

Ziraai SSI: A Blockchain-Based Self-Sovereign Identity Model for Agricultural Supply Chains

Tariq Alar^{1*}, Gnana Bharathy², Usha Batra³, Mukesh Prasad⁴

Department of Computer Sciences-College of Engineering and Computer Sciences, Jazan University, Jazan, Saudi Arabia¹

School of Computer Science, University of Technology Sydney, Sydney, NSW, Australia^{1,2,4}

University of Technology Sydney, Sydney, NSW, Australia³

Skill Department of CS & IT-Faculty of Engineering & Technology, Shri Vishwakarma Skill University, Palwal, India³

Abstract—The agricultural supply chain plays a critical role in ensuring food security and sustainability; however, it continues to face challenges related to data fragmentation, limited transparency, and insufficient trust among participating stakeholders. Existing supply chain systems are primarily based on centralized identity and data management models, which introduce single points of failure, restrict auditability, and raise privacy concerns. More critically, the absence of decentralized and stakeholder-controlled identity mechanisms limits accountability and verifiable governance across agricultural ecosystems. In this work, we present Ziraai SSI, a blockchain-based self-sovereign identity (SSI) prototype designed to support identity-centric governance and trust establishment in agricultural supply chains. The proposed approach integrates blockchain-based trust anchoring with self-sovereign identity principles using decentralized identifiers (DIDs) and verifiable credentials (VCs). Through this integration, stakeholders retain direct control over their digital identities while enabling cryptographically verifiable and privacy-preserving interactions across organizational boundaries. The system architecture follows a multi-layered design that addresses identity management, credential lifecycle handling, authentication, access control, and governance. To move beyond conceptual analysis, the framework is realized as a functional research prototype using standardized SSI technologies and an agent-based architecture. The implemented system supports end-to-end credential workflows, including secure connection establishment, credential issuance, selective disclosure, and proof-based verification, without reliance on centralized identity providers or authentication authorities. Experimental validation conducted in a controlled environment confirms correct execution of identity and credential lifecycles, decentralized authentication, and privacy-preserving verification. The evaluation focuses on functional validation within a controlled prototype environment and does not include large-scale scalability benchmarking. These results demonstrate the feasibility of identity-centric governance mechanisms in agricultural supply chains using standardized SSI technologies.

Keywords—Blockchain; self-sovereign identity (ssi); agricultural supply chain; verifiable credentials; decentralized identity; privacy-preserving authentication

I. INTRODUCTION

The agricultural supply chain (ASC) plays a fundamental role in global food systems by linking producers, processors, distributors, and consumers through a sequence of interdependent activities that ensure food availability, quality, and safety. Despite its critical importance, the ASC continues to

face persistent challenges related to traceability, data integrity, and trust among participating entities [1]. In practice, these challenges are exacerbated by fragmented information flows and limited mechanisms for independently verifying stakeholder actions across organizational boundaries. Traditional supply chain management systems, which are predominantly centralized and fragmented, often fail to provide end-to-end visibility, thereby limiting the ability to verify product authenticity and ensure compliance with quality and safety standards. Moreover, information asymmetry and data silos across stakeholders significantly hinder transparency and impede effective coordination throughout production, logistics, and distribution stages [2].

Issues related to identity verification and data authenticity are particularly pronounced in agricultural supply chains. Farmers, cooperatives, logistics providers, and certification bodies often rely on third-party intermediaries for authentication, certification, and market access. While such intermediaries simplify coordination, they also concentrate trust and control within centralized entities, increasing operational overhead and introducing privacy and accountability risks. Consequently, the absence of a unified, tamper-resistant, and stakeholder-centric identity mechanism represents a major barrier to the development of transparent, equitable, and verifiable agricultural value chains [3]. These traceability failures and certification disputes in agri-food systems further highlight that transparency without verifiable stakeholder identity remains insufficient for ensuring accountability and timely dispute resolution [4], [5].

Blockchain technology has been widely recognized as a promising approach to addressing several of these challenges. By maintaining a distributed, immutable ledger of transactions, blockchain enables auditability, data integrity, and tamper-resistance without requiring centralized control [6]. However, blockchain-based transparency alone does not guarantee trust if the identities of participating entities cannot be reliably verified or held accountable [7]. In parallel, Self-Sovereign Identity (SSI) has emerged as a paradigm in digital identity management that enables individuals and organizations to create, own, and manage their digital identities independently of centralized authorities. SSI systems rely on decentralized identifiers (DIDs) and verifiable credentials (VCs) to support cryptographically verifiable and selectively disclosable identity assertions [8]. The convergence of blockchain and SSI technologies, therefore, offers a complementary mechanism for managing both

*Corresponding author.

transactional data and stakeholder identities in a decentralized and verifiable manner.

Within agricultural supply chains, such an integration has the potential to empower stakeholders, particularly smallholder farmers, by granting them direct control over their digital identities and credentials, while simultaneously enabling verifiable, privacy-preserving data exchange across the supply chain [9]. Prior research has demonstrated the applicability of blockchain for enhancing traceability and transparency in agri-food logistics [10], [11]. Nevertheless, most existing solutions emphasize product-centric traceability and transactional logging, with limited attention to decentralized identity management, stakeholder authentication, and governance. Similarly, although SSI frameworks have been extensively explored in domains such as finance, healthcare, and education [12], their systematic application to agricultural supply chains remains comparatively underexplored. Beyond theoretical promise, the effective adoption of blockchain-enabled SSI solutions in agriculture requires practical validation through implemented systems that demonstrate real operational workflows [5],[13]. Without such validation, proposed frameworks risk remaining abstract and disconnected from deployment-level considerations, including identity lifecycle management, credential exchange, user consent, and interoperability among heterogeneous stakeholders.

