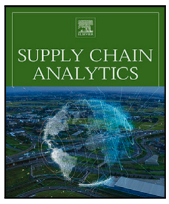
Supply Chain Analytics 12 (2025) 100161

Contents lists available at ScienceDirect

Supply Chain Analytics

journal homepage: www.sciencedirect.com/journal/supply-chain-analytics



Full length article

An analytical approach to blockchain-driven identity management in sustainable forest supply chains

Robertas Damaševičius [a,*], Rytis Maskeliūnas [b]

[a] Department of Applied Informatics, Vytautas Magnus University, Akademija, Lithuania
[b] Centre of Real Time Computer Systems, Kaunas University of Technology, Kaunas, Lithuania

ARTICLE INFO

Keywords:
Forest analytics
Supply chain transparency
Digital identity
Sustainable logistics

ABSTRACT

This study explores the application of Self-Sovereign Digital Identity (SSDI) and blockchain technology in forest supply chain management to improve traceability, sustainability and regulatory compliance. It addresses how these technologies can overcome the limitations of traditional identity management and improve forestry operations' transparency, efficiency, and environmental accountability. An Ethereum-based blockchain framework was used for this study, focusing on metrics such as transaction throughput and latency. Experimental tests were conducted to analyze the performance of SSDI in forest supply chains, focusing on real-time data management and secure identity control. A framework aligned with the Forest 4.0 initiative was proposed to evaluate the efficacy of SSDI. The results show that the integration of SSDI with blockchain significantly improves traceability and sustainability within forest supply chains, with high transaction rates and reduced latency. The decentralized system improves transparency and trust, promotes efficient identity management among stakeholders, and improves compliance with environmental regulations. Our study is among the first to apply SSDI in forestry, advancing digital transformation in this sector. Demonstrating SSDI's capacity to streamline data handling and boost traceability, it offers practical recommendations for stakeholders seeking sustainable and digitally secure supply chain management practices.

1. Introduction

Traditional centralized relational databases or even legacy card-based identity systems suffer from critical inefficiencies that cannot provide effective supply chain management given the demands of the 21st century data [1], first experiencing significant security vulnerabilities, second operating with high administrative costs, and third struggling with data silos and interoperability issues, leading to fragmented information between supply chain partners. Blockchain, and especially Artificial Intelligence (AI) enhanced approaches decrease errors in about 5%–10% of transactions compared to traditional verification means in conventional database systems [2], which not only decrease operational costs, but also significantly improves the ability to track and verify sustainable practices throughout the supply chain, making it less challenging to meet increasingly stringent environmental regulations and consumer demands for transparency. Clearly, the advent of the latest digital technologies has inaugurated a new era in identity management, with profound implications for multiple industry sectors, including supply chain management [3]. Modern supply chains must evolve into intelligent, adaptable systems by improving visibility, agility, and sustainability while integrating emerging technologies such as AI, Internet of Things (IoT), and blockchain to address modern challenges. To thrive, they need to encourage innovation, automate execution and leverage tools such as Digital Supply Chain Twins and Circular Supply Chains [4]. In the forest industry, where supply chain complexity is a significant challenge, the concept of self-governing digital identity (SSDI) [5] offers a promising solution, disrupting traditional supply chain practices that centrally manage identities, leading to inefficiencies and vulnerabilities. The rise of digital identity offers an opportunity to improve the security and efficiency of supply chain management [6]. Such a transformation presents challenges in privacy, security, and data control in very different sectors, such as agriculture [7], food supply [8] vs. health care [9,10]. SSDI represents a paradigm shift in digital identity management, embracing a user-centric approach that empowers individuals and entities to autonomously own, control, and present their identity data, reducing the dependency on centralized authorities [11]. The core principles of SSDI include user control, consent, transparency, interoperability, and portability, ensuring that identity data are managed with the highest privacy and optimized efficiency [12]. The forest sector, known for its complex supply chains [13], can benefit from adopting SSDI. Given the crucial

* Corresponding author.
E-mail addresses: robertas.damasevicius@vdu.lt (R. Damaševičius), rytis.maskeliunas@ktu.lt (R. Maskeliūnas).

https://doi.org/10.1016/j.sca.2025.100161
Received 8 December 2024; Received in revised form 22 July 2025; Accepted 2 September 2025
Available online 19 September 2025

Nomenclature

Acronym	Explanation
SSDI	Self-Sovereign Digital Identity
AI	Artificial Intelligence
IoT	Internet of Things
GIS	Geographic Information Systems
RS	Remote Sensing
VC	Verifiable Credentials
DID	Digital Identifier
IDMS	Digital Identity Management System
FMS	Forest Management System
VDR	Verifiable Data Registry
EA	Edge Agent
DDO	DID Document
CR	Community Resolver
UR	Universal Resolver
W3C	World Wide Web Consortium
TPS	Transactions per Second
SCM	Supply Chain Management
FSC	Forest Stewardship Council
CoC	Chain of Custody
PoW	Proof-of-Work
PoS	Proof-of-Stake
PEFC	Forest Certification Program

role of traceability in verifying the legality, sustainability, and quality of products in forestry, SSDI has the potential to advance this aspect. By providing immutable and verifiable records detailing the journey of each product through the supply chain, SSDI improves traceability [14], which not only facilitates compliance with environmental and trade regulations, but also builds trust between consumers and stakeholders.

Our study is directly aligned with the emerging concept of Forest 4.0, an innovative approach that integrates advanced digital technologies to optimize forest management [15]. Forest 4.0 integrates automation, data analytics, and interconnected systems, similar to the principles of Industry 4.0, to improve the sustainability and efficiency of forest resource management [16,17]. By applying SSDI and blockchain, the study offers a robust framework for traceability and transparency in the forest supply chain, which are critical to real-time monitoring and decision-making capabilities central to the Forest 4.0 initiative. Such integration not only supports sustainable forest practices, but also ensures compliance with environmental and trade regulations, propelling the forestry sector toward more advanced, digitized management practices.

The integration of blockchain technology with Self-Sovereign Digital Identity (SSDI) establishes a robust framework [18,19] for the secure and transparent management of identity within forest supply chains. The decentralized nature of blockchain ensures tamper-proof record keeping, a critical component in monitoring the movement of forest products, allowing the automation of the supply chain process through smart contracts, improving efficiency and minimizing errors [20]. Barati et al.[21] explored how blockchain technology can improve the accuracy of demand forecasting and reduce associated costs in supply chain management through system dynamics modeling, while allowing real-time data sharing, reducing information asymmetry and improving decision-making. The approach demonstrated that blockchain adoption decreases forecast errors and operational costs, providing practical insights for supply chain optimization and paving the way for future research on its scalability and broader applications. Forest supply chains face challenges such as illegal logging, counterfeit products, and logistic inefficiencies. SSDI, supported by blockchain technology, addresses these issues by providing a secure and transparent method to verify the authenticity and legality of forest products. The approach improves supply chain management, increases compliance with environmental standards, and fosters consumer trust [22]. The adoption of SSDI aligns with the global trend towards sustainable supply chain management [23] and ensuring the traceability and authenticity of forest products, SSDI actively contributes to sustainable forest management practices, helping to conserve forest resources and meeting consumer demand for ethically sourced products [24]. As digital technologies evolve, the role of SSDI in forest supply chains is set to expand, paving the way for more innovative and sustainable practices [25].

Our research aims to:

- Improve traceability using blockchain-enabled identity systems in forest supply chains.
- Enhance transparency with decentralized records and digital identity verification.
- Analyze performance through transaction rates and latency metrics in real-time.
- Streamline data handling with efficient credential issuance and verification.
- Promote sustainability through intelligent integration of digital and monitoring tools.

2. Technological landscape

2.1. Overview of technologies in global forestry supply chains

Sustainability is paramount in the supply chains, given the significant environmental impacts of forest practices [26]. Governments, environmental organizations, and consumers subject the entire supply chain to ever more strict regulations, requiring a high degree of traceability and accountability [27], ensuring compliance with legal and environmental standards from harvest to final product.

In recent years, there has been a surge in the adoption of technology in forest supply chains [28] to improve efficiency, transparency, and sustainability [29]. Geographic Information Systems (GIS) and Remote Sensing (RS) integrate into these chains[30], enabling precise mapping and monitoring of forest resources for sustainable management and planning. The data they provide are invaluable for informed decision making on forest utilization [31], covering aspects such as deforestation rates, forest health, and biodiversity [32]. Agent-based modeling was suggested by Helo et al.[33] to simulate key elements such as GIS routing, fleet size, and facility location optimization, with agents interacting within the supply chain, operating on results through time series charts and evaluating scenarios to determine optimal facility locations and fleet sizes.

Blockchain technology has emerged as a transformative tool, offering a secure and decentralized means of recording transactions and tracking the movement of goods in forest supply chain management [34]. By creating a tamper-proof ledger, the blockchain ensures the integrity and transparency of supply chain data [35], necessary to verifying the legality and sustainability of forest products [36].

Implementing these technologies in global forest supply chains still faces challenges, such as high costs, lack of technical expertise, and resistance to change [37]. Concerns about data privacy and security, particularly with sensitive information, are prevalent [38]. Ensuring interoperability between different technologies and systems between various stakeholders is another significant challenge [28].

2.2. The role of digital transformation in smart forestry

Smart Forestry is transforming the forest industry by integrating advanced technologies to address its challenges [39]. The paradigm shift covers the entire spectrum of forest operations, from timber harvesting [40] to processing and distribution, with a focus on sustainability, efficiency, and data-driven decision making [41] and decision

shaping. Central to this transformation [42] is the incorporation of technologies such as the Internet of Things, Artificial Intelligence, and blockchain [43]. In forests, IoT tools, such as sensors and unmanned aerial vehicles, collect real-time data on environmental parameters, such as forest health, soil moisture, and tree growth rates, facilitating sustainable forest management [44] and informed harvesting decisions [45], while supporting emergency response in the event of disasters such as wildfires.

Blockchain technology ensures traceability and transparency in the supply chain [46]by establishing a secure and immutable record of the journey of each product [47]. It helps to combat illegal logging [35] and ensures compliance with international standards, guaranteeing the authenticity and legality of timber products.

Precision forestry [48], similar to precision agriculture [49], uses data and technologies, including GPS and GIS, for accurate mapping and granular forest management. The approach improves resource use, minimizes environmental impact, and increases productivity. Smart forest management faces challenges, particularly the digital divide in remote and rural areas where forestry operations are prevalent. Limited access to technology and connectivity hinders the adoption of advanced tools, requiring significant investment in training and education for personnel to operate and interpret data. Despite these challenges, smart forest management represents a multifaceted shift toward sustainable, efficient and data-driven practices. As technology becomes more accessible, smart forestry practices are poised to become increasingly prevalent [16], shifting to a new era in sustainable forest management.

Integrating the SSDI framework with GIS and IoT poses specific challenges. First, data interoperability remains a critical issue [50]. GIS systems generate complex geospatial data (for example, forest health metrics, deforestation rates), while IoT devices produce continuous streams of environmental sensor data (e.g., soil moisture, tree growth). Harmonizing these heterogeneous data formats into blockchain-compatible verifiable credentials (VC) requires robust middleware to ensure semantic consistency and avoid loss of information [51]. Second, real-time processing and connectivity in remote forested regions could strain the system. IoT devices in such areas often face intermittent connectivity, delaying data uploads to the blockchain [52], while GIS datasets (e.g., high-resolution satellite imagery) are bandwidth-intensive, complicating on-chain storage. Baziyad et al.[53] investigated the role of IoT and cyberphysical systems in digital supply chains, finding that at the implementation level both are still in their infancy within digital supply chains and logistics, highlighting the need for more research to address existing gaps and advance both applicability and theoretical development. Third, security vulnerabilities can arise at integration points [54]. While blockchain ensures tamper-proof records, IoT sensors and GIS interfaces could be compromised (e.g., spoofed sensor data, manipulated geospatial input), necessitating edge computing solutions for prechain validation. Fourth, scalability challenges emerge as IoT networks expand: high-frequency IoT data from thousands of sensors, combined with large GIS files, could exceed throughput limits, especially in permissioned blockchain setups like Hyperledger Aries. Finally, the standardization gaps [55] in geospatial data protocols (e.g. ISO/TC 211) and IoT communication (e.g. MQTT vs. LoRaWAN) could fragment interoperability, requiring cross-sector governance frameworks to align with Forest 4.0 principles.

2.3. Blockchain technology in forestry supply chains

Blockchain holds promise to advance forestry supply chains by addressing key challenges through improved traceability, transparency, and authenticity [56]. Incorporation of blockchain technology into forest supply chains [57] represents an advance in the management and monitoring of these intricate networks [58]. Renowned for its decentralized and distributed ledger capabilities, blockchain ensures transparent, secure and immutable record keeping [59], and addressing persistent challenges such as traceability, transparency, and authenticity of forest products [60].

Blockchain in forest management can improve traceability [61] by "recording" every transaction and movement of forest products, guaranteeing a clear and unalterable history for each item from harvesting to the end consumer. It provides transparent and verifiable information about the origin, journey, and processing of the product [62], required to boost consumer confidence and compliance with sustainable forest practices and anti-illegal forest regulations [63]. In addition, blockchain promotes transparency in forestry supply chains [64], allowing all stakeholders to verify the authenticity and sustainability credentials of products [65], increasing transparency to increase trust between stakeholders and environmentally conscious consumers, ensuring responsible purchasing and the protection of environmental standards throughout the supply chain [66].

The role of blockchain in verifying the authenticity of forestry products is another significant benefit. The tamper-proof ledger makes it almost impossible for counterfeit products to enter the supply chain undetected [67], protecting the integrity of the forest industry and protecting natural resources [68]. In addition to traceability and transparency, blockchain facilitates supply chain automation through smart contracts [69]. Self-executing contracts streamline payments and transfer of ownership based on predefined conditions, accelerating transactions, reducing human error, and minimizing the potential for fraud. Despite its potential, the implementation of blockchain in forest supply chains faces challenges, including significant investment in infrastructure and expertise. Widespread adoption by all stakeholders is necessary for effectiveness, a process that can be slow and complex [56]. There are also concerns about the environmental impact of blockchain technology, particularly regarding the energy consumption of certain networks [70].

3. Theoretical framework

3.1. Concept of self-sovereign digital identity

SSDI is a user-centric model of digital identity that grants individuals or entities full control over the creation, management, and use of their digital identities [71]. Unlike traditional identity models where third-party organizations hold and manage identity data, SSDI empowers users to directly manage their digital identities without intermediary oversight. The concept has evolved from the need to address the limitations of centralized identity management systems, particularly the issues related to privacy, security, and data portability [72, 73].

The SSDI architecture is built around several key principles:

- User control—Individuals have complete control over their identity data, including how, when, and to whom it is shared.
- Consent—Data sharing under SSDI is based on user consent, ensuring that individuals have a say in how their identity information is used.
- Transparency—The mechanisms and algorithms used in SSDI systems are transparent, allowing users to understand how their data are managed and protected.
- Interoperability—SSDI systems are designed to be interoperable across different platforms and networks, facilitating seamless data exchange and verification.
- Portability—Users can transport their identity data across different services, avoiding vendor lock-in and improving data utility.
- Security and Privacy—SSDI places a strong emphasis on robust security protocols and privacy-preserving techniques to protect identity data.

