*sustainability*

MDPI

*Article*

# Land Registry Framework Based on Self-Sovereign Identity (SSI) for Environmental Sustainability

**Mohammed Shuaib [1,2], Noor Hafizah Hassan [1], Sahnius Usman [1], Shadab Alam [2], Surbhi Bhatia [3], Parul Agarwal [4] and Sheikh Mohammad Idrees [5,*]**

1 Razak Faculty of Technology and Informatics (RFTI), Universiti Teknologi Malaysia (UTM), Kuala Lumpur 54100, Malaysia; talkshuaib@gmail.com (M.S.); noorhafizah.kl@utm.my (N.H.H.); sahnius.kl@utm.my (S.U.)
2 College of Computer Science and Information Technology, Jazan University, Jazan 45142, Saudi Arabia; s4shadab@gmail.com
3 Department of Information Systems, College of Computer Science and Information Technology, King Faisal University, AlAhsa 31982, Saudi Arabia; sbhatia@kfu.edu.sa
4 Department of Computer Science and Engineering, Jamia Hamdard, New Delhi 110062, India; pagarwal@jamiahamdard.ac.in
5 Department of Computer Science (IDI), Norwegian University of Science and Technology, 2815 Gjovik, Norway
* Correspondence: sheikh.m.idrees@ntnu.no

**Abstract:** Providing a system user with a unique and secure identity is a prerequisite for authentication and authorization aspects of a security system. It is generally understood that the existing digital identity systems store the identity details in centralized databases, and users store the identity details in centralized databases in which users do not have any control over them. These vulnerabilities in the traditional digital identities make them susceptible to various malicious assaults and modifications. Users' personally identifiable information (PII) may leak through these identity solutions that can consequently affect other applications being used by the users, and they have no control over them. Land registration is a major domain of governance that defines civilians' well-being and needs to be handled properly to avoid conflict and to support Environmental Sustainability. These traditional land registry applications also lack identity parameters due to weaknesses in identity solutions. A secure and reliable digital identity solution is the need of the hour. Self-sovereign identity (SSI), a new concept, is becoming more popular as a secure and reliable identity solution for users based on identity principles. SSI provides users with a way to control their personal information and consent for it to be used in various ways. In addition, the user's identity details are stored in a decentralized manner, which helps to overcome the problems with digital identity solutions. This article reviews existing SSI solutions and analyzes them using SSI principles. It also assesses the SSI components required for constructing SSI frameworks that adhere to the SSI principles. Furthermore, it defines the procedures for establishing an SSI ecosystem, explores the laws governing digital identity that governments have adopted, and identifies SSI applications in several fields. Finally, a review of SSI applications in the domain of land registry systems is given in order to propose an SSI-based land registry framework for a secure and reliable land registry system.

**Keywords:** land registry; SSI compliance; identity principle; SSI components; self-sovereign identity; environmental sustainability



**Citation:** Shuaib, M.; Hassan, N.H.; Usman, S.; Alam, S.; Bhatia, S.; Agarwal, P.; Idrees, S.M. Land Registry Framework Based on Self-Sovereign Identity (SSI) for Environmental Sustainability. *Sustainability* **2022**, *14*, 5400. https://doi.org/10.3390/su14095400

Academic Editors: Saqib Iqbal Hakak, Thippa Reddy Gadekallu and Pierfrancesco De Paola

Received: 20 February 2022
Accepted: 20 April 2022
Published: 30 April 2022



## 1. Introduction

A recent survey highlighted that 37% of employees in US firms reset their passwords more than 50 times each year and have been losing around 426 USD annually due to password glitches, in addition to the fact that this is affecting their efficacy at work [1]. Additionally, a world bank survey revealed that around 14% of the global population

lacks proof of identity in any form [2,3]. Providing individuals with an identity and maintaining secure and reliable identity storage are major challenges. Compared with providing individuals with an identity, managing a secured and reliable identity is a far more significant challenge. In a recent incident, Cambridge Analytica leaked 87 million Facebook users' PII details due to a security breach in the system of a third-party service provider [3]. There are many examples of data breaches due to the centralized nature of data recordings and the use of third-party service providers. Digital identities and their security are becoming more critical with the advancement and adaptation of online services.

The land registry system provides a way to transfer land ownership while protecting the rights of the people, which increases the trust among people. There are numerous loopholes in the current land registry system which pose risks for crimes such as land stealing or force land-grabs, resulting in most civil court cases. Most of these cases take months, years, or even decades to resolve since they go from local courts to the Supreme Court. Plus, majority of people in the country do not have the time and money they would need to spend on these cases [4,5].

The main problem with the current system is inadequately coordinated information across different government departments that are not coordinated adequately, making it easy for unscrupulous officials to modify official land records. Many fraud cases related to land titling are only detected locally, which means that a centralized system is insufficient in this case [6]. As a result, land records may be tampered with, and forged.

Verifying the identity of all participants in a transaction is essential to avoid fraud [7]. Current land registry systems have several shortcomings which can be avoided by utilizing blockchain technology [8]. A limitation in blockchain-based land registry systems is the lack of suitable identity solutions [9–11]. The use of a digital identity in blockchain-based land registry systems saves time, decreases the fraud risk, and reduces data loss [12]. The SSI concept fills this gap by providing a decentralized identity and giving individuals complete control over their identities and personal data [13].

Self-sovereign identity (SSI) is a next-generation identity management model that secures and manages reliable identity records [14]. The identity records are stored in a decentralized manner and provide users with control over their identity details [15]. In this way, SSI can handle the shortcomings of traditional identity solutions. Users of SSI solutions have full control over their personal identity information (PII), and give their consent for using the PII. Therefore, the issues with the centralized storage and identity theft can be resolved [16,17]. SSI is a new paradigm, and several researchers are working in this domain to review it and analyze its applications; however, the academic literature is still limited. Some of the related literature can be found in [15,18–20]. In [18], the authors explored the concept of self-sovereign identity and presented its challenges and opportunities in a rather informal way. However, in [15,19–21], the authors focused on the application of self-sovereign identity to explore how a self-sovereign identity system could be built and developed.

SSI was designed based on Christopher Allen's ten identity principles. SSI solutions must adhere to the following principles: existence, control, access, transparency, persistence, portability, interoperability, consent, minimalization, and protection [22]. At present, several initiatives and government agencies are actively developing SSI solutions on the blockchain platform. Several blockchain-based SSI frameworks, such as Sovrin [1], uPort [23], Civic [24], Blockstack [25], Selfkey [26], and ShoCard [27], are available and are being used in various domains. A successful SSI solution needs to comply with all the SSI principles [19,28]. None of the existing self-sovereign identity frameworks fully comply with the SSI principles. There are several building blocks for the development of an SSI framework. These building blocks are also referred to as SSI components. To identify SSI components for the SSI framework in compliance with SSI principles.

The essential purpose of SSI for land registry is to provide people with IDs so that they may communicate with land management services. There are approximately one billion people who have no access to identifying themselves. SSI allows individuals to

build a gradually more secured and trustworthy identity in place of a government-issued identification document by collecting certificates from reputable third parties, such as a land registry and financial institutions [29]. Even with the lack of legal documents, SSI can help the public to establish evidence of property ownership, such as a certified survey plan or a notarized declaration. The SSI's credentials should not be limited to only the digital equivalent of the traditional paper-based certificate, but should also provide a framework for transforming data into credentials that administrative entities can trust. For example, a person can submit proof of ownership claims utilizing their verified location history using a mobile carrier's location verification, transaction details and land registry certificates [30].

In the absence of land registries, SSI may directly connect people to land plots while also providing a means for recording property claims and related data to gain access to additional services such as banking, loans, and government benefits. SSI holders can use a verifiable claim to land ownership. Individuals could submit a digital title to seek financial aid or agricultural subsidies. A verifiable claim is a permanent document established by a government institution that acknowledges the rights of a property owner at a specific point in time. The provable verifiable claim will be kept, even if property certificates are lost or the owners relocate [31,32]. The major contributions of this research work are:

- To compare the current SSI solution with the principles of SSI;
- To identify the steps and requirements for the SSI adoption;
- To identify the components of SSI to comply with the principles of SSI;
- To discuss the applications of SSI in land registry and design a framework for the SSI-based land registry system.

This study explores the SSI concept and principles, compares four prominent SSI solutions based on identified SSI principles, and highlights the steps and requirements for adopting SSI solutions in Section 2. Section 3 presents a brief description and visualization of the SSI framework, component architecture, and various SSI components. It also provides a detailed critical analysis of SSI components and their usefulness for developing SSI solutions in compliance with each SSI principle. Section 4 gives a brief overview of possible use cases for SSI applications, including land registries. Finally, Section 5 provides a detailed elaboration of the SSI-based land registry framework with different implementation phases, followed by the conclusion in Section 6. Figure 1 conclusively demonstrates the organization of the paper.

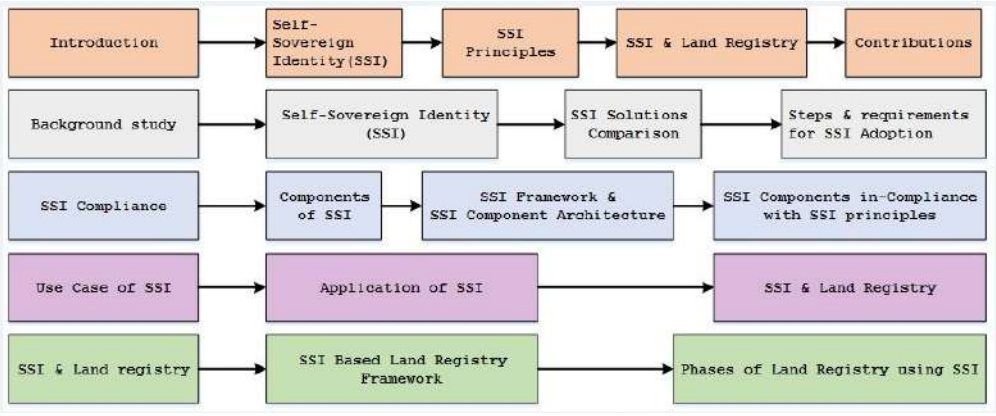


**Figure 1.** Organization of the paper.

## 2. Background

### *2.1. Land Registry System*

The Land Registry is a mechanism used to register and record land ownership and rights for a government body. It verifies land title records, facilitates land transactions and avoids corruption. The land registry is also a system in which government agencies record land-ownership rights and land-ownership amendments in compliance with existing

legislation and regulations to protect landowners' rights [33]. The land is also the most important of all resources or the most common and important property rights [34].

A. Land Registry Process

Laws governed by each country for the process of land registry and ownership systems could are described in the following steps:

- The land documentation is submitted to the jurisdiction in which the property is located. The approved seller and buyer signatures must be displayed, including witnesses for the agreement between seller and buyer.
- Payment receipt/proof shall be shown to the Sub-Registrar along with the Property Paper.
- The buyer and seller should provide proof of identification to the authorities involved in the land registration.
- If a third party is involved during a property contract, the representative must bring the authorized registration documents, such as a letter of authorization or legal authority, under various country laws.
- The authority has the right to refuse the registration process and registration papers for inconsistencies.

Since the procedures are complicated, it is often the third parties that carry out some or most of the work in place of the seller and buyer. However, online land registry systems have reduced some of the burdens by eliminating the need for third-party. People could pay fees online and start the transaction.

B. Limitations in the current land registry system

Records of the existing land registry are not up-to-date and are unclear, as they are poorly administered and cannot match with the ground coordinates. The government encounters challenges preserving these records and providing the updated information of these records as these records are maintained and updated by the different departments at the district and village levels. The lack of coordination among these departments leads to non-synchronized information resulting in dissimilar records and mismatches with the ground coordinates [35]. The limitations of the existing land registry system are given below:

- High time complexity: In the traditional land registry process, the transaction between the involved parties (sellers, buyers, banks and real estate agents) is time-consuming and expensive. The process for the trading of land in real estate includes various logical steps such as housing assessment and collection of documents. A complete property document depends upon completing the main contract, transfer of money, and registration, which makes the overall process more complex [28]. In [36], the authors discussed that the Swedish land registry system usually takes more time starting from the purchase contract signed for sale up to the actual transfer of the property [10,37,38]. Furthermore, in the Swedish land registry system, the absence of officials in the land transaction reduces the transparency and trust of the system [39–41].
- Centralized control: In the traditional land registry, records are stored in a centralized database, which is likely to have various security risks. Additionally, issues such as fault tolerance and adaptability are of primary concern [42–44].
- Physical property site visit and verification: The involved parties for land transactions first conduct a historical verification for each other. The buyer checks the physical location and coordinates of the property, history, and previous loan details on the property. This verification process is carried out manually, making the process more complicated and making the system vulnerable to fraud and loss of information [10,45]. In Kosovo, the verification of the land property and relevant documents is carried out only by the request of the notary service [43,44].
- More cost: The cost required to perform a transaction includes the cost of negotiation, signing, supervisory activity, and contract execution [46–49]. It signifies that the changes in the transaction cost will affect the housing affordability for Canadian

citizens [46]. The transaction cost is due to the information asymmetry regarding the hidden cost for the objects in real estate [28,50] and regulations [38,51–54].