Motivated by this research gap, this study not only proposes a blockchain-based self-sovereign identity framework but also realizes the proposed design through a functional research prototype, referred to as Ziraai SSI. The implemented system operationalizes decentralized identifiers, verifiable credentials, and privacy-preserving authentication mechanisms using agent-based SSI technologies. As a result, farmers, issuers, and verifiers can interact through secure, standards-compliant credential workflows without relying on centralized identity providers. Accordingly, this work addresses the limitations of existing approaches by developing a blockchain-based self-sovereign identity framework tailored to agricultural supply chains. The framework leverages blockchain-based trust anchoring to ensure data integrity and auditability, while SSI principles aim to decentralize identity control and authentication. The main contributions of this study are summarized as follows:

- The design of a multi-layered blockchain–SSI framework that explicitly centers on stakeholder identity, authentication, and governance within agricultural supply chains.
- The formulation of a credential lifecycle mechanism encompassing issuance, selective disclosure, verification, and governance processes aligned with agricultural traceability requirements.
- The practical implementation and validation of the proposed framework, through the Ziraai SSI research prototype, demonstrate end-to-end decentralized identity and credential management for agricultural stakeholders.
- A prototype-level evaluation emphasizing functional feasibility and security-property realization within a controlled environment.

The remainder of this study is organized as follows. Section II reviews related work on blockchain- and SSI-based approaches in supply chain contexts and identifies key research gaps. Section III presents the proposed Blockchain-Based SSI framework and its architectural components. Section IV describes the system design and implementation details of the Ziraai SSI prototype. Section V discusses the experimental results and validation outcomes. Finally, Section VI concludes the study and outlines directions for future research.

II. RELATED WORK AND MOTIVATION

The agricultural supply chain (ASC) has historically relied on centralized information systems for data management, certification, and identity verification. Siloed databases, manual record-keeping processes, and limited interoperability across organizational boundaries are typically characteristic of such systems. As a consequence, trust is often established procedurally rather than cryptographically, making verification dependent on institutional authority rather than on independently verifiable evidence. These limitations expose agricultural ecosystems to data inconsistencies, unauthorized modifications, and operational inefficiencies, ultimately undermining trust among supply chain participants [1]. In particular, the absence of a unified, verifiable digital identity framework for stakeholders—such as farmers, processors, distributors, and regulators—amplifies risks of fraud, accountability gaps, and asymmetric information sharing within agricultural ecosystems.

A. Traditional Traceability and Identity Systems

Conventional agricultural traceability mechanisms have primarily relied on study-based documentation or centralized databases that record transactions at isolated points in the supply chain [14]. While these approaches provide some oversight, they lack real-time synchronization and are vulnerable to data loss, manipulation, and delayed verification. In centralized architectures, trust is concentrated in a single authority, creating single points of failure and increasing exposure to security breaches and unauthorized access [15]. From a governance perspective, such architectures also constrain independent auditing, as verification processes remain tightly coupled with the system operator.

Efforts to digitalize agricultural operations—through enterprise resource planning (ERP) systems, cloud-based farm management platforms, and centralized certification portals—have partially addressed traceability concerns. However, these systems often suffer from limited interoperability and opaque auditing mechanisms, leading to fragmented data ownership and asymmetric access to information [16]. Moreover, identity verification within these platforms typically relies on username–password credentials or centralized authentication services, which provide limited assurance regarding the real-world legitimacy of participating entities and introduce risks related to credential compromise, privacy leakage, and misuse of personal data [17].

B. Blockchain for Agricultural Traceability

Blockchain technology has emerged as a promising approach for enhancing transparency and integrity in supply chain systems by enabling distributed, immutable record-

keeping among mutually untrusted entities. Numerous studies have explored blockchain-based approaches for improving agricultural traceability, food safety, and quality assurance. For example, Kamble et al. [6] proposed a blockchain-enabled model to enhance provenance tracking and operational efficiency in agricultural supply chains, while Feng et al. [3] demonstrated the potential of smart contracts for automating quality assurance processes. Zhao et al. [9] provided a comprehensive synthesis of blockchain applications in agri-food value chains, highlighting improvements in accountability and auditability.

Despite these advances, blockchain-based agricultural systems frequently treat identity as an implicit or external assumption rather than as a first-class design concern. In many implementations, identity verification is either delegated to centralized authorities or represented through application-specific identifiers that lack cryptographic portability across systems. It weakens the overall trust model, as the integrity of on-chain data ultimately depends on the authenticity and accountability of off-chain actors who generate it [11].

C. Evolution of Self-Sovereign Identity (SSI)

Self-Sovereign Identity (SSI) represents a paradigm shift in digital identity management by emphasizing user autonomy, decentralization, and privacy preservation [18]. SSI frameworks are built on decentralized identifiers (DIDs) and verifiable credentials (VCs), enabling individuals and organizations to control their identity attributes and selectively disclose information without relying on centralized identity providers [19]. A defining characteristic of SSI systems is privacy by design, in which sensitive identity data remains under the control of the credential holder and is shared only via cryptographically verifiable proofs [20].

SSI has gained significant traction in domains where trust, privacy, and regulatory compliance are paramount, including finance, healthcare, and education [21]. In contrast, its application within agricultural supply chains remains comparatively limited [13]. This gap is particularly notable given the multi-actor, cross-organizational, and trust-fragmented nature of agricultural ecosystems, where stakeholders often lack shared identity infrastructure or centralized governance mechanisms [22].

D. Combining Blockchain and SSI for Secure Supply Chains

The integration of blockchain and SSI technologies offers complementary benefits for building decentralized trust infrastructures. Blockchain provides immutability, transparency, and distributed consensus, while SSI enables user-centric identity ownership and selective credential disclosure [23]. Together, these technologies support identity-aware trust architectures in which entities can interact securely without dependence on centralized intermediaries.

Several studies have examined partial integrations of blockchain and SSI across different application domains. Shehu

et al. [24] discussed the role of SSI in enabling interoperable and verifiable identity ecosystems when combined with distributed ledgers. Khoualdi et al. [25] investigated the challenges associated with integrating SSI, IoT, and blockchain for traceability applications, identifying scalability and standardization as key obstacles. Ahmed et al. [26] further emphasized the potential of blockchain-based identity management to enhance transparency and governance in future supply chains. However, most existing works remain limited to architectural discussions or small-scale experimental demonstrations. In particular, they provide limited insight into complete system realization, end-to-end credential workflows, and implementation-level validation within agricultural environments [27].