Blockchain technology forms the foundation of SSDI, offering a decentralized system for an immutable and transparent ledger that securely records identity transactions. Employing cryptographic methods, including public and private keys, ensures secure and private

communication of identity data. SSDI relies on digital credentials, acting as digital equivalents to physical documents such as passports or driver's licenses. Issued, stored and verified digitally, these credentials are easily accessible and verifiable on digital platforms.

Digital Identifiers (DID) are unique identifier types that enable verifiable self-sovereign digital identities. Completely controlled by the DID subject, they operate independently of centralized registries, identity providers, and certificate authorities [74]. Verifiable credentials, representing digital statements from an issuer on a topic, allow establishing trust and verification mechanisms for secure digital interactions. In supply chain management, SSDI transforms the identification and verification of stakeholders, including producers, distributors, retailers, and consumers. The shift improves transactional trust and transparency, particularly in sectors such as forestry, where product provenance and authenticity are required for transparent tracability.

3.2. Mathematical definition of self-Sovereign digital identity

SSDI is defined through a further series of mathematical definitions and concepts that underlie its digital framework. Central to this are the notions of decentralized identifiers, cryptographic functions, and blockchain-based verifiability. A DID as a unique identifier associated with a digital identity is represented as:

$$\text{DID} = \text{did:method:unique\_value} \tag{1}$$

where *method* represents the DID method specific to a particular blockchain or network, and *unique_value* is a string generated to uniquely identify a digital identity within the method-specific namespace.

The foundation of SSDI security lies in cryptographic key pairs consisting of a private key (k_{pr}) and a public key (k_{pu}). The keys are generated using cryptographic algorithms such as RSA or ECC, represented as:

$$k_{pu}, k_{pr} = \text{KeyGen}(\text{security\_parameter}) \tag{2}$$

A digital signature (σ) is used to verify the authenticity and integrity of a message (m) or document. It is generated using the private key of the signer and can be verified by anyone holding the corresponding public key, formalized as:

$$\sigma = \text{Sign}(k_{pr}, m) \tag{3}$$

$$\text{Verify}(\sigma, k_{pu}, m) \rightarrow \text{true}, \text{false} \tag{4}$$

A VC is a set of claims made by an issuer about a subject. Mathematically, a VC can be represented as a tuple:

$$\text{VC} = (\text{issuer}, \text{subject}, \text{claim}, \sigma) \tag{5}$$

where *issuer* is the entity that issues the VC, *subject* is the entity to whom the VC refers, *claim* is the assertion made about the subject and σ is the digital signature of the issuer.

SSDI uses blockchain technology for decentralized and tamper-proof record keeping. A blockchain ($\mathcal{B}$) can be mathematically conceptualized as a linked list of blocks, each containing a set of transactions (T), represented as:

$$\mathcal{B} = B_1, B_2, \ldots, B_n \tag{6}$$

$$B_i = \mathcal{T}_i, \text{prev\_hash}, \text{hash}(B_i) \tag{7}$$

where *prev_hash* refers to the hash of the previous block in the chain, ensuring the immutability of the ledger.

3.3. IoT enabled smart forestry model

The Internet of Things serves as a transformative solution [75] to modernize forest practices, alleviate operational pressures, and facilitate the real-time management of forest resources. Extensive research in this domain is illustrated by the diverse applications of IoT in forestry, including remote monitoring of forest conditions, continuous monitoring of tree growth and health, and integration with wearable devices to enhance safety and operational efficiency for forest workers. Interestingly, it also parallels the healthcare sector, where Bai et al. [76] discussed IoT-enabled applications and proposed a unique self-identity model for healthcare systems. Fig. 1 shows an IoT enabled Smart Forestry system, which includes various stakeholders in the forestry: sector—forest managers, logging companies, processing plants, conservation agencies, regulatory bodies and the main entities, forests. An integral aspect of IoT-enabled Smart Forestry involves deploying sensors throughout the forest to collect extensive data. Data are then transmitted to storage servers, such as cloud platforms, blockchain systems, or databases. Subsequently, end-user applications access these data for analysis, support decision making, and the provision of forestry services. Machine learning, deep learning, and computational modeling are used to extract actionable insights from the collected data.

Our work identifies the four key players in Smart Forestry as follows:

- Forestry Consumers—These are individuals or entities directly involved in forest management and operations. They access forestry data to make informed decisions about resource management, conservation, and use.
- Forestry Regulators—Governmental bodies or environmental agencies responsible for regulating forestry practices. They monitor forest health and activities, develop policies related to sustainable forestry, and process aggregated data to develop new frameworks or guidelines for forest management.
- Forestry Service Providers—Entities that offer various forestry-related services. This group includes forest managers, logging companies, conservationists, and others responsible for the actual implementation of forestry activities. They collect and utilize forestry data to enhance service delivery.
- Industry Representatives—This includes timber processing companies, environmental technology companies, equipment manufacturers, and research institutions. They are instrumental in driving the forestry sector forward by providing advanced solutions and technologies for sustainable forest management. They use forest data to develop innovative products and services that advance the sector.

3.4. Digital identity management system in smart forestry

In the domain of Smart Forestry, a Digital Identity Management System (IDMS) plays a core role in the safe and efficient management of digital identities linked to various forest stakeholders and resources. The system involves a set of regulations and protocols that govern authentication, authorization, and access control, ensuring that only authorized entities can access specific services and data. The key components of an IDMS in Smart Forestry include users (such as forest managers, conservationists, and logging companies), identity issuers (such as forest regulatory bodies and certification authorities) and service providers (including forest management software and IoT platform providers).

Within the decentralized model, the SSDI subset is of specific relevance in the context of Smart Forestry. SSDI facilitates the development of trust between entities such as forest owners, conservation agencies and logging companies. The model empowers stakeholders by giving them complete control over their digital identities, enabling secure and efficient interactions within the forest ecosystem [45].

There are three primary IDMS models:

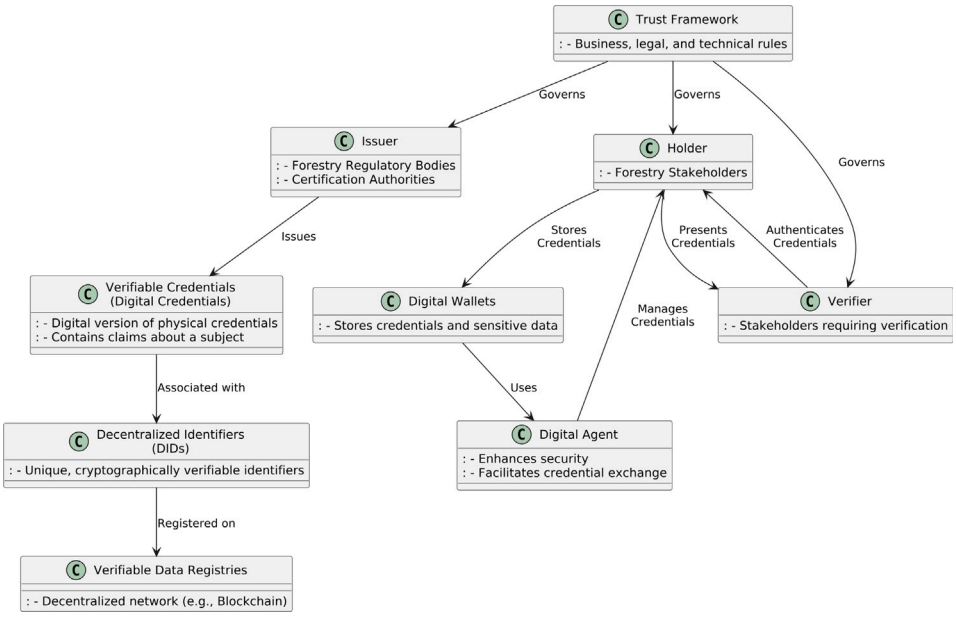


Fig. 1. Components of the SSDI model.
Source: Authors own work

- Centralized Identity Model. Here, a single central authority, such as a forest management organization or government body, controls and owns digital identities (ID). The model is similar to traditional systems such as government-issued identification cards or organizational identity cards. In Smart Forestry, this could be represented by centralized databases managed by forestry departments or regulatory bodies.
- Federated Identity Model could be used in Smart Forestry to integrate different service platforms, such as those for environmental monitoring, timber tracking, and regulatory compliance, to manage the identities of service providers.
- User-Centric/Decentralized Identity Model. The users control their own identifiers and set policies to share information with service providers. The identity model, which operates on a peer-to-peer basis, does not rely on a centralized authority for identity management. Examples applicable to the context of Smart Forestry are blockchain-based systems such as uPort or Sovrin. Such systems would theoretically allow various stakeholders in the forest supply chain to manage their own identities and securely exchange data.

3.5. Architecture of SSDI model in smart forestry

The SSDI model is proposed to foster a secure, persistent, and interoperable identity framework for forest stakeholders. Fig. 2 (conceptual) represents the key components of the SSDI model in Smart Forestry. The architecture comprises four primary layers: Identifiers and Keys (DID), Secure Communication and Interfaces, Verifiable Credentials, and Governance. To realize the objectives of user-centric identity management in forestry, the model incorporates seven building blocks:

- Issuer, Holder, and Verifier in Smart Forestry perform the following functions. Issuers (such as forestry regulatory bodies or certification authorities) provide credentials. Holders (forestry stakeholders) store these credentials in digital wallets and present proof of claims to verifiers (other stakeholders requiring verification). Then, the verifiers authenticate the presented credentials.
- Digital credentials are digital versions of physical credentials that contain claims about a subject (e.g., sustainable forest practices, legal compliance). They are issued by recognized entities within the Smart Forestry network.

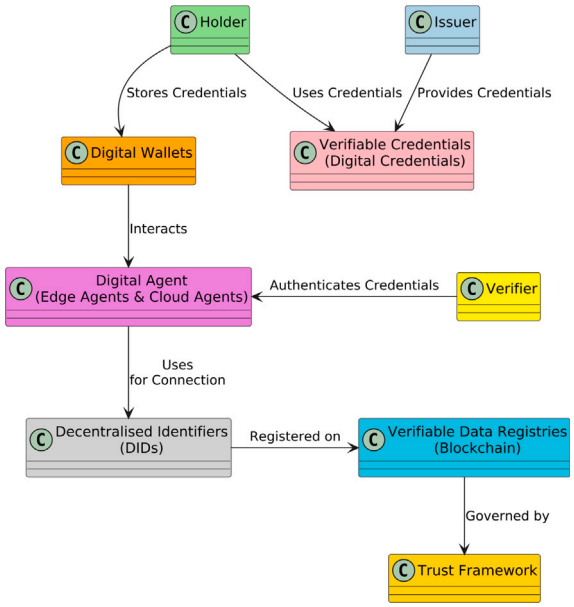


Fig. 2. Model of SSDI.
Source: Authors own work

- Digital wallets in Smart Forestry store credentials and other sensitive data. They interact with digital agents to securely exchange credentials.
- The digital agent embedded in digital wallets improves security, facilitates secure credential exchanges, and establishes connections using a decentralized messaging protocol. Edge Agents and Cloud Agents are two categories of digital agents.
- DID are unique identifiers that are cryptographically verifiable and resolvable. They represent a combination of private and public keys and enable secure peer-to-peer connections between parties.
- Verifiable Data Registries in a DID can be registered on any decentralized network or exchanged peer-to-peer. Blockchain is

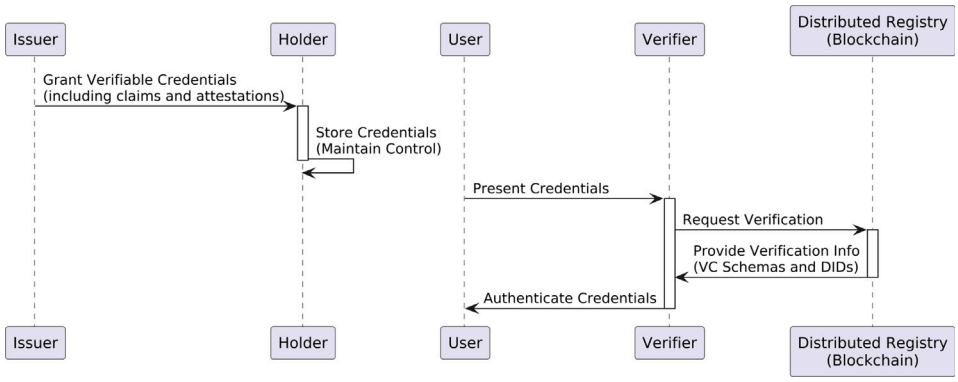


Fig. 3. Information flow in SSDI model.
Source: Authors own work

an ideal choice for this registry due to its tamper-resistant and distributed nature.
- Trust Framework includes business, legal, and technical rules for using the SSDI infrastructure, which facilitates interoperable digital trust ecosystems.

3.6. Information flow in SSDI

The SSDI model in Smart Forestry represents an evolutionary step beyond traditional IDMS, prioritizing user control, interoperability, and consent-driven data sharing. Oriented by ten principles that emphasize user identity control, system transparency, fairness, and interoperability, the implementation of the SSDI model in the forest sector is shaped. These principles serve as a framework for customizing SSDI according to the distinctive requirements and challenges of Smart Forestry. The information flow in Smart Forestry's SSDI model follows these basic steps (see Fig. 3):

- Issuers grant verifiable credentials to identity owners/holders, which include claims and attestations.
- Holders store these credentials and maintain complete control over them.
- When accessing services, users present their credentials to the verifiers.
- Verifiers authenticate credentials independently of the issuers, typically by connecting with a distributed registry (such as a blockchain) that holds VC schemas and DIDs for verification.

Fig. 3 visually represents the flow of information and interactions among different entities in the Smart Forestry's SSDI model:

- Issuers grant verifiable credentials, including claims and attestations, to Holders.
- Holders store these credentials and maintain complete control over them.
- Users, when accessing services, present their credentials to Verifiers.
- Verifiers authenticate credentials. They do this by connecting with a distributed registry (like a blockchain) that holds the VC schemas and DIDs necessary for verification.

3.7. High-level system architecture of SSDI model for smart forestry

We created a specialized SSDI model designed for digital identity management in a Smart Forestry system. Our model encompasses IoT devices used in forestry operations and assigns digital identities to various stakeholders, from logging companies to conservation agencies. To protect Personally Identifiable Information, the model empowers data owners with complete control during information sharing. Authentication is required from the requester to the data owner when accessing another user's data, reinforcing security and privacy in forestry data transactions. Derived from standard SSDI models, the architecture revolves around three primary roles: Identity Issuer, Identity Holder, and Identity Verifier (see Fig. 4).