- Lack of efficiency: There are inefficiencies in the land registry system such as inaccurate information, information that is hard to access and hard to search, and insecure ledgers [41,54].
- Vulnerable to error: The nation of Honduras made a law based on the property to create a general legal framework and enhanced land administration. Additionally, changes are making the system institutionalized for land registry SINAP, which facilitates the platform for the country's legal registry system [45,55]. Unluckily these frameworks are vulnerable to manipulation, including land title fraud. Moreover, it creates concern about the reliability of information for the Honduras land registry system [56]. The paper-based system is hard to access and also valuable for human-made or natural disasters [44].
- Corruption and fraud: The traditional land registry process is centralized, which makes corruption and fraud more likely [38,48]. The centralized nature of authorities in the land registry makes corruption and fraud easier [42,57]. Based on the various reports, Canada's real estate market has severe problems with fraud. The currently used process of the closed binding system makes it difficult to prove the fraud by brokers in the land registration process [58]. Among the other fraud in the Canadian real estate market, the most severe problem is title fraud, which victimizes financially [46,59].
- Less secure: The use of trustless ledger technology will change the property law and lower the price to release disorderly and scalable applications. Currently, the property registry is a mixture of almost inaccurate, insecure, and expensive ledgers [41]. The centralized architecture of the application raises concerns regarding the attack on the system and corruption, which makes the system untraceable [28,43].
- Complex process: The procedure for the sale of the property requires many logical steps such as the collection of documents, assessment of property, signing of the primary contract, registration, and transfer of money, which makes the process more complex [28]. The land registry system forces the involved parties (buyer, real estate agents, and banks) to create a separate complex red tape process for agreement [36].
- Lack of transparency: The current land registry process lacks transparency for the transaction, such as leasing, purchasing, and sale. Although the current land registry system fails to achieve the confidential and authenticity of the data [52,53], the trading of property is troubled to become an essential liquid asset that includes hidden costs, regulations, financial assurance, and public accountability. Moreover, it also risks the rights of an individual user [10,37,50,51,56]. In the Kosovo Cadastral system, information on land ownership data is only accessible to the notaries, lawyers, and intermediaries [44]. The official in the Swedish land registry is the more trusted authority in the process. Their absence in the earlier phase of the land transaction causes a lack of transparency and trust [36,42].
- Third-party involvement: In the traditional land registry process, there are lots of entities involved during the transaction, such as brokers, land inspectors, attorney, notaries, and government authority, which results in unnecessary cost, complexity and delay in the process [28,48,52,53]. All the parties involved in the land transaction process have to trust the third party, which results in fraud related to ownership of title and the validity of ownership title [37,38,45,46,57,58,60].
- Less reliability: In the traditional land registry system, obtaining reliable information is challenging for investors. Additionally, the political person may restrict investors from gaining reliable information due to the closure of government offices or the abolishment of the government. The lack of reliable information influences the financial flow and ownership transfer that is required to acquire the piece of land [56].
- Authenticity issue: The nation of Honduras introduced a new law on the property by creating a legal framework to improve land administration. Unfortunately, this

framework is unsafe for manipulation, which results in land title fraud. Moreover, there are concerns related to the authenticity of the Honduras land registration [56].

- Lack of effectiveness: The real estate market affects the country's economy. Lack of effectiveness in the real estate market causes various transparency problems like more transaction costs, delays in the process, and prejudice [44].
- Paper-based process: The respective department manually stores the land transaction records on paper. However, the departments are currently upgrading from paper-based storage to computerized systems [28,39]. However, unfortunately, the documents that prove the land title ownership are still stored on paper, making the real estate system more complicated and time-consuming [42].
- Lack of trust: There is a lack of trust in the property verification process by the board of revenue. The sale deed is verified and then forwarded to another department, leading to a lack of trust [43]. Double spending is a major concern of trust in the system. When the buyer spends currency multiple times for the same property, they cannot trust the payment system of the land registry [41,60,61]. No statistics are available in the Kosovo Cadastral system related to the real estate transaction. However, there is no compensation mechanism for covering the loss that occurred due to the inaccurate information provided by the immovable property register, which results in a lack of trust in the system [44]. In the Swedish land registry (Lantmäteriet), officials are the most trusted actor in the land registry. Their absence in earlier phases of land transaction results in a lack of trust and transparency [39,40].
- Ownership issue: The present land registry system in Sri Lanka has issues like a large number of land disputes, lawsuits, unclear ownership over land encroachment, and misuse of land [62]. The ownership of the land title is not guaranteed. Many users claim ownership for the same land title [37,43,57,61].

### C. Land Registry and Identity issues

The land registry system is a way to store, protect, and publish land records and facilitate the transfer of land ownership while protecting the rights of the people who own it, which makes people more likely to trust each other. To prevent fraud, it is essential to verify the identity of the people involved in a transaction. There are several drawbacks to the current land registry systems. However, these drawbacks can be avoided by using a blockchain technology. Existing land registry systems have been replaced by a variety of blockchain-based systems [63]. Nevertheless, the usage of blockchain in land registry systems has several constraints regarding the identity that must be addressed when creating a blockchain-based land registry system. Among these considerations are: independent verification [10,64–67], the necessity for an identity solution [64,68,69], compliance with the identification principles [66,70], user control [11,67,71,72], and legal validity [9,39,64]. It is necessary to solve those constraints for a successful deployment of blockchain technology in the land registry system as well as to overcome its drawbacks.

Many recent studies have shown that a digital identity is essential for performing a secure real estate transaction and verifying ownership of the real estate. According to the Money Laundering Directive 2018/843, verifying the identity of the parties in a transaction can help avoid cyber fraud and crimes [7]. Unfortunately, the current land registry system lacks a digital identity solution that allows users to manage their personal data. According to some studies and analyses, users need to have control and ownership over their digital identities [9–11]. Additionally, using digital identity in the land registry system would reduce the time required, the risk of fraud, and the information loss. The problem with the current use of blockchain for identity management is that it does not comply with the SSI principles [65].

An identity model must ensure that the user's personal information is safe against data breaches and fraud [13]. Digital identity models fall into four categories: centralized identity, federated identity, user-centric identity, and the SSI model [22,73]. The SSI model is the only one that allows users to retain control over their personal identification data;

all other systems' identity models rely on the identity providers [13]. SSI provides a decentralized identity and gives users complete control over their personal data [74].

### *2.2. Self-Sovereign Identity (SSI)*

SSI solutions allow users to gain control over their personal identities. Users will decide precisely what information they need to reveal about themselves, to whom, and in which contexts. Under the SSI model, no one can prohibit a person from exercising basic human rights, such as the right to be expression and privacy. Individuals do not need to retain their identities physically. They can choose any identity operator. The pre-requisite for SSI is that digital identities must be scalable and interoperable across different platforms. Therefore, individuals are free to choose the identity operator and switch from one operator to another [75,76]. While no clear definition of SSI exists so far, a set of requirements have been defined as the key principles needed to function as an SSI [22]. These principles can be regarded as a criterion to check the existing identity solution to comply with these principles.

- Existence: Users have an independent existence and are not dependent on the details found in their digital identifiers.
- Control: Users have full control their identities and be able to transform, update, refer and hide them. Users have full authority to disclose or choose privacy on their identity details.
- Access: Individuals should have access to their data and should have the ability to be able to retrieve it when necessary.
- Transparency: Systems and algorithms used to handle and run digital identities must be accessible and transparent. The public must be able to track the operation and maintenance of the system.
- Persistence: The identity must be long-lived, and the individual's identity must be preserved for as long as the individual wants.
- Portability: Information and resources concerning identity must be transportable, and not owned by a single third party, even though they are trusted.
- Interoperability: Identities are available for common use in all contexts instead of being limited to one siloed environment.
- Consent: Individuals should give consent to use their identities. The data sharing by third parties must occur with the consent of the data subject.
- Minimization: The disclosure of claims should be kept to a minimum and should only be disclosed when necessary to perform a task.
- Protection: The individual's right to privacy must be protected at all costs, even though this would go against the identity providers' interests.

These principles would benefit the users and form the basis of the SSI solution and need compliance to provide an SSI solution to the users [22]. None of the SSI solutions today comply with all these principles [77]. Several competing SSI solutions have emerged during the development process, adopting various ideas and using different blockchains [78,79]. In [80], the authors reviewed the available SSI solutions based on blockchain and discuss their implementations concerning the SSI principles. An analysis of the SSI concept's potential and evaluation of blockchain-based SSI solutions, namely Sovrin, Multichain, Blockstack and uPort has been carried out [74]. Comparative analyses of uPort and Sovrin were performed by reference [81]. A detailed analysis of the ShoCard Sovrin, Civic and uPort was carried out. These systems use certain decentralization techniques based on the author's criteria and principles, none of which complied with the SSI requirements [77]. However, it is still rare for SSI systems to be compared with the SSI design principles. Therefore, to fill this gap in the next section, the researchers compared the existing blockchain-based self-sovereign identity (BC-SSI) solution uPort, Sovrin, Civic and ShoCard on the principle of SSI to identify whether the existing BC-SSI solution complies with the SSI principles or not.

### *2.3. Comparison of Self-Sovereign Identity Solutions on the SSI Principle*

There are several SSI solutions available based on the blockchain platform. In this section, only uPort, Civic, ShoCard, and Sovrin have been shortlisted for comparison because of their innovative SSI identity management approaches. These SSI solutions cover the broader landscape of BC-SSI solutions. The analysis for each selected SSI solution to comply with the SSI principles is shown in Table 1. First, the analysis with uPort, which is an identity and communication platform based on the Ethereum blockchain [23], was conducted. Second, the Sovrin Foundation has set out to standardize and implement the SSI architecture using blockchain so that anyone can issue and verify [1]. Third, Civic offers an SSI ecosystem to allow low-cost and reliable access to identity verification and customer know your customer (KYC) processes [24]. Finally, the ShoCard-based identity ecosystem provides authentication, an attestation to the credentials, and proper authentication [27].

**Table 1.** Comparison of SSI solutions based on SSI principles.

| SSI Principle | SSI Solutions | | | |
|---|---|---|---|---|
| | **uPort** | **ShoCard** | **Sovrin** | **Civic** |
| Control | Y | Y | Y | Y |
| Access | Y | X | Y | X |
| Transparency | Y | Y | Y | Y |
| Persistence | X | X | X | X |
| Portability | Y | Y | Y | X |
| Interoperability | Y | Y | Y | Y |
| Consent | Y | Y | Y | Y |
| Minimalization | Y | Y | Y | Y |
| Protection | Y | X | X | X |
| Existence | X | Y | Y | X |

#### 2.3.1. uPort

uPort enables users to manage their online network of identities by utilizing an Ethereum blockchain [23]. The uPort mobile app creates keys and creates the corresponding three smart contracts for each identity. The uPort registry stores identity information in a cryptographically secure manner and securely links it to an identifier.

Analysis: uPort is developed with open international standards and open-source applications (3). The user's key identity is stored on the Ethereum blockchain and then distributed on thousands of computers worldwide (4). Individuals build and control their own personal identity (1). Personal identity information is stored securely on the computer and in the Interplanetary file system (IPFS) and is available to the user (2). Users may share information with a third party of their own choice (7). Private data are stored locally on the users' computer and uses Java script object notation (JSON) is applied instead of Extensible markup language (XML) (5). uPort has a "Selective Disclosure Request" regarding confidential information. However, the JSON user profile for the registry is public, which compromises users' privacy (8). Some centralized components include a message server that allows the transfer of attributes, an application manager, and a push notification center (9). uPort can validate an individual's identity with various attributes and generate JSON web tokens (JWTs) to verify claims (6). The cost of using Ether is directly related to the price of Ether on the Ethereum network (10).

#### 2.3.2. Sovrin

The Sovrin Foundation has come together to standardize and develop an environment to store the self-sovereign identities on a blockchain so that everyone can use and verify

them [1]. Sovrin has developed a specific framework that is built on top of Hyperledger Indy. Sovrin uses a permissioned blockchain called Stewards to achieve global consensus.

Analysis: In Sovrin, the Identity Owner's cryptographic key pairs are the only way to access and do all the user has permission to do (1). Personal data are collected on the user's device or preferred agents who are not the third-party service providers (2). Sovrin and agents are used to store attributes associated with the identity (6). The code that runs, validates and gives access to the ledgers is open source (3). An encrypted and private local container with an agent can be used to maintain and backup storage (4). The datasets can be accessed using system-independent semantic Web formats such as JavaScript object notation for linked data (JSON-LD) to ensure data portability (5). Identity Attributes are exchanged only by obtaining consent from the Identity Owner (7). Sovrin utilizes decentralized identifiers and public keys for each relationship to provide selective disclosure of verifiable statements using zero information proof (8). Although the ledger has a decentralized framework and several nodes, the permissioned ledger requires a governing body (9). Identity owners will have unrestricted access to their identities, but Sovrin supports "Premium Claims" to create identity issuers' economic opportunities (10).

#### 2.3.3. Civic

Civic is developing a single identity verification ecosystem where anyone can quickly request identity verification services at a low cost [24]. Civic is built on an ERC20 token based on the Ethereum blockchain that generates keys on a third-party platform. All personal information is set to own by the user, and only the hash of the personal information is stored on the blockchain.