E. Research Gaps and Motivation

Based on the reviewed literature, several research gaps can be identified:

- Limited integration of decentralized identity mechanisms within agricultural blockchain systems, with most solutions focusing primarily on transactional traceability.
- Insufficient empirical validation of SSI-based approaches in agricultural contexts, despite their demonstrated applicability in other regulated domains.
- Lack of identity-centric governance models capable of supporting heterogeneous stakeholders without centralized control.
- Scarcity of implementation-level studies demonstrating complete issuer–holder–verifier workflows using standardized SSI protocols.

Notably, there is a lack of research demonstrating a complete and operational SSI-based agricultural identity system that explicitly supports issuer, holder, and verifier roles using standardized SSI protocols and evaluates these interactions through implemented, end-to-end workflows. As a result, much of the existing literature remains either conceptual or limited to partial demonstrations that do not fully address identity lifecycle management and governance requirements. This gap motivates the design and implementation of Ziraai SSI as an identity-centric, standards-compliant prototype tailored specifically to agricultural supply chain governance. To further clarify the positioning of the proposed approach, Table I provides a comparative analysis of Ziraai SSI against representative categories of existing agricultural traceability systems, blockchain-based solutions, and SSI frameworks. The comparison highlights that most existing approaches either focus on transactional traceability without decentralized identity support or explore SSI concepts without domain-specific, implementation-level validation. In contrast, Ziraai SSI integrates blockchain-based trust anchoring with self-sovereign identity mechanisms, delivering a functional research prototype that supports complete, end-to-end credential workflows in an agricultural context.

TABLE. I. COMPARISON OF ZIRAAI SSI WITH EXISTING BLOCKCHAIN- AND SSI-BASED APPROACHES

Approach Category	Blockchain	SSI	DID	VC	Selective Disclosure	Prototype
Conventional agricultural traceability systems	x	x	x	x	x	✓
Blockchain-based agricultural traceability	✓	x	x	x	x	Partial
SSI frameworks (non-agricultural domains)	x	✓	✓	✓	✓	✓
Blockchain-SSI conceptual models for supply chains	✓	✓	✓	✓	✓	x
Ziraa'i SSI (this work)	✓	✓	✓	✓	✓	✓

While decentralized systems improve transparency and privacy, they require more coordination between participating organizations and can be more complex to deploy than centralized identity systems. Scalability and secure wallet key management are also important practical considerations in real-world implementations [28].

III. PROPOSED BLOCKCHAIN-BASED SSI FRAMEWORK FOR AGRICULTURE

This section presents the conceptual and architectural design of the proposed blockchain-based self-sovereign identity (SSI) framework for agricultural supply chains. The framework is intended to address persistent challenges related to stakeholder authentication, data integrity, transparency, and trust in decentralized agricultural ecosystems. Rather than treating identity as a supporting component of traceability, the proposed framework positions identity as a foundational element of supply chain governance. By combining blockchain-based trust anchoring with SSI principles, the framework establishes a generalizable model for identity-centric supply chain interactions that is independent of specific implementation technologies. While the framework is presented at an abstract level to ensure reusability across different agricultural contexts, its design is explicitly informed by practical deployment considerations, and it directly guides the concrete realization described in Section IV.

A. Design Objectives

The design of the proposed blockchain-based self-sovereign identity (SSI) framework is guided by a set of objectives derived from the structural characteristics, trust relationships, and governance requirements of agricultural supply chains. These objectives aim to address limitations observed in existing centralized and semi-decentralized identity and traceability systems, while ensuring compatibility with standardized SSI

ecosystems. The following design objectives therefore guide the framework:

- **Decentralized Identity Control:** Empower agricultural stakeholders to manage their own digital identities using decentralized identifiers (DIDs) and verifiable credentials (VCs), without reliance on centralized identity or certification authorities. This objective reflects the need for stakeholder autonomy and for identity to be long-term portable across organizational and institutional boundaries [29].
- **Tamper-Resistant Identity and Data Management:** Ensure that identity-related metadata, credential schemas, and verification artifacts are anchored on a decentralized ledger, providing integrity, authenticity, and accountability for identity-linked interactions without dependence on mutable centralized databases or trusted third parties.
- **Privacy and Selective Disclosure:** Enable entities to disclose only the minimum necessary identity attributes during verification processes through selective disclosure mechanisms and cryptographic proof-based credential presentation. This objective is particularly critical in agricultural contexts, where stakeholders may be reluctant to share sensitive personal or organizational information [30].
- **Transparency and Auditability:** Provide stakeholders and oversight entities with verifiable and independently auditable identity-related records, while ensuring that sensitive credentials and personal information remain under the exclusive control of their respective holders [25].
- **Scalability and Interoperability:** Support integration with existing agricultural platforms and interoperability with consortium-based or multi-network identity infrastructures. This ensures that the framework can adapt to heterogeneous deployment environments and evolving governance models [20].

Together, these objectives define the conceptual scope of the proposed framework and guide the architectural and implementation choices discussed in subsequent sections.

B. Framework Overview

The proposed framework adopts a multi-layered architectural design that separates identity management, authentication, access control, data interaction, and governance concerns. This separation of concerns enables modularity and extensibility, allowing individual layers to evolve independently while preserving cryptographic trust guarantees across the system. Within this framework, blockchain technology is employed primarily as a decentralized trust anchor rather than as a general-purpose transaction execution platform. Specifically, the blockchain component anchors decentralized identifiers (DIDs), credential schemas, credential definitions, and governance-related metadata, enabling verifiable identity resolution and long-term auditability. This design deliberately avoids unnecessary on-chain transaction overhead while retaining tamper resistance for identity-critical information. The

framework is structured into five logical layers that collectively support secure, privacy-preserving interactions in the agricultural supply chain. Each layer addresses a distinct functional responsibility, ranging from stakeholder identity representation to governance and trust management.

