributes, thereby preserving user privacy. The request is then prepared for presentation to the user and is stored temporarily by the backend for subsequent verification.

```
[
    {
      "circuitId": "credentialAtomicQuerySigV2",
      "id": 1754136501,
      "query": {
        "allowedIssuers": [
          "did:iden3:polygon:amoy:xH577MLAj2Y67FM8L5859G1Pzf1eEPToMq3UB3ChY"
        ],
        "context": "ipfs://Qmd3nzUyUi45HEbxEikgrjAG8crpE971vJg5NibjWsL7jY",
        "credentialSubject": {
          "ConcertName": {
            "$eq": "Midnight Echoes Tour"
          }
        },
        "type": "ConcertCredentialAttendance"
      }
    },
    {
      "circuitId": "credentialAtomicQuerySigV2",
      "id": 1754013968,
      "query": {
        "allowedIssuers": [
          "did:iden3:polygon:amoy:xH577MLAj2Y67FM8L5859G1Pzf1eEPToMq3UB3ChY"
        ],
        "context": "ipfs://Qmd3nzUyUi45HEbxEikgrjAG8crpE971vJg5NibjWsL7jY",
        "credentialSubject": {
          "ConcertDate": {
            "$eq": "2025-07-03"
          }
        },
        "type": "ConcertCredentialAttendance"
      }
    }
  ];
```

FIGURE 5.4. Credential Authentication Query Example

5.4.2. User Actions

Each user interacts with their personal interface (or wallet) which displays all relevant credentials and pending verification requests. The available actions for a user related to service interaction verification are as follows:

- **Pending Requests:** If a verifier has made a request for proof of service interaction, this option appears. The request will be displayed ,has shown in figure 5.5 , allowing the user to either scan it using their Privado ID wallet or open it via a

deep link. Once the request is presented to the user's wallet, the wallet processes it, constructs a cryptographic proof based on the user's stored Verifiable Credentials and their DID, and sends this proof back to the verifier through the specified callback URL. The callback sends the proof to the application's backend, which forwards it to the Privado ID verifier for validation.

- **Proof Verification Process:** The Privado ID verifier then processes the received proof by checking several critical aspects:
  - **VC Schema Conformance:** Ensures the presented VC's schema matches the intended one for proving service interaction.
  - **VC Ownership:** Verifies that the ownership claim, typically involving a cryptographic proof, corresponds to the DID associated with the user who presented the proof.
  - **VC Revocation Status:** Checks if the VC has been revoked by the issuer.
  - **VC Expiration Status:** Ensures the VC has not expired.
  - **VC Signature:** Verifies the VC's cryptographic signature to ensure it was issued by a trusted entity (e.g., the service provider), preventing forgery or unauthorized issuances.
- **Verify Service Interaction:** This option (if presented to the user) mirrors the workflow of pending requests but allows the user to initiate the proof presentation independently, enhancing user-centricity and control over their verifiable data.

By following these steps, proofs of service interaction are effectively verified, providing a decentralized and trustworthy mechanism for confirming past engagements.