Analysis: Civic enables identity data to be stored on the users' computer to access and control its identity information (1). Users' control and access are guaranteed if the device controls the user (2). In Civic, the Ethereum network is likely to be available in the future in which real data rely on the user-maintained long-term storage (3). The information may be used in Civic applications but is not portable outside such Civic applications (4). Identity information is accessible in the civic environment but is not portable beyond the civic ecosystem (5). Civic will enable password-less access to services as well as self-declared and checked identity attributes (6). When data are stored on the user's device, then the data owner must decide who has access to the identification information (7). Selective parts of the Merkle tree can be revealed with hashes for any elements that the user prefers not to reveal (8). Information held on the Civic Network can be used to carry out applications within the Civic Ecosystem. Information should be revealed selectively as per the customer's request (9). The fees are calculated by Ether's cost on Ethereum and the likelihood of CVC tokens for some services (10).

#### 2.3.4. ShoCard

ShoCard was created in 2015 to provide a more reliable authentication mechanism than conventional methods [27]. ShoCard utilizes alternative security methods such as the blockchain, which guarantees authenticity and does not require any personal data. It supports zero-knowledge proof as well as the complete KYC process.

Analysis: ShoCard is partially centralized and dependent on the ShoCard infrastructure. It creates a future existence problem for ShoCard (4). Users construct, maintain and control their digital ID (1). The public blockchain is generally open to the public, but issues can compromise identity data with the ShoCard service (2). ShoCard has received four patents and nine patents pending and now shares its inventions and algorithms on open-source standards (3). ShoCard can use multiple blockchains simultaneously to better support future blockchain (5). Using ShoCard, there are a couple of different choices for identification and authorization, such as KYC and attesting credentials (6). Users will determine how and with whom they want to share their identity information (7). Users will decide which data they want to share and do not need to share irrelevant data (8).

The central server partly centralizes the ShoCard (9). ShoCard is an independent blockchain, theoretically operating on the public ledger, with transaction fees (10).

### *2.4. Steps and Requirements for SSI Adoption*

For adopting and standardizing any new technology, there are several guidelines and regulations prescribed by government agencies and autonomous institutions authorized for standardizing such technologies. There is a range of guidelines for developing a digital identity framework. Some of the sources are International Telecommunication Union (ITU) [82], Financial Action Task Force (FATF) [83], European Union [84] and the Open Identity Exchange (OIX) [85]. Although these guidelines were not exclusive to self-sovereign identity, they also refer to the SSI application. Identity systems may be classified into three groups, depending on the legislation's origins that define liability. There are three types of identity structures [85]. The Digital Identity Level I scheme is the law applicable to all digital identity solutions. Tier II is a public law applicable only to certain jurisdictions. Tier III is a contract law that many businesses are complying with. The type of digital identity scheme, according to the OIX, is shown in Table 2.

**Table 2.** Digital identity scheme and governing laws as per OIX.

| Source for Rules Regulating Liability | General Law | Identity-Specific Law | Contract-Based Rules |
|---|---|---|---|
| Level | 1 | 2 | 3 |
| Type of rule | Public Law | Public Law | Private Law |
| Usefulness | Everyone within the jurisdiction | Persons in ID system jurisdiction covered by the statute | Entities that adhere to the terms of the contract |

Numerous steps are required to create a scalable, operational and autonomous SSI ecosystem. Such measures can differ based on the amount of government involvement. Table 3 shows the requirements for the governments to adopt the SSI model. Many governments allow users to use digital identities at the national level. In Estonia, the national ID card system offers access to all electronic facilities, such as banking, and is used by 98% of the population [86].

**Table 3.** Requirement for the adoption of SSI by governments.

| S.No | Requirements | Description |
|---|---|---|
| 1 | Creating a trustworthy registry | The government shall establish and manage the public register. If people want to use a blockchain network, they need to define who can join the network and who can not. |
| 2 | Build new digital wallets | Certain government organizations have been granted the authority to trusted digital wallets providers. |
| 3 | Attractions of individuals | The government would allow its citizens to register their digital IDs for government-based services to promote e-government services. |
| 4 | Development of DIDs | The government would require one DID method and allow wallet providers to use it. |
| 5 | Identification of standards | Recognition of decentralized identifiers and verifiable credentials must be adopted by world leaders such as ISO, ITU, IEEE or NIST. |
| 6 | Issuing of verifiable credentials/certifications | The government will develop relevant systems and protocols for issuing digital ID documents (e.g., a digital passport). |
| 7 | Acceptance by service providers | The authentication of SSI-compliant digital identities is more convenient for service providers because they can verify customers more easily, more effectively and with higher security levels. |

The SSI approach would allow governments to issue digital IDs that can be used to access any digital services without significant infrastructure and additional obligations. Governments register identity records in blockchain and trust lists using a self-sovereignty strategy. The government will no longer have the responsibility of verifying to make sure that the certificates are valid. In the SSI system, the government only needs to issue digital certificates and register cryptographic proofs in certificates in a public and decentralized network, removing the government's need to maintain additional infrastructure [87,88]. Individuals will have full control over the sharing of data. The government does not need to validate and authorize digital credentials issued by government agencies explicitly.

## 3. SSI Compliance

### *3.1. Components of SSI*

There are various SSI components available that can be used to develop an SSI solution and comply with SSI principles. These SSI components have been briefly described in this section. A graphical representation of different SSI components has been illustrated in Figure 2.

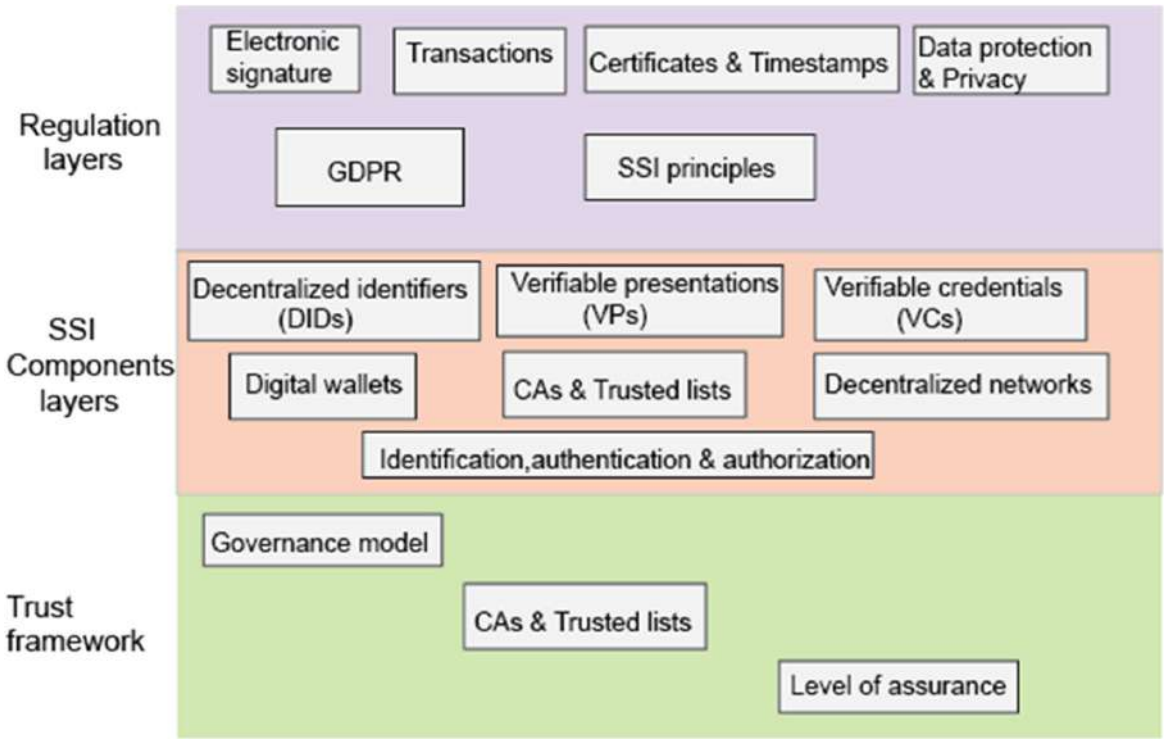


**Figure 2.** SSI framework.

#### 3.1.1. Decentralized Identifiers (DIDs)

A global working group has been set up to develop the Decentralized Identifiers (DIDs) standard [89]. A DID is a digital identity that facilitates having a verifiable and decentralized identity. A DID is an identifier associated with a subject (e.g., a person, an agency, an object, a data model, an abstract entity, etc.) that the DID controller considers to be defined [90]. The various types of DID standards to be followed shall be known as DID methods.

- DID Documents: The DID refers to the DID document that provides specific information about the authentication mechanisms to prove the DID, endpoints, and other attributes.
- DID Registries: The number of DID implementations with DIDs is required to have a DID registry. Due to the decentralized existence of DIDs, centralized and autonomous

DID registries are not feasible. DID registries are intended to act as identifiers for a variety of purposes.

- DID Methods: The DID standard is made using DID methods. DID methods differ concerning the mechanisms for establishing and validating DIDs, the authentication systems. Currently, there is no officially recognized list of DID methods available. However, the World Wide Web Consortium (W3C) and Digital identity function (DIF) maintain unofficial lists.

#### 3.1.2. Verifiable Credentials (VCs)

The first step to having an SSI solution is to provide a trustworthy signing issuer that issues verifiable credentials (VC). A credential is a digital file that contains one or more credentials about a person from another source, authenticated by the verifier. The W3C working group is currently developing standards related to Verifiable Credentials (VC). The claims and the proof shall support the Verifiable Credential (VC). The proof determines the legitimacy of one's credentials. A claim is a statement about the topic of research on which claims could be made.

- Credential Registry Exchange: There are three methods for exchanging credentials. In the first instance, the credential is sent from the issuer to the holder. Secondly, the credential is passed from the requester to the holder. Finally, the credential is transmitted from the holder to the verifier. It is essential that the credential exchange between the credential repository (i.e., the digital wallet) and the service that creates or utilizes the credential be secured.
- Revocation: Credentials represent the individual's status and can be revoked or suspended at the consent of the person who holds them. A specific guideline seems fundamental when revoking a credential and modifying the credential status.

#### 3.1.3. Verifiable Presentations (VPs)

The W3C facilitated the concept of Verifiable Presentations within the Verifiable Credentials specification [91]. The verifiable presentation is presented through verifiable credentials and has been packaged so that its authorship is verifiable. When the Verifiable credentials are presented, expressly will become verifiable presentations.

- Selective Disclosure Mechanisms and Zero-Knowledge Proofs (ZKP): In self-sovereign identification systems, individuals regulate both their identities and credentials. Therefore, they have the right to present themselves and decide on how many details they should share. They have multiple verifiable credentials provided by various issuers and they build a presentation with explicit statements from such credentials so that it may not disclose any other claims included in it.
- Traceability and Monitoring: The sharing of credentials takes place off-chain, which means that the credential is not registered. Verification of the certificate ensures that there is no traceable record of the transaction. This helps to reduce data privacy issues. However, in certain situations, the sharing and verification of credentials are supposed to be transparent. It is mainly the case when measuring and providing feedback on solutions is essential.

#### 3.1.4. Digital Repositories and Wallets

In the case of self-sovereign identity, a digital wallet enables private repositories of users to secure information such as keys, identities, and credentials. A digital wallet can protect access to the holder by ensuring that only authorized individuals have access to the wallet. It secures and protects data with encryption. In addition, it also verifies the transfer of DID documents, trustworthy lists, and cryptographic proof of DID documents. It also provides a mechanism for individuals to update their credentials.

- Key Recovery: The first layer to establish a digital identity contains a private key and an authenticator. It protects the users from unexpected events and inappropriate uses

of their identifiers and credentials. Therefore, it is essential to ensure digital wallets' recovery due to the loss or misuse of digital wallets.

- Recovery of Credentials: A digital wallet allows for storing and managing digital credentials. If the wallet is lost or passwords are compromised, it is possible to retrieve the password using a digital wallet. Essential recovery methods should be in place to back up credentials in both cloud and offline computers. For example, cloud back-ups or other back-ups facilitated by the wallet provider should describe how or when the users can retrieve the credentials. The recovery process of credentials must be a balance between usability and security.

#### 3.1.5. Identity Proofing, Authentication, and Authorization

Authentication, proof of identity and authorization occur when an electronic transfer of knowledge by the service provider takes place. Identity proof relies on the verifiability of the requester. Authentication is a way of ensuring that the service has already been delivered and consumed securely. Authorization requires that the requester have the necessary authorization to use the service, allowing them access to the service.

- Identity Proofing: The identity proofing process begins with the requesting entity requesting identity credentials. Next, the identity issuer authenticates the user's identity. The customer then receives a digital identity certificate from the issuer. Finally, the credential is saved in the secure repository.
- Authentication: Authentication is dependent on three distinct factors: firstly, the password, which is essential; secondly, the user's credentials, which can include a mobile, ID card, or cryptographic key; and thirdly, the use of biometric data sources such as fingerprints.
- Authorization: When applying for a service, the service provider shall check that the credential issued is legitimate. The issuer is acknowledged, and the presenter is authorized to request the credential. When a verifiable certification is issued, two different behaviors toward providing certificates are observed: Authorization for the Presenter and Authorization of Purpose.