C. Layer 1 – Stakeholder Identity and Credential Layer

This foundational layer defines how digital identities are created, represented, and managed within the agricultural supply chain.

- Each stakeholder (e.g., farmer, cooperative, distributor, certification authority, regulator) is associated with a decentralized identifier (DID) compliant with W3C standards.
- Authorized entities issue verifiable credentials (VCs) that attest to stakeholder attributes, certifications, or roles.
- The holder controls the credentials and can present them selectively for verification.
- Credential revocation and status information are conceptually supported by publicly verifiable registries, enabling detection of expired or invalid credentials.

By decoupling identity ownership from centralized authorities, this layer establishes accountability while preserving stakeholder autonomy.

D. Layer 2 – Data Recording and Verification Layer

This layer governs how supply-chain events and identity-linked actions are recorded and verified.

- All interactions are cryptographically bound to verified identities.
- Data submissions are accepted only after successful credential validation.
- Immutable records enable retrospective auditing and compliance verification.

Rather than prioritizing transaction throughput, this layer emphasizes the integrity and authenticity of identity-bound data, which is particularly critical in agricultural governance and certification scenarios.

E. Layer 3 – Trust and Authentication Layer

The trust and authentication layer ensures that all interactions occur between verified participants.

- Mutual authentication is performed using cryptographic proofs derived from DIDs and VCs.
- Selective disclosure mechanisms enable attribute-level verification without revealing full credentials.
- Authentication policies prevent unauthorized access to identity-protected resources.

This layer enables privacy-preserving trust establishment across heterogeneous agricultural stakeholders without requiring shared identity infrastructure.

F. Layer 4 – Access Control and Policy Layer

This layer defines how access permissions and disclosure policies are enforced.

- Access control decisions are based on credential attributes rather than static roles.
- Stakeholders retain control over what data is shared, with whom, and under what conditions.
- Policy enforcement is auditable and aligned with regulatory requirements.

By decoupling identity from application-specific logic, this layer supports flexible and context-aware governance models.

G. Layer 5 – Governance and Consensus Layer

The governance layer defines the rules under which identities and credentials are recognized as trustworthy.

- Credential schemas and issuer policies are governed collectively.
- Regulatory authorities can participate as oversight entities without assuming centralized control.
- Trust anchors ensure long-term verifiability of identity claims.

This layer enables institutional trust without centralization, which is a key requirement in multi-stakeholder agricultural ecosystems. In the current prototype, governance follows a consortium-based trust model in which authorized issuers are pre-approved before registering credential schemas on the ledger. Schema registration requires prior agreement among consortium participants before activation. Disputes related to credential validity are addressed through revocation registry updates and publicly verifiable status checks. Formal on-chain voting or automated consensus mechanisms were not implemented in this prototype; however, the architecture allows such mechanisms to be incorporated in future extensions.

H. Framework Workflow

At a conceptual level, the framework supports the following workflow:

- Stakeholder identity establishment through decentralized identifiers (DIDs)
- Credential issuance by authorized entities
- Identity-bound data interaction across supply chain stages.
- Selective disclosure and cryptographic verification.
- Auditability and compliance validation.

This abstract workflow directly informs the concrete realization described in Section IV.

I. Security Considerations

The proposed framework addresses core security requirements, including integrity, authentication, confidentiality, non-repudiation, and unlinkability, through cryptographic identity mechanisms rather than centralized

enforcement. These properties are derived from decentralized identifiers, verifiable credentials, and proof-based authentication, ensuring distributed trust, resilience to compromise, and reduced reliance on centralized authorities.

IV. SYSTEM DESIGN AND IMPLEMENTATION DETAILS

This section describes the practical realization of the proposed blockchain-based self-sovereign identity framework through the Ziraai SSI research prototype. In contrast to the conceptual focus of Section III, this section details how the framework is instantiated using standardized self-sovereign identity technologies, thereby validating its feasibility under realistic interaction and governance assumptions. The implementation is intentionally designed as a research prototype and prioritizes standards compliance, architectural traceability, and workflow correctness over production-scale optimization.

A. Implementation Environment

The Ziraai SSI platform is implemented using an agent-based SSI architecture aligned with current industry and standards-body specifications. The selected implementation environment reflects explicit design decisions motivated by interoperability, modularity, and alignment with widely adopted SSI ecosystems.

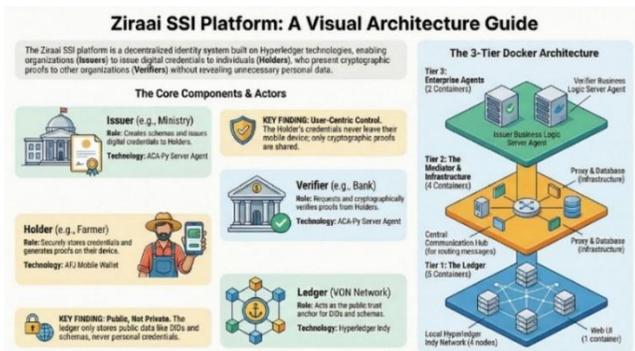


Fig. 1. Ziraai SSI Platform visual architecture.

- Identity ledger: Hyperledger Indy (local development network), used exclusively as a decentralized trust anchor for DIDs, credential schemas, and definitions
- SSI framework: Hyperledger Aries, implemented through ACA-Py agents and Aries-compatible wallets
- Communication protocol: DIDComm, enabling secure, peer-to-peer agent communication
- User interfaces: Web-based dashboards for issuer and verifier roles, and a mobile wallet application for farmers and credential holders
- Deployment: Containerized microservices orchestrated using Docker to support modular experimentation and reproducibility

The choice of Hyperledger Indy and Aries enables strict separation between identity anchoring, credential exchange, and application logic, which is essential for evaluating identity-centric architectures. Fig. 1 provides a visual architecture of the Ziraai SSI platform.

B. System Architecture and Modules

The system architecture mirrors the layered framework described in Section III while introducing concrete implementation components.