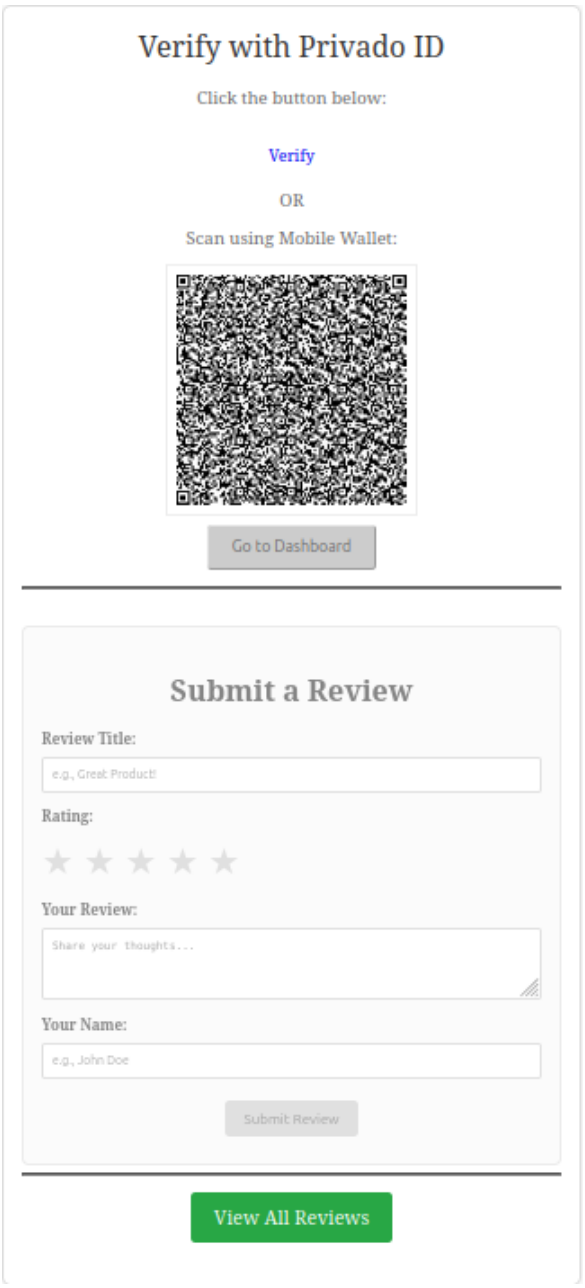


FIGURE 5.5. Unverified Form (Before Authentication)

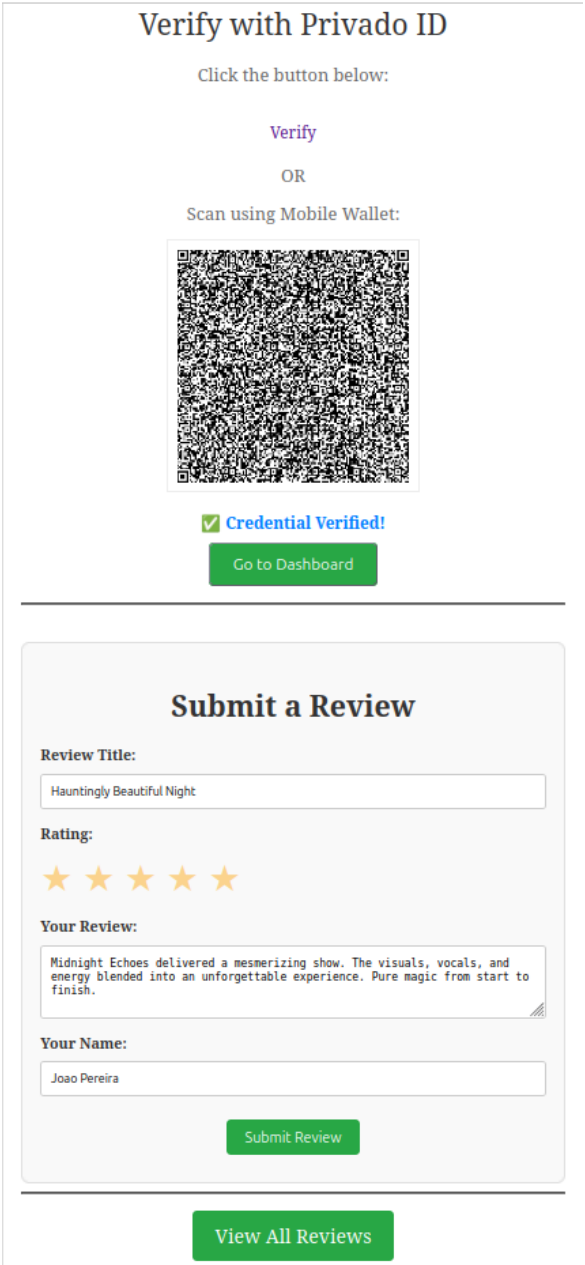


FIGURE 5.6. Verified Form (After Successful Authentication)

5.5. Conclusion

The implementation of the decentralized review system prototype is based on a focused architecture that leverages JavaScript (Node.js) for backend logic, React.js for the frontend, and Privado ID as the central component for Self-Sovereign Identity. The primary objective of this prototype is to securely manage the verification of Verifiable Credentials that prove service interaction.

The system architecture facilitates interaction between the user's wallet, the frontend, and a backend logic layer that communicates with Privado ID. Data persistence for the prototype is handled minimally using local JSON files, reflecting its narrowed scope.