#### 3.1.6. Certificate Authorities (CAs and Trusted Lists (TLs)

In the digital identity system of public key infrastructure, the certificate authority issues identity credentials accepted by others with a relative degree of assurance. Others can trust multiple profit and non-profit organizations such as CAs for various purposes. Currently, there is a range of trustworthy lists (TLs). The first trustworthy list is the CAs approved by the recognized authority that individuals may trust. The second trust list is the certificates provided by the CAs that each person owns and the certificates' status. This allows us to verify that a digital certificate issued by an agency that we do not recognize or trust is certified by an entity that we fully trust.

#### 3.1.7. Distributed Ledger Technology (DLT)

SSI must use decentralized ledgers to store cryptographic proofs for DIDs, verifiable credentials and presentations. Blockchain enables SSI to achieve the highest degree of security and scalability required. Moreover, blockchain has been using public ledgers that are distinguished using smart contracts. It is believed that the distributed distributed ledger technology is better suited than most other decentralized technologies for establishing proof of identity, blockchain addresses can be used as DIDs, and smart contracts can be used as trusted lists.

- Permissionless: Permissionless DLT allows users to access the network at any time, such as Bitcoin and Ethereum. Many networks use cryptographic technology. They have access to the system, but with high transaction fees and anonymity, every individual is anonymous.

- Permissioned private: Permissioned DLT consists of a finite network of well-defined identities that deploy, run, and manage all nodes. Generally, such networks are developed and managed by a blockchain provider.
- Permissioned public: Permissioned public access to the network provides participants with access to the network and asks whether they comply with specific laws and regulations. Publicly accessible networks are open, transparent, decentralized and do not require any fees. At the same time, the identity of everyone guarantees not only anonymity but also regulatory compliance.

### *3.2. SSI Framework and Component Architecture*

The SSI framework has three main layers: the regulations layer, components layer, and trust framework layer. This layered SSI framework has been presented in Figure 2. Furthermore, the interaction among SSI components has been explicitly defined in the form of SSI component architecture. The objective of SSI architecture is to demonstrate to the user a visualization of the components and how they interact with each other. The SSI component architecture is shown in Figure 3. The SSI components architecture consists of three layers of functionality. The first layer is a Decentralized public key interface (DPKI) where different ledgers with different DID methods contain DIDs for an organization to make it publicly recognizable at this level. The second layer is a decentralized key management system (DKMS). A DID is a public key that contains one or more private keys. DKMS handles all these keys using a structured structure. The third layer is characterized by verifiable credentials such as a driver's license, a degree, or residency proof. These verifiable credentials contribute to additional personal information about other individuals. Any user can create, verify, and hold the credentials. The fourth and final stage uses verifiable presentations to create verifiable statements and verifiable credentials. These are designed to securely show the personal identity data of an individual to third parties, sharing only as much information as required, thus maintaining the owner's privacy.

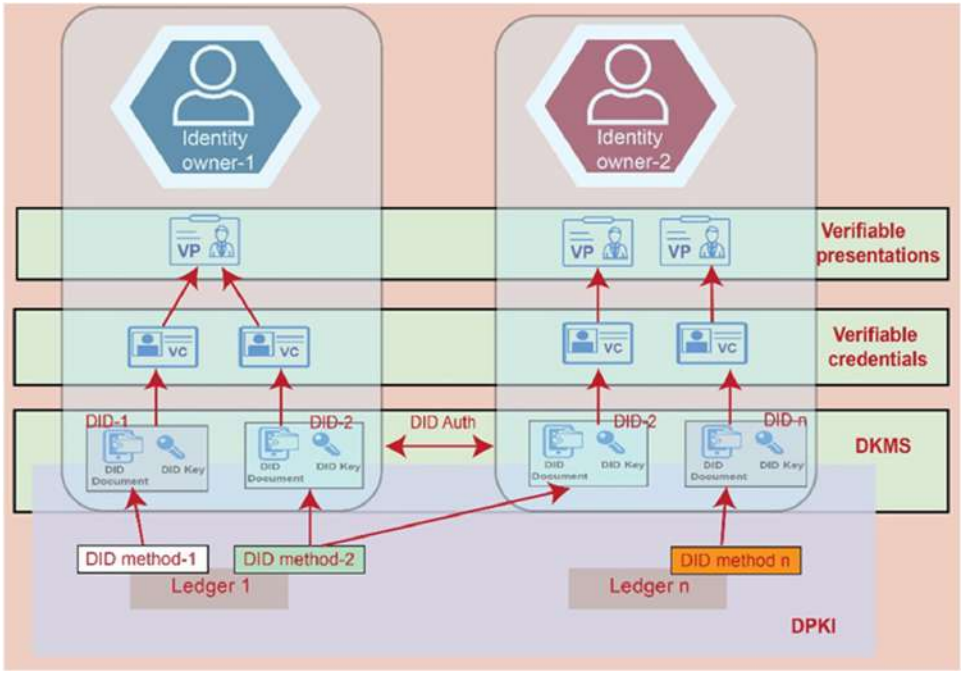


**Figure 3.** SSI components architecture.

### *3.3. Components of SSI in Compliance with SSI Principles*

The explanation principles of digital identity are extensive. Some of these principles may be more specific. For example, the first concept can be divided into the user control and consent. Some identity solutions may satisfy one but not the other. Given that at the time of

writing these principles, there was no self-sovereign identification, it was more remarkable to have the majority of principles adopted from "The Evolution of Digital Identity Concepts guiding principles" by Christopher Allen [22]. In a well-known post, "The Path to Self-Sovereign Identity", Allen outlined SSI principles, including specific guidelines from other sources such as Kim Cameron and the W3C Verifiable Statements Task Force [92]. These 10 principles are taken from Allen's paper [22] and serve as guidelines for SSI-adapting participants. A concise description of these SSI principles and which SSI component can be used to comply with these principles are presented in Table 4.

**Table 4.** Overview of SSI principles and required SSI components for its compliance.

| SSI Principle | Description | SSI Components |
| --- | --- | --- |
| Control | The user controls and has authority over identity and personal data. Files are kept in a decentralized manner to the fullest extent. | Asymmetric cryptography authentication protocol DPKI (DID holder) |
| Access | User can access their data and identities quickly and directly. | DID naming system Digital credential wallet |
| Transparency | The operation and system used need to be transparent. Additionally, how an identity scheme operates, is managed and maintained should be publicly available and easily understood. | Open protocols and open standards |
| Persistence | The identity will last long since user identities will exist from birth to death. | Time revocation Revocation list Proof of non- revocation DKMS key recovery |
| Portability | The services of the identity system must be transportable. The user identification is not limited to any network. Additionally, users should be able to move their names, certificates and proofs from one network to another. | Open standard DID |
| Interoperability | Identities should be as universally accepted. The organizations, databases or registries can interact internationally easily and securely via an identity system. | JSON-LD universal resolver DID Auth protocol |
| Consent | Users can explicitly authorize other entities to use their identity data. | Verifiable credential asymmetric cryptography authentication protocol |
| Existence | Users must have an independent existence | DID documents verifiable presentation Multiple identifiers Anonymous credentials |
| Minimalization | Prevents detailed disclosure of identity information as minimizing the disclosure of identity information will enhance privacy. | ZK capable verifiable credentials |
| Protection | The rights of user privacy need to be protected. The identity solution must include the "privacy by design" principle. | pairwise-pseudonymous DIDs Verifiable presentations DKMS endpoints |

#### 3.3.1. Control

Every user has an identity and knows a secret that only he knows. The possession of the secret is equivalent to the possession of the credential or the right to use the credential. It needs the owners' identity to keep private keys on their computers.

1. DPKI: Decentralized public key infrastructure (DPKI) does not require a centralized authority to create keys for actors since actors themselves create them in a decentralized manner. The DID holder has a private key that allows them to control their DID [93,94]. User keys are generated on the client side without relying on a central authority.

2. Asymmetric cryptography authentication protocol: Zero-knowledge proof of asymmetric cryptography protocol enables the identity owner to prove the identity ownership by using the private key stored on the blockchain. Most SSI systems use the asymmetric cryptography authentication protocol for authentication [93].

#### 3.3.2. Access

Digital credentials: Mobile devices are useful as they provide users with full control and are always available. A mobile device can be installed with a secure wallet account to store and retrieve keys. We can create more links by scanning the codes with a smartphone. The links help establish the credentials which have been issued to the user and to store the digital credentials [95].

#### 3.3.3. Transparency

Open protocols and open standards: The Internet is an open network. Web, DNS, and applications are open-source software. The solutions are built using open-source software so they can be used by anyone but are not owned by anyone. In addition, everyone can improve them. An identity system based on a public blockchain needs to function the same way to provide all identities. The Sovrin is built using open- source software and will provide open governance. Sovrin and the Stewards operate with complete openness and transparency [1,96]. Other than that, personal information should be cryptographically encrypted to prevent unauthorized access.

#### 3.3.4. Persistence

Credential holders have complete power over how to use their credentials, whereas credential issuers have the right to revoke them for unauthorized usage. If the conditions for the credential are not fulfilled, the issuer shall revoke the credential. The identifier attached to the credential, or any other form of credential, will be included in the revocation list. The revocation list is kept on the ledger and can be reviewed by the verifiers if the credential presented to them has been revoked. The following approaches revoke the credential [97].

1. Time-revocation: expired part of the credential data.
2. Revocation list: Mapping the credential ID with the revocation list.
3. Proof of non-revocation: ZKP of a credential that has not been revoked is contained in Hyperledger Indy.
4. DKMS Key recovery: The recovery process requires users to make backups of their wallets. DKMS can provide the requisite features to retrieve passwords safely. Users must maintain several backups of their wallets and store them in secure digital storage, such as a cloud-based agent [1,94].

#### 3.3.5. Portability

An identity using open standards makes a portable identity available to multiple standards [1].

1. Open standard DID: This is a portable DID developed using an open standard, and which is described and addressed by a private key on a ledge.

#### 3.3.6. Interoperability

1. JSON-LD: The DID documents are developed using the JSON-LD. The JSON-LD will share data in a consistent format that can be understood by both systems [98].
2. Universal resolver: A community-based project of the "Decentralized Identifier Foundation" (DIF) was formed to develop a universal resolver to create an interoperable system. It can resolve any DID form on the underlying ledgers of any DID method that can be used to resolve the DID method in the SSI ecosystem. It offers details regarding DIDs recorded with the DID method based on the DID. DID methods are linked with each other to make cross-border interactions easier. One of the most

important parts of interoperability is DKMS, which describes how DIDs interact with one another and the ledger. It also offers useful tools for key management, such as key recovery [99].

3. DID Auth protocol: This utilizes open standard, Secure Quick Reliable Login (SQRL) and the Web Auth protocol that present the challenge of authenticating the user. The standardizing of specifications using open standardizing using SQRL will ensure all DIDs perform according to the designed specifications and enable interoperability [93,94].

#### 3.3.7. Consent

1. Verifiable credential: This allows users to save their identity credentials in wallets installed on personal devices and make them accessible via the Internet. It provides the user with full control and consent of the credentials stored in the wallet so that users can also choose with whom to share information and how long the information can be shared [89].
2. A symmetric cryptography authentication protocol: This allows the users to fully control and possess all their personal information with the public key stored in blockchain through the zero-knowledge proof (ZKP) feature of asymmetric cryptography [93,94].

#### 3.3.8. Existence

1. Decentralized identifiers are persistent, ensuring that the holder is authenticated to be cryptographically secure if the private key is present with the identity holder [94]. The domain also has several services, including a website and an agent service. The identity holder will probably have multiple data points, such as a mailing address, telephone number, or other information which might be used to develop a relationship [100].
2. Verifiable presentation: A verified credential contains evidence of authenticity from the identity issuer. It enables the identity issuer to verify the identity owner digitally [89]. A verified presentation is made by the identity owner and eventually will be forwarded to the verifier who verifies it.
3. Multiple identifiers: An identity owner may obtain multiple identifiers and build a new identity when required. The ID claims may not depend on an identifier. The identifiers and credentials will continue to be separate. It impacts the combination of credentials with any identifier. Additionally, the DID will be shared with the verifier whenever necessary.
4. Anonymous credentials: The identity owner who gives the verifier credentials does not wish to reveal his ID. Alternatively, identity ownership is shown in a one-way using zero-knowledge proof [97].

#### 3.3.9. Minimalization

1. Zero-knowledge capable verifiable credentials: This helps users to keep their claims of credentials hidden and proves only the existence of those claims that can be used to compare claims against numbers without disclosing the actual information. ZKPs are an effective cryptographic technique that can prove claims without disclosing the actual value [101]. The users should be able to access their credentials on their personal device. The use of ZKPs based credentials presentations is required. Consequently, the user is forced to rely on a third party for storing the credentials [89,102].

#### 3.3.10. Protection

1. Pairwise-pseudonymous DIDs: These preserve privacy by preventing the linkage of identities. Whenever two services want to analyze their users' interests, the better solution is to compare a DID, which only recognizes a particular connection. Additionally, there is only one information service provider that will be stored in the DID. However, the file's information is difficult to trace as it is not assigned to a user's

account. The pairwise pseudonym DID, with public and private keys, is created on the user side [94].

2. Verifiable presentations: The system promises enhanced privacy and balances individual integrity using ZKP cryptography techniques by verifying proof of one's identity without revealing actual private information [89].
3. DKMS Endpoint: This enhances privacy by providing a way for endpoints to protect their data and establish trust with other endpoints. Endpoints are used as DIDs and DID keys that provide the anonymity of identity to prove a person's identity [93,94].

