Hindawi
Mobile Information Systems
Volume 2022, Article ID 8930472, 17 pages
https://doi.org/10.1155/2022/8930472

Review Article

Self-Sovereign Identity Solution for Blockchain-Based Land Registry System: A Comparison

Mohammed Shuaib,[1,2] **Noor Hafizah Hassan**,[1] **Sahnius Usman**,[1] **Shadab Alam**,[2] **Surbhi Bhatia**,[3] **Arwa Mashat**,[4] **Adarsh Kumar**,[5] **and Manoj Kumar**[5]

[1]*Razak Faculty of Technology and Informatics (RFTI), Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia*
[2]*College of Computer Science & IT, Jazan University, Saudi Arabia*
[3]*Department of Information Systems, College of Computer Science and Information, Technology, King Faisal University, Al Hasa, 36362, Saudi Arabia*
[4]*Faculty of Computing & Information Technology, King Abdulaziz University, P.O. Box 344, Rabigh 21911, Saudi Arabia*
[5]*Department of Systemics, School of Computer Science, University of Petroleum and Energy Studies, Dehradun, India*

Correspondence should be addressed to Adarsh Kumar; adarsh.kumar@ddn.upes.ac.in
and Manoj Kumar; wss.manojkumar@gmail.com

Received 20 January 2022; Accepted 17 March 2022; Published 4 April 2022

Academic Editor: Sebastian Podda

Providing an identity solution is essential for a reliable blockchain-based land registry system. A secure, privacy-preserving, and efficient identity solution is essential but challenging. This paper examines the current literature and provides a systematic literature review in three stages based on the three research questions (RQ) that show the assessment and interpretation process step by step. Based on the parameters and RQ specified in the research methodology section, a total of 43 primary articles have been selected from the 251 articles extracted from various scientific databases. The majority of these articles are concerned with evaluating the existing self-sovereign identity (SSI) solutions and their role in the blockchain-based land registry system to address the compliance issues in the existing SSI solutions with SSI principles and find the best possible SSI solution to address the identity problems in the land registry. The existing digital identity solutions cannot handle the requirements of the identity principle and are prone to various limitations like centralization and dependency on third parties that further augment the chance of security threats. SSI has been designed to overcome these limitations and provide a secure, reliable, and efficient identity solution that gives complete control to the users over their personal identity information (PII). This paper reviews the existing SSI solutions, evaluates them based on the SSI principles, and comes up with the best possible SSI solution for a blockchain-based land registry system. It further provides a detailed investigation of each SSI solution to present its functionalities and limitations for further improvement.

1. Introduction

The land registry is an important economic pillar for any country in nation-building. Blockchain technology can improve the security and transparency in the land registry by recording land-related details on the blockchain. Blockchain technology also hastens property identification and enhances trust and accuracy in transactions by enabling digital monitoring by stakeholders. Through an increasingly digital world, robust, useful, and flexible digital identity management systems are critical to electronically identifying and authenticating ourselves and to know who we communicate. As per McKinsey, "Good Digital ID" contains a high level of digital channel protection, verification, and authenticated identity, specially created with the user consent [1]. In 2005, Cameron wrote "The Law of Identity as an Identity and Access Architect" at Microsoft Corporation [2]. This law consists of 7 principles that translate several guidelines on managing and disclosing a user's identity and identifying various entities with different types of identification. These

principles describe digital identity systems' success and failure. So digital identity solutions are needed to facilitate the users of the land registry system to initiate a transaction [3]. However, many researchers [4, 5] working in the field of applying digital identity solutions for blockchain-based land registry systems confirmed the issue of noncompliance with digital identity principles given by Cameron [2]. So while developing an identity solution for a blockchain-based land registry system, these issues need attention [6, 7].

A digital identity is a collection of credentials and identifiers expressed in an appropriate context, for instance, the name, ID, and other relevant attributes [8, 9]. Digital identity describes the attribute of an entity digitally in providing access to systems and application of identity management process [10]. Traditionally, digital identities are mediums to validate users at the workplace. Existing digital identities are controlled by identity providers, not by the users themselves. Identity providers have complete ownership over an individual's identity, making it vulnerable to identity misuse. Identity owners often share their credentials for registering or accessing a service with no standard or guidelines on what data they need to share and store on the Internet. In addition, oversharing of data contributes to privacy issues for the identity owner [11]. Since the challenges of current digital identity are severe and damaging, a new concept of digital identity is required. That can offer users complete control over their identities, reduce management costs, increase efficiency, and improve overall online identity [12].