The core functionality centers on an authentication mechanism that connects a user's Privado ID wallet, enabling them to present proofs. This leads directly into the detailed credential verification flow for service interaction, which involves verifier requests for specific attributes of a service interaction credential and user presentation of cryptographic proofs via their wallet. The prototype rigorously checks VC schema conformance, ownership, revocation, expiration, and cryptographic signatures to ensure the integrity and validity of these proofs.

The user interfaces, built with React.js, provide intuitive interaction points for both users (to present proofs) and verifiers (to request and validate proofs). Through these components, the prototype delivers a secure and efficient solution for managing the verification of service interaction proofs, with a strong emphasis on decentralized identity, user privacy, and verification transparency, thereby directly addressing the core focus of this thesis.

CHAPTER 6

A Technical Comparison: The SSI-Based Review System Vs Traditional Review System

Traditional online review systems, exemplified by platforms like Amazon, rely on a centralized model. While familiar, this approach faces significant, inherent challenges, particularly with data privacy and the perpetual struggle against review fraud. This thesis proposes an alternative: a novel review system leveraging Self-Sovereign Identity (SSI) technology. This SSI-based model creates a more secure and user-centric environment that operates independently of the e-commerce provider. This chapter will conduct a direct technical comparison between this proposed decentralized SSI architecture and the established centralized model, highlighting the advantages of the former.

6.1. Understanding the Two Review Systems

Traditional review platforms like Amazon operate on a simple principle: the review system is an extension of the e-commerce store. This means that a user's ability to review a product is directly tied to their purchase on that specific website. The system is designed to create a closed loop where the user's experience and identity are owned and managed by the platform itself. While this provides a "Verified Purchase" badge and a sense of authority, it also creates an inherent conflict of interest. The platform is incentivized to maintain good relations with vendors and may be susceptible to review manipulation, as it has a vested interest in the products it sells.

In contrast, the proposed review platform operates as a third-party service, completely detached from the point of sale. A user who purchases an item—be it a book, a piece of clothing, or electronics—receives a Verifiable Credential (VC) from the e-commerce store. This VC is a cryptographically verifiable proof that they had a genuine purchasing experience. The user then takes this credential to the review platform to submit their review. The platform verifies the credential, ensuring the review is authentic, but it never has access to the user's personal data or their identity. This model creates a critical separation between the e-commerce provider and the review platform, ensuring that the integrity of the review process is maintained by an impartial, third-party authority.

6.2. Core Principles and Use Cases

The decision to adopt a specific review system architecture is not a simple technical choice; it is a fundamental business strategy that is often dictated by a company's existing position in the market. A business with an established e-commerce platform will likely opt for a traditional, centralized model to leverage its existing user base. In contrast, an

independent entity, such as a startup, will choose the credential-based model to build trust and authority from the ground up. These two divergent paths lead to distinct advantages and disadvantages related to strategic rationale, target audience, and governance, which are explored in the following sections.

6.2.1. Control and Governance

The use case for a traditional platform like Amazon is to maintain full control over the user experience and moderation, allowing a single company to make rapid decisions to ban fraudulent accounts or remove malicious content. While this top-down control can offer a predictable and consistent user experience, it also centralizes power in a single entity. This model concentrates control at the point of purchase, where the user is merely a consumer of a service. This structure can lead to misaligned incentives, as the platform's governance may prioritize its own financial and strategic interests over the community's needs. The control is very focused on the entity that made the purchase, which doesn't create great incentives for a truly balanced ecosystem.

In contrast, the use case for starting the proposed review system is to democratize trust from the outset. This Thesis is rooted in the concept that a third-party, credential-verified system will be more resilient and trustworthy than one controlled by a single e-commerce corporation. This approach begins by establishing the rules of the platform and separating the review process from the point of purchase. The value proposition is a platform that cannot be manipulated by the vendor, ensuring that the integrity of the review data is preserved for everyone. This is a third-party platform that is more detached from the initial service being reviewed, while still maintaining control. This separation ensures better governance.

6.2.2. Target Audience

The use case for starting a traditional review platform is to capture a mainstream, non-technical audience. The goal is to create a product with a frictionless onboarding process that anyone can use. A traditional centralized design removes the complexities of digital wallets and decentralized identifiers, allowing the platform to quickly become a one-stop-shop for a wide variety of reviews. This frictionless integration allows the platform to capture a high volume of reviews directly from the point of sale, making it easier to build a large and comprehensive review database. The value proposition is convenience and a large network of users, which are powerful motivators for a broad market.