The forest management system (FMS) issues verifiable credentials, based on Decentralized Identifiers (DID), to stakeholders such as logging companies, processing facilities, regulatory bodies, and environmental groups. The subjects, which include all stakeholders in the forestry supply chain, including IoT devices that facilitate end-to-end information flow, receive verifiable credentials. Verifiers, such as regulatory bodies, independently verify the identity of entities such as logging companies without relying on intermediary assistance from the FMS. All stakeholders participate in a unified blockchain network (FMS-BT). Entities engaged in forest-related services must register on this network. Identity-related transactions are documented on the FMS-BT blockchain distributed ledger (Li) [77], as elaborated in subsequent sections. The owners of IoT devices integral to the operations of Smart Forestry register their devices on FMS-BT, providing both the DID of the devices and their own. The SSDI model uses blockchain not only as a ledger, but also as a verifiable data registry (VDR).

The VDR establishes rules for entities within the distributed system to create and manage identifiers according to specific needs. It serves as a mediator for the creation and verification of identifiers, verifiable credential schemas, keys, and pertinent data such as public keys and revocation registries. This role is crucial in verifying verifiable credentials, ensuring a secure and trustworthy digital identity management framework [78] within Smart Forestry.

Fig. 4 outlines the key components of the Smart Forestry SSDI model:

- Subject—Represents identity holders such as logging companies and IoT devices in the forestry supply chain.
- Issuer—The forestry management system responsible for issuing verifiable credentials.
- Verifier—Entities such as regulatory bodies that verify the credentials and identities.
- FMS-BT Blockchain Network—The blockchain network that manages transactions and stores DIDs and credentials.
- VD—Mediates the creation and verification of identifiers, manages credential schemas, and keys.

3.8. Communication flow in smart forestry

The communication flow in the Smart Forestry SSDI model revolves around DIDinteractions among Edge Agents belonging to different forestry stakeholders. A typical user set-up includes the user's Edge Agent, a front-end DID wallet, a secure element, and a micro ledger. The system features a community resolver (CR) for DIDs, which includes drivers for DID methods and a caching mechanism.

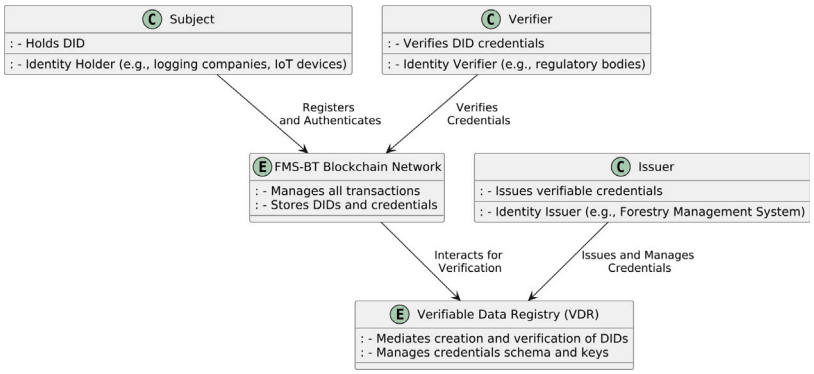


Fig. 4. Key components of the Smart Forestry SSDI Model.
Source: Authors own work

For illustration, we used a forestry-focused adaptation of Sovereign to showcase DID interactions among users. Key components include a steward for network oversight, a DID syntax checker, cache and resolution result constructor, and an serialisation on validators. The VDR here is a dedicated blockchain network specifically designed for forestry. An agent acts as a delegated entity by the DID subject, managing agent-to-agent DID communication, cryptographic operations related to the DID wallet, and sharing credentials with authorized agents based on established relationships. Agents are categorized as Edge Agents and cloud agents. Edge agents are located within the wallet software, while cloud agents, located in the cloud, offer extended features such as identity wallet backup, continuous DID communication, data storage, and key management [79]. The system primarily employs an Edge Agent (EA).

To exemplify this architecture, consider a common Smart Forestry scenario where a forest manager (equivalent to a patient in healthcare) aims to share data and device readings with a regulatory body (equivalent to a doctor) for certifications or approvals. The forest manager's Edge Agent queries the regulatory body's DID from the CR within a universal resolver (UR). DID methods then provide the DDO (DID Document) of the regulatory body's EA through VDR interaction. The forest manager's EA retrieves the DDO from the UR and establishes DID communication based on the data present in the DDO. The Smart Forestry Identity Architecture is discussed in two parts: a high-level user interaction termed "SSDI-SF: SSDI for Smart Forestry System" and "SSDI-SF-IoT: Interaction of IoT with SSDI-SF," which focuses on the network among sensors and forest managers (referred to as the IoT network in Smart Forestry). The term "IoT" encompasses all types of forest device, sensors, and other smart devices used in forest management, as shown in a Fig. 4 representing the high-level SSDI-SF architecture.

3.9. Use cases

3.9.1. Registration in smart forestry SSDI model—identity wallet and agent installation

In the initial phase of the SSDI model for Smart Forestry, stakeholders establish their digital identity using a digital wallet and Edge Agent, which involves several key steps:

1. **Installation and Edge Agent Creation:**
   - Stakeholders install the digital wallet software, initiating the Edge Agent.
   - The digital wallet is used to receive and present credentials for system authentication.

2. **DID Creation and Credential Setup:**

$$\mathrm{EA}_{\mathrm{forestry}} \rightarrow \mathrm{DID}_{\mathrm{EA}}, \mathrm{Cred}_{\mathrm{SE}}, \mathrm{linksecret} \tag{8}$$

The Edge Agent creates a DID and generates credentials for secure communication and relationship establishment.

3. **Requesting Verifiable Credentials (VC):**

$$\mathrm{EA}_{\mathrm{forestry}}\ \mathrm{Req}(VC, VCP, CS) \rightarrow SE \tag{9}$$

The Edge Agent requests the Secure Element to create verifiable credentials and their presentation for specific credential schemas.

4. **Secure Element Storage:**

$$SE \leftarrow \mathrm{stores}\ VC, \mathrm{PR}_{\mathrm{forestry}}, \mathrm{D.Key}_{\mathrm{wallet}}, \mathrm{Key}_{\mathrm{AP}} \tag{10}$$

The Secure Element stores the credentials and keys necessary for secure operations.

5. **Credential Presentation Return:**

$$SE\ \mathrm{return}(D.\mathrm{Key}_{\mathrm{wallet}}, VCP, \mathrm{PR}_{\mathrm{forestry}}) \rightarrow \mathrm{DigitalWallet}_{\mathrm{frontend}} \tag{11}$$

The Secure Element returns necessary data for the presentation of the credentials to the front-end wallet.

6. **Front-end Wallet Storage:**

$$\mathrm{DigitalWallet}_{\mathrm{frontend}} \leftarrow \mathrm{store}(EA_{\mathrm{forestry}ID}, \mathrm{linksecret}, P_{AP}) \tag{12}$$

The Edge Agent instructs the storage of crucial data in the front-end wallet for secure and authenticated operations.

The diagram in Fig. 5 illustrates the process in which the stakeholders in Smart Forestry install digital wallet software and initiate the Edge Agent, which then creates a DID and generates credentials. The Edge Agent requests verifiable credentials from the Secure Element, which stores these credentials and keys necessary for secure operations, and returns the necessary data for credential presentation to the front-end wallet. Finally, the front-end wallet stores crucial data for secure and authenticated operations. The structured process ensures the self-sovereignty of digital identities in the Smart Forestry sector, adhering to principles of privacy and controlled disclosure.

3.9.2. Authentication using DID method in smart forestry

Following the installation of the agent and identity wallet, the authentication process in the Smart Forestry domain involves steps similar to those in a healthcare system but adapted to forestry stakeholders, such as forest managers and regulatory bodies. The sequence of the authentication process is outlined below:

Step 1. Initiate DID Communication Request

$$\mathrm{EAforestry\_managerconnect(DIDforestry\_manager)} \rightarrow \mathrm{EA}_{\mathrm{stakeholder}} \tag{13}$$

A forestry manager sends a DID communication request to a stakeholder, which is received by the stakeholder's Edge Agent.

Step 2. Query to Community Resolver

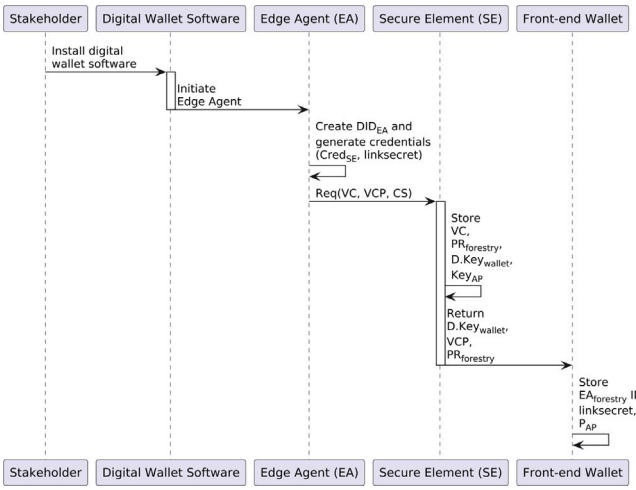


Fig. 5. Identity Wallet and Agent Installation process.
Source: Authors own work

$$\text{EAstakeholderquery(DIDforestry\_manager)} \tag{14}$$

The stakeholder's Edge Agent queries the CR of the UR.

Step 3. Cache Check and DID Document Retrieval The CR checks its cache and returns the stored DDO if available.

$$\text{CR return(DDO, DIDforestry\_manager)} \rightarrow \text{EAstakeholder} \tag{15}$$

Step 4–16. Resolution Process and DDO handling The steps involve the resolution process, cache checks, DID format validation, and interaction with the VDR. The process ensures the retrieval and validation of the DDO.

Step 17. Verification and Communication Initiation

$$\text{EAstakeholder send(DIDcommn, encryptPREA}(\Delta L)) \tag{16}$$

Upon verifying the DDO, if the stakeholder agrees to connect, the Edge Agent sends a DID communication message with updates of the micro ledger.

Steps 18–24. Micro-Ledger Synchronization and Transaction Recording The steps involve the exchange of microledger deltas between the forest manager and the stakeholder, ensuring that both parties have synchronized records of DID events. The identity ledger records the transaction with details such as the requester and provider Edge Agents, transaction status, and a time-stamped ledger hash.

$$\text{Tx(EAstakeholder, EAforestry\_manager, status, timestamp, hash}(L)) \tag{17}$$

The diagram in Fig. 6 illustrates the authentication process using the DID method in Smart Forestry. It details the steps from the initiation of DID communication by a forestry manager to the stakeholder, through the resolution process involving the CR and the VDR, and finally to the recording of the transaction on the identity ledger, showcasing a decentralized approach without the need for a centralized forestry authority. The process ensures privacy and security, especially important in Smart Forestry, where multiple IoT devices are involved and exposed to external vulnerabilities.

3.9.3. Authentication of IoT on network in smart forestry

In Smart Forestry, the forest manager, who is the owner of the IoT device, has complete control over the data collected by his IoT device. Below is a detailed description of how a verifier (such as a regulatory authority) accesses data from an IoT device with the consent of the forest manager:

Step 1. Providing Device DID

- The forest manager provides the DID of a device to the verifier to access the data.
- Upon receiving the DID, the verifier calls the smart contract 'DIDMaster', passing the DID of the device to the forest manager.

Step 2. Smart Contract Returns Device Details

- The smart contract returns details of the device: hash of the DID, hash of DDO, status, and URI of the device.

Step 3. Verification of Device Status

- If the status is active, the verifier sends the DID to a verifier agent to verify the DID.

Step 4–6. AccessData Smart Contract

- The Verifier's Edge Agent retrieves the address for "AccessData".
- The Verifier's Edge Agent calls "AccessData" with specific parameters to request data access.
- The execution of 'AccessData' is saved on the blockchain.

Step 7. Forest manager EA Resolves forester's DID

- The forest manager's Edge Agent resolves the verifier's DID and follows similar steps as in "Phase 2: Authentication using the DID Method".

Step 8. Granting Access

$$\text{Tx(EApatient, DIDdev, EAdoctor, statusdev, timestamp, hash}(L)) \tag{18}$$

- If the verifier's data request is valid, the forest manager's EA grants access and records the transaction on the identity ledger.

Step 9–13. Data Access and Validation

- The verifier obtains an access token from the transaction event and requests to download data.
- The forest manager sends a challenge to the verifier for identity confirmation.
- The forest manager validates the access token and verifies the verifier's response.
- If all validations pass, the forest manager generates a download link for the verifier; otherwise, the request is rejected.

Fig. 7 illustrates the process by which a forest manager provides a verifier with access to data from an IoT device. The steps include providing the device's DID, calling the DIDMaster smart contract, verifying the device status, interacting with the AccessData smart contract, and finally, the validation and granting of access to the requested data. The process ensures secure and consensual data access in Smart Forestry, maintaining control over IoT device data, while enabling authorized data sharing with verifiers [80]. It outlines the authentication process of IoT devices on a network within the Smart Forestry domain. It details the steps involved in verifier access to IoT data (the control of the forest manager over their device data) and the necessary steps for secure and consensual data sharing.

4. Implementation in smart forestry

Our Smart Forestry SSDI model prototype employs blockchain technology, specifically implementing the Forestry Blockchain Network (FBN) on the Hyperledger Aries framework, comprising of nodes representing stakeholders throughout the forest supply chain, including logging companies, processing facilities, transportation entities, regulatory bodies, and conservation organizations. In this context, the ledger functions as a verifiable directory that stores identity records and transactions relevant to the forestry supply chain. Identity records

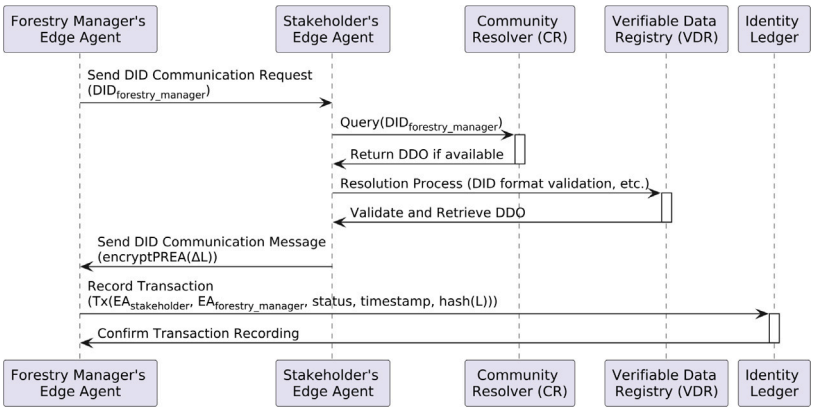


Fig. 6. Authentication Using DID Method.
Source: Authors own work

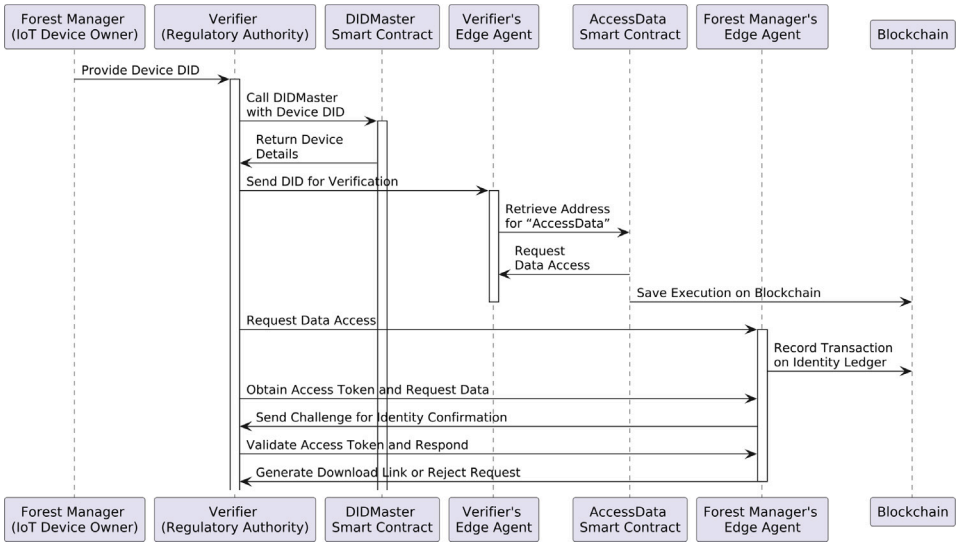


Fig. 7. Authentication of IoT device.
Source: Authors own work

consist of public data such as public keys, service endpoints, credential schemas, and definitions, each uniquely linked to a DID, ensuring a one-to-one relationship [81]. Unique DID are resolved through an identity ledger, eliminating the need for a centralized third-party authority. Entities such as forestry management organizations, regulatory bodies, and environmental groups serve as trust anchors. Thesanchors, acknowledged and verified within the ledger, are used for onboarding other entities into the blockchain network, establishing a foundational level of trust and authenticity in the system.