In [13], the author presented the privacy-preserving blockchain-based identity management system for remote healthcare. The author evaluated the proposed system on the parameters like transaction gas cost, transaction per second, number of blocks lost, and block propagation time. The developed identity system can be applied to cancer patients and can be further extended by integrating the blockchain with IPFS. Additionally, in [14], purpose the scheme of digital coupon and explained the desired properties and features in the couponing system, which can be utilized to identify the nonrepudiation property using malicious issuers. Further in [15], the author presented a privacy-preserving blockchain architecture for IoT using Hierarchical Identity Based Encryption (HIBE) suitable for IoT devices and mobile edge and cloudlet environments. The presented architecture is evaluated in a simulation environment named Contiki OS. The presented architecture provides the confidentiality, integrity, and availability of the data for the mobile edge nodes.

SSI provides a decentralized identity and fully controls their identity and personal data. It only shares the necessary information with a third party, known as selective disclosure [16]. Issuing identity credential built on the trusted network among two parties is the main objective of self-sovereign identity. Blockchain technology utilizes a distributed ledger to achieve consensus using a cryptographic protocol, fulfilling the requirement of providing a decentralized system in self-sovereign identity [17, 18]. While several blockchain-based SSI frameworks are available, no SSI model is available specifically for the land registry systems. The SSI used in the land registry will provide individuals with identities that can be used for communication with land management services. SSI can also allow individuals to create evidence of their property, such as a certified survey plan or a notarized declaration. SSI offers an opportunity to design a gradually more secure and trustworthy identity in lieu of a government-approved identity document by collecting certificates issued by reliable third parties, such as a land registry and financial institutions [19]. SSI can provide a framework for data transformation into credentials to use their verified location history from a mobile provider and land registry certificates to provide proof of ownership claim [20]. SSI may directly connect individuals to land plots and provide a mechanism for recording land claims and related data.

An SSI holder can use a verifiable claim issued for land ownership to access other services such as banking, loans, and government benefits. Individuals could submit a digital title to obtain financial assistance or agricultural subsidies. A verifiable claim will be a permanent record by government authority acknowledging the rights of a property owner at a certain stage. If property certificates are lost, or the owners were relocated, the verifiable claim will remain [21]. SSI development is still at the initial stage. Many governments and enterprises are currently involved in developing SSI solutions that are mainly based on blockchain technology. Some of the prominent SSI solutions are Sovrin [22], UPort [23], Civic [24], Blockstack [25], Selfkey [26], and ShoCard [27]. These SSI solutions are being used in different domains. These SSI solutions should satisfy the principles of digital identity solutions given by Cameron [2]. In [2], Cameron looked at SSI solutions to figure out the cause of their failure and market adaptability. He also came up with a requirement to comply with the SSI principles for building a successful SSI solution [27]. So every SSI solution should comply with the SSI principles [28].

This study is aimed at identifying how the self-sovereign identity solves the issues of compliance with the digital identity principle in a blockchain-based land registry system. This paper tries to identify the role of SSI in a blockchain-based land registry system. It further aims to review the various SSI principles by different researchers and come up with an evaluation criterion to evaluate the existing SSI solutions. Finally, it evaluates the existing SSI solutions to identify the most suitable one for applying in the blockchain-based land registry system. Various classification of the principle of SSI is given by [29] [11]. However, none of these classifications is complete since several properties are still missing. However, it appears that some principles under one group can be irrelevant, as described in [29]. We identified the criteria based on the classifications given by [11, 30] to compare the SSI solutions in SSI compliance principles, which should be taken care of while designing an SSI-based identity model for a blockchain-based land registry. A systematic analytical study of existing SSI solutions has been conducted based on the defined SSI principles and finalized evaluation criteria.

This article is divided into five sections. Section 2 provides a detailed background study. Section 3 presents the research methodology that includes identified research questions (RQ), data sources used, search mechanism, and

inclusion/exclusion criteria to shortlist the study sources. Section 4 presents a detailed analysis of the outcomes extracted from the literature based on each research question. Finally, Section 5 concludes the findings and reviews.

2. Background and Literature Review

This section provides a detailed study of the background literature required for this study that includes concepts of self-sovereign identity (SSI), the role of SSI in information flow, blockchain technology, and its application in SSI and applications of SSI in the land registry system.