Conversely, the use case for starting a credential-based review system is to cater to a niche, quality-conscious audience with a forward-looking strategy for mainstream adoption. While the project begins with the understanding that not all users are comfortable with giving up control of their data, it operates on the premise that SSI technology will mature and become more widely accepted. The initial user base is likely to be a smaller group motivated by digital self-sovereignty. However, the system's underlying architecture is designed to be perfectly scalable, and its success will be measured by the integrity

and reliability of its community. This trustworthiness, in turn, can be used to attract a broader audience as the technology becomes more commonplace.

6.2.3. Business Strategy

The business strategy of a traditional review platform is based on a high barrier to entry. This requires an established platform to have a massive, pre-existing user base and products to be reviewed—like Amazon's e-commerce store—before it can begin collecting reviews. Monetization then relies on leveraging this captive audience through advertising, premium features, or data analytics. This "walled garden" approach treats the user and their data as a primary asset.

In contrast,the proposed credential-based system has a very low barrier to entry. A new platform can be created from scratch, offering an immediate and valuable service by leveraging verifiable credentials from existing e-commerce providers. The platform's business model is thus based on the value and integrity of verified data, not on the user's personal information. However, this model faces the significant challenge of competing with the market dominance and network effects of established market leaders who have already captured the mainstream audience. Its success depends on its ability to attract users who prioritize integrity and privacy over convenience.

6.3. Use Cases and Limitations

Traditional platforms like Amazon serve the primary use case of providing consumers with a vast volume of reviews to inform their decisions. They offer a familiar and accessible user experience. However, they are continuously vulnerable to fraud and review manipulation. Moreover, the centralized authority can act as a censor, controlling all content and user data, which presents a significant limitation to true user autonomy.

The primary use case for an credential-based system is to provide a more secure and privacy-focused review platform where users truly own their data and identity. This model addresses the core issues of trust and data ownership that centralized systems cannot. A significant limitation, however, is that this technology is still in its early stages of adoption and faces challenges with user experience. It can be difficult to implement features like a dispute resolution system without a central authority, requiring new models for moderation and governance.

6.4. Login Systems and User Identity

In the current digital landscape, we're all familiar with the traditional login systems used by companies like Amazon. You create a user account, complete with a username and password, and that identity is stored on the company's central server. This model, while convenient for platforms, creates a significant vulnerability: a single point of failure where a data breach can expose countless users' personal information. Furthermore, the company maintains control over your digital identity. While this allows for useful features like Amazon's "Verified Purchase" badge, it means you're trusting them to manage and protect your data.

The proposed system offers a fundamental shift in how we manage our online identity. This approach, built on Self-Sovereign Identity (SSI), is not about creating an account, but about having a unique identifier that only you control. It works through a Decentralized Identifier (DID), which is under your exclusive control. This means your personal data is never stored on a company's central server, providing a much higher degree of privacy and security. You, and you alone, are the owner of your identity and can decide exactly what information to share.

Instead of a password, this system uses Verifiable Credentials (VCs). These are cryptographically secure proofs that confirm you had a genuine experience, such as making a purchase, without revealing your real-world identity. This allows for the same functionality as a "Verified Purchase" badge but without the need for a user account or centralized data. It's not about making things more complex, but rather about using the internet in a different way. Over time, as users become accustomed to this new model of digital ownership, it will become just as easy and intuitive as the login systems we use today.

6.5. Security and Fraud Detection

Traditional systems rely on a top-down security model to combat fraud. Amazon uses a mix of AI and human oversight to analyze user behavior, flag suspicious patterns, and remove fraudulent content. The "Verified Purchase" badge confirms that a review comes from a legitimate buyer. This approach is highly scalable, allowing a central authority to quickly address threats. However, it's a constant, reactive battle against fraud, leaving these systems vulnerable to sophisticated, large-scale attacks and schemes designed to manipulate rankings or reviews.