4.1. DID creation

The creation of DIDs follows a specific method defined in the DID framework. The nodes provide minimal information necessary for DID creation, adhering to specifications maintained by regulatory and standardization bodies, such as the World Wide Web Consortium (W3C). For example, forest IoT devices, such as sensors for monitoring tree growth or health, generate cryptographically secure public and private keys in a trusted execution environment. The private key is securely stored on the device, while the public key is used to generate the DID.

An example of the DID creation function, generateDID, might look like this:

```
generateDID("publicKeyParameters")
```

This function returns a DID for the subject in a format such as:

```
did:fbn:H3C2AVvLMv6gmMNam3uVAjZpfkcJCwDwnZn6z3wXmqPV
```

Here, did is the scheme, fbn (Forestry Blockchain Network) is the DID method, and the remaining part is a method-specific identifier.

4.2. DID documents

The DID document, which must stay consistent with the W3C standards, contains the necessary parameters to create a new DID for a node. It expresses cryptographic equations, verification methods, services, and controls, facilitating secure and trusted interactions within the forestry supply chain network. An example of a Decentralized Identifier Document for a blockchain-based security implementation in a forest supply chain context is as follows:

```
{
 "@context": "https://www.w3.org/ns/did/v1",
 "id": "did:fbn:123456789abcdefghi",
 "authentication": [
  {
   "id": "did:fbn:123456789abcdefghi#keys-1",
   "type": "Ed25519VerificationKey2018",
   "controller": "did:fbn:123456789abcdefghi",
```

```
    "publicKeyBase58": "GfHq2tTVk9z4eXgyeLv5N2Jy
      W5Fc8dNkH6BGZ1RYz5qW"
   }
  ],
  "service": [
   {
    "id":"did:fbn:123456789abcdefghi#forestry-service",
    "type": "ForestrySupplyChainService",
    "serviceEndpoint": "https://forestry.example.com/
     endpoint/123456789abcdefghi"
   }
  ],
  "created": "2020-10-10T17:00:00Z",
  "updated": "2021-10-10T17:00:00Z",
  "proof": {
   "type": "Ed25519Signature2018",
   "created": "2021-10-10T17:00:00Z",
   "proofPurpose": "assertionMethod",
   "verificationMethod": "did:fbn:123456789abcdefghi#
    keys-1",
   "jws": "eyJhbGciOiJFZERTQSIsImI2NCI6ZmFsc2UsImNya
    XQiOlsiYjY0Il19..YUJjZEFna1lJbG..."
  }
}
```


In this example:

- "@context" specifies the JSON-LD context, which is a standardized format.
- "id" is the unique identifier for the DID.
- Under "authentication", there is a public key listed which is used to authenticate the DID. This section can contain multiple keys.
- "service" lists the services associated with this DID, in this case a forestry supply chain service with its unique endpoint.
- "created" and "updated" fields denote the timestamps for when the DDO was created and last updated.
- The "proof" section provides cryptographic proof of the DDO, ensuring its integrity. It contains the type of cryptographic signature, the date it was created, the purpose of the proof, the verification method, and the actual digital signature ("jws").

The DDO acts as a public-facing document that allows others within the blockchain network to discover and verify public keys, services, and other important information associated with the DID.

4.3. Verifiable credentials

The credential schema is required to provide verifiable credentials for timber products in the forest supply chain, certifying aspects such as the origin of the timber, the date of harvest, the species of the tree and relevant sustainability certifications [82]. The schema ensures that all parties in the supply chain can refer to and verify these details in a standardized and secure manner.

In the context of Smart Forestry, verifiable credentials represent statements made by an issuer (such as a forest certification body) in a secure and respecting way of privacy [83]. When an organization issues verifiable credentials, they attach their public DID to the credential [84]. The verifier can then verify this credential without needing to contact the issuing authority directly. The credentials include proofs and claims related to various aspects of forest management, such as legal harvesting, sustainable practices, and regulatory compliance. An example of a blockchain-based security implementation credential schema, particularly designed for a forest supply chain, in a JSON format:


```
{
  "@context": ["https://www.w3.org/2018/credentials/v1",
  "https://www.w3.org/2018/credentials/examples/v1"],
  "id": "did:fbn:123456789abcdefghi#credential-schema",
  "type": ["VerifiableCredential", "ForestryCredential"],
  "issuer": "did:fbn:123456789abcdefghi",
  "issuanceDate": "2021-11-01T19:73:24Z",
  "credentialSubject": {
   "id": "did:fbn:987654321hgfedcba",
   "timberOrigin": "Brazilian Rainforest",
   "harvestDate": "2021-10-20",
   "species": "Mahogany",
   "sustainableHarvestCertification": true,
   "chainOfCustodyCertification": "COC-123456"
  },
  "proof": {
   "type": "RsaSignature2018",
   "created": "2021-11-01T19:73:24Z",
   "proofPurpose": "assertionMethod",
   "verificationMethod": "did:fbn:123456789abcdefghi#
    keys-1",
   "jws": "eyJhbGciOiJSUzI1NiIsImtpZCI6ImRpZDpmbm..."
  }
}
```


In this schema:

- "@context" defines the context of the credential, linking to the standard definitions for terms used in the document.
- "id" is the unique identifier for the credential schema.
- "type" specifies the type of credential; in this case, a Verifiable Credential with a specific type related to forestry.
- "issuer" is the DID of the entity that issued this credential.
- "issuanceDate" marks the date and time when the credential was issued.
- "credentialSubject" contains details about the subject of the credential, including information such as timber origin, harvest date, species, and certifications.
- The "proof" section provides cryptographic proof of the credential, detailing the type of signature, the creation date, the purpose, the verification method, and the digital signature itself.

4.4. Error-handling mechanisms in the blockchain framework

To ensure fault tolerance and operational robustness of the SSDI system in Smart Forestry applications, we formalize its error handling architecture in three interdependent layers: blockchain consensus, identity validation, and smart contract execution. These mechanisms are designed to mitigate the risks posed by validator node failures, incorrect data inputs, or transactional inconsistencies in ecosystem service operations, such as timber traceability or carbon credit certification.

Let the permissioned blockchain network be modeled as a finite set of validator nodes $\mathcal{N} = \{n_1, n_2, \ldots, n_k\}$, where each $n_i \in \mathcal{N}$ executes the consensus protocol C to maintain a global ledger state Σ. The system tolerates up to f Byzantine faults, satisfying the constraint: $k \geq 3f + 1$, as required by the Practical Byzantine Fault Tolerance (PBFT) model, to guarantee both safety and liveness in the presence of faulty or unresponsive nodes.

Let $\mathcal{T} = \{t_1, t_2, \ldots, t_m\}$ denote a sequence of transactions submitted to the ledger. Each transaction t_i consists of structured input data D_i, cryptographic proofs π_i, and a function $\phi(t_i)$ that triggers a state transition $\Sigma \rightarrow \Sigma'$ if valid. A transaction is deemed *admissible* if it satisfies:

$$\forall t_i \in \mathcal{T}, \quad \mathcal{V}(D_i, \pi_i) = \texttt{true}, \tag{19}$$

where $\mathcal{V}$ is a verification function enforcing schema compliance, signature correctness, and semantic integrity of the data. In the context of identity operations, each VC is defined as a tuple:

$$\text{VC} := \langle \text{DID}_h, \text{Schema}, \text{Claims}, \text{Proof} \rangle, \tag{20}$$

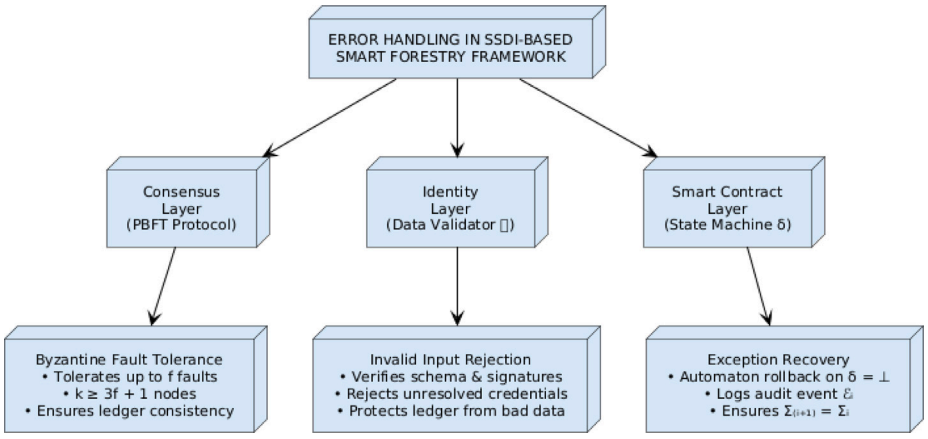


Fig. 8. Error-handling architecture across consensus, identity, and smart contract layers in SSDI-based Smart Forestry framework.

where DID_h is the holder's Decentralized Identifier, and the associated schema must be resolvable from the verifiable data registry $\mathcal{R}$. The VC is rejected if:

$$\texttt{Resolve}(\text{Schema}) = \emptyset \quad \text{or} \quad \neg\texttt{VerifySignature}(\text{Proof}). \tag{21}$$

At the smart contract layer, we define a contract $\mathcal{S}$ as a finite deterministic automaton (Q, δ, q_0, A), where: Q is the set of contract states, $\delta : Q \times \mathcal{T} \to Q$ is the state transition function, $q_0 \in Q$ is the initial state, $A \subseteq Q$ are accepting (final) states.

If the execution of δ on a transaction t_i results in an invalid state or exception, then $\delta(q, t_i) \notin Q$ and the contract triggers an automatic rollback:

$$\delta(q, t_i) = \perp \Rightarrow \Sigma_{i+1} = \Sigma_i, \tag{22}$$

ensuring no state changes are committed. This rollback is logged via an audit event $\mathcal{E}_i = \langle t_i, q, \perp, \texttt{timestamp} \rangle \in \mathcal{L}_{\text{audit}}$ for post-failure inspection.

Fig. 8 summarizes the multilayered architecture for error handling within the SSDI framework. It depicts failure detection and recovery pathways across validator nodes, credential verifiers, and smart contract agents, each enforcing domain-specific correctness invariants, which collectively enable resilient operation under failure-prone real-world forestry network conditions, without compromising ledger integrity or identity authenticity.

5. Examples of real-life applications of SSDI in smart forestry

5.1. Traceability of timber from harvest to market

The implementation of SSDI in Smart Forestry has transformed the traceability of timber throughout its lifecycle. Using blockchain technology, SSDI establishes a secure and immutable digital ledger that documents every transaction related to timber, from harvesting to distribution to the market.

To allow traceability, a unique digital identity is assigned to each harvested log, encompassing various details such as tree species, harvest date and location, chain of custody, processing specifics, and sustainability certifications. The blockchain records every transaction as the timber changes hands, updating the digital identity of the log. Regulators, consumers, and participants in the supply chain can access the blockchain ledger through secure interfaces to verify the authenticity, origin, and history of the timber. The SSDI system ensures transparency and trust in product sustainability, deterring illegal logging by making the supply chain visible and accountable.

A practical application of this technology is its role in combating illegal logging and deforestation. SSDI provides a transparent and easily verifiable record of the origin of the wood, guaranteeing that only legally harvested wood enters the supply chain, thus promoting ethical and sustainable forestry practices. Consumers and retailers benefit as they can verify the authenticity and sustainability of purchased timber, influence purchasing decisions, and promote market demand for responsibly sourced products.

Fig. 9 details the process of tracking the timber from harvest to market, utilizing SSDI and blockchain technology:

- Assigning Unique Digital Identity to Each Log. The harvesting site assigns a digital identity to each log, including details like tree species and harvest location.
- Recording Harvest Transaction on Blockchain. The identity and associated transaction are recorded on the blockchain via the SSDI system.
- Updating Log's Identity at Each Stage. As the timber is processed and moves through the supply chain, each transaction (like processing details) is updated in the SSDI and recorded on the blockchain.
- Timber Changes Hands to Distributors/Retailers. The chain of custody is updated as timber is transferred to distributors or retailers, with each transaction recorded on the blockchain.
- Verifying Authenticity and Origin. Consumers and regulators can access the blockchain ledger to verify the history and origin of the timber, ensuring its authenticity and legality.
- Ensuring Transparency and Trust. The blockchain provides a transparent history of the timber to consumers, while regulators can audit the supply chain to ensure accountability and deter illegal practices.