2.1. Concept of Self-Sovereign Identity. Self-sovereign identity (SSI) is a revolutionary way to address identity. In the early days, centralized organizations controlled digital identities, while in the real world, people stored their issued identity information in a decentralized manner using a physical wallet. SSI's objective is to connect online identity systems to the actual world and give users control over their identities. In the actual world, after the birth of a child, identity credentials like birth certificates, identification numbers, etc., are provided by the government authorities [16]. The person utilizes these credentials on several occasions to identify themselves or establish a relationship throughout life.

The self-sovereign identity is a well-developed concept in the academic and industry fields. However, there is still no consensus on its exact definition. Generally, the SSI is defined by considering the principles of self-sovereign by de Marneffe [31] and descriptions of identity by [32]. Self-sovereign identity is a digitalized form of personal features, details, and attributes. No entity can breach the right to choose a level of privacy or reputation of identity attribute. While working as an identity and access architect in Microsoft Corporation, Cameron wrote identity laws in 2005. The identity law [2] follows a distributed ledger [33], which first explains the concept of SSI [34]. Although Cameron was unaware of the advancement of distributed ledgers in the upcoming years, proposing the Microsoft Passport is an unnecessary reliance on a single organization without user control and can lead to identity failures. The necessity of user access, minimal disclosure, and a portable, interoperable structure is required. The first occurrence of sovereign identity happened in 2019 [35].

In 2016, Allen presented ten principles of the self-sovereign identity (SSI) [34], focusing upon identity laws by describing how identity could work, why systems and algorithms need to be transparent, and how is it permanent despite being portable and interoperable. The details required for the concept of self-sovereign identity were proposed by [36]. The definition provided by Abraham is congruent with the ten principles provided by Allen [34]. Abraham extends the control concept and adds, "All user identity information will be recorded for further authentication." It is trade-of-security and privacy, which should be based on the chosen user. SSI is considered as a long-lasting identity possessed and controlled by the individual without any external authority sans the possibility of identity removal. It requires user consent for interoperability of user identity across several locations and ownership over the identity to provide user autonomy. SSI may prove to be the new normal in the evaluation of identity management.

2.2. Roles of Self-Sovereign Identity. The self-sovereign identity (SSI) environment structure is defined as a peer-to-peer model where the independent identity works as a peer and communicate with each other. Communication is done so that people and organizations can affirm the information from individuals by assigning claims or credentials [12, 16]. The significant elements in SSI are identity verifier, identity issuer, and credential issuer. The functions of each entity of SSI are represented in Figure 1.

Figure 1 explains the roles of SSI in the credential flow order. The issuer provides the credential for making the statement as it is often given through off-chain. The credentials and self-attached data of the identity owner are available in the wallet. Issuers may withdraw credentials if requirements are not fulfilled. The identity owner stores the credentials provided in a digital wallet, which function as an agent in the SSI environment. The entire identity credential is held in a digital wallet as proof of verification displayed in a disclosed manner. The identity owner has complete control over data sharing and usage. The consent of the identity owner is required to access information for verifier services. Accessible records in public registries such as the issuer's identification key, DID, are confirmed to ensure the actual issuer issues these credentials. When the identity owner's information meets the criteria, access is given, where the presented credentials are checked without contacting an issuer.

Similarly, offering alternative credentials like a student ID does not require the university's permission in the actual world. The blockchain uses a distributed ledger technology which allows the creation of identity without a central authority where the ledger acts as a basis of trust. An essential feature of SSI is the backend data storage in off-ledger. Most DID methods use a public or private repository, such as a private database or IPFS (Interplanetary File System), to collect off-ledger information. IPFS generates content-based hashes using particular IPFS data. Wallet files are stored as a backup in the backend off-ledger, making it easy to recover if lost.