In contrast, the proposed system approach security from the ground up, with its foundation built on a cryptographic design. The authenticity of an experience is confirmed by a Verifiable Credential (VC). This credential is issued by the e-commerce vendor—for example, a bookseller—and is a cryptographically signed proof stored in the user's digital wallet. When a user wants to post a review, they present this proof, and the network can verify its authenticity. This design makes it nearly impossible to generate fake reviews at scale, since each review requires a unique VC from a genuine experience. While this model is highly resilient to fraud, its integrity depends on the trustworthiness of the organizations that issue these credentials.

6.6. Portability

One of the most significant architectural differences between the two review models is the concept of data and review Portability. In Traditional Review Systems, the system's review capabilities are strictly limited to interactions that occurred and can be verified within the platform's own walled garden. Since all user data is centralized and tied to the platform's database, the user has no control over their history. This architecture restricts users to reviewing only services consumed on that specific site and results in a restrictive data lock-in effect, severely limiting the scope of a user's influence to that single service.

The SSI-Based Review System, by contrast, is designed around the principle of user control and ownership of their digital assets, fundamentally changing the scope and ownership of the review process. The user can review any service or experience for which a valid Verifiable Credential (VC)—the proof of experience or service—can be issued by the service provider. This VC is the only truly portable element; it is stored securely in the user's digital wallet, detaching the proof of interaction from the platform that facilitated the service. The portability of this foundational VC empowers the user to present a verifiable history of interactions to any compliant decentralized application, establishing trust and legitimacy across a broader ecosystem.

6.7. Interoperability

Interoperability is a critical differentiator between the two review system architectures, defining their ability to seamlessly exchange and utilize information. In a Traditional Review System, interoperability is inherently low, restricted by proprietary data formats and closed APIs. Each platform acts as a silo, making it difficult for external services to verify user data or for users to easily migrate information. This lack of standardization inhibits innovation and prevents the formation of a broader, connected ecosystem.

The SSI-Based Review System is built upon open standards for decentralized identifiers and verifiable credentials, making Interoperability a core feature. The use of standardized credential schemas ensures that the proof of experience or service issued by one provider is technically readable and verifiable by any other SSI-compliant application in the ecosystem. This ability for distinct, independent systems to understand and trust the same cryptographic proof without relying on a central intermediary is essential. It allows for the creation of a vast, interconnected market of service providers and reviewers, significantly enhancing system resilience and expanding the utility of the user's verified history.

6.8. Usability

Usability is a critical factor for adoption, and here the review system models present different trade-offs. A Traditional Review System typically offers a very high level of usability at the point of entry: the user accesses the platform, creates an account with a username and password, and immediately begins consuming services and leaving reviews. This familiarity with centralized login models ensures a minimal learning curve for the common user, prioritizing immediate access and ease of use.

The SSI-Based Review System, on the other hand, presents an initial usability challenge due to the introduction of new concepts. The user must first install a Digital Wallet to manage their credentials, learn how to receive a Proof of Experience or Service (VC), and understand how to selectively present it to an application to perform a review. While this setup process is more complex than a traditional login, it is a fundamental requirement for achieving security and data sovereignty. However, once the user is familiar with the wallet's operations, the process of proving an experience becomes quick and secure,

ensuring that long-term usability is optimized by the deep security and control the system provides.

6.9. Scalability

Scalability in a review context is not just about handling more users; it is also about the system's ability to expand its scope of operation and integrate with new offerings. A Traditional Review System is inherently capped in its service reach because its review capability is strictly limited by the specific set of products and services that the central platform provides and can internally verify. Its growth is confined to the market segment it controls. If a user wishes to review a product or service not available on that platform, the traditional system cannot scale to accommodate that interaction.

The SSI-Based Review System, by contrast, achieves a superior form of operational scalability. Because its foundation relies on cryptographically verified Verifiable Credentials (VCs)—the proofs of experience or service—its capacity to encompass new services is practically unlimited. The system can scale to cover any product or service in the world, provided only that the service provider issues a compliant VC upon interaction. Critically, this massive expansion in scope is achieved while maintaining the same confirmation integrity and security of the experience proof, since the burden of verification and data storage remains distributed across the network of users and VC issuers, not the central review service.

6.10. Conclusion

While traditional systems have dominated the online review landscape for years, the future may lie in a credential-based model for e-commerce. The core difference between the two is a shift from a system of trust built on a central authority to one built on cryptographic verification and user-owned data. Amazon has created a successful ecosystem, but it is fundamentally vulnerable to fraud and a lack of user control. A credential-based system offers a promising, more secure, and privacy-centric alternative for online shopping. By giving users ownership of their identity and data and using verifiable credentials to prove authentic purchasing experiences, this new model has the potential to redefine trust in the digital age.A summary of the core differences and their implications for each system is presented in Table 6.1.