5.2. Certification of carbon credits

The application of SSDI goes beyond tracking timber origins, extending to environmental conservation initiatives such as the certification of carbon credits. In the fight against climate change, carbon credits are now common, facilitating the exchange of emission allowances and encouraging carbon sequestration activities. Certifying carbon credits involves an intricate process that demands meticulous validation of carbon sequestration efforts undertaken by forestry operations. SSDI acts as a foundational technology, ensuring the credibility and legitimacy. By assigning a unique digital identity to each forest land parcel, stakeholders can document and authenticate activities such as afforestation, reforestation, and sustainable forest management practices that contribute to carbon capture. Digital identities encompass a comprehensive data set that incorporates geospatial coordinates, species diversity, biomass calculations, and historical carbon sequestration data. Actions taken to improve carbon storage capacity, such as planting trees or implementing soil conservation techniques, are recorded on a blockchain, which serves as a transparent and verifiable

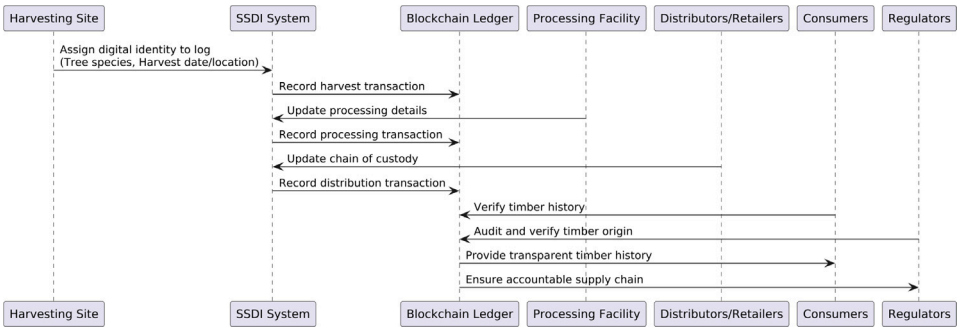


Fig. 9. Traceability of Timber from Harvest to Market.

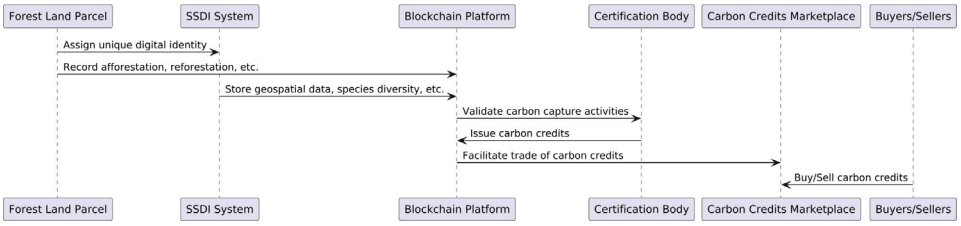


Fig. 10. Certification of Carbon Credits Using SSDI System.

audit trail, allowing certification bodies to assess and issue carbon credits. SSDI facilitates the establishment of a carbon credits marketplace, where buyers and sellers can confidently trade credits. Entities seeking to offset their carbon footprint can acquire credits from forestry operations with documented contributions to carbon sequestration, anchored by SSDI.

The diagram presented in Fig. 10 illustrates the process of certifying carbon credits in Smart Forestry using SSDI:

- Each forest land parcel is assigned a unique digital identity through the SSDI system.
- Activities such as afforestation and reforestation that contribute to carbon capture are recorded on the blockchain associated with the SSDI of the parcel.
- The SSDI system stores detailed data about each parcel, such as geospatial coordinates and species diversity, on the blockchain.
- The blockchain platform provides data to certification bodies for the validation of carbon sequestration activities.
- Once validated, the certification body issues carbon credits for the verified carbon sequestration efforts.
- The blockchain platform facilitates the creation of a marketplace for the trade of carbon credits.
- Buyers and sellers trade carbon credits in the marketplace, allowing entities to offset their carbon footprint by purchasing credits from forestry operations that have verifiably contributed to carbon sequestration.

Each step in the above process ensures the transparency, traceability, and credibility of carbon sequestration efforts and the carbon credits derived from them.

5.3. Automated payment systems for ecosystem services

Incorporating SSDI into Smart Forestry practices streamlines the implementation of automated payment systems for critical ecosystem services such as carbon sequestration and biodiversity conservation. Traditionally, compensating ecosystem services involves complex verification and transaction procedures. SSDI simplifies and automates this process, assigning a unique digital identity to each forest parcel along with detailed information, such as size, provided services, amount of carbon sequestration, and biodiversity index. For example, a forest that contributes to carbon sequestration can be registered on a blockchain platform using its unique SSDI. The absorbed CO2 is converted into carbon credits, automatically sold in markets, and the proceeds are distributed among stakeholders, including landowners, local communities, and conservation organizations, based on predefined terms in smart contracts. Blockchain's transparent and immutable nature secures and records all transactions, fostering trust among stakeholders and encouraging further investment in ecosystem services. Integrating SSDI with remote sensing and IoT devices provides real-time forest data, allowing immediate and accurate compensation for services, incentivizing conservation, and ensuring fair compensation for land stewards.

The sequence diagram presented in Fig. 11 and explained in Table 1 illustrates how the integration of SSDI and blockchain technology in Smart Forestry can streamline and secure the process of monetizing ecosystem services such as carbon sequestration. By automating key steps and ensuring transparency and fairness, our system can contribute to sustainable forest management and conservation efforts.

6. Experimental evaluation

6.1. Setup

The experimental environment integrates a peer-to-peer network of validator nodes, a permissioned blockchain (Hyperledger Aries and Indy), and virtualised agents simulating key forestry stakeholders. Table 2 details the hardware configuration, while Table 3 outlines the secure network topology and static IP routing used to ensure data integrity during distributed transactions.

The blockchain platform, described in Table 4, supports the decentralized identity ledger and smart contract execution for credential validation and provenance tracking. Back-end services are based on a suite of open-source libraries (see Table 5) to implement cryptographic proofs, zero-knowledge presentations and policy-based data access, while Table 6 describes the user interfaces that enable interactive wallet and credential management.

Simulated stakeholder agents (Table 7) reflect real-world forest management roles, including landowners, regulators, and certification bodies.

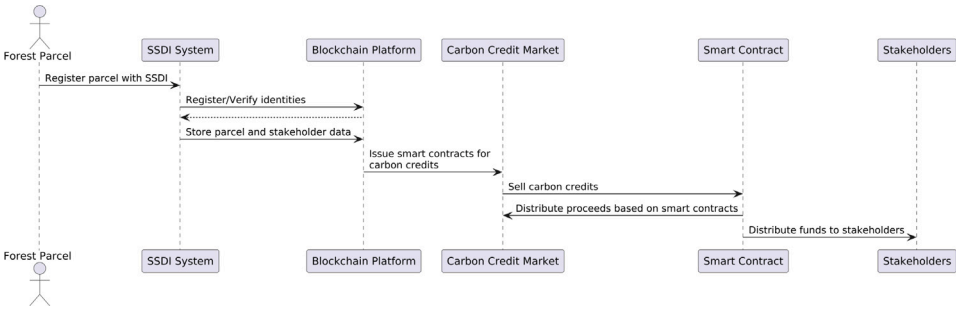


Fig. 11. Automated Payment Systems for Ecosystem Services Using SSDI.

Table 1
Processes and purposes in automated payment systems for ecosystem services with SSDI.

Process	Purpose
Registering Forest Parcel with SSDI	The forest parcel is registered with the SSDI system. In this step a unique digital identity is assigned to the forest parcel, encapsulating information such as size, type, and carbon sequestration capacity.
Managing Stakeholder Identities	Stakeholders, such as landowners, conservation organizations, and forest managers, register and verify their identities with the SSDI system, which ensures that all entities involved in the ecosystem service marketplace are authenticated and their roles and rights are clearly defined.
Storing Forest Parcel and Stakeholder Data on Blockchain	The SSDI system sends forest parcel data and stakeholder identity information to the blockchain platform for secure storage, which uses the blockchain's immutability and transparency to maintain an accurate and tamper-proof record of forest parcels and stakeholders involved.
Issuing Smart Contracts for Carbon Credit Transactions	The blockchain platform issues smart contracts specifically designed for carbon credit transactions. These automate the carbon credit sales process, ensuring that transactions adhere to predefined rules and conditions.
Selling Carbon Credits in the Market	The smart contracts facilitate the sale of carbon credits, derived from the carbon sequestration of the forest parcels, in the carbon credit market, which allows the conversion of ecosystem services into tradable and valuable assets, incentivizing forest conservation.
Distributing Proceeds to Stakeholders	After the sale of carbon credits, the market distributes the proceeds to stakeholders based on the terms specified in the smart contracts, which ensures fair and automated distribution of revenue derived from ecosystem services among all participating stakeholders.

Table 2
Hardware configuration.

Component	Specification
Processor	Intel Core i9-11900K @ 3.5 GHz, 8 Cores, 16 Threads
RAM	64 GB DDR4
Storage	2 TB NVMe SSD (PCIe Gen 4.0)
GPU	NVIDIA RTX 3080
Network Interface	Dual Gigabit Ethernet (10/100/1000 Mbps)
Operating System	Ubuntu Server 22.04 LTS (64-bit)

Note: Testbed was virtualised using VirtualBox 7.1.6 for isolation and snapshot management.

Table 3
Network configuration.

Element	Configuration
Network Topology	Peer-to-peer (P2P) decentralized
Blockchain Nodes	4 full validator nodes over LAN
IP Addressing	Static IPv4 (192.168.10.0/24)
Firewall	UFW allowing 7050, 7051, 7053, 8080, 443
DNS	Internal (dnsmasq)
Communication	TLS 1.3 with mutual authentication
Service Discovery	mDNS and gRPC

Evaluation metrics (Table 8) such as latency, throughput, and fault tolerance were measured to assess performance under realistic workloads.

Table 4
Blockchain platform configuration.

Component	Configuration
Framework	Hyperledger Aries and Indy
Consensus Mechanism	Plenum (BFT)
Identity Ledger	Sovrin TestNet
Node Types	Validator, Steward, Observer
Smart Contracts	GoLang Chaincode via Docker
Storage Engine	LevelDB

Performance metrics such as transaction throughput and latency were selected as critical indicators of system efficiency, responsiveness, and scalability in real-world forestry supply chains. Throughput, measured in transactions per second (TPS), reflects the system's ability to handle high volumes of identity verifications, timber traceability records, or carbon credit exchanges without bottlenecks, an essential feature for large-scale multistakeholder forestry ecosystems. Latency, the time taken to complete a transaction from initiation to final confirmation, impacts the speed with which data, such as ownership transfers or certification status, are updated and accessed across the supply chain. Low latency ensures timely decisions, such as compliance verification during timber export or real-time carbon credit issuance.

Table 5
Software and library Stack.

Category	Libraries/Tools
Backend Stack	Node.js v18.16.0, Express.js, PostgreSQL 14, Redis 7.0
Credential Management	aries-framework-javascript, did-jwt-vc, libursa, OpenSSL 3.x
Blockchain Interface	indy-sdk, Aries CLI, Docker Compose
Networking	Nginx, WebSocket (socket.io), GraphQL

Table 6
Front-end Stack.

Component	Tools
UI Framework	React.js v18
State Management	Redux Toolkit
Styling	Tailwind CSS
Wallet Interaction	Web Wallet SDK

Table 7
Simulated stakeholder agents.

Role	Device type	Emulated using
Forest Owner	Raspberry Pi 4	Debian Buster ARM64
Regulator	Ubuntu 20.04 VM	DigitalOcean Droplet
Verifier	Android Emulator	Flutter SDK
Certification Body	Local Server	Native Debian 11

Table 8
Evaluation parameters.

Parameter	Purpose
Latency (ms)	DID resolution + VC verification
Throughput (tx/sec)	Credential issuance/verification rate
Disk I/O (MB/sec)	Blockchain performance under load
CPU/GPU Usage	Cryptographic load profiling
Fault Tolerance	Ledger recovery post-node failure
Interoperability	W3C VC/DID compatibility testing

6.2. Results

We tested the blockchain 100 times with 100 nodes using the Ethereum [85] based Truffle Ganache framework, which generates blocks on localhost (see Table 9). The "Open" feature facilitates the establishment of a user account and is a measure of how many individuals are online and ready to join the network. The "Query" is an estimate of the hash computation instructions provided to the nodes. Stakeholders are reimbursed for computing hashes in exchange. "Transfer" refers to the process of transferring transaction fees to the companies that maintain the smart contract. The Send Rate is the number of transactions completed per second. The time taken between submitting a transaction to the network and receiving the first indication of acceptance from the network is defined as latency. The rate at which the blockchain system under test commits valid transactions in a particular time period was used as throughput measure.

We also assessed the registration time for user identification, including the DID registration time and the time to issue the credentials. DID registration time was calculated by taking the time between when a user sent a DID registration request and when the blockchain provided the response. Subsequently, the time to issue the credential was calculated as the period between when a user submitted a request to an issuer and when the user got the credential. Table 10 shows the registration time for various numbers of concurrent users on the blockchain. DID registration and credential issuance take less than 30 s on average, making it a one-time activity that can be carried out in the background. With a variety of simulated users, our method took between 1.2 and 2.1 s to authenticate. As predicted, the overall authentication time increased with the number of users; however, we believe that this variation would be imperceptible to consumers while still providing stability, integrity, privacy, and tamper-proofing.

Table 11 displays the performance parameters of our self-sovereign forest supply chain blockchain with 100 peers from 10 simulated furniture board manufacturing firms at a transmit rate of 1000 query transactions per second. The average query latency is 0.03 s, with a CPU usage of 4.2% and a RAM usage of 5.6%. The query throughput is roughly 980.50 transactions per second, with a success rate of 99.98%. The average delay to initiate operations is 2.35 s, with a CPU usage of 6.5% and a memory utilization of 7.8%. The throughput for invoke operations is around 690.20 transactions per second, with a 99.95% success rate.

We also performed extensive TPS tests for invoke and query operations with varying numbers of peers, as shown in Table 12. Despite a slight decrease in TPS for invoke operations with an increase in the number of peers, our platform consistently achieves about 1000 TPS in query operations and more than 600 TPS in invoke operations, demonstrating the scalability of our model for identity transactions within the forest supply chain scenario.

6.3. Sensitivity analysis

To evaluate the robustness and adaptability of the proposed SSDI framework in Smart Forestry, a sensitivity analysis was performed under various stress scenarios. We aimed to assess the behavior of the system when subjected to real-world fluctuations in network and operational conditions. Specifically, we examined performance metrics under increased transaction throughput and induced network latency to simulate rural or bandwidth-constrained environments. A series of controlled tests were performed by issuing and verifying VCs at increasing transaction rates. Transaction throughput ranged from 50 to 1,000 VCs per minute in distributed nodes, simulating large-scale stakeholder onboarding or real-time credential exchanges during forest product certification.

As shown in Table 13, the SSDI system maintained acceptable latency up to 500 transactions per minute. Beyond that, response times and failure rates increased, primarily attributed to agent resource saturation and concurrent cryptographic operations. Optimizations such as parallel credential pipelines and message queueing are recommended to scale beyond 1,000 VCs/min.

We introduced artificial network delays ranging from 50 ms to 500 ms to evaluate the framework's behavior in connectivity-challenged environments, typical of remote forestry areas.

As seen in Table 14, the system performance degrades gracefully with increasing network delay. While verification latency increases, the system continues to synchronize VCs successfully up to 500 ms latency. It is enabled by the asynchronous nature of DIDComm and the use of local caching and retry mechanisms in edge agents. The results confirm the viability of the SSDI architecture for Smart Forestry under fluctuating load and connectivity conditions typical of large-scale environmental monitoring and regulatory systems.