2.3. Blockchain Technology and Self-Sovereign Identity. Self-sovereign identity systems are based on blockchain technology. The blockchain is an evolving technology that uses cryptocurrency to provide a decentralized, open shared ledger [37] that can be used for electronic voting [38] land registration [39, 40]. It is evident that cryptocurrency is not the only feasible use case for blockchain [41, 42]. Blockchain technology is well placed due to its technical features in facilitating a notable change in digital identity [43]. The self-sovereign identity is based on the sharing and storing verifiable claims held in off-ledger [44]. The authenticity of these signed data objects is assured by storing a hash of the thing on a blockchain. Once subjects submit a verifiable claim to a relying party, the hash of the claim with available blockchain record can be compared and verified through an integrated signature where the relying party can quickly and precisely ascertain the claim's validity. A blockchain provides a way to revoke or store an auditable record of consent behavior and maintain the security of data

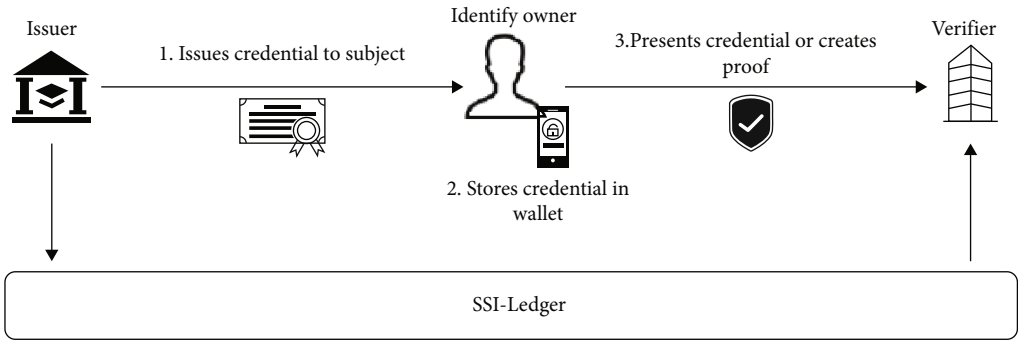

Figure 1: Roles of SSI with information flow [12].

objects to assure the integrity of the data object. Blockchain is built on a decentralized public-key infrastructure and provides robust methods that can be used for encryption and authentication, apart from self-sovereign identity [45, 46]. Additionally, [47], blockchain offers several key features that have ample opportunities for identity systems, including immutability, usability, and low transaction cost [48, 49].

2.4. Self-Sovereign Identity and Land Registry. The self-sovereign identity (SSI) fundamental application for the land registry is to provide individuals with identities so that they can be used for communication with land management services. There is no identification record for one billion people across the world. SSI offers an opportunity to design a gradually more secure and trustworthy identity in lieu of a government-approved identity document by collecting certificates issued by reliable third parties, such as a land registry and financial institutions [19]. In the absence of legal documentation, SSI can also allow individuals to create evidence of their property, such as a certified survey plan or a notarized declaration. SSI credentials are robust and should not be limited to the digital version of the traditional paper [50]. SSI can provide a framework for data transformation into credentials so that administrative agencies trust it. For example, a person can use their verified location history from a mobile provider and land registry certificates to provide proof of ownership claim [20].

In the absence of land registries, the self-sovereign identity may directly connect individuals to land plots and provide a mechanism for recording land claims and related data to access other services such as banking, loans, and government benefits. An SSI holder can use a verifiable claim issued for land ownership. Individuals could submit a digital title to obtain financial assistance or agricultural subsidies. A verifiable claim will be a permanent record by government authority acknowledging the rights of a property owner at a particular stage. In the case of property, if the certificate is lost or the owner relocated, and the verifiable claim will remain [51].

(i) *User Control.* Self-sovereign identity solutions using a cryptographic signature, pairwise connection, and digital identities provide the user with complete control over his identity information. The user or the groups will be attached to the assets through self-sovereign identity, which improves the functions and scope of the land registry. Moreover, verifying and exchanging identity information will evolve to provide validated credentials and manage the remaining registry components that do not benefit through Self-sovereign identity

(ii) *Facilitate Access to Finance.* Self-sovereign identity-based land registers can also provide more detailed and trusted information about potential borrowers in developing countries. The financial-market specialists at the Inter-American Development Bank, Juan Antonio Ketterer, and Gabriela Andrade, acknowledged that transparent and more accurate asset registers as collateral could mitigate knowledge-related asymmetry constraints and provide financial access [52]. As shown in recent initiatives in the United States of America, The expansion of mobile assets can have a major impact on economic growth for small and medium scale enterprises [53]

(iii) *Efficiency in Real Estate Markets.* To reduce the possibility of fraud in the real estate markets, a high degree of due diligence is required for the identity of the involved parties, leading to inefficiency and more transaction fees. A self-sovereign identity solution will securely associate the owner with its properties and legally bind the digital signature to provide trusted and transparent online working