- SSI agents implement identity and credential logic for each stakeholder.
- Application controllers mediate interactions between user interfaces and agents.
- Wallet components provide secure credential storage and user-controlled disclosure.
- Verification services enable proof validation and audit support.

Each implementation module maps directly to a corresponding conceptual layer of the proposed framework, ensuring architectural consistency and traceability between design intent and system realization. Fig. 2 shows the architecture of the Ziraai SSI platform and the modules.

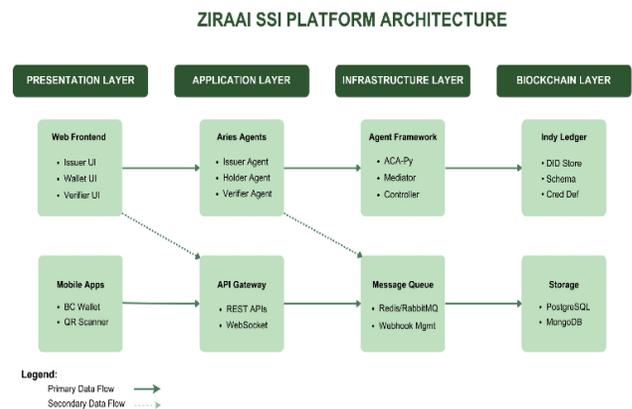


Fig. 2. Architecture and layers of the Ziraai SSI platform.

C. SSI Credential Lifecycle and Workflow

Ziraai SSI implements a complete SSI credential lifecycle consistent with standardized SSI protocols.

- Secure connection establishment using agent-mediated invitations
- Credential issuance with explicit holder consent
- Credential storage within a holder-controlled wallet
- Privacy-preserving credential verification through selective disclosure

The issuance and verification processes follow established SSI interaction patterns, ensuring compatibility with external SSI agents and minimizing reliance on application-specific extensions. The sequence of interactions shown in Fig. 3 demonstrates how issuer, holder, and verifier roles collaborate through standardized SSI protocols to support an end-to-end, trust-preserving credential lifecycle.



Fig. 3. Modules of the Ziraai SSI platform.

1) *Credential issuance workflow*: The process of issuing a verifiable credential (VC) involves the farmer (Holder), the issuer, and their respective agents as specified in Algorithm 1.

Algorithm 1: Credential Issuance

1. Issuer Admin (Web UI): Clicks "Create Invitation".
2. Issuer Controller: Calls ACA-Py agent to create a connection invitation.
3. Issuer Agent: Generates invitation and returns it.
4. Issuer Controller: Displays invitation as a QR code on the UI.
5. Farmer (Wallet): Scans the QR code.
6. Wallet Agent: Sends a connection request to the Issuer Agent.
7. Issuer Agent: Responds with a connection-response. Connection is now 'active'.
8. Issuer Admin (Web UI): Selects the active connection and fills out the credential details.
9. Issuer Controller: Calls ACA-Py agent to send a credential offer.
10. Issuer Agent: Sends the credential offer to the Wallet Agent.
11. Farmer (Wallet): Accepts the offer.
12. Wallet Agent: Sends a credential-request to the Issuer Agent.
13. Issuer Agent: Issues the signed credential and sends the issue-credential message.
14. Wallet Agent: Receives and stores the credentials securely.
15. Farmer (Wallet): Receives a notification that the credential has been stored.

2) *Credential verification workflow*: The process of verifying a credential involves the farmer (Holder), the Verifier, and their agents, as given in Algorithm 2.

Algorithm 2: Verification Flow

1. Verifier Admin (Web UI): Clicks "Create Proof Request Invitation".
2. Verifier Controller: Calls its ACA-Py agent to create a connection invitation.

3. Farmer (Wallet): Scans the QR code to establish a connection
4. Verifier Admin (Web UI): Selects the active connection and initiates a proof request.
5. Verifier Controller: Calls its ACA-Py agent to send a proof request.
6. Verifier Agent: Sends the proof-request to the Wallet Agent, specifying the required attributes.
7. Farmer (Wallet): Is prompted to share the requested information. The wallet automatically finds the required credentials.
8. Farmer (Wallet): Consents to sharing.
9. Wallet Agent: Generates a zero-knowledge proof and sends the present proof message.
10. Verifier Agent: Receives the proof and cryptographically verifies it against the public information on the Indy ledger.
11. Verifier Agent: If verification is successful, it notifies the Verifier Controller.
12. Verifier Admin (Web UI): Sees the verification result updated on the dashboard.

D. Agent-based Communication and Authentication

All interactions within the Ziraai SSI system use peer-to-peer agent communication.

- Pairwise decentralized identifiers are used for each bilateral relationship, preventing identifier reuse across contexts.
- Encrypted DIDComm messaging ensures the confidentiality and integrity of exchanged messages.
- Authentication is achieved through cryptographic proof of DID control rather than password-based or centralized mechanisms.

This communication model demonstrates the feasibility of decentralized, identity-bound authentication in agricultural supply chain environments, where centralized identity infrastructure is often unavailable or impractical.

E. Security and Privacy Mechanisms

The Ziraai SSI prototype enforces security and privacy guarantees through cryptographic identity primitives and agent-mediated protocols.

- Credential integrity and authenticity are ensured through digitally signed verifiable credentials.
- Authentication relies on cryptographic proof of control over decentralized identifiers.
- Privacy preservation is achieved through selective disclosure and proof-based verification.
- Pairwise decentralized identifiers mitigate correlation across interactions.

Private keys and credentials are stored within secure wallet environments under the exclusive control of credential holders, minimizing centralized aggregation of sensitive identity data and reducing systemic risk. Table II summarizes the security properties and how they are achieved in the Ziraai SSI platform.