6.4. Scalability analysis

Scalability is a key design requirement for SSDI systems operating in distributed, multi-stakeholder environments such as Smart Forestry. As the number of network participants increases, including forest parcels, landowners, certification bodies, and regulators, it is required to ensure that transaction performance remains stable and that the system can

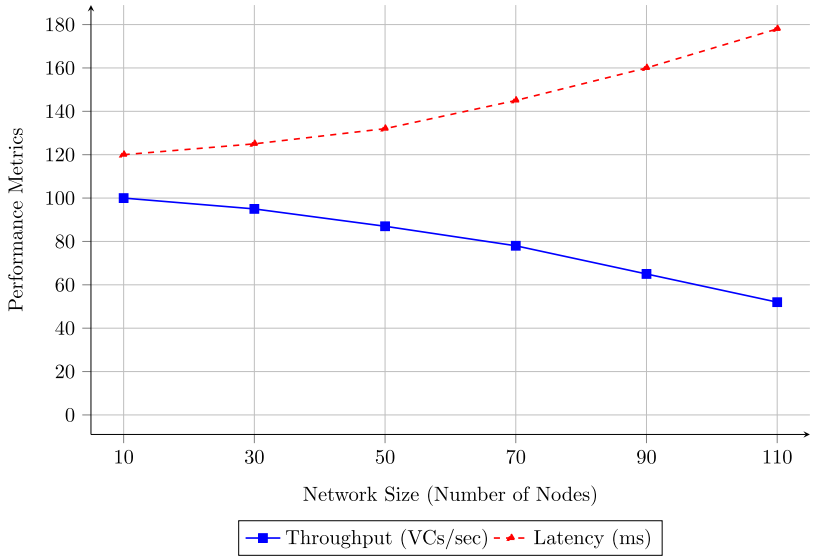


Fig. 12. Scalability Trends in SSDI Framework: Throughput and Latency vs. Network Size.

handle increasing volumes of credential issuance, verification, and identity resolution requests.

To evaluate scalability, we simulated network sizes ranging from 10 to 1,000 nodes. Each node represents an independent agent with its own edge wallet and communication channel via DIDComm. All agents interact through a shared permissioned blockchain (Hyperledger Indy TestNet) configured with dynamic gossip-based state replication. We measured two primary performance indicators:

- **Transaction Throughput (tx/sec):** Number of verifiable credentials issued and verified per second in the network.
- **End-to-End Latency (ms):** Time between the request of the credential and the verification of the presentation.

Table 15 shows that the system maintains high throughput and reasonable latency for up to 250 nodes. As the network grows beyond 500 participants, a decline in performance is observed, which is attributed to increased DID resolution traffic between nodes, a higher load on blockchain consensus, leading to queueing delays, and bottlenecks in the execution of smart contracts under concurrent access.

Fig. 12 illustrates the inverse relationship between throughput and network size and the exponential increase in latency with increasing node count. The results confirm the ability of the framework to scale for national forest systems with hundreds of agents, while pointing to optimizations needed for ultralarge deployments.

Fig. 13 illustrates the variation in transaction throughput, measured in TPS, for both query and invoke operations as the number of peers in the Smart Forestry blockchain network increases. The graph demonstrates an inverse relationship between peer count and throughput, reflecting the performance impact of increasing consensus overhead in distributed environments. Query operations maintain higher TPS due to their read-only nature and minimal consensus requirements, while invoke operations exhibit a steeper decline in throughput as they require state changes and validation across peers. The comparative analysis highlights the scalability limitations and performance considerations necessary to optimize SSDI-based smart forestry deployments in real-world multistakeholder scenarios.

Table 9
Forest supply chain network performance analysis (100 Nodes).

Name	Send rate (TPS)	Throughput (TPS)	Avg latency (s)	Max latency (s)	Min latency (s)	Success	Failure
Open	20.45	15.78	4.32	5.87	3.21	98	2
Query	50.21	40.11	2.67	3.45	2.01	99	1
Transfer	15.74	8.93	6.42	8.79	5.61	92	8

Table 10
Authentication time in forest supply chain self-sovereign framework.

Scenario	Concurrent users	DID registration time (s)	Credential issued time (s)	Total authentication time (s)
Low Demand	50	10.5	8.2	1.7
	100	12.1	9.8	1.9
	150	14.3	11.5	2.1
Medium Demand	200	16.2	13.7	2.0
	250	18.5	15.4	2.2
	300	20.1	17.2	2.1
High Demand	350	22.3	19.8	2.0
	400	24.6	21.5	2.1
	450	26.8	23.2	2.2

Table 11
Performance metrics in forest supply chain Self-Sovereign Blockchain.

Operation	Avg CPU utilization (%)	Avg Memory utilization (%)	Avg latency (s)	Throughput (TPS)	Success rate (%)
Query	3.471 **4.2**	5.058 **5.6**	0.026 **0.03**	997.36 **980.50**	100.00 **99.98**
Invoke	5.938 **6.5**	7.110 **7.8**	2.102 **2.35**	720.46 **690.20**	100.00 **99.95**

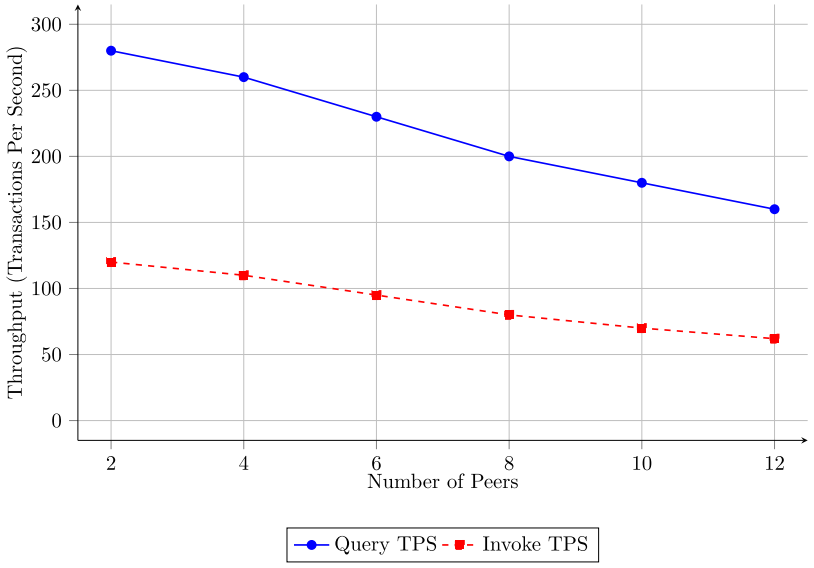


Fig. 13. Transaction Throughput vs. Number of Peers in a Permissioned Blockchain Network.

Table 12
TPS for invoke and query operations with different peers.

Number of peers	Query TPS	Invoke TPS
8	980.50	690.20
12	975.80	650.30
16	970.20	620.15

Table 13
System performance under increasing transaction volume.

VCs/min	Avg latency (ms)	CPU utilization (%)	Failure rate (%)
50	280	25	0
200	340	38	0
500	480	61	1.2
1000	750	85	3.9

Table 14
Effect of network latency on credential verification.

Network Delay (ms)	Verification time (ms)	Timeout rate (%)	VC sync success (%)
50	310	0.1	99.8
150	365	0.3	99.4
300	520	1.7	97.6
500	790	4.2	93.1

6.5. Statistical analysis

To validate the significance of the performance improvements introduced by the optimized SSDI framework in Smart Forestry, we performed a statistical evaluation on determining whether the observed gains in throughput, latency, and reliability were statistically significant compared to a baseline configuration. Two configurations of the SSDI system were tested: the baseline system, without parallel processing or credential caching, and the optimized system, which incorporated batching mechanisms, edge caching, and pre-resolved DID documents. Each configuration was subjected to 30 independent test runs, during which key performance metrics were recorded, namely throughput (measured as verifiable credentials per second), average latency (measured in milliseconds) and failure rate (percentage of timed-out or rejected operations). Table 16 summarizes the descriptive statistics for both configurations. The optimized system demonstrated marked improvements across all three metrics. Throughput increased from a mean of 71.2 VCs/sec to 89.5 VCs/sec, latency decreased from 612.4 ms to 421.3 ms, and the failure rate declined from 3.1% to just 0.9%.

To assess the statistical significance of these differences, we performed independent two-sample t-tests for each metric, assuming unequal variances. The null hypothesis for each test stated that there was no significant difference between the baseline and optimized configurations, while the alternative hypothesis posited that the optimized system performs significantly better. As shown in Table 17, all p-values were far below the significance threshold of 0.05, indicating that performance differences are statistically significant. The t-statistic for throughput was 8.72 ($p < 0.001$), for latency it was −12.14 ($p < 0.001$), and for failure rate it was −5.63 ($p < 0.001$), which confirms a high degree of confidence in the results.

Table 15
Effect of network size on SSDI system performance.

Number of nodes	Throughput (tx/sec)	Avg latency (ms)
10	95	260
50	88	310
100	81	410
250	70	580
500	58	780
1000	42	1130

Table 16
Descriptive statistics for baseline and optimized configurations.

Metric	Mean (Baseline)	Mean (Optimized)	Std. Dev. (Optimized)
Throughput (VCs/sec)	71.2	89.5	4.6
Latency (ms)	612.4	421.3	25.8
Failure Rate (%)	3.1	0.9	0.7

Table 17
t-Test results (Confidence Level = 95%).

Metric	t-statistic	p-value	Significant ($p < 0.05$)
Throughput	8.72	< 0.001	Yes
Latency	−12.14	< 0.001	Yes
Failure Rate	−5.63	< 0.001	Yes

Our findings confirm the effectiveness of the optimizations implemented. The average throughput improvement of 25.7% and the latency reduction of 31.2% contribute to a more responsive and scalable identity management solution. The reduction in the failure rate by more than two-thirds improves the reliability of the system, particularly under network or load stress.

6.6. Evaluation

Our results have shown high transaction throughput (up to 15.78 TPS for open operations) and low latency (as low as 2.01 s for authentication), indicating the efficiency of the system in real-time data management. The Forest 4.0 initiative emphasizes digital transformation through automation, data analysis, and interconnected systems to achieve sustainable resource management. The proposed framework aligns well with Forest 4.0 principles by leveraging decentralized systems to automate processes through smart contracts, reduce fraud (for example, counterfeit origin very common to circumvent US and European sanctions established for countries participating in Ukrainian conflict), and improve stakeholder trust. The IoT-enabled Smart Forestry model further integrates sensors and devices for real-time monitoring, addressing operational inefficiencies and environmental risks. By decentralizing identity management, the framework reduces the dependency on centralized authorities, empowering stakeholders (e.g., loggers, regulators) to autonomously verify supply chain data, which aligns directly with Forest 4.0's vision of democratizing data access while maintaining security, critical to combating illegal logging and ensuring chain-of-custody integrity. In addition, we comply with the Forest 4.0 challenge of balancing efficiency with environmental accountability. The low latency (2.01 to 2.2 s for authentication) and high performance support real-time monitoring of forest resources enables proactive responses to environmental threats. For example, IoT sensors that track tree health or soil moisture can trigger alerts for unsustainable practices, fostering adaptive management. The integration of verifiable credentials and smart contracts automates compliance checks (e.g., validating certifications), reducing administrative burdens and errors, and potentially advancing Forest 4.0's goal of creating data-driven, sustainable supply chains that meet regulatory demands while optimizing resource use.

6.7. Comparative analysis with existing supply chain systems

To contextualize the advantages of the SSDI framework in Smart Forestry, we can compare it with established supply chain management (SCM) systems currently employed in various industries, including forestry. Among the prominent platforms are SAP Ariba, a widely used enterprise procurement network; IBM Food Trust, a blockchain-based supply chain for food traceability; and the Forest Stewardship Council (FSC) Chain of Custody (CoC) system, which is forestry-specific and focuses on tracking certified wood products through the supply chain. Although these platforms offer varying degrees of traceability, governance, and digital workflow integration, they are predominantly built upon centralized or semi-centralized architectures. For example SAP Ariba is facilitating end-to-end procurement, but also relying heavily on centralized user directories and third-party certification authorities for identity verification. Similarly, IBM Food Trust introduced blockchain for food traceability, but did not support decentralized identity ownership or peer-based credential verification. The FSC CoC system ensured compliance with sustainable sourcing standards, but was restricted by manual verification procedures, paper-based documentation, and delayed certification issuance.

In contrast, the proposed SSDI-based Smart Forestry framework employs a decentralized identity architecture where each stakeholder — whether a landowner, processor, certifier, or regulator — controls their own cryptographically verifiable identity via DIDs and exchanges tamper-proof VCs without relying on intermediaries. The use of blockchain and smart contracts ensures real-time automation of compliance verification, transaction finality, and equitable revenue distribution (e.g., from carbon credits or sustainable timber), providing necessary transparency, auditability, and interoperability far beyond what existing centralized SCM systems offer. Table 18 presents a comparative summary of key functional capabilities in the SSDI framework and the aforementioned SCM platforms.

As illustrated in Table 18, the SSDI-based framework offers superior control over digital identity, decentralized trust mechanisms, and interoperability grounded in global standards such as W3C's DID and Verifiable Credential specifications. These enhancements enable not only improved traceability and compliance in Smart Forestry but also cross-domain integration with carbon markets, sustainable product certification, and ecosystem service payment systems. By eliminating the dependency on centralized authorities and manual verification cycles, the SSDI architecture enables a transparent, scalable, and user-centric supply chain infrastructure for the forestry domain.

7. Discussion

Our study demonstrated that the integration of SSDI with blockchain technology significantly improves traceability, sustainability, and compliance in forest supply chains. Using Ethereum-based frameworks and IoT-enabled data collection, the system achieves high transaction throughput (up to 1,000 TPS for queries) and low latency (0.03 s), while ensuring immutable records and decentralized trust. However, blockchain scalability remains a critical concern for large-scale forestry operations. Current blockchain architectures, such as Ethereum, face limitations in transaction processing speed and energy efficiency, which could impact real-time data management in vast and geographically dispersed forestry networks. For example, while our prototype handled 100 nodes effectively, scaling to thousands of simulated stakeholders (e.g., logging companies, regulators, IoT devices) may strain network performance due to latency spikes and computational overhead. Energy-intensive consensus mechanisms such as Proof-of-Work (PoW) conflict with sustainability goals, a core focus of Forest 4.0. To address these challenges, hybrid solutions combining layer-2 protocols (e.g., state channels, sidechains) with energy-efficient consensus algorithms (e.g., Proof-of-Stake PoS)) could further optimize scalability. Adopting modular blockchains or enterprise-focused frameworks such as Hyperledger Fabric, designed for high throughput and permissioned access, may better suit the need of the forestry sector for both scalability and regulatory compliance, helping with the viability of the

Table 18
Comparative analysis of SSDI with Existing supply chain systems.