(iv) *Land Ownership in Postconflict Situations.* Legal reestablishment of land for refugees and internally displaced persons (IDPs) helps postconflict restoration. However, the restoration process is complicated as many refugees do not have any essential land records or fear consequences [54]. An SSI secures land ownership records and receives verifiable credentials from an NGO to help record a claim in lieu of a proper land registry [1]

(v) *Natural Disaster Resilience.* Land ownership is important for preparing for disasters and can improve the restoration process. New programs for disaster preparedness use innovative

technologies. Nevertheless, a solution to SSI will give users a safer and more accessible tool to show their land ownership and submit a request for assistance and restoration grants. Decentralized record management will guarantee the preservation of land ownership records. The use of biometrics in SSI allows people to prove their identities and authorized services, even though documents are deleted or lost

3. Research Methodology

This paper performs a systematic literature review to explore the latest state-of-the-art academic research on self-sovereign identities and blockchain. Additionally, to examine the role of self-sovereign identity in the land registry system. To have the most comprehensive coverage of all published literature, our systematic review methods were carefully planned using the guidelines of Kitchenham and Charters [55] to identify the need for review and create a review plan. Our systematic review method includes the research questions, data sources used for retrieving papers, search strategy, inclusion and exclusion criteria, and screening and final selection description are summarized in Figure 2.

3.1. Research Questions. The first stage of the systematic literature review was to identify research questions (RQs) for a detailed review of available topics. The main research question addressed in this study is as follows.

(RQ): how to select the most appropriate self-sovereign identity for the blockchain-based land registry?

To answer the main research question of this study, we outlined three guiding questions.

RQ1: how self-sovereign identity solves the issue of noncompliance with digital identity principles in the blockchain-based land registry?

RQ2: which criteria can be used to compare the most appropriate blockchain-based self-sovereign identity solution?

RQ3: what is the evaluation result of various blockchain-based self-sovereign identity solutions?

To address the above guiding questions, we used the guidelines given by Kitchenham and Charters for a systematic review [55] and the standard procedure for selecting the literature for our research.

3.2. Data Sources. In this systematic research, material collection was performed through various scholarly databases such as Scopus, Web of Science, ACM Digital Library, and IEEE Xplore to collect more articles. These databases were chosen as they contain peer-reviewed papers and enable logical expressions (keywords, names, and/or abstracts) to be searched. Grey's literature, such as reports on government projects, working papers, and documents on assessment, was also included. The blockchain-based self-sovereign identity implementation subject is a new study area, and the various blockchain-based firms are currently working on it. Including grey literature extends state-of-the-art research sources by using a broader research source. Each selected database was checked separately by the specified search words, and the results were combined after removing duplicates using Mendeley software. Table 1 shows the number of articles generated by search string in each database. Some found publications are available in more than one database. The total number of articles with duplication is 251.

3.3. Search Strategy. The search strategy is carried out between 2008 and 2021. This systematic review study took the starting point from 2008 when the first actual research in the blockchain was published. The grey literature includes magazines, company whitepapers, and books. To identify different blockchain-based self-sovereign identity solutions, and to be as generic as possible, the search string used to retrieve the articles from databases is ("self-sovereign identity" AND "Blockchain") OR ("self-sovereign identity" AND "identity management ") OR ("self-sovereign identity" AND "Blockchain" AND "identity management"). Also, semantic search words were identified in the fields of digital identity, and self-sovereign identity and blockchain are also searched in the databases. Moreover, our search string is restricted only to the article's title, abstract, and subject terms. It was done to exclude irrelevant articles referencing the search words only in the body's text.

The next step was to search for all related papers. A final search was carried out on 17 November 2020, covering years from 2008 to 2022. The search consists of conferences, journals, workshops, government project reports, working papers, review documents, and book sections. The searched terms are "blockchain", "land registry", "Identity model", and "Law of identity" to check the title, keywords, and abstracts of academic papers. Some research papers use real estate in place of land registry, so we have modified the search strategy and used only the real estate & blockchain keywords.

Additionally, some researchers use identity management in place of the identity model. As a result, we finally decided to discover all papers based on strings ("land registry" AND "Blockchain" or "real estate" AND "Blockchain" or "Identity model" AND "Law of identity", "identity principle" or "Identity management" AND "Law of identity", "identity principle"). Table 2 displays the search string and the results from scholarly databases.