## 4. Self-Sovereign Identity (SSI) and Land Registry

These days, usernames and passwords are typically used by service providers for identification and authentication purposes. The widespread use of this so-called centralized identity model is a result of its simplicity of deployment and the complete control that service providers have over it, which enables them to mitigate risk. Additionally, users appreciate the fact that they only need to transmit information relevant to the current situation [103,104]. However, the rising use of online services has made this model inconvenient for consumers, as they must remember their login credentials for each additional site, and attributes must be manually entered or verified repeatedly [105]. As a result, consumers' tendency for reusing passwords across several services leads to poor user experiences and security problems. Additionally, service providers typically store data in large data silos, which are a preferred target of hackers [106].

The development of the so-called federated identification concept attempted to improve the user experience [107]. As a result of implementing this notion across systems and organizations, digital identities can be used for attribute authentication and verification [14]. Third-party digital identities are managed and distributed by an identity provider, for example Facebook or Google. There must be confidence between the identity supplier and a relying party for this identification paradigm to work. With federated identity management, users no longer need to remember several usernames and passwords to access multiple services simultaneously [108].

If the digital identities and the related data are better protected, no third parties should have access to them. Decentralization of power is the way to go. Decentralized identifiers (DIDs) can be created using public-key cryptography, allowing users to prove their ownership. The user can then customize these unique identifiers by adding further data. In some scenarios, where certain attested attributes need to be confirmed, credentials obtained from a trusted authority such as a government authority or company can be used [89,109]. A "digital wallet" is a place where people keep their DIDs and cryptographic keys. They can keep them on their phones, PCs, or in the cloud with their preferred service provider. A comparable system exists for the actual credentials that we carry in our physical wallets, such as plastic cards [110]. Because people have complete control over their data, it is referred to as self-sovereign. This technology is required for an open-source and open-standards strategy. According to World Wide Web Consortium W3C's DID standard, there are numerous ways to implement SSI, although many implementations are now based on this standard [94].

The identifiers can be registered, resolved, updated, or revoked without requiring a centralized authority [111]. In this respect, DIDs are not necessarily required for SSI but they give functionality beyond decentralized PKI (DPKI). Digital certificates are cryptographic credentials that prove who developed them and for whom they were created. The World Wide Web Consortium is currently attempting to standardize a new type of credential known as verifiable credentials (VCs) [89,107]. A public but private revocation registry and the issuer's digital signature can be used to verify the credentials' validity and expiration without communicating with the issuer. However, a verifier and the credential issuer must trust one other [21]. The use of DLT enables a decentralized system for providing reliable and trustworthy public information required to authenticate VCs. As a single point of truth, DLT serves as a place where standards, VC issuers (e.g., their public signing keys),

and VC revocation status can be stored and managed. Figure 4 illustrates SSI's key roles and components (already drawn in Figure 3: SSI components architecture).

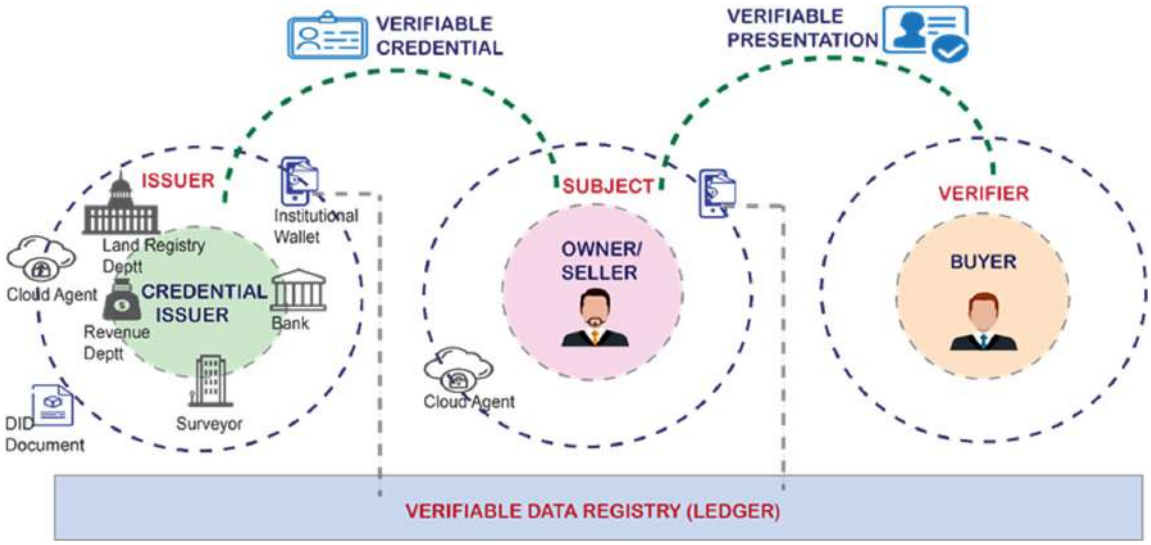


**Figure 4.** SSI-based land registry framework.

Other benefits of SSI include improved privacy, which is commonly acknowledged. Different identities, known as "pairwise DIDs", can be used in different interactions by default. Credential issuers, for example, need a global DID if they want to aggregate their reputation or credibility. The validity of claims, such as the existence of the issuer's signature on the VC, can be proven without revealing the content of the signature that is attested to the credential. In addition to preserving privacy, the digital signature provides the information essential to building the trust link required for interactions and business [112,113]. SSI enables users to maintain personal IDs and credentials across multiple contexts using a single app [114]. The following are the advantages of applying the SSI solution to the land registry:

- User sovereignty: Self-sovereign identification systems that use cryptographic signatures, pairwise connections, and digital identities provide the user with complete control over his identity data. SSI enables the user or a group of users to be linked to assets, enhancing the capabilities and scope of land registration. Furthermore, the challenges of validating and transferring identity information will evolve to give verified credentials and maintain the remaining registry components that do not benefit from Self-sovereign identity.
- Enhancing access to financial assistance: It also eases the financial assistance for people in poor nations through the use of SSI land registries. According to Inter-American Development Bank financial market analysts, Juan Antonio Ketterer and Gabriela Andrade, "transparent and more accurate asset registrations as collateral could eliminate knowledge-related asymmetry obstacles and provide financial access" [115]. Recent US initiatives suggest that mobile assets could help small and medium-sized firms expanded faster [116].
- Real estate market efficiency: Identifying participants is critical to reducing the likelihood of fraud in real estate markets, which leads to inefficiencies and higher transaction fees. A self-sovereign identification system can legally bind and securely link digital signatures to their owners, enabling trusted and transparent online functioning.
- Post-conflict land ownership: legal re-establishment of land ownership for refugees and internally displaced persons (IDPs) can aid in the restoration of a country's economy after a conflict has ended. However, the restoration procedure is complex since many refugees lack vital land records or are afraid of the consequence of claims [117].

In the absence of a competent property register, SSI collects land ownership documents and receives valid credentials from an NGO to assist in registering a claim [118].

- Disaster preparedness: In the event of a natural disaster, land ownership is critical for disaster preparedness and recovery. There are innovative techniques that have been incorporated into new disaster preparedness strategies. By incorporating the SSI in the land registry, users will benefit from an improved system to prove their land ownership and requesting assistance and restoration grants. Alternatively, decentralizing record administration will ensure that land ownership records are preserved. The usage of biometrics in SSI can help people authenticate their identities and access permitted services even if their documents are deleted or otherwise misplaced.

## 5. SSI-Based Land Registry Framework

A framework design based on the explanation given in Section 3 was developed to solve the challenges of land registry processes and to facilitate inter-departmental cooperation (a collaboration between the land registry department, bank, surveyor and revenue department, etc.) in the land registry. According to the findings of this article, an inter-departmental land registry collaboration is possible because of an SSI-based land registry architecture. However, the proposed framework design appears crucial from the perspective of data protection, particularly the privacy issues associated with maintaining owner and property data.

There are three main players involved in the proposed SSI-based land registry architecture: (i) the owner/seller (holder), (ii) the Buyer (verifier), and (iii) an issuer (government agency such as the land registry department, bank, surveyor and revenue department) [111]. When a land transaction occurs in the land registration system, the subject that is defined in the core of the framework is the owner/seller (see Figure 4). The owner/seller can manage their digital identity using user agents by establishing and saving DIDs and cryptographic keys in their digital wallets, storing passwords and credentials, creating backup files, and configuring permissions. It is possible to communicate with the agents via a variety of devices, including mobile phones and PCs. In all cases, the owner/seller is in complete command of their data, including any land-related papers represented by virtual certificates (VCs). Furthermore, verifiers that use conventional certificate-based methods must be provided with the entire certificate in order to validate the signature.

The proposed SSI-based land registry framework employs cloud agents and wallets to store credentials redundantly, make SSI documents more accessible, and enable secure communications with other entities. The blockchain is a decentralized platform for storing publicly verifiable information. It maintains public signing keys as well as other institutional data. Furthermore, the schemas of the land registry VCs are stored on-chain so that the public can validate their authenticity. Furthermore, revocation data are maintained on a blockchain, allowing the public to verify the privacy-preserving nature of revocation data. Credential issuers rely on institutional agents that are designed expressly for issuing credentials. These agents also verify the authenticity of credentials and engage directly with owners/sellers before and after the land registry procedure.

### *5.1. Phases of Land Registration System Using SSI*

The key SSI concept is a credential, which is a set of claims made by an issuer regarding an owner/seller. This definition of credential includes degrees, certificates, licenses, and digital badges. Humans are frequently used to verify credentials, while the SSI approach depends on standards, cryptography, distributed ledgers, and front-facing applications that allow machines to verify credentials.

#### 5.1.1. Roles and Relationships

In an SSI ecosystem, there are four main roles:

- The subject/owner plays a key role in the exchange of verifiable credentials.

- The issuer is the agent (individual or organization) responsible for creating the verifiable credential, such as the land registry department, bank, surveyor and revenue department.
- The verifier/relying party, when a buyer receives a verifiable credential, he or she is often interested in verifying its authenticity.
- A verifiable data registry (ledger) is a system that keeps track of data needed to verify a credential.

Credentials relevant to a subject are issued by a recognized credential issuer. The topic of the presentation provides verified credentials to relying parties. The dependent party validates credentials using a standard-based verification approach. It is possible to achieve this purpose in a secure manner by combining the credential with a verified data registry, such as the one that holds the issuer's cryptographic keys. As long as the issuer uses verifiable data registries, a regulator can regulate and indicate verifiable credentials without requiring dependent parties to contact the issuer via verifiable data registries directly.

#### 5.1.2. Scenario 1: Registration Phase

The land registry process begins with the registration of buyers and sellers who do not have an SSI agent or wallet, nor do they have any VCs. UML sequence diagrams are used to illustrate this scenario [111]. Figure 5 demonstrates the process sequence for the registration phase. To enable SSI-based registration, land registry departments must undertake a one-time bootstrapping procedure in which a public DID and an associated DID document are first stored in a distributed ledger.

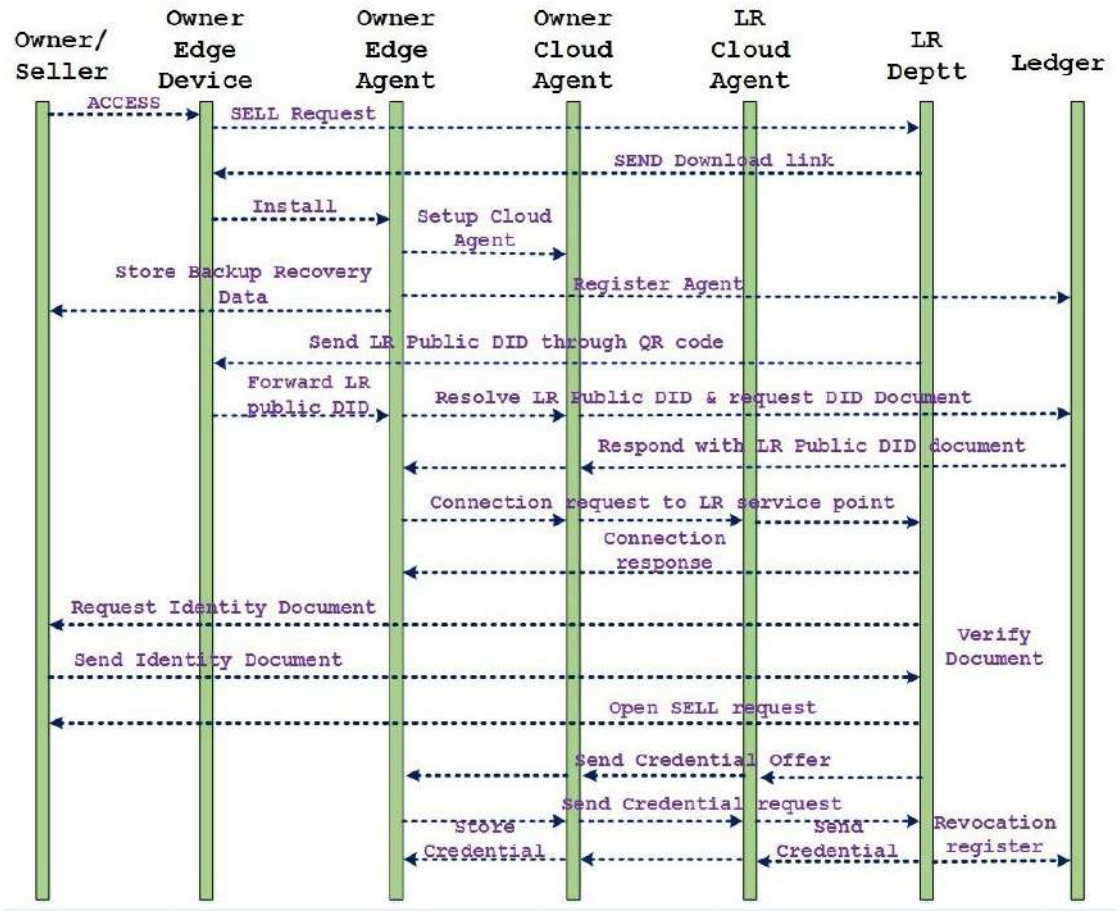


**Figure 5.** Process sequence for Registration phase.

For the owner/seller to sell their property, he first contacts the land registry department's website using a smartphone or laptop or physically visits a local branch. Because the owner/seller does not have an SSI user wallet or the appropriate KYC credentials, the land registry department recommends or offers the owner/seller a user wallet and provides a link to download the wallet from the official SSI website. Any digital wallet that supports public DID, peer DID, and VC and protects credentials and keys with a password or biometrics is available to the owner or seller. It is also possible that the land registry department will supply a cloud-based edge agent for backup and recovery purposes. A user wallet that is encrypted generates a new DID and stores it in the wallet itself. As part of this process, the user establishes a link secret, which will be used to link numerous credentials together in a virtual certificate, prohibiting selective credential sharing in the future. A link secret is not required in the VP, but any credentials containing the owner's or seller's name or similar strongly binding property must be included.