Feature	SAP Ariba	IBM food trust	FSC CoC system	SSDI smart forestry
Identity Ownership	Centralized user account	Centralized membership	Third-party certified entities	Self-owned DIDs
Credential Verification	Central directory lookup	Limited support	Manual audit reports	Verifiable Credentials with cryptographic proofs
Traceability Mechanism	ERP integration	Blockchain ledger	Paper-based CoC documentation	Real-time blockchain-based DID ledger
Auditability	Internal logs	Ledger snapshots	Periodic third-party inspections	Continuous, immutable on-chain audits
Automation Level	Workflow-based triggers	Smart contracts (partial)	Manual logging and validation	Fully automated via smart contracts
Transparency and Trust	Trust through vendor reputation	Moderate via consortium chain	Trust in FSC intermediaries	Cryptographic trust via peer-verified credentials
Standards and Interoperability	Proprietary APIs	Hyperledger Fabric-based	FSC internal standards	W3C DID, VC, JSON-LD

system for large-scale operations without compromising sustainability or operational efficiency.

Although the decentralized blockchain ledger offers tamper-proof records and transparency, the environmental impact of its energy consumption, particularly for public blockchain networks such as Ethereum, remains a critical concern. We acknowledge energy consumption as a challenge. For example, Ethereum's original PoW consensus mechanism requires substantial computational power and contributes to high carbon emissions. Our approach, as shown by the experimental setup using 100 nodes on a private Hyperledger network (which is more energy efficient than public blockchains) highlights scalability trade-offs: higher transaction throughput (e.g., 980 TPS for queries) may increase energy use, albeit less severely than PoW systems. To mitigate the environmental impact of blockchain, we advocate for the transition to energy-efficient consensus mechanisms such as PoS or hybrid models, which reduce computational overhead. For example, Ethereum's move to PoS in 2022 reduces energy use by 99.95%, a critical consideration for forest applications aiming to align with carbon-neutral goals. Adopting private or permissioned blockchains (as in our Hyperledger implementation) inherently lowers energy use by limiting participation to trusted nodes, avoiding the energy-intensive mining of public networks. The near-term future work plan also optimizes smart contract code and data storage (e.g., off-chain solutions like IPFS) to minimize on-chain transactions. Finally, considering ever-widening integration of renewable energy sources for blockchain nodes and leveraging carbon offset programs could further reconcile the benefits of technology with environmental stewardship.

7.1. Challenges

The overall usability of the proposed SSDI framework depends on its accessibility and intuitiveness for various stakeholders in forest management, including forest managers, regulatory bodies, loggers, and IoT device operators. Although the study demonstrates technical success in transaction throughput and latency, real-world usability challenges emerge in the interaction design of decentralized systems. For example, if processes are not well automated, forest managers in remote areas may struggle with managing DIDs and verifiable credentials through digital wallets, particularly where technical knowledge is limited. The requirement for stakeholders to navigate cryptographic key pairs, DID resolution, and blockchain-based verifications introduces complexity, necessitating user-friendly interfaces and training programs. The integration of IoT devices, which is critical for real-time data collection, depends on reliable connectivity, which is often lacking in forested regions. The framework's reliance on Edge Agents and cloud-based systems assumes consistent internet access, a barrier in areas with poor infrastructure. Without simplified tools and localized support, stakeholder adoption is stifled by operational friction, which undermines the system's potential for scalability.

The reliability of smart contracts is another challenge. First, code vulnerabilities pose significant risks. For example, reentry attacks, where malicious actors exploit flawed contract logic to drain funds, could disrupt automated payments or certification processes. In forestry, where smart contracts might trigger payments upon sustainable harvesting verified by the Internet of Things, a single coding error could allow fraudulent claims or financial losses. Second, data integrity at the source is paramount. Compromised IoT devices, whether through cyberattacks, calibration errors, or environmental interference, could feed inaccurate data into the system. For example, tampered sensors can falsely validate unsustainable logging practices, affecting compliance with certifications such as the FSC. The third issue here is the rigidity of smart contracts that complicates adaptation to dynamic regulatory environments. Forestry regulations, such as updated sustainability standards or carbon credit protocols, often evolve. Smart contracts, once deployed, are immutable by design, requiring costly and time-consuming upgrades to reflect new rules, whose inflexibility could lock supply chains into outdated compliance frameworks, creating legal and operational risks. Fourth, dispute resolution mechanisms remain underdeveloped. Although blockchain eliminates intermediaries, disputes over contract execution (e.g., conflicting sensor data or certification disputes) can still require arbitration, potentially forcing stakeholders to revert to off-chain centralized authorities, a contradiction to the paper's vision of full decentralization.

Despite the technical validation of the framework, barriers to systemic adoption persist. The first is the digital divide: Forestry operations typically occur in remote regions that often lack infrastructure (e.g., high-speed Internet, IoT sensors), and forest operators also often lack the technical expertise required for the implementation of blockchain and SSDI. The high upfront costs of IoT devices, blockchain nodes, and training programs pose financial risks for small to medium enterprises (SMEs) in the sector. Resistance to change from entrenched paper-based systems and centralized identity management further complicates adoption, as stakeholders can perceive decentralized systems as disruptive or unnecessary. Regulatory uncertainty also plays a role; existing frameworks rarely recognize blockchain-based credentials, creating legal ambiguities around compliance and liability. Environmental concerns, such as blockchain energy consumption, may deter eco-conscious stakeholders. To overcome these barriers, the study suggests phased integration, public–private partnerships for infrastructure investment, and policy advocacy to recognize digital credentials legally.

However, without addressing these sociotechnical challenges, the theoretical benefits of the framework may remain isolated to pilot projects, failing to achieve sector-wide transformation.

Next, such approaches also introduce social and policy challenges. Socially, stakeholders such as logging companies, regulatory bodies, and local communities can resist adoption due to entrenched practices, distrust in decentralized systems, or lack of technical background. For example, small-scale forest operators might perceive SSDI as a threat to traditional workflows or fear exclusion from decision-making processes, exacerbating existing power imbalances. Policymakers face the challenge of designing frameworks that recognize digital credentials as legally binding while ensuring interoperability with legacy systems. Regulatory issues include reconciling blockchain immutability with data privacy laws (e.g., GDPR), particularly in cross-border supply chains where conflicting national regulations may impede compliance. The energy consumption of blockchain networks could clash with sustainability goals, requiring policies to incentivize eco-friendly consensus mechanisms.

Finally, the economic feasibility of using our approach for small to medium-scale forest operations (SMFO) is another interesting point of discussion as it depends on balancing upfront costs with long-term benefits. We acknowledge that SMFOs often face resource constraints, making initial investment in blockchain infrastructure (e.g., nodes, IoT sensors, and edge agents) and training a significant barrier. However, reduced fraud through tamper proof records could reduce compliance costs related to illegal logging audits, while automated smart contracts could streamline payments and certifications, cutting administrative overhead. SSDI's decentralized verification could allow SMFOs to access premium markets (e.g., FSC-certified products) by providing verifiable sustainability credentials, enhancing revenue streams.

7.2. Scalability considerations for larger networks

While the proposed SSDI framework demonstrated high throughput (up to 997 TPS) and low latency (as low as 2.01 s) in a 100-node environment, we recognize that a significantly larger network—comprising thousands of stakeholders and IoT devices may introduce scalability challenges. These include increased communication overhead, potential latency spikes, and reduced transaction throughput due to consensus delays and network congestion. To mitigate such issues, future iterations of the framework may incorporate Layer-2 solutions (e.g. state channels, side chains) and transition to energy-efficient consensus mechanisms such as PoS. Permissioned blockchain networks (e.g., Hyperledger Fabric) offer superior scalability for enterprise use cases through selective node participation. The integration of edge computing and data aggregation techniques can further reduce on-chain transaction loads by preprocessing IoT data locally. The enhancements overall are essential for ensuring that the SSDI framework remains performant and sustainable at scale, particularly in complex and data-intensive forestry ecosystems.

7.3. Future possibilities

The future of digital identity management in Forest 4.0 and other sectors will likely be shaped by evolving technologies such as artificial intelligence, machine learning, and ongoing blockchain innovations. Anticipated trends include a shift toward more user-centric identity models, increased interoperability between systems and sectors, and the integration of advanced biometric verification methods. As digital identity management systems advance, they will play a daily role in the global transition to a more secure, efficient, and sustainable economy.

Although the experimental results demonstrate high transaction throughput (for example, 15.78 TPS for "Open" operations) and reduced latency, the choice of Ethereum still introduces inherent limitations. Ethereum's PoW consensus mechanism (used in the Truffle Ganache test environment) is somewhat prone to scalability bottlenecks, especially in real-world scenarios with thousands of stakeholders and IoT devices. For example, Ethereum's current mainnet supports only 15–45 TPS, which may not be sufficient for large-scale forest supply chains that require real-time data from sensors, logging operations and regulatory checks. Gas fees could escalate during periods of network congestion, making frequent microtransactions (e.g., IoT data uploads) economically unviable for smallholders or remote forestry operations. To address these limitations, future work is exploration of layer-2 scaling solutions (e.g., Optimism, Polygon) or hybrid blockchain architectures (e.g., Hyperledger Fabric for permissioned data sharing with Ethereum for public audit trails). Edge computing could preprocess IoT data locally, reducing on-chain storage needs, while zero-knowledge proofs (e.g., zk-SNARKs) might enhance privacy for sensitive forestry data. Transitioning to PoS or Delegated Proof-of-Stake (DPoS) consensus mechanisms could reduce energy consumption and improve TPS. Finally, integrating decentralized identity standards (for example, W3C DID v2.0) with AI-driven analytics could automate compliance checks and fraud detection, aligning with Forest 4.0's vision of smart and sustainable ecosystems.

The interoperability of the proposed SSDI framework is the adhesion to open standards and modular design. GS1 standards, widely used in supply chain management for product identifiers (e.g. GTIN) and event data (e.g. EPCIS), could bridge blockchain-based provenance data with ERP systems. For IoT integration, the MQTT or OPC UA protocols standardize sensor data transmission, while ISO/IEC 18000–63 (RFID for item tracking) align physical asset identifiers with blockchain records. Our use of Ethereum's JSON-RPC API for smart contracts could be further extended to RESTful APIs for seamless ERP integration, allowing automated updates of inventory or compliance statuses. To address cross-system interoperability, blockchain-agnostic protocols such as Hyperledger Cactus or Cosmos IBC allow the SSDI framework to interact with heterogeneous blockchain networks used by stakeholders (e.g., logging companies or regulators). For data governance, adopting ISO 14001 (environmental management) and Forest Certification Program (PEFC)/FSC certification schemas would harmonize sustainability metrics across systems. The reliance on Ethereum's ERC-725 (for DID management) could be complemented by OpenChain specifications to align with enterprise-grade blockchain systems. EDIFACT or RosettaNet messaging standards facilitate legacy system integration, ensuring that verifiable credentials (e.g., harvest certifications) are machine readable by older ERP modules. Having such compatibility makes it possible to integrate with certification programs such as the FSC and the PEFC, where VCs can automate compliance checks for chain-of-control documentation. For example, smart contracts could validate the origin of wood against geospatial data from IoT sensors, ensuring adherence to the EU Timber Regulation. The use of DIDs enhances interoperability across jurisdictions by providing a unified identity layer for stakeholders (e.g., loggers, regulators, and NGOs). For example, cross-border timber exports could use VCs to streamline customs verification under the Convention on International Trade in Endangered Species.

Considering the rapid progress, the reliance on blockchain cryptographic security could be further revolutionized by quantum computing. Current blockchain systems, including Ethereum, use elliptic-curve cryptography (ECC) and RSA, which are vulnerable to quantum attacks via Shor's algorithm. Future enhancements could integrate post-quantum cryptographic algorithms (e.g., lattice-based cryptography) into the SSDI framework to ensure long-term security. For example, the Forest 4.0 system could adopt quantum-resistant DIDs and verifiable credentials, protecting against future threats. Quantum computing could optimize supply chain logistics by optimizing ultra-fast route optimization for timber transport, further increasing the reduction of carbon footprints.

Similarly, advancements in AI-driven IoT sensors and edge computing could further enhance such frameworks and is our next objective. Next-gen IoT devices with embedded machine learning (e.g., federated

learning models) could analyze data locally (e.g., detecting illegal logging via acoustic sensors or predicting pest outbreaks) without relying on centralized cloud servers, still aligning with the emphasis on decentralized systems and reduces latency in decision making. Edge computing could also enable in situ smart contracts, where IoT devices autonomously trigger blockchain transactions (e.g., verifying sustainable harvesting practices) without the need for centralized verification.

8. Conclusion

The key findings of the experimental evaluation support the substantial impact of blockchain technology on improving transparency, operational efficiency, and trust mechanisms within the forest supply chain ecosystem. The proposed system exhibited strong performance capabilities, achieving a maximum query throughput of **997.36 TPS** and an invoke throughput of **720.46 TPS**, making it considerable for real-world forestry scenarios where timely and secure data exchanges are of essence.

Authentication processes also proved to be consistently responsive, with total authentication times ranging between **2.01 and 2.2 seconds** in varying levels of user demand (50 to 450 concurrent users). The responsiveness ensures seamless user interaction and enables efficient data access without perceptible latency, an essential feature for systems deployed in dynamic operational contexts such as forest resource monitoring and logging.

The implementation of the SSDI framework within Smart Forestry showed promise in mitigating identity fraud and securing the provenance of the data. **DID registration and credential issuance times of the DID averaged less than 30 seconds**, demonstrating the low temporal overhead of the identity setup processes even under higher concurrent user loads. We believe this reinforces the viability of SSDI in supporting real-time secure identity verification essential to trace timber legality and maintain credible chain-of-custody records.

In addition, the system maintained impressive reliability and robustness under test conditions. Transaction success rates reached **99.98% for query operations** and **99.95% for invoke operations** with a network of 100 nodes, confirming consistent functionality and fault tolerance at scale. In terms of computational efficiency, the average CPU utilization was as low as **4.2%** and RAM usage at **5.6%**, highlighting the fairly lightweight resource requirements of the system and its potential for long-term sustainable deployment across distributed forest networks.

CRediT authorship contribution statement

Robertas Damaševičius: Writing – review & editing, Writing – original draft, Visualization, Validation, Supervision, Software, Resources, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization. **Rytis Maskeliūnas:** Writing – review & editing, Writing – original draft, Validation, Supervision, Software, Resources, Project administration, Methodology, Investigation, Funding acquisition, Formal analysis, Data curation, Conceptualization.

Funding

This research paper has received funding from Horizon Europe Framework Programme (HORIZON), call Teaming for Excellence (HORIZON-WIDERA-2022-ACCESS-01-two-stage) - Creation of the centre of excellence in smart forestry "Forest 4.0" No. 101059985. This research has been co-funded by the European Union under the project FOREST 4.0 - "Ekscelencijos centras tvariai miško bioekonomikai vystyti" No. 10-042-P-0002.5.

Declaration of competing interest

The authors declare that they have no known competing financial interests or personal relationships that could have appeared to influence the work reported in this paper.

Acknowledgments

The latest versions of AI-based tools, Writefull for Overleaf and Grammarly, were utilized to ensure grammatical accuracy and enhance language clarity in the preparation of this document.