3.4. Inclusion/Exclusion Criteria. Not all of the articles found were important to the subject, and thus, the next step was to identify the article that satisfies the scope of our study. We have done this by specifying criteria for inclusion and exclusion, as seen in Table 3. These criteria are applied to all titles, abstracts, and keywords of the identified article to classify them according to the scope of our study. Titles and abstracts in some cases have not been all appropriate; therefore, the whole paper has been examined to ensure the compactness of criteria for inclusion and exclusion.

3.5. Screening and Final Selection. The initial screening process was carried out on collected papers to verify compliance with our scope of the study. In this Systematic Literature Review, 251 articles were collected mainly from the scholarly databases (grey literature has been omitted from the

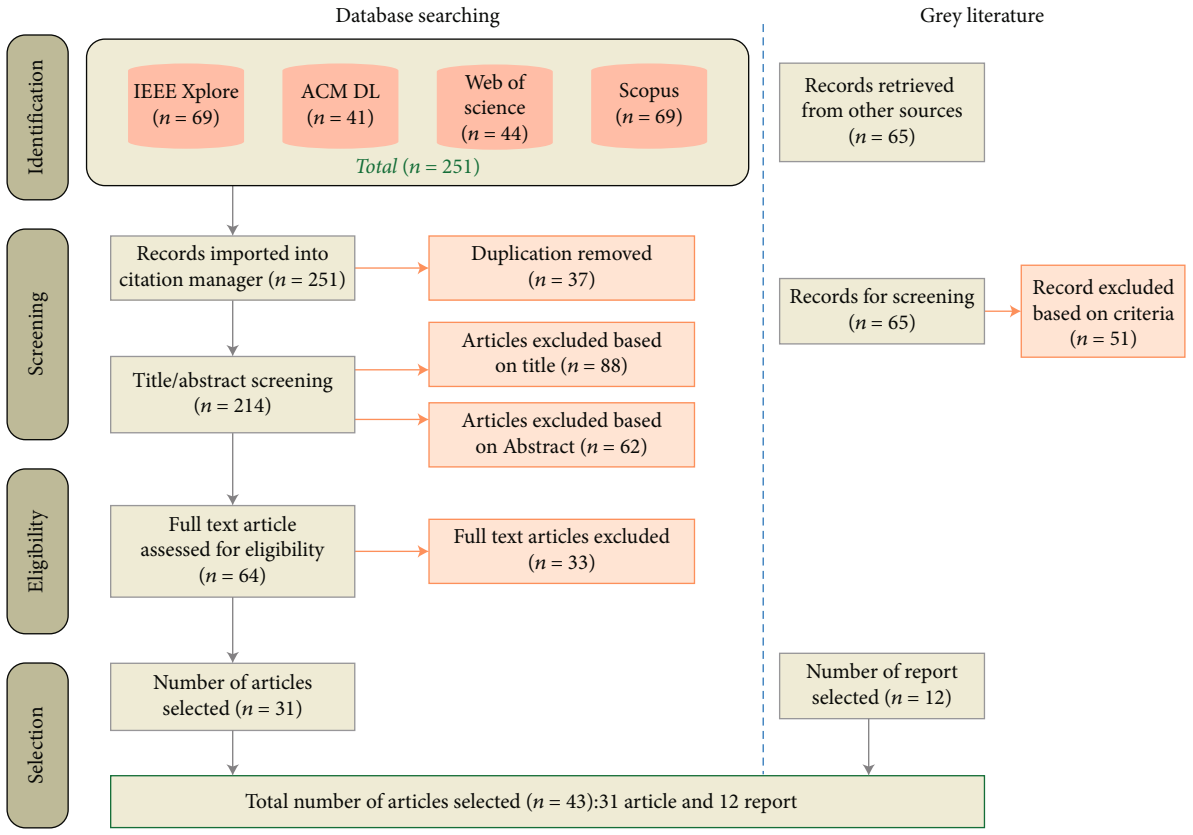

Figure 2: Procedural steps for the selection process.

Table 1: Search string and results for scholarly databases.

Database	Scopus	Web of Science	ACM Digital Library	IEEE Xplore
("self-sovereign identity" AND "Blockchain")	48	19	19	25
("self-sovereign identity" AND "identity management")	27	14	11	18
("self-sovereign identity" AND "Blockchain" AND "identity management")	22	11	11	26
Total with duplicates	97	44	41	69

Table 2: Search terms and results from different scholarly databases.