TABLE. II. SECURITY PROPERTIES AND THEIR IMPLEMENTATION IN ZIRAAI SSI

Security Property	Implementation Mechanism in Ziraai SSI
Integrity	Digitally signed verifiable credentials
Authentication	DID-based cryptographic proof of control
Privacy	Selective disclosure via attribute proofs
Confidentiality	Encrypted DIDComm messaging
Non-repudiation	Identity-bound credential issuance
Unlinkability	Pairwise decentralized identifiers

F. Implementation Scope and Limitations

The Ziraai SSI system is implemented as a research prototype intended to validate architectural design choices and demonstrate the functional feasibility of blockchain-enabled self-sovereign identity in agricultural supply chains. Accordingly, the implementation prioritizes correctness, transparency, and standards alignment over performance optimization or large-scale deployment.

Several limitations are acknowledged. First, the prototype is evaluated in a controlled environment. It does not include large-scale ledger deployment or stress testing, which limits conclusions regarding scalability and throughput under real-world workloads. Second, while the underlying SSI infrastructure supports credential revocation, recovery, and status management, these capabilities are not fully exposed through user-facing interfaces in the current implementation. Third, user interface design is intentionally minimal and may require further refinement to support adoption by non-technical stakeholders. These limitations are inherent to the scope of a research prototype and serve to identify concrete directions for future enhancement rather than deficiencies in the proposed framework.

V. RESULTS AND DISCUSSION

This section presents the results of implementing and evaluating the proposed blockchain-based self-sovereign identity framework using the Ziraai SSI research prototype. The discussion focuses on functional validation, security and privacy behavior, and governance implications, rather than performance benchmarking, in alignment with the identity-centric role of the proposed system within agricultural supply chains.

A. Evaluation Objectives and Metrics

The primary objectives of the evaluation were as follows:

- To verify the feasibility of implementing decentralized identity and credential management for agricultural stakeholders using standardized SSI technologies.
- To validate end-to-end identity and credential workflows, including identity creation, credential issuance, storage, and privacy-preserving verification.
- To assess how the implemented system improves transparency, trust, and privacy compared with conventional centralized identity management approaches commonly used in agricultural supply chains.

The evaluation deliberately emphasizes functional correctness, interaction completeness, and security behavior, rather than throughput- or latency-oriented performance metrics. This choice reflects the governance-oriented nature of identity systems, where correctness and trust guarantees are often more critical than raw performance.

B. Practical Workflow Validation

The Ziraai SSI prototype was evaluated through a series of end-to-end workflow executions involving issuer, holder (farmer), and verifier roles, as described in Section IV.

- Identity creation: Each stakeholder successfully generated a decentralized identifier (DID) and established secure, pairwise connections using agent-based communication. It validated correct DID generation, key binding, and mutual authentication without reliance on centralized identity services.
- Credential issuance: Authorized issuers issued verifiable credentials following consent-driven workflows. Credentials were securely transmitted and stored in holder-controlled wallets, confirming the correct execution of issuance protocols and the preservation of holder autonomy.
- Credential verification: Verifiers issued proof requests specifying required attributes. Holders responded using selective disclosure mechanisms, and cryptographic verification was completed successfully without disclosure of unnecessary credential attributes.

Collectively, these observations confirm that the implemented system supports a complete and operational SSI credential lifecycle, consistent with the conceptual workflow defined in Section III and the implementation described in Section IV.

C. System Behavior and Performance Discussion

The implemented system was evaluated with respect to key security and privacy properties relevant to agricultural identity management.

- Integrity: Credential authenticity and integrity were preserved through cryptographic signatures and verification against issuer decentralized identifiers and ledger-anchored credential definitions.
- Authentication: Only entities controlling valid decentralized identifiers and corresponding private keys were able to participate in issuance and verification workflows, demonstrating identity-bound authentication without centralized intermediaries.
- Privacy: Selective disclosure mechanisms enabled attribute-level verification, minimizing data exposure during credential presentation. The use of pairwise decentralized identifiers further reduced the risk of cross-context correlation.
- Accountability: Identity-bound interactions ensured that credential issuance and verification events could be attributed to authenticated entities, supporting auditability without exposing sensitive identity data.

- **Invalid or Malicious Submissions:** Basic negative test cases were performed to evaluate system robustness. Replayed proof messages were rejected due to nonce-based challenge–response mechanisms, and invalid or improperly signed credentials failed cryptographic verification against ledger-anchored definitions. These results indicate that the prototype is resistant to replay and forgery attempts within the evaluated environment.

These observations indicate that the security and privacy objectives outlined in Section III are realized in practice through the implementation mechanisms described in Section IV.

D. Comparative Discussion with Centralized Systems

When compared with conventional centralized identity management systems, the proposed framework exhibits several notable advantages. First, the framework eliminates single points of trust and failure by decentralizing identity ownership and verification. This is particularly relevant in agricultural ecosystems, where stakeholders are geographically distributed and often operate across institutional boundaries. Second, auditability and transparency are improved through verifiable credential workflows rather than opaque database records controlled by a single authority. Verification can be performed independently by any authorized verifier without prior trust relationships. Third, privacy protection is enhanced, as stakeholders retain control over identity attributes and disclosure decisions. Unlike centralized systems, sensitive identity information is not persistently stored or aggregated by service providers. These characteristics suggest that blockchain-enabled self-sovereign identity provides qualitative governance advantages over centralized approaches, particularly in trust-fragmented agricultural environments. The comparison focuses on architectural and governance differences rather than performance benchmarking. Unlike centralized systems, the proposed framework distributes trust and enables cryptographic verification without reliance on intermediary authorities.

E. Discussion of Strengths and Limitations

While the Ziraai SSI prototype demonstrates functional feasibility and standards-compliant identity workflows, several practical considerations were observed during implementation and evaluation. First, establishing SSI connections introduces additional interaction steps compared to traditional username–password authentication models. Although these steps improve security and trust, they may increase initial onboarding complexity, particularly for non-technical users. Second, the use of decentralized identifiers and pairwise relationships increases the number of cryptographic artifacts managed by agents and wallets. This trade-off is inherent to privacy-preserving identity systems and necessitates robust wallet usability and key management support. Third, the evaluation was conducted in a controlled environment and did not include large-scale deployment or performance-stress testing. As a result, conclusions regarding scalability and operational performance under real-world workloads remain limited. These trade-offs reflect design choices rather than implementation deficiencies and highlight areas where usability engineering and system optimization will be required for production deployment.