References

[1] Ahmed Md Rayhan, et al., Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey, IEEE Access 10 (2022) 113436–113481.
[2] Christos Roumeliotis, et al., Blockchain and digital twins in smart industry 4.0: The use case of supply chain-a review of integration techniques and applications, Designs 8 (6) (2024) 105.
[3] Y. Liu, et al., Design pattern as a service for blockchain-based self-sovereign identity, IEEE Softw. 37 (5) (2020) 30–36.
[4] Madjid Tavana, Reinventing the future supply chains with disruptive technologies, Supply Chain Anal. 4 (2023) 100047.
[5] D.E.D.I. Abou-Tair, et al., A distributed and secure self-sovereign-based framework for systems of systems, Sensors 23 (17) (2023).
[6] Rosanna Cole, Mark Stevenson, James Aitken, Blockchain technology: implications for operations and supply chain management, Supply Chain Manag.: An Int. J. 24 (4) (2019) 469–483.
[7] I.A. Omar, et al., Blockchain-based approach for crop index insurance in agricultural supply chain, IEEE Access 11 (2023) 118660–118675.
[8] U. Tokkozhina, A.L. Martins, J.C. Ferreira, Multi-tier supply chain behavior with blockchain technology: evidence from a frozen fish supply chain, Oper. Manag. Res. 16 (3) (2023) 1562–1576.
[9] B. Houtan, A.S. Hafid, D. Makrakis, A survey on blockchain-based self-sovereign patient identity in healthcare, IEEE Access 8 (2020) 90478–90494.
[10] M. Tcholakian, et al., Self-sovereign identity for consented and content-based access to medical records using blockchain, Secur. Commun. Netw. 2023 (2023).
[11] J.St. Clair, et al., Blockchain, interoperability, and self-sovereign identity: Trust me, it's my data, Blockchain Heal. Today 3 (2020).
[12] Š. Čučko, M. Turkanović, Decentralized and self-sovereign identity: Systematic mapping study, IEEE Access 9 (2021) 139009–139027.
[13] Philip Tetteh Quarshie, Abdul-Rahim Abdulai, Evan D.G. Fraser, Africa's "seed" revolution and value chain constraints to early generation seeds commercialization and adoption in ghana, Front. Sustain. Food Syst. 5 (2021) 665297.
[14] L. Cocco, R. Tonelli, M. Marchesi, Blockchain and self sovereign identity to support quality in the food supply chain, Futur. Internet 13 (12) (2021).
[15] Zhaoyuan He, Paul Turner, Blockchain applications in forestry: A systematic literature review, Appl. Sci. (2022).
[16] Fabian Müller, D. Jaeger, M. Hanewinkel, Digitization in wood supply - a review on how industry 4.0 will change the forest value chain, Comput. Electron. Agric. 162 (2019) 206–218.
[17] Yan Feng, J. Audy, Forestry 4.0: a framework for the forest supply chain toward industry 4.0, GestÃo & ProduÇÃo (2020).
[18] M.R. Ahmed, A.K.M.M. Islam, S. Shatabda, S. Islam, Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey, IEEE Access 10 (2022) 113436–113481.
[19] M. Popa, S.M. Stoklossa, S. Mazumdar, ChainDiscipline - towards a blockchain-IoT-based self-sovereign identity management framework, IEEE Trans. Serv. Comput. 16 (5) (2023) 3238–3251.
[20] Shuchih Ernest Chang, Yi-Chian Chen, Ming-Fang Lu, Supply chain re-engineering using blockchain technology: A case of smart contract based tracking process, Technol. Forecast. Soc. Change 144 (2019) 1–11.
[21] SeyyedHossein Barati, A system dynamics approach for leveraging blockchain technology to enhance demand forecasting in supply chain management, Supply Chain Anal. 10 (2025) 100115.
[22] S. Ismail, H. Reza, K. Salameh, H. Kashani Zadeh, F. Vasefi, Toward an intelligent blockchain IoT-enabled fish supply chain: A review and conceptual framework, Sensors 23 (11) (2023).
[23] Alok Raj, Abheek Anjan Mukherjee, Ana Beatriz Lopes de Sousa Jabbour, Samir K Srivastava, Supply chain management during and post-COVID-19 pandemic: Mitigation strategies and practical lessons learned, J. Bus. Res. 142 (2022) 1125–1139.
[24] Hans Pretzsch, et al., Maintenance of long-term experiments for unique insights into forest growth dynamics and trends: review and perspectives, Eur. J. For. Res. 138 (2019) 165–185.

[25] Wendy L. Tate, et al., Seeing the forest and not the trees: Learning from nature's circular economy, Resour. Conserv. Recycl. 149 (2019) 115–129.
[26] Luísa Pinto, Green supply chain practices and company performance in portuguese manufacturing sector, Bus. Strat. Environ. 29 (5) (2020) 1832–1849.
[27] Pradana, et al., Blockchain-based traceability system for Indonesian coffee digital business ecosystem, Int. J. Eng. Trans. B: Appl. 36 (5) (2023) 879–893.
[28] SA Nitoslawski, et al., The digital forest: Mapping a decade of knowledge on technological applications for forest ecosystems, Earth's Futur. 9 (8) (2021) e2021EF002123.
[29] Virendra Balon, Green supply chain management: Pressures, practices, and performance—An integrative literature review, Bus. Strat. Dev. 3 (2) (2020) 226–244.
[30] I. Wayan Gede Krisna Arimjaya, Muhammad Dimyati, Remote sensing and geographic information systems technics for spatial-based development planning and policy, Int. J. Electr. Comput. Eng. 12 (5) (2022) 5073.
[31] Salla Rantala, et al., Governance of forests and governance of forest information: Interlinkages in the age of open and digital data, For. Policy Econ. 113 (2020) 102123.
[32] Akshaya K Verma, et al., Biodiversity and sustainability, Sustain.: Fundam. Appl. (2020) 255–275.
[33] Petri Helo, Javad Rouzafzoon, An agent-based simulation and logistics optimization model for managing uncertain demand in forest supply chains, Supply Chain Anal. 4 (2023) 100042.
[34] Michaela A. Balzarova, Blockchain technology–a new era of ecolabelling schemes? Corp. Gov.: Int. J. Bus. in Soc. 21 (1) (2021) 159–174.
[35] Lukas Stopfer, Alexander Kaulen, Thomas Purfürst, Potential of blockchain technology in wood supply chains, Comput. Electron. Agric. 216 (2024) 108496.
[36] Y. Kang, Y.B. Park, Secure access control realization based on self-sovereign identity for cloud CDM, Appl. Sci. 12 (19) (2022).
[37] Alex Vinicio Gavilanes Montoya, Danny Daniel Castillo Vizuete, Marina Viorela Marcu, Exploring the role of ICTs and communication flows in the forest sector, Sustainability 15 (14) (2023) 10973.
[38] Bin Jia, et al., Blockchain-enabled federated learning data protection aggregation scheme with differential privacy and homomorphic encryption in iIoT, IEEE Trans. Ind. Inform. 18 (6) (2021) 4049–4058.
[39] Sarah Prebble, Jessica McLean, Donna Houston, Smart urban forests: An overview of more-than-human and more-than-real urban forest management in Australian cities, Digit. Geogr. Soc. 2 (2021) 100013.
[40] Nate G McDowell, et al., Pervasive shifts in forest dynamics in a changing world, Science 368 (6494) (2020) eaaz9463.
[41] Teijo Palander, Lauri Vesa, Data-driven optimization of forestry and wood procurement toward carbon-neutral logistics of forest industry, Forests 13 (5) (2022) 759.
[42] Andreas Holzinger, et al., Digital transformation in smart farm and forest operations needs human-centered AI: Challenges and future directions, Sensors 22 (8) (2022) 3043.
[43] A. Falayi, Q. Wang, W. Liao, W. Yu, Survey of distributed and decentralized IoT securities: Approaches using deep learning and blockchain technology, Futur. Internet 15 (5) (2023).
[44] Nicholas C Coops, et al., Framework for near real-time forest inventory using multi source remote sensing data, Forestry 96 (1) (2023) 1–19.
[45] Sophie A Nitoslawski, et al., Smarter ecosystems for smarter cities? A review of trends, technologies, and turning points for smart urban forestry, Sustain. Cities Soc. 51 (2019) 101770.
[46] Piera Centobelli, et al., Blockchain technology for bridging trust, traceability and transparency in circular supply chain, Inf. Manag. 59 (7) (2022) 103508.
[47] E.S. Fathalla, et al., PT-SSIM: A proactive, trustworthy self-sovereign identity management system, IEEE Internet Things J. 10 (19) (2023) 17155–17169.
[48] Dimitrios Panagiotidis, Azadeh Abdollahnejad, Martin Slavík, Assessment of stem volume on plots using terrestrial laser scanner: A precision forestry application, Sensors 21 (1) (2021) 301.
[49] Uferah Shafi, et al., Precision agriculture techniques and practices: From considerations to applications, Sensors 19 (17) (2019) 3796.
[50] Mohammed Musa, et al., Distributed geospatial information systems challenges and opportunities, Explor. Remote. Sensing-Methods Appl. (2024).
[51] Md Shohidul Islam, et al., Blockchain-enabled cybersecurity provision for scalable heterogeneous network: A comprehensive survey., CMES Comput. Model. Eng. Sci. 138 (1) (2024).
[52] Johan Henriques, William Westerlund, Digitalization of forest management: Next generation unsupervised monitoring using internet of things and blockchain, 2020.
[53] Hamed Baziyad, Vahid Kayvanfar, Aseem Kinra, A bibliometric analysis of data-driven technologies in digital supply chains, Supply Chain Anal. 6 (2024) 100067.
[54] Love Allen Chijioke Ahakonye, Cosmas Ifeanyi Nwakanma, Dong-Seong Kim, Tides of blockchain in IoT cybersecurity, Sensors 24 (10) (2024) 3111.
[55] Didier G Leibovici, et al., Geospatial standards, in: The Routledge Handbook of Geospatial Technologies and Society, Taylor & Francis, 2023, p. 60.
[56] Lukas Stopfer, Alexander Kaulen, Thomas Purfürst, Potential of blockchain technology in wood supply chains, Comput. Electron. Agric. 216 (2024) 108496.
[57] Zhaoyuan He, Paul Turner, A systematic review on technologies and industry 4.0 in the forest supply chain: A framework identifying challenges and opportunities, Logistics 5 (4) (2021) 88.
[58] R.M. Ellahi, L.C. Wood, A.E.-D.A. Bekhit, Blockchain-based frameworks for food traceability: A systematic review, Foods 12 (16) (2023).
[59] Razatulshima Ghazali, et al., Blockchain for record-keeping and data verifying: proof of concept, Multimedia Tools Appl. 81 (25) (2022) 36587–36605.
[60] Alexander Kaulen, et al., Systematics of forestry technology for tracing the timber supply chain, Forests 14 (9) (2023) 1718.
[61] A. De Salve, et al., A multi-layer trust framework for self sovereign identity on blockchain, Online Soc. Networks Media 37–38 (2023).
[62] Justin Sunny, Naveen Undralla, V. Madhusudanan Pillai, Supply chain transparency through blockchain-based traceability: An overview with demonstration, Comput. Ind. Eng. 150 (2020) 106895.
[63] Michaela Balzarova, Celia Dyer, Michael Falta, Perceptions of blockchain readiness for fairtrade programmes, Technol. Forecast. Soc. Change 185 (2022) 122086.
[64] William Nikolakis, Lijo John, Harish Krishnan, How blockchain can shape sustainable global value chains: An evidence, verifiability, and enforceability (EVE) framework, Sustainability 10 (11) (2018) 3926.
[65] Michaela A. Balzarova, Blockchain technology – a new era of ecolabelling schemes? Corp. Gov.: Int. J. Bus. in Soc. 21 (1) (2020) 159–174.
[66] Robert F. Keefe, Eloise G. Zimbelman, Gianni Picchi, Use of individual tree and product level data to improve operational forestry, Curr. For. Rep. 8 (2) (2022) 148–165.
[67] Pankaj Dutta, et al., Blockchain technology in supply chain operations: Applications, challenges and research opportunities, Transp. Res. Part E: Logist. Transp. Rev. 142 (2020) 102067.
[68] Peter Howson, et al., Cryptocarbon: The promises and pitfalls of forest protection on a blockchain, Geoforum 100 (2019) 1–9.
[69] M. Dieye, et al., A self-sovereign identity based on zero-knowledge proof and blockchain, IEEE Access 11 (2023) 49445–49455.
[70] A. Farao, et al., INCHAIN: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain, Int. J. Inf. Secur. (2023).
[71] K.C. Toth, A. Anderson-Priddy, Self-sovereign digital identity: A paradigm shift for identity, IEEE Secur. Priv. 17 (3) (2019) 17–27.
[72] Š. Čučko, V. Keršič, M. Turkanović, Towards a catalogue of self-sovereign identity design patterns, Appl. Sci. 13 (9) (2023).
[73] S. Cucko, S. Becirovic, A. Kamisalic, S. Mrdovic, M. Turkanovic, Towards the classification of self-sovereign identity properties, IEEE Access 10 (2022) 88306–88329.
[74] M.S. Ferdous, U. Cali, U. Halden, W. Prinz, Leveraging self-sovereign identity & distributed ledger technology in renewable energy certificate ecosystems, J. Clean. Prod. 422 (2023).
[75] T. M., K. Makkithaya, N. V.G., A trusted IoT data sharing and secure oracle based access for agricultural production risk management, Comput. Electron. Agric. 204 (2023).
[76] Pinky Bai, et al., Self-sovereignty identity management model for smart healthcare system, Sensors 22 (13) (2022).
[77] S. Manski, Distributed ledger technologies, value accounting, and the self sovereign identity, Front. Blockchain 3 (2020).
[78] E. Samir, et al., DT-SSIM: A decentralized trustworthy self-sovereign identity management framework, IEEE Internet Things J. 9 (11) (2022) 7972–7988.
[79] F. Schardong, R. Custódio, Self-sovereign identity: A systematic review, mapping and taxonomy, Sensors 22 (15) (2022).
[80] M. Šestak, D. Copot, Towards trusted data sharing and exchange in agro-food supply chains: Design principles for agricultural data spaces, Sustainability 15 (18) (2023).
[81] A. Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, A survey on essential components of a self-sovereign identity, Comput. Sci. Rev. 30 (2018) 80–86.
[82] M. Shuaib, et al., Land registry framework based on self-sovereign identity (SSI) for environmental sustainability, Sustainability 14 (9) (2022).
[83] M. Shuaib, et al., Identity model for blockchain-based land registry system: A comparison, Wirel. Commun. Mob. Comput. 2022 (2022).
[84] R. Soltani, U.T. Nguyen, A. An, A survey of self-sovereign identity ecosystem, Secur. Commun. Netw. 2021 (2021).
[85] Gavin Wood, et al., Ethereum: A secure decentralised generalised transaction ledger, Ethereum Proj. Yellow Pap. 151 (2014) (2014) 1–32.