The owner/seller can now use their generated DID to establish a secure end-to-end connection with the land registry department to complete the land transfer. The land registry department could perhaps send a QR code to the customer to provide this data (e.g., via e-mail). The customer is linked to the land registration public service endpoint (cloud agent) and completes the transaction after scanning it with their wallet app. The land registry service endpoint delivers a connection request to the owner/seller service endpoint, which in turn sends the connection request to the cloud agent after generating a new pairwise DID and key pair for this association. This connection request includes the pairwise DID of the land registry department, the bank's public key, and the service endpoint through which the customer can contact the land registry department. Following that, the owner/seller digital wallet validates the connection and generates a pairwise DID and keys for the land registry department. A connection answer is then delivered to the land registry department's cloud agent/wallet, which forwards it to the interface. The land registry department now has an encrypted end-to-end link with the owner/seller, allowing the owner to exchange messages, public keys, VCs, and VPs safely. Because the owner/seller does not yet have any VCs, their identification must be verified. The owner/seller sends the necessary physical identity data to the land registry department, either on paper or scanned and delivered via email or the newly formed link. If the owner/seller opens an account, these physical identity data and land documents can be verified directly at a land registry branch.

After the verification of data and client identity, the land registry department can send a credential offered to the owner/seller edge user agent. Additionally, included in this credential offer is a preview of the data to be attested as well as the credentials' expiration dates and revocation information. It is then sent to the land registry department, along with the link secret in blinded form. With this certificate, selective disclosure is possible. This means that the owner/seller can blend claims from multiple VCs and only include the attributes attested by the VC that are required by the verifier.

#### 5.1.3. Scenario 2: Pre-Agreement and Verification

Owners and sellers who wish to sell their property during the pre-agreement phase must have a pairwise DID and a key pair in order to send a request to the (land registry) LR cloud agent, which was built during the previous registration phase.

The owner/seller and the land registry department now have a safe end-to-end encrypted link that can be used to exchange messages, public keys, VCs, and VPs. The seller submits the necessary DID and VPs of the credential (property documents) to the land registration department for verification using his cloud agent/wallet. When the owner/data seller's identity is validated, the land registry department's LR cloud agent will publish the property sale request on the ledger. Credential expiration and revocation information, as well as a preview of the verified data, can be found in the sale request.

The buyer can use a smartphone or laptop to search for properties for sale on the land registry department's website, or they can visit a local branch to search for the appropriate

property in person. Because the buyer does not have a wallet, the land registry department suggests or offers a user wallet and provides the buyer with a link to download it, as the buyer does not have one. To generate the DID, credentials, and associated keys, simply the buyer has to complete the processes outlined in the previous registration section. Figure 6 presents the process sequence for the pre-agreement and verification phase in the SSI-based land registry framework.

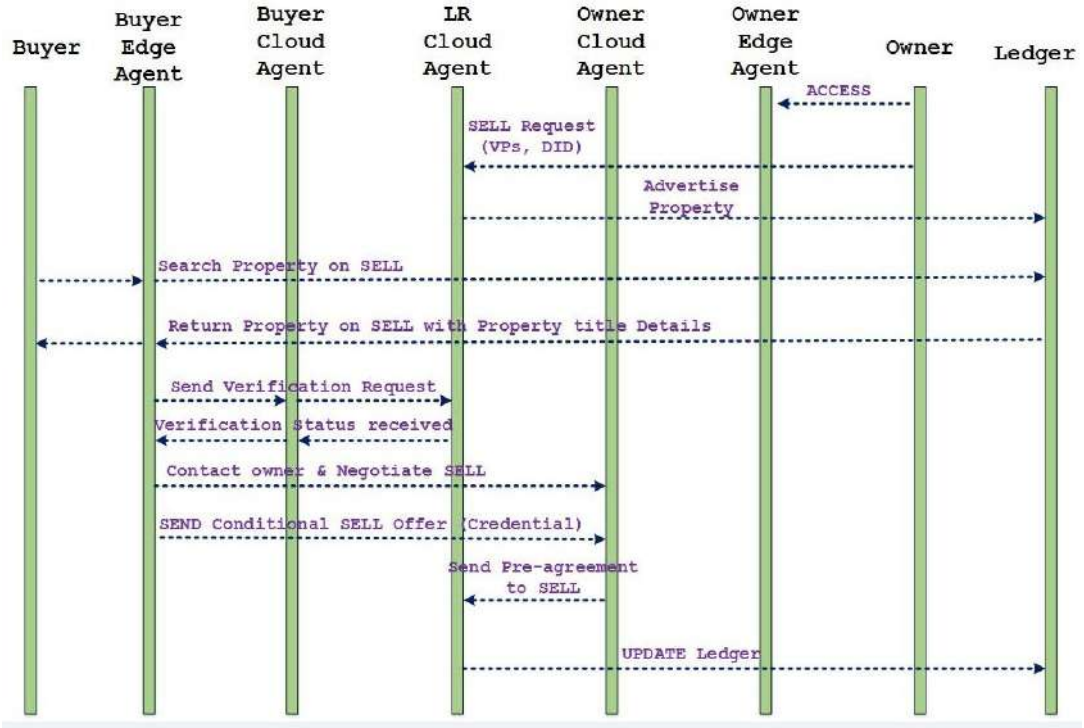


**Figure 6.** Process sequence for pre-agreement and verification phase.

After viewing the property's specific details, the buyer will submit a verification request to the LR cloud agent, who will then evaluate the correctness of the VPs linked with the VC and provide consumers with the needed proof of non-revocation. Once the property verification status is deemed OK by the LR cloud agent, the buyer can submit a credential offer to the owner/seller edge user agent over the established connection. This credential offer contains a preview of the data that will be confirmed, such as information about the credential issuer, the VC's expiration date, and credential revocation information. After that, the owner/seller verifies the credential offer and sends it to the LR Cloud agent. Additionally, it will contain the identity of the credential issuer, the expiration date of the VC, and information regarding its revocation in this pre-agreement sell request to the ledger.

#### 5.1.4. Scenario 3: Bank Fund Transfer and Certificate Generation

As the pre-agreement request to sell the property is updated on the ledger, the Land Registry department cloud agent now notifies the owner and buyer cloud agents regarding the property sales initiation. After receiving notification from the LR department, the buyer will send a confirmed request for the purchase of property to the LR department cloud agent. Figure 7 depicts the process sequence for bank fund transfer and certificate generation.

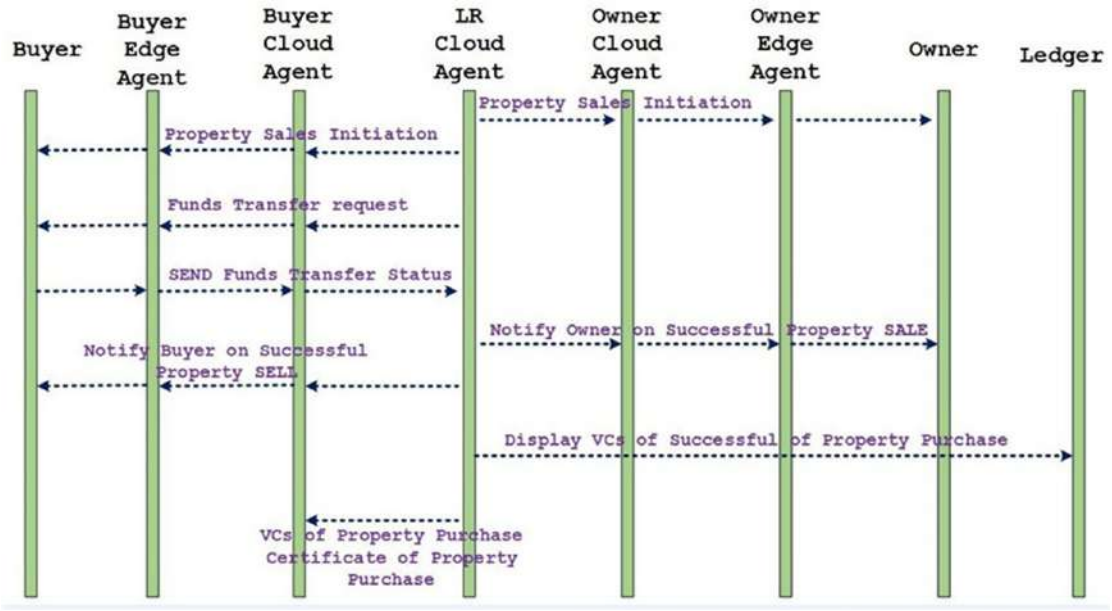


**Figure 7.** Process sequence for bank fund transfer and certificate generation.

The LR department cloud agent will send a fund transfer request to the buyer containing the DID, VPs of property, with options of online payments of funds through banks. After successful payment of the fund, the buyer cloud agent sends the VCs of fund transfer status and payment details. Furthermore, the LR department cloud agent will notify the owner and buyer cloud agents regarding the successful property sale and send VCs which contain all the details of the property purchase to the ledger so that it is displayed on the land registry department website. At the same time, the LR department cloud agent will generate the VC for the property certificate with the new owner's name and transactions details and send it to the buyer cloud agent.

## 6. Conclusions

This paper has highlighted the importance of SSI and compared the major SSI solutions uPort, Civic, ShoCard, and Sovrin SSI solutions based on SSI principles. This comparison concludes that none of the existing SSI solutions fully complies with the SSI principles. It also highlights the steps and requirements for SSI adoption. It discusses how governments can implement a fully scalable, fully functioning, and fully SSI ecosystem and numerous digital identity governance laws that the government should adopt. This paper has presented the SSI framework and component architecture. This paper has reviewed the SSI components required for developing any SSI solution and how these SSI components are fulfilling the requirements of SSI principles compliance individually. In the end, this paper elaborates on the SSI application in land registries and provides an SSI-based land registry framework for resolving the issues of traditional land registry systems. Lastly, a detailed phase involved in the process of the land registration system that includes the registration phase, pre-agreement and verification, bank fund transfer and certificate generation using SSI has been elaborated.

The limitation of this research is that the proposed framework has not been practically implemented and hence it cannot be evaluated from real-world entities involved in the process of land registry. There are few more dimensions that are required to be studied in future, such as: (1) involvement of governments and policy makers for evaluating the SSI-compatible identity and technological framework; (2) understanding of the new phenomenon (SSI) by the jurists, regulators, notaries and other involved parties in land registry process for ease of transition and implementation; (3) evolving the regulatory policy for recognizing the verifiable credentials such as digital identifiers. Finally, the adaption of

the state-of-the-art IT infrastructure for the issuance and verification of SSI credentials and accessing digital services is essential for successful implementation.

**Author Contributions:** Conceptualization, N.H.H. and S.M.I.; Data curation, M.S.; Formal analysis, M.S., N.H.H., S.U., S.B. and P.A.; Investigation, S.U., S.A., S.B., P.A. and S.M.I.; Methodology, M.S.; Project administration, P.A. and S.M.I.; Resources, S.M.I.; Supervision, S.U.; Validation, S.M.I.; Visualization, S.M.I.; Writing—original draft, M.S. All authors have read and agreed to the published version of the manuscript.

**Funding:** This research received no external funding.

**Data Availability Statement:** There is no underlying data set used, although the article contains the detailed analysis of the previous research done in the field and proposes a SSI framework for land registry.