F. Implications for Agricultural Supply Chain Governance

The evaluation results indicate that self-sovereign identity can serve as a feasible architectural foundation for identity-centric governance in agricultural supply chains. By enabling stakeholders to authenticate, certify, and verify interactions without centralized intermediaries, the proposed framework supports distributed trust establishment while preserving privacy and accountability. In particular, the ability to issue and verify credentials—such as farmer registrations, certification attestations, and compliance proofs—through standardized SSI protocols creates new opportunities for transparent yet privacy-aware governance models involving regulators, cooperatives, and market participants. Although regulator-operated nodes and multi-issuer governance competition were not experimentally simulated in the current prototype, the architecture is designed to accommodate such roles in future multi-institutional deployments.

VI. CONCLUSION AND FUTURE WORK

This study presented Ziraai SSI, a blockchain-based self-sovereign identity prototype designed to enhance transparency, security, and decentralized trust in agricultural supply chains. By integrating blockchain-based trust anchoring with self-sovereign identity mechanisms, the proposed approach addresses fundamental limitations of conventional centralized identity and data management systems, including fragmented trust relationships, limited auditability, and privacy risks. Rather than focusing solely on transactional traceability, the proposed framework explicitly positions identity as a core governance primitive within agricultural ecosystems. A key contribution of this work lies in the design of a layered, identity-centric blockchain–SSI framework tailored to the structural and governance characteristics of agricultural supply chains, and in its realization through a functional research prototype. The Ziraai SSI implementation operationalizes decentralized identifiers, verifiable credentials, and privacy-preserving authentication using standardized SSI technologies, enabling interactions among issuers, holders, and verifiers through secure, standards-compliant credential workflows. The prototype-level evaluation demonstrates the feasibility of decentralized authentication, selective disclosure, and identity-bound accountability without reliance on centralized identity providers.

The results indicate that self-sovereign identity can serve as a feasible architectural foundation for establishing trust and governance in distributed agricultural environments, particularly when stakeholders are heterogeneous and centralized identity infrastructures are impractical or undesirable. By enabling cryptographically verifiable identity interactions while preserving stakeholder autonomy and privacy, the proposed approach supports more transparent and accountable supply chain governance models. While the current implementation is research-oriented and limited to a controlled consortium setting, it provides a concrete baseline for future system extensions and deployment-oriented investigations. Several directions for future work are identified. First, the system can be extended to support comprehensive credential lifecycle governance, including user-facing credential revocation, recovery, and status management mechanisms.

Second, large-scale deployment studies involving multiple institutions and regulatory authorities are required to evaluate scalability, interoperability, and operational resilience under realistic conditions. Third, integration with complementary technologies—such as IoT-based data collection and analytics—may further enhance traceability, monitoring, and decision support within agricultural supply chains. Finally, improving usability and accessibility for non-technical stakeholders remains a critical requirement for real-world adoption and warrants focused human-centered design efforts.