Table 6.1: Comparison of E-commerce Review Systems

Section	**Traditional Review System (e.g., Amazon)**	**Credential-Based Review System**
Operating Principles of Review Systems	Integrated with the e-commerce store. Reviewer's identity is managed and owned by the platform, creating a "closed loop" and potential conflicts of interest.	A third-party service, separate from the point of sale. Users prove a genuine purchase with a Verifiable Credential (VC), ensuring authenticity without sharing personal data.
Core Principles & Use Cases	Typically adopted by established companies with existing user bases. The business strategy is to maintain a "walled garden" for full control.	Adopted by new entities or startups to build trust from scratch. Focuses on democratizing trust and creating an impartial, third-party authority.
Control & Governance	Top-down control model where a single entity makes decisions about user experience and content moderation. Power is centralized and can lead to misaligned incentives.	A decentralized trust model that separates the review process from the point of purchase. Ensures better governance and less manipulation from vendors.
Target Audience	Mainstream, non-technical audience. The goal is a frictionless user experience with a one-stop-shop for a wide variety of reviews.	Niche, quality-conscious audience with a forward-looking view on digital privacy. Success is measured by the integrity of the community.
Business Strategy	High barrier to entry, requiring a pre-existing user base. Monetization relies on leveraging a captive audience through advertising or data analytics.	Low barrier to entry, allowing new platforms to start from scratch. The business model is based on the value of verified data, not on user's personal information.
Use Cases & Limitations	Provides a vast volume of reviews with a familiar user experience. Primary limitation is continuous vulnerability to fraud and a lack of user autonomy.	Provides a secure, privacy-focused platform where users own their data. A key limitation is the early stage of technology adoption and challenges with moderation.

Table 6.1: Comparison of E-commerce Review Systems (continued)

Section	Traditional Review System (e.g., Amazon)	Credential-Based Review System
Login Systems & User Identity	Relies on traditional account-based login systems where user data is stored on a central server. This creates a single point of failure and vulnerability to data breaches.	Uses Self-Sovereign Identity (SSI) with a Decentralized Identifier (DID) and Verifiable Credentials (VCs). Users own their data, and it's never stored on a central server.
Security & Fraud Detection	Uses a top-down security model with AI and human oversight to combat fraud. The "Verified Purchase" badge is a key feature but is part of a constant, reactive battle.	Employs a cryptographic security model from the ground up. Each review requires a unique VC, making it nearly impossible to generate fake reviews at scale.
Portability	Review capabilities are strictly limited to interactions verified within the platform.	the proof of experience or service (VC) is portable, allowing users to review services both inside and outside the platform's scope.
Interoperability	Low. Restricted by proprietary data formats and closed APIs, creating data silos.	High. Built on open standards for seamless, trustless exchange and verification of credentials across the entire network of SSI-compliant applications.
Usability	High. Familiarity with centralized login and a low initial learning curve.	Initial challenge due to the requirement for a Digital Wallet and new processes, but optimized long-term by security and user control.
Scalability	Scope is capped by the platform's internal product/service offerings, limiting review capability to that closed market.	Scope is virtually unlimited; the system can scale to cover any service or product that issues a verifiable credential, maintaining verification integrity.

CHAPTER 7

Conclusion and Future Work

7.1. Conclusion

This thesis established a prototype for an e-commerce review system that uses decentralized solutions to enhance trust and combat fraud in online review environments through the use of Self-Sovereign Identity (SSI) principles and blockchain technology. The research addressed a gap in academic literature, as the application of SSI to online review systems remains largely unexplored. The core contribution lies in establishing a robust, decentralized foundation built on cryptographic verification and user-owned data that serves as a verifiable model for mitigating the prevalent issues of fake reviews, excessive centralization, and lack of user control found in traditional platforms.