**Conflicts of Interest:** The authors declare no conflict of interest.

## References

1. Windley, P.; Reed, D. *Sovrin$^{TM}$: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust*; Sovrin Foundation: Provo, UT, USA, 2018. Available online: https://sovrin.org/wp-content/uploads/Sovrin-Protocol-and-Token-White-Paper.pdf (accessed on 1 August 2020).
2. World Bank. *ID4D 2018 Global Dataset*; World Bank Group: Washington, DC, USA, 2018. Available online: https://id4d.worldbank.org/global-dataset (accessed on 21 December 2020).
3. Idrees, S.; Nowostawski, M. *Transformations through Blockchain Technology*; Springer: Berlin/Heidelberg, Germany, 2022.
4. Toaha, M.; Khan, S. Automated digital archive for land registration and records. In Proceedings of the 11th International Conference on Computer and Information Technology, Khulna, Bangladesh, 24–27 December 2008; pp. 46–51. [CrossRef]
5. Rahman, A.; Hossain, R. The uncomfortable truth about land disputes in Bangladesh: Insights from a household survey. *Land Use Policy* **2020**, *95*, 104557. [CrossRef]
6. Rabbani, M.; Hossain, F. Digitisation of land administration. *The Daily Star*, 28 November 2019.
7. Antonio, T.; Lilyana, P. Directive (EU) 2018/843 of the European parliament and of the council. *Off. J. Eur. Union* **2018**, *2018*, 32.
8. Aslam, T.; Maqbool, A.; Akhtar, M.; Mirza, A.; Khan, M.A.; Khan, W.Z.; Alam, S. Blockchain based enhanced ERP transaction integrity architecture and PoET consensus. *Comput. Mater. Contin.* **2022**, *70*, 1089–1109. [CrossRef]
9. Andrew, S.; Andrew, B. *The Future of Real Estate Transactions*. 2019. Available online: https://www.sbs.ox.ac.uk/sites/default/files/2019-03/FoRET-ReportSummary_0.pdf (accessed on 2 April 2022).
10. Krupa, K.S.; Akhil, M.S. Reshaping the Real Estate Industry Using Blockchain. In *Lecture Notes in Electrical Engineering*; Springer: Singapore, 2019; Volume 545, pp. 255–263.
11. Graglia, J.M.; Mellon, C. Blockchain and Property in 2018: At the End of the Beginning. *Innov. Technol. Gov. Glob.* **2018**, *12*, 90–116. [CrossRef]
12. Idrees, S.M.; Nowostawski, M.; Jameel, R.; Mourya, A.K. Security aspects of blockchain technology intended for industrial applications. *Electronics* **2021**, *10*, 951. [CrossRef]
13. Bouras, M.A.; Lu, Q.; Zhang, F.; Wan, Y.; Zhang, T.; Ning, H. Distributed Ledger Technology for eHealth Identity Privacy: State of The Art and Future Perspective. *Sensors* **2020**, *20*, 483. [CrossRef]
14. Shuaib, M.; Hassan, N.H.; Usman, S.; Alam, S.; Bhatia, S.; Mashat, A.; Kumar, A.; Kumar, M. Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison. *Mob. Inf. Syst.* **2022**, *2022*, 8930472. [CrossRef]
15. Stokkink, Q.; Pouwelse, J. Deployment of a Blockchain-Based Self-Sovereign Identity. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1336–1342. [CrossRef]
16. European Commission. *Trends in Electronic Identification: An Overview*; European Commission: Brussels, Belgium, 2018.
17. ESSIF. *European Self-Sovereign Identity Framework*; European Commission: Den Haag, The Netherlands, 2021.
18. Der, U.; Jahnichen, S.; Sürmeli, J. Self-sovereign Identity $-$ Opportunities and Challenges for the Digital Revolution. *arXiv* **2017**, arXiv:1712.01767.
19. Baars, D. *Towards Self-Sovereign Identity Using Blockchain Technology*; University of Twente: Twente, The Netherlands, 2016.
20. Coelho, P.; Zúquete, A.; Gomes, H. Federation of Attribute Providers for User Self-Sovereign Identity. *J. Inf. Syst. Eng. Manag.* **2018**, *3*, 32. [CrossRef]
21. Muhle, A.; Gruner, A.; Gayvoronskaya, T.; Meinel, C. A survey on essential components of a self-sovereign identity. *Comput. Sci. Rev.* **2018**, *30*, 80–86. [CrossRef]
22. Allen, C. The path to self-sovereign identity. *Coin Desk*. 25 April 2016. Available online: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html (accessed on 18 May 2020).
23. Lundkvist, C.; Heck, R.; Torstensson, J.; Mitton, Z. *Uport: A Platform for Self-Sovereign Identity*; Blockchainlab: London, UK, 2016.

24. Civic Technologies Inc. Civic Whitepaper. 2017. Available online: https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf (accessed on 13 January 2021).
25. Ali, M.; Shea, R.; Nelson, J.; Freedman, M.J. Blockstack: A New Internet for Decentralized Applications. Doylestown, United States. 2017. Available online: https://github.com/stacksgov/stacks-co (accessed on 2 August 2020).
26. SelfKey Foundation. Self-Sovereign Identity for more Freedom and Privacy—SelfKey. *Selfkey*. September 2017. Available online: https://selfkey.org/ (accessed on 13 April 2020).
27. Ebrahimi, A. Identity management verified using the blockchain. *ShoCard, Tech. Rep.* 2019. Available online: https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf (accessed on 22 April 2020).
28. Mehendale, D.K.; Masurekar, R.S.; Patil, H.V. Implications of Block Chain in Real Estate Industry. *Int. J. Recent Technol. Eng.* **2019**, *8*, 500–503.
29. Graglia, M.; Mellon, C.; Robustelli, T. The Nail Finds a Hammer Self-Sovereign Identity, Design Principles, and Property Rights in the Developing World. *New America Weekly*, 17 October 2018; p. 93.
30. Senturk, S. Future of property rights: Self-Sovereign Identity and Property Rights. *New America Weekly*, 12 June 2019; p. 2.
31. Shang, Q.; Price, A. A Blockchain-based Land Titling Project for the Republic of Georgia. *Innovations* **2018**, *12*, 72–78. [CrossRef]
32. Piore, A. Can Blockchain Finally Give Us The Digital Privacy We Deserve? *Newsweek* **2019**, *172*, 1–16. Available online: http://ezproxy.library.yorku.ca/login?url=https://search.proquest.com/docview/2185863710?accountid=15182 (accessed on 14 November 2021).
33. Dobhal, A.; Regan, M.; Property, M.R.; Dobhal, M.; Regan, A. Immutability and Auditability: The Critical Elements in Property Rights Registries. In Proceedings of the Annual World Bank Conference on Land and Property, Washington, DC, USA, 15 March 2016; pp. 1–8.
34. Oliveira, E. Land Ownership and Land Use Development: The Integration of Past, Present, and Future in Spatial Planning and Land Management Policies. *Landsc. J.* **2017**, *36*, 119–121. [CrossRef]
35. Kalkuhl, M.; Milan, B.F.; Schwerhoff, G.; Jakob, M.; Hahnen, M.; Creutzig, F. *Fiscal Instruments for Sustainable Development: The Case of Land Taxes*; Munich Personal RePEc Archive: Munich, Germany, 2017.
36. Kempe, M. The Land Registry in the Blockchain. 2016. Available online: http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf (accessed on 5 November 2020).
37. Kumar, P.; Dhanush, G.A.; Srivatsa, D.; Nithin, A.; Sahisnu, S. A Buyer and Seller's Protocol via Utilization of Smart Contracts Using Blockchain Technology. In *Communications in Computer and Information Science*; Springer: Singapore, 2019; Volume 1075, pp. 464–474.
38. Themistocleous, M. Blockchain technology and land registry. *Cyprus Rev.* **2018**, *30*, 195–202.
39. McMurren, J.; Young, A.; Verhulst, S. Addressing Transaction Costs Through Blockchain and Identity in Swedish Land Transfers. Boston, MA, USA. October 2018. Available online: https://blockchan.ge/blockchange-land-registry.pdf (accessed on 1 August 2020).
40. Idrees, S.M.; Aijaz, I.; Jameel, R.; Nowostawski, M. Exploring the Blockchain Technology: Issues, Applications and Research Potential. *Int. J. Online Biomed. Eng.* **2021**, *17*, 48–69. [CrossRef]
41. Fairfield, J.A.T. BitProperty. *S. Cal. L. Rev.* **2015**, *88*, 805.
42. Mukne, H.; Pai, P.P.S.R.; Raut, S.; Ambawade, D. Land Record Management using Hyperledger Fabric and IPFS. In Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT), Kanpur, India, 6–8 July 2019; pp. 1–8. [CrossRef]
43. Abhishek, G. *Property Registration and Land Record Management via Blockchains*; Indian Institute of Technology Kanpur: Kanpur, India, 2019.
44. Hoxha, V.; Sadiku, S. Study of factors influencing the decision to adopt the blockchain technology in real estate transactions in Kosovo. *Prop. Manag.* **2019**, *37*, 684–700. [CrossRef]
45. Raquel Benbunan, F.; Arturo, C. Digitization of Land Records: From Paper to Blockchain. In Proceedings of the International Conference on Information Systems 2018, ICIS 2018, San Francisco, CA, USA, 13–16 December 2018; Volume 2, pp. 1–9. Available online: https://www.researchgate.net/publication/329222337 (accessed on 17 May 2020).
46. Mashatan, A.; Roberts, Z. An enhanced real estate transaction process based on blockchain technology. *AMCIS 2017 Am. Conf. Inf. Syst. A Tradit. Innov.* **2017**, *2017*, 1–5.
47. Taxation Researcher. Buying Property in Mexico | How To Buy a House in Mexico. *Global Property Guide*; Maxico, North America, 2020; pp. 1–8. Available online: https://www.globalpropertyguide.com/Latin-America/Mexico/Buying-Guide (accessed on 2 April 2022).
48. Kalyuzhnova, N. Transformation of the real estate market on the basis of use of the blockchain technologies: Opportunities and problems. In Proceedings of the MATEC Web of Conferences, Irkutsk, Russia, 26–27 April 2018; Volume 212, p. 6004. [CrossRef]
49. Xie, Z.; Yin, J.; Guo, J. The research of transaction costs between real estate developers and their partners. In Proceedings of the 2nd International Conference on Logistics, Informatics and Service Science LISS 2012, Beijing, China, 3 January 2013; Springer: Berlin/Heidelberg, Germany, 2013; pp. 1151–1156. [CrossRef]
50. Miller, N.; Pogue, D. Sustainable real estate and corporate responsibility. In *Routledge Handbook of Sustainable Real Estate*, 1st ed.; Wilkinson, S.S.S., Dixon, T., Miller, N., Eds.; Routledge: Abingdon, UK, 2018; pp. 19–36.