Search terms	IEEE Xplore	Scopus	ACM	Science direct	Web of Science
"Land registry" AND "Block chain"	7	28	19	36	14
"Real estate" AND "Blockchain"	20	77	67	77	33
"Identity model", "Identity" AND "Law of identity", "identity principle"	7	9	5	8	2
"Identity management" AND "Law of identity", "identity principle"	6	21	8	22	11
Total with duplicates	40	135	99	143	60

Table 3: Inclusion/exclusion criteria.

Inclusion criteria	Exclusion criteria
(i) Publication between 2008 and 2022 (ii) papers with research scope of blockchain technology and subscope—the application of that technology for the domain related to the self-sovereign identity, identity management (iii) original research paper instead of review/survey paper	(i) Duplicate (ii) not English language paper (iii) papers that had some other meaning other than one relevant to the blockchain-based self-sovereign identity (iv) articles addressing technical aspects of blockchain technology

descriptive analyzes for conformity). The number of articles chosen as primary studies has been reduced to 214 after eliminating (37) duplicate papers, resulting in 214 articles. Subsequently, we read each publication's titles, abstracts, and keywords to keep them relevant to the next stage of screening. We also carefully reviewed whether they are inside or outside the scope through the inclusion and exclusion criteria by reading the abstract, conclusion, and discussion sections. Eighty-eight articles are excluded based on the title, and 62 articles are excluded based on the abstract. A limited number of publications passed the primary screening stage for many factors. Finally, the first screening of the article ended with 64 articles. In the final screening, the remaining 64 articles were read in detail, thereby removing the publications that have little significance to the scope of our study. Finally, 31 papers and 12 reports have been selected for our study.

4. Research Questions and Analysis

This section is further divided into three subsections (A, B, and C). Section A presents the issues of noncompliance with identity principles in the blockchain-based land registry system and how SSI solves this issue. Section B describes the criteria for evaluating the blockchain-based SSI solutions. Section C shows evaluation results of various blockchain-based SSI solutions based on the defined criteria.

4.1. RQ1: How Self-Sovereign Identity Solves the Issue of Noncompliance with Digital Identity Principles in the Blockchain-Based Land Registry? Through an increasingly digital world, robust, useful, and flexible digital identity management systems are critical to electronically identifying and authenticating ourselves and to know who we communicate. As per McKinsey1, "Good Digital ID contains a high level of digital channel protection" verification and authenticated identity, specially created with the user consent [56]. It helps us to decide with whom and for what reasons we choose to exchange data to ensure user's privacy and control of personal data. "This would" unlock value by encouraging inclusion, formalization, and digitalization.

For instance:

(i) 45% of females aged around 15+ in low-income countries lack ID, and only 30% of males do

(ii) Digital ID could increase 3-13 percent of GDP in 2030

In 2005, Cameron wrote The Law of Identity as an Identity and Access Architect at Microsoft Corporation [2]. A basic definition of identity requires concepts that can be focused on the design of additional services by involved parties. The principles can also be used as a goal to build trust and interoperability between services in the environment. This law consists of 7 principles that translate several guidelines on managing and disclosing a user's identity and identifying various entities with different types of identification. These principles describe digital identity systems' success and failure. These are briefly explained below.

(i) *Law 1: User Control and Consent*. "Identity systems only disclose user identification with user consent"

(ii) *Law 2: Minimum Disclosure*. The most successful long-term solution is one that discloses the lowest quantity of information and limits its use

(iii) *Law 3: Justifiable Parties*. Digital identity systems should be established to limit information disclosure to parties with the necessary, justifiable position in a particular identity relationship

(iv) *Law 4: Directed Identification*. The universal identity scheme must recognize omnidirectional identifiers for public entities and unidirectional identifications for private entities, simplifying discovery and preventing unnecessary correlation disclosures

(v) *Law 5: Pluralism of Operators and Technology*. The identity system should manage multiple identity technologies run by different providers and allow them to communicate

(vi) *Law 6: Human Integration*. The human user must be represented as part of the distributed system that can be integrated into communication mechanisms between people and machines to safeguard from identity attacks

(vii) *Law 7: Consistent Experience across Contexts*. A unifying identity metasystem must ensure that its users have a clear and consistent experience, enabling operators and technologies to differentiate between different contexts

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 user control and consent. Some identity solutions may satisfy one but not the other. Given that there was no self-sovereign identification at the time of writing these principles. It was all the more remarkable to have the majority of principles adopted from "The Evolution of Digital Identity Concepts guiding principles" by Allen [34]. In a well-known post, "The Path to Self-Sovereign Identity," Allen outlined SSI principles, including specific guidelines from other sources such as Cameron and the W3C Verifiable Statements Task Force [57]. These ten principles are taken from Allen's paper [34] and serve as guidelines for SSI adaptation.