By defining the roles of Issuers, Holders, and Verifiers within the SSI paradigm, the system ensures that reviews are authentic and verifiable while prioritizing user privacy and control over personal data. The prototype successfully validated the key concept of verifying credentials to prove service interaction. This mechanism makes it virtually impossible to generate fraudulent reviews at scale, as each review requires a unique Verifiable Credential (VC) from a genuine experience. Ultimately, the proposed design serves as a foundation for a transparent, secure, and user-centric review ecosystem, setting a new standard for trust and reputation management in the digital age.

7.2. Future Work

The implementation of this prototype provides a strong foundation for future research and development. To advance this work, the following areas should be explored:

- **Addressing Usability and User Experience**: The complexity of managing cryptographic keys and understanding SSI concepts can be a barrier for mainstream adoption. Future work should focus on developing a user-friendly interface that simplifies the management of digital wallets and credentials, making the technology as intuitive as the login systems used today.
- **Enhancing Security and Regulatory Compliance**: While the cryptographic design is highly resilient to fraud, its integrity depends on the trustworthiness of credential issuers. Future research should investigate more sophisticated mechanisms for verifying and ensuring the integrity of issuers. Additionally, as legal frameworks are still evolving, further study is needed to ensure full compliance with regulations like GDPR across different jurisdictions.

- **Interoperability Between Platforms**: The fragmented ecosystem of various DID methods and credential formats can create silos, hindering seamless interactions. Future work should explore standardization and integration points to ensure the system can interoperate with other decentralized identity implementations, fostering a more connected and universal web of trust.

Bibliography

[1] E. Chang, F. K. Hussain, and T. Dillon, "Ccci metrics for the measurement of quality of e-service," *Proceedings of the 2005 IEEE/WIC/ACM International Conference on Intelligent Agent Technology*, 2005.

[2] A. S. adn Anushka Subedi and M. Nowostawski, "A framework for online document verification using self-sovereign identity technology," *Sensors*, 2022.

[3] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, *Decentralized identifiers (dids) v1.0*, 2025-03-20, 2022. [Online]. Available: `https://www.w3.org/TR/did-1.0/`.

[4] M. Sporny, D. Longley, D. Chadwick, and I. Herman, *Verifiable credentials data model v2.0*, 2025-03-20, 2025. [Online]. Available: `https://www.w3.org/TR/did-1.0/`.

[5] A. D. Salve, D. D. F. Maesa, P. Mori, L. Ricci, and A. Puccia, "A multi-layer trust framework for self sovereign identity on blockchain," *Online Social Networks and Media*, 2023.

[6] A. Y. Doifode, M. S. D. Mali, D. T. S. Rao, *et al.*, "Online reviews system using aspect based sentimental analysis opinion mining," *International Journal on Recent and Innovation Trends in Computing and Communication*, vol. 11, no. 7, pp. 381–385, 2023.

[7] J. POÓR and G. HORVÁTH, "E-wom on the online booking interfaces – a comparative analysis of the online travel agencies' guest review systems," *THE CENTRAL EUROPEAN JOURNAL OF REGIONAL DEVELOPMENT AND TOURISM*, vol. 13, no. 1, pp. 58–73, 2021.

[8] D. P. Adane, M. A. Jadhav, M. S. Kodgire, M. A. Agrawal, and M. S. Kumar, "Integration of self sovereign identity in security systems," *International Journal of Next-Generation Computing*, vol. 12, no. 5, 2021.

[9] K. Peffers, T. Tuunanen, M. A. Rothenberger, and S. Chatterjee, "The design science research process: A model for producing and presenting information systems research," *arxiv*, 2006.

[10] Y. YASUNO, R. TATEISHI, R. SHIROISHI, and S. HOSONO, "A trustworthy architecture for web3 service," *Journal of Advanced Mechanical Design, Systems, and Manufacturing*, vol. 18, no. 7, 2024.

[11] D. H. Hardman, *Vc triangle of trust*, Accessed: 2025-05-08, 2019. [Online]. Available: `https://commons.wikimedia.org/wiki/File:VC_triangle_of_Trust.svg`.

[12] L. Cocco and R. Tonelli, "A self-sovereign identity–blockchain-based model proposal for deep digital transformation in the healthcare sector," *Future Internet*, 2024.

[13] C. H.-J.Braun, V. Papanchev, and T. Käfer, "Sissi: An architecture for semantic interoperable self-sovereign identity-based access control on the web," *The ACM Web Conference*, 2023.