REFERENCES

- [1] M. M. Aung and Y. S. Chang, "Traceability in a food supply chain: Safety and quality perspectives," *Food Control*, vol. 39, pp. 172–184, May 2014, doi: 10.1016/j.foodcont.2013.11.007.
- [2] Y. Dong, S. F. Ahmad, M. Irshad, M. Al-Razgan, Y. A. Ali, and E. M. Awwad, "The Digitalization Paradigm: Impacts on Agri-Food Supply Chain Profitability and Sustainability," *Sustainability*, vol. 15, no. 21, p. 15627, Nov. 2023, doi: 10.3390/su152115627.
- [3] H. Feng, X. Wang, Y. Duan, J. Zhang, and X. Zhang, "Applying blockchain technology to improve agri-food traceability: A review of development methods, benefits and challenges," *J. Clean. Prod.*, vol. 260, p. 121031, Jul. 2020, doi: 10.1016/j.jclepro.2020.12.1031.
- [4] F. Anastasiadis, I. Apostolidou, and N. Tsolakis, "Challenges and opportunities of supply chain traceability: insights from emergent agri-food sector," *Supply Chain Management: An International Journal*, vol. 30, no. 1, pp. 106–126, Feb. 2025, doi: 10.1108/SCM-05-2024-0322.
- [5] J. Khoualdi, N. Ellouze, H. K. Ben Ayed, and J.-P. Kokora, "Blockchain-Driven SSI for Securing Privacy and Quality Assurance in Agri-Food Supply Chains," in *2025 International Wireless Communications and Mobile Computing (IWCMC)*, IEEE, May 2025, pp. 485–490. doi: 10.1109/IWCMC65282.2025.11059697.
- [6] S. S. Kamble, A. Gunasekaran, and R. Sharma, "Modeling the blockchain enabled traceability in agriculture supply chain," *Int. J. Inf. Manage.*, vol. 52, p. 101967, Jun. 2020, doi: 10.1016/j.ijinfomgt.2019.05.023.
- [7] G. Lv, C. Song, P. Xu, Z. Qi, H. Song, and Y. Liu, "Blockchain-Based Traceability for Agricultural Products: A Systematic Literature Review," *Agriculture*, vol. 13, no. 9, p. 1757, Sep. 2023, doi: 10.3390/agriculture13091757.
- [8] P. Vern, A. Panghal, R. S. Mor, and S. S. Kamble, "Blockchain technology in the agri-food supply chain: a systematic literature review of opportunities and challenges," *Management Review Quarterly*, vol. 75, no. 1, pp. 643–675, Feb. 2025, doi: 10.1007/s11301-023-00390-0.
- [9] G. Zhao et al., "Blockchain technology in agri-food value chain management: A synthesis of applications, challenges and future research directions," *Comput. Ind.*, vol. 109, pp. 83–99, Aug. 2019, doi: 10.1016/j.compind.2019.04.002.
- [10] C. G. Schmidt and S. M. Wagner, "Blockchain and supply chain relations: A transaction cost theory perspective," *Journal of Purchasing and Supply Management*, vol. 25, no. 4, p. 100552, Oct. 2019, doi: 10.1016/j.pursup.2019.100552.
- [11] Y. Wang, J. H. Han, and P. Beynon-Davies, "Understanding blockchain technology for future supply chains: a systematic literature review and research agenda," *Supply Chain Management: An International Journal*, vol. 24, no. 1, pp. 62–84, Jan. 2019, doi: 10.1108/SCM-03-2018-0148.
- [12] M. Shuaib et al., "Land Registry Framework Based on Self-Sovereign Identity (SSI) for Environmental Sustainability," *Sustainability (Switzerland)*, vol. 14, no. 9, 2022, doi: 10.3390/su14095400.
- [13] T. Alar, G. Bharathy, U. Batra, and M. Prasad, "Evaluating self-sovereign identity solutions for agricultural supply chains: a systematic review," *Frontiers in Blockchain*, vol. 8, Jan. 2026, doi: 10.3389/fbloc.2025.1672752.
- [14] R. M. Ellahi, L. C. Wood, and A. E.-D. A. Bekhit, "Blockchain-Based Frameworks for Food Traceability: A Systematic Review," *Foods*, vol. 12, no. 16, p. 3026, Aug. 2023, doi: 10.3390/foods12163026.
- [15] A. Panwar, M. Khari, S. Misra, and U. Sugandh, "Blockchain in Agriculture to Ensure Trust, Effectiveness, and Traceability from Farm Fields to Groceries," *Future Internet*, vol. 15, no. 12, p. 404, Dec. 2023, doi: 10.3390/fi15120404.
- [16] A. Banerjee, "An ERP and Planning System Enabled Decentralized Supply Chain Using Blockchain Technology," in *Blockchain Driven Supply Chains and Enterprise Information Systems*, Cham: Springer International Publishing, 2023, pp. 63–96. doi: 10.1007/978-3-030-96154-1_4.
- [17] E. Ahoa, A. Kassahun, C. Verdouw, and B. Tekinerdogan, "Challenges and Solution Directions for the Integration of Smart Information Systems in the Agri-Food Sector," *Sensors*, vol. 25, no. 8, p. 2362, Apr. 2025, doi: 10.3390/s25082362.
- [18] Christopher Allen, "The Path to Self-Sovereign Identity," <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>. Accessed: Jan. 20, 2026. [Online]. Available: <https://www.lifewithalacrity.com/article/the-path-to-self-sovereign-identity/>
- [19] A. Preukschat and D. Reed, *Self-sovereign identity*. Manning Publications, 2021.
- [20] L. Cocco, R. Tonelli, and M. Marchesi, "Blockchain and Self-Sovereign Identity to Support Quality in the Food Supply Chain," *Future Internet*, vol. 13, no. 12, p. 301, Nov. 2021, doi: 10.3390/fi13120301.
- [21] J. F. B. Duarte, G. S. Junior, G. F. C. da Silva, M. Pillon, G. P. Koslovski, and C. C. Miers, "COTTONTRUST: Reliability and Traceability in Cotton Supply Chain Using Self-sovereign Identity," 2024, pp. 85–97. doi: 10.1007/978-3-031-57853-3_8.
- [22] I. A. Ibrahim and J. M. Truby, "FarmTech: Regulating the use of digital technologies in the agricultural sector," *Food Energy Secur.*, vol. 12, no. 4, Jul. 2023, doi: 10.1002/fes3.483.
- [23] Md. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-Based Identity Management System and Self-Sovereign Identity Ecosystem: A Comprehensive Survey," *IEEE Access*, vol. 10, pp. 113436–113481, 2022, doi: 10.1109/ACCESS.2022.3216643.
- [24] A.-S. Shehu, A. Pinto, and M. E. Correia, "SPIDVerify: A Secure and Privacy-Preserving Decentralised Identity Verification Framework," in *2023 International Conference on Smart Applications, Communications and Networking (SmartNets)*, IEEE, Jul. 2023, pp. 1–7. doi: 10.1109/SmartNets58706.2023.10215588.
- [25] J. Khoualdi, I. Abedlmoula, H. Kaffel, and D. Bensedrine, "Secure and Transparent Agri-Food Supply Chain Traceability with SSI and Blockchain-Enabled IoT," 2025, pp. 388–398. doi: 10.1007/978-3-031-87775-9_33.
- [26] I. Ahmed, K. Toyoda, T. Nakano, S. Kasahara, S. R. Goyal, and T. H. Tran, "A Systematic Review on Blockchain-Enabled eKYC: Leveraging SSI and DID for Secure and Efficient Identity Verification," *IEEE Internet Things J.*, pp. 1–1, 2025, doi: 10.1109/IIOT.2025.3597356.
- [27] U. Peddibhotla, S. C. Chandran, P. Kumar, and R. Kumar, "Enhanced Supply Chain Management in Indian Agriculture Using SSI and Blockchain Leveraged by Digital Wallet," in *2024 16th International Conference on Communication Systems & NETWORKS (COMSNETS)*, IEEE, Jan. 2024, pp. 427–429. doi: 10.1109/COMSNETS59351.2024.10427356.
- [28] A. M. Buttar, M. A. Shahid, M. N. Arshad, and M. A. Akbar, "Decentralized Identity Management Using Blockchain Technology: Challenges and Solutions," 2024, pp. 131–166. doi: 10.1007/978-3-031-49593-9_8.
- [29] C. Mazzocca, A. Acar, S. Uluagac, R. Montanari, P. Bellavista, and M. Conti, "A Survey on Decentralized Identifiers and Verifiable Credentials," *IEEE Communications Surveys & Tutorials*, vol. 27, no. 6, pp. 3641–3671, Dec. 2025, doi: 10.1109/COMST.2025.3543197.
- [30] A. De Salve, A. Lisi, M. Cascino, P. Mori, and L. Ricci, "Selective Disclosure Approaches in Self-Sovereign Identity: An Experimental Comparison," *IEEE Access*, vol. 14, pp. 1152–1181, 2026, doi: 10.1109/ACCESS.2025.3649167.