51. Cerutti, E.; Dagher, J.; Dell'Ariccia, G. Housing finance and real-estate booms: A cross-country perspective. *J. Hous. Econ.* **2017**, *38*, 1–13. [CrossRef]
52. Danielsen, B.; Harrison, D. Liquidity, Accounting Transparency, and teh Cost of Capital: Evidence from Real Estate Invetment Trusts. *J. Real Estate* **2014**, *36*, 212–252.
53. Norta, A.; Fernandez, C.; Hickmott, S. Commercial Property Tokenizing With Smart Contracts. In Proceedings of the 2018 International Joint Conference on Neural Networks (IJCNN), Rio de Janeiro, Brazil, 8–13 July 2018; pp. 1–8. [CrossRef]
54. Kaplanov, N.M. Nerdy Money: Bitcoin, the Private Digital Currency, and the Case Against Its Regulation. *SSRN Electron. J.* **2012**, *25*, 1–65. [CrossRef]
55. Dobhal, A.; Property, M.R. Immutability and Auditability: The Critical Elements in Property Rights Registries. *Annu. World Bank Conf. L.* **2018**, 1–20.
56. Lemieux, V.L. Evaluating the Use of Blockchain in Land Transactions: An Archival Science Perspective. *Eur. Prop. Law J.* **2017**, *6*. [CrossRef]
57. Thakur, V.; Doja, M.N.; Dwivedi, Y.K.; Ahmad, T.; Khadanga, G. Land records on Blockchain for implementation of Land Titling in India. *Int. J. Inf. Manag.* **2020**, *52*, 1–9. [CrossRef]
58. Malik and T. Foxcroft Real estate agents caught breaking the rules on Marketplace's hidden camera. *CBC News*. 3 November 2016. Available online: https://www.cbc.ca/news/business/real-estate-agents-caught-breaking-the-rules-on-marketplace-s-hidden-camera-1.3825841 (accessed on 2 April 2020).
59. Myrick, C. Top 6 Real Estate Scams-and How to Avoid Them. *The Globe and Mail*. 9 August 2018. Available online: https://www.theglobeandmail.com/real-estate/mortgages-and-rates/top-6-real-estate-scams-and-how-to-avoid-them/article13108985 (accessed on 2 April 2020).
60. Shenderovich, E.; Sarva, A. *The Blockchain Network of Commercial Real Estate*; Baya: Carlsbad, CA, USA, 9 August 2019; pp. 1–18.
61. Agarwal, B. *Conclusive Land Title System for India*; Panjab University: Chandigarh, India, 2018.
62. Fernando, D.; Ranasinghe, N. Permissioned Distributed Ledgers for Land Transactions; A Case Study. *Lect. Notes Bus. Inf. Process.* **2019**, *361*, 136–150. [CrossRef]
63. Alam, S.; Shuaib, M.; Khan, W.Z.; Garg, S.; Kaddoum, G.; Hossain, M.S.; Bin Zikria, Y. Blockchain-based Initiatives: Current state and challenges. *Comput. Netw.* **2021**, *198*, 108395. [CrossRef]
64. Maza, M.V. El auge de blockchain y sus posibilidades reales de aplicación en los registros de las administraciones públicas. *IDP Rev. Internet Derecho Y Política* **2019**, *28*, 109–126. [CrossRef]
65. Kaczorowska, M. Blockchain-based Land Registration: Possibilities and Challenges. *Masaryk Univ. J. Law Technol.* **2019**, *13*, 339–360. [CrossRef]
66. Sylvester, G. *E-Agriculture in Action:Blockchain for Agriculture Opportunities and Challanges*, 2018th ed.; Food and Agriculture Organization of the United Nations and the International Telecommunication Union: Bangkok, Thailand, 2019.
67. Ekmekci, H.S. Applicability of Blockchain Technology to Turkish Land Registry System. Master's Thesis, Tilburg University, Tilburg, The Netherlands, 2019.
68. Mintah, K.; Baako, K.T.; Kavaarpuo, G.; Otchere, G.K. Skin lands in Ghana and application of blockchain technology for acquisition and title registration. *J. Prop. Plan. Environ. Law* **2020**, *12*, 147–169. [CrossRef]
69. Yapicioglu, B.; Leshinsky, R. Blockchain as a tool for land rights: Ownership of land in Cyprus. *J. Prop. Plan. Environ. Law* **2020**, *12*, 171–182. [CrossRef]
70. Mehdi, N. *Blockchain: An Emerging Opportunity for Surveyors?* RICS Insight: London, UK, 2020; Available online: https://www.rics.org/globalassets/blockchain_insight-paper.pdf (accessed on 2 April 2020).
71. Konashevych, O. Constraints and benefits of the blockchain use for real estate and property rights. *J. Prop. Plan. Environ. Law* **2020**, *12*, 109–127. [CrossRef]
72. Krigsholm, P.; Ridanpaa, K.; Riekkinen, K. Blockchain as a Technological Solution in Land Administration-What are Current Barriers to Implementation? *FIG Peer Rev. J.* **2019**, *XV*, 14–22. Available online: https://www.fig.net/resources/proceedings/fig_proceedings/fig2019/papers/ts08i/TS08I_krigsholm_ridanpaeae_et_al_9829.pdf (accessed on 17 February 2022).
73. Liu, Y.; He, D.; Obaidat, M.S.; Kumar, N.; Khan, M.K.; Choo, K.K.K.-K.R. *Blockchain-Based Identity Management Systems: A Review*; Elsevier Ltd.: Amsterdam, The Netherlands, 2020; Volume 166, p. 102731.
74. Schaffner, M. *Analysis and Evaluation of Blockchain-Based Self-Sovereign Identity Systems*; Technical University of Munich: Munich, Germany, 2020.
75. Alam, S. Identity Model for Blockchain-Based Land Registry System: A Comparison. *Wirel. Commun. Mob. Comput.* **2022**, *2022*, 1–17. [CrossRef]
76. Wang, F.; de Filippi, P. Self-Sovereign Identity in a Globalized World: Credentials-Based Identity Systems as a Driver for Economic Inclusion. *Front. Blockchain* **2020**, *2*, 28. [CrossRef]
77. Ellingsen, J. Self-Sovereign Identity Systems: Opportunities and Challenges. Master's Thesis, Norwegian University of Science and Technology, Trondheim, Norway, 2019.
78. Shuaib, M.; Alam, S.; Alam, M.S.; Nasir, M.S. Self-sovereign identity for healthcare using blockchain. *Mater. Today Proc.* **2021**, 1–8. [CrossRef]
79. Shuaib, M.; Alam, S.; Nasir, M.S.; Alam, M.S. Immunity credentials using self-sovereign identity for combating COVID-19 pandemic. *Mater. Today Proc.* **2021**, 1–6. [CrossRef] [PubMed]

80. van Bokkem, D.; Hageman, R.; Koning, G.; Nguyen, L.; Zarin, N. Self-Sovereign Identity Solutions: The Necessity of Blockchain Technology. *arXiv* **2019**, arXiv:1904.12816.
81. Naik, N.; Jenkins, P. Governing Principles of Self-Sovereign Identity Applied to Blockchain Enabled Privacy Preserving Identity Management Systems. In Proceedings of the 2020 IEEE International Symposium on Systems Engineering (ISSE), Vienna, Austria, 12 October–12 November 2020; pp. 1–6. [CrossRef]
82. Naik, N.; Jenkins, P. *Digital Identity Roadmap Guide*; International Telecommunications Union: Geneva, Switzerland, 2019.
83. The National Archives. *Guidance on Digital Preservation*; 2013. Available online: http://www.nationalarchives.gov.uk/information-management/projects-and-work/guidance.htm (accessed on 13 January 2021).
84. Lyons, T.; Courcelas, L.; Timsit, K. Blockchain for Government and Public Services. In Proceedings of the Eupopean union Blockchain Observatory & Forum, Brooklyn, NY, USA, 7 December 2018.
85. OIX. The Open Identity Exchange. 2019. Available online: https://openidentityexchange.org/members/anon/new.html?destination=%2Findex.html (accessed on 13 January 2021).
86. e-Estonia. e-Identity. 2019. Available online: https://e-estonia.com/solutions/e-identity/id-card/ (accessed on 13 January 2021).
87. López, M.A. *Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain*; Inter-American Development Bank: Washington, DC, USA, 2020.
88. Bamasaq, O.; Alghazzawi, D.; Bhatia, S.; Dadheech, P.; Arslan, F.; Sengan, S.; Hassan, S.H. Distance Matrix and Markov Chain Based Sensor Localization in WSN. *Comput. Mater. Contin.* **2022**, *71*, 4051–4068. [CrossRef]
89. Sporny, M.; Longley, D.; Chadwick, D. Verifiable Credentials Data Model 1.0, 2019. Available online: https://www.w3.org/TR/vc-data-model/ (accessed on 2 February 2021).
90. Kumar, A.; Bhatia, S.; Kaushik, K.; Gandhi, S.M.; Devi, S.G.; Pacheco, D.A.D.J.; Mashat, A. Survey of Promising Technologies for Quantum Drones and Networks. *IEEE Access* **2021**, *9*, 125868–125911. [CrossRef]
91. Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M. Decentralized Identifiers (DIDs) v1.0 Properties id. *www.w3c.org*. 2021. Available online: https://w3c.github.io/did-core (accessed on 19 August 2021).
92. W3C Credentials Community Group. Verifiable Claims Task Force. 4 May 2017. Available online: https://w3c.github.io/vctf/ (accessed on 2 August 2021).
93. Christopher, A.; Arthur, B.; Vitalik, B.; Jon, C.; Duke, D.; Christian, L.; Kravchenko, P.; Nelson, J.; Reed, D.; Sabadello, M.; et al. Decentralized Public Key Infrastructure. White Paper, Rebooting the Web of Trust. 2015. Available online: https://www.weboftrust.info/downloads/dpki.pdf (accessed on 2 April 2022).
94. Reed, D.; Sporny, M.; Longley, D.; Allen, C.; Grant, R.; Sabadello, M. Decentralized Identifiers (DIDs): Data Model and Syntaxes for Decentralized Identifiers. 2019. Available online: https://w3c-ccg.github.io/did-spec/ (accessed on 13 December 2021).
95. Government of Canada. Pan-Canadian Trust Framework Overview. *Github*. Available online: https://canada-ca.github.io/PCTF-CCP/ (accessed on 25 February 2021).
96. Palanisamy, T.; Alghazzawi, D.; Bhatia, S.; Malibari, A.A.; Dadheech, P.; Sengan, S. Improved Energy Based Multi-Sensor Object Detection in Wireless Sensor Networks. *Intell. Autom. Soft Comput.* **2022**, *33*, 227–244. [CrossRef]
97. Hyperledger. MSP Implementation with Identity Mixer—Hyperledger-Fabricdocs Master Documentation. 2018. Available online: https://hyperledger-fabric.readthedocs.io/en/release-1.3/idemix.html#what-is-idemix (accessed on 23 March 2022).
98. Sporny, M.; Longley, D.; Kellogg, G.; Lanthaler, M.; Lindström, N. *JSON-LD 1.1*. 16 July 2020. Available online: https://www.w3.org/TR/json-ld/ (accessed on 19 February 2022).
99. Sabadello, M. A Universal Resolver for Self-Sovereign Identifiers. *Medium*. 1 November 2017. Available online: https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c (accessed on 19 January 2022).
100. Tobin, A.; Reed, D. *The Inevitable Rise of Self-Sovereign Identity*; Sovrin Foundation: Provo, UT, USA, 2017. Available online: https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf (accessed on 17 December 2021).
101. Sharaff, A.; Kamal, C.; Porwal, S.; Bhatia, S.; Kaur, K.; Hassan, M.M. Spam message detection using Danger theory and Krill herd optimization. *Comput. Netw.* **2021**, *1389*, 199–1286. [CrossRef]
102. Glauser, R. *Self-Sovereign Identities in Cardossier*; ETH Zürich: Zurich, Switzerland, 11 June 2019. Available online: https://pub.tik.ee.ethz.ch/students/2018-HS/MA-2018-34.pdf (accessed on 20 January 2022).
103. Clauß, S.; Köhntopp, M. Identity management and its support of multilateral security. *Comput. Netw.* **2001**, *37*, 205–219. [CrossRef]
104. Shuaib, M.; Daud, S.M.; Alam, S.; Khan, W.Z. Blockchain-based framework for secure and reliable land registry system. *Telkomnika* **2020**, *18*, 2560–2571. [CrossRef]
105. el Maliki, T.; Seigneur, J.-M. A Survey of User-centric Identity Management Technologies. In Proceedings of the International Conference on Emerging Security Information, Systems, and Technologies (SECUREWARE 2007), Valencia, Spain, 14–20 October 2007; pp. 12–17. [CrossRef]
106. Rajput, A.; Gopinath, K. Towards a more secure aadhaar. In *Lecture Notes in Computer Science (Including Subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*; Springer: Cham, Switzerland, 2017; Volume 10717, pp. 283–300. [CrossRef]
107. Lim, S.Y.; Fotsing, P.T.; Almasri, A.; Musa, O.; Kiah, M.L.M.; Ang, T.F.; Ismail, R. Blockchain technology the identity management and authentication service disruptor: A survey. *Int. J. Adv. Sci. Eng. Inf. Technol.* **2018**, *8*, 1735–1745. [CrossRef]
108. Maler, E.; Reed, D. The Venn of Identity: Options and Issues in Federated Identity Management. *IEEE Secur. Priv. Mag.* **2008**, *6*, 16–23. [CrossRef]

109. Singla, R.; Kaur, N.; Koundal, D.; Lashari, S.A.; Bhatia, S.; Rahmani, M.K.I. Optimized Energy Efficient Secure Routing Protocol for Wireless Body Area Network. *IEEE Access* **2021**, *9*, 116745–116759. [CrossRef]
110. Avellaneda, O.; Bachmann, A.; Barbir, A.; Brenan, J.; Dingle, P.; Duffy, K.H.; Maler, E.; Reed, D.; Sporny, M. Decentralized Identity: Where Did It Come From and Where Is It Going? *IEEE Commun. Stand. Mag.* **2019**, *3*, 10–13. [CrossRef]
111. Soltani, R.; Nguyen, U.T.; An, A. A New Approach to Client Onboarding Using Self-Sovereign Identity and Distributed Ledger. In Proceedings of the 2018 IEEE International Conference on Internet of Things (iThings) and IEEE Green Computing and Communications (GreenCom) and IEEE Cyber, Physical and Social Computing (CPSCom) and IEEE Smart Data (SmartData), Halifax, NS, Canada, 30 July–3 August 2018; pp. 1129–1136. [CrossRef]
112. Davie, M.; Gisolfi, D.; Hardman, D.; Jordan, J.; O'Donnell, D.; Reed, D. The Trust over IP Stack. *IEEE Commun. Stand. Mag.* **2019**, *3*, 46–51. [CrossRef]
113. Hardman, D. No Paradox Here: ZKPs Deliver Savvy Trust-Evernym. 2020. Available online: https://www.evernym.com/blog/no-paradox-here-zkps-deliver-savvy-trust/ (accessed on 29 January 2022).
114. Sedlmeir, J.; Smethurst, R.; Rieger, A.; Fridgen, G. Digital Identities and Verifiable Credentials. *Bus. Inf. Syst. Eng.* **2021**, *63*, 603–613. [CrossRef]
115. ketterer, J.A.; andrade, G. Blockchain Asset Registries: Approaching Enlightenment?—CoinDesk. 2 December 2017. Available online: https://www.coindesk.com/blockchain-asset-registries-entering-slope-enlightenment (accessed on 14 November 2021).
116. International Finance Corporation. *Secured Transactions Systems and Collateral Registries*; World Bank: Washington, DC, USA, 7 February 2017. [CrossRef]
117. Hendow, M. Bridging Refugee Protection and Development. 7 January 2019. Available online: https://www.researchgate.net/publication/331530630_Bridging_refugee_protection_and_development_Policy_Recommendations_for_Applying_a_Development-Displacement_Nexus_Approach (accessed on 2 April 2022).
118. Dempsey, J.; Graglia, M. Case Study: Property Rights and Stability in Afghanistan. *New America*, 5 May 2017; p. 4.