[14] F. Buccafurri, A. L. Canino, V. D. Angelis, A. Laurenda, and G. Lax, "An ssi-based solution to support lawful interception," *Appl. Sci*, 2025.

[15] D. Naicker and M. Moodley, "Challenges of user data privacy in self-sovereign identity verifiable credentials for autonomous building access during the covid-19 pandemic," *Front. Blockchain*, 2024.

[16] J. LUÍS, J. SANTOS, T. R. DIAS, and M. P. CORREIA, "Real estate documentation authentication with blockchain and self-sovereign identity," *ACM Trans. Graph.*, vol. 37, no. 4, 2024.

[17] H. SAIDI, N. LABRAOUI, A. A. A. ARI, L. A. MAGLARAS, and J. H. M. EMATI, "Dsmac: Privacy-aware decentralized self-management of data access control based on blockchain for health data," *IEEE SYSTEMS, MAN AND CYBERNETICS SOCIETY SECTION*, 2024.

[18] E. Samir, H. Wu, M. Azab, C. Xin, and Q. Zhang, "Dt-ssim: A decentralized trustworthy self-sovereign identity management framework," *IEEE INTERNET OF THINGS JOURNAL*, vol. 9, no. 11, pp. 7972–7988, 2022.

[19] M. Tcholakian, K. Gorna, M. Laurent, H. K. B. Ayed, and M. Naghmouchi, "Self-sovereign identity for consented and content-based access to medical records using blockchain," *Hindawi Security and Communication Networks*, 2023.

[20] W. Song, R. N. Zaeem, D. Liau, *et al.*, "Self-sovereign identity and user control for privacy-preserving contact tracing," *Association for Computing Machinery*, 2021.

[21] K. W. CHO, B.-G. JEONG, and S. U. SHIN, "Verifiable credential proof generation and verification model for decentralized ssi-based credit scoring data," *The Institute of Electronics, Information and Communication Engineer*, 2021.

[22] L. Cocco and R. Tonelli, "Digital transformation in the construction sector: Blockchain, bim and ssi for a more sustainable and transparent system," *Future Internet*, 2024.

[23] E. Tan, E. Lerouge, J. D. Caju, and D. D. Seuil, "Verification of education credentials on european blockchain services infrastructure (ebsi): Action research in a cross-border use case between belgium and italy," *Big Data and Cognitive Computing*, 2023.

[24] F. Khadeer, H. E. Chang, and T. S. Dillon, "Towards defining an ontology for reputation," *IEEE International Conference on Systems, Man and Cybernetics*, 2005.

[25] X. Liang, X. Li, R. Lu, X. Lin, and X. (Shen, "Seer: A secure and efficient service review system for service-oriented mobile social networks," *IEEE International Conference on Distributed Computing Systems*, 2012.

[26] C. Niu, H. Luo, M. Fan, and R. Shen, "On feedback similarity measurement in web of trust," *Global Congress on Intelligent Systems*, 2009.

[27] C. Lee and J. Huh, "Web site trust evaluation as cognitive information processing and the moderating role of involvement and knowledge," *International Journal of Internet Marketing and Advertising*, vol. 6, no. 2, pp. 258–260, 2010.

[28] Y. A. Kim and R. Phalak, "A trust prediction framework in rating-based experience sharing social networks without a web of trust," *Information Sciences*, 2012.

[29] M. J. Page, J. E. McKenzie, P. M. Bossuyt, *et al.*, "The prisma 2020 statement: An updated guideline for reporting systematic reviews," *Journal of Clinical Epidemiology*, pp. 178–189, 2021.

[30] "Privado id: Building unified identity." (), [Online]. Available: `https://www.privado.id/` (visited on 09/19/2025).

[31] "Alchemy: The web3 development platform." (), [Online]. Available: `https://www.alchemy.com/` (visited on 09/19/2025).

[32] "Html." (), [Online]. Available: `https://developer.mozilla.org/en-US/docs/Web/HTML` (visited on 09/19/2025).

[33] "Javascript." (), [Online]. Available: `https://developer.mozilla.org/en-US/docs/Web/JavaScript` (visited on 09/19/2025).

[34] "Node.js." (), [Online]. Available: `https://nodejs.org/` (visited on 09/19/2025).

[35] "Ngrok." (), [Online]. Available: `https://ngrok.com/` (visited on 09/19/2025).