(1) *Control: Users Must Control Their Identities*. The user is the ultimate authority of his identity, subject to well-understood and safe algorithms that ensure that the identity and its arguments remain valid. He should be able to identify, update, or even hide it. The user is free to pick actors or privacy as he wishes. The user does not regulate all identity claims: other users can make claims about a user, but they should not be central to its identity

(2) *Access: Users Must Have Access to Their Own Data*. A user must always be able to easily access and recover all the claims and other identification details. There must be no hidden data and no gatekeepers

(3) *Transparency: Transparent Systems and Algorithms*. The systems for managing and running an identity network must be transparent in terms of their functioning, management, and updating. The algorithms should be open source, well-documented, and autonomous from any particular architecture

(4) *Persistence: Identities Must Be Long-Lived*. The user can only remove identities. Claims can be updated and removed, but the identity that belongs to these claims should be long-lived. Identities can ideally remain permanently or probably as long as the consumer wants. Although private keys could have to be rotated and data need to be changed, the identity remains. In the rapidly evolving world of the Internet, this goal may not be entirely feasible, but identities at least remain until new identity systems outdate them

(5) *Portability: Identity Information and Services Must Be Transportable*. A trusted third-party entity should not hold the identity. It should be transportable, although a trusted entity behaves in the customer's best interests. Transportable identities ensure that the individual stays in charge of their identity, which can increase identity persistence over time

(6) *Interoperability: Identities Should Be Used as Widely as Possible*. Identity is of little benefit if used only in small niches. A modern-day digital identity system aims to access identity information widely and across international borders to create global identities without relinquishing user control

(7) *Consent: Users Must Agree to the Use of Their Identity*. Any identity system is designed to share identity and claims, and an interoperable system improves the number of shares occurring. However, data sharing must only occur with user consent. While other users such as an employer, credit office, or spouse can make claims, the user must also confirm consent

(8) *Existence: Users Must Have an Independent Existence*. An SSI fundamentally depends on the ineffable "I" at the core of identity. It will never fully exist in digital form. It needs to be the self-supporting kernel to support this

(9) *Minimalization: Disclosure of Claims Must Be Minimized*. It should include the least amount of data required to perform the task when sharing data. It is supported by selective disclosure and zero-knowledge proof. However, noncorruptibility is a difficult task. The best possible way to solve this is to use minimization to promote privacy

(10) *Protection: The Rights of Users Must Be Protected*. If the identity network priorities vary from those of the rights of individuals, the network should commit to protecting the rights and freedom of users over the network

SSI is considered as a long-lasting identity possessed and controlled by the individual without any external authority sans the possibility of identity removal. It requires user consent for interoperability of user identity across several locations and ownership over the identity to provide user autonomy. SSI may prove to be the new normal in the era of digital identity. The self-sovereign identity is a potential solution since it provides people, organizations, and companies sovereignty over their identifiers and full control on how and to whom information is shared or utilized. Only the necessary information will be revealed to third parties in what is known as selective disclosure [12, 16]. Issuing identity credential built on the trusted network among two parties is the main objective of self-sovereign identity. Through the use of an easy, automated process and standard format, SSI can create a convenient communication method.

4.2. RQ2: What Are the Criteria for Evaluating Blockchain-Based Self-Sovereign Identity Solutions?

4.2.1. Related Work. The various evaluation criteria taken by multiple researchers to evaluate self-sovereign identity and comparative studies of blockchain-based self-sovereign solutions are discussed below.

Cameron (2005) explained the seven laws discussed in the earlier section, where he outlined the strengths and weaknesses of digital identity concepts [2]. These laws are vital to prevent any repercussions where the laws of identity and the requirement of self-sovereign identity are described in detail. Certain blockchain-based solutions may not satisfy certain properties of self-sovereign identity. Based on these seven laws, Christopher (2016) outlined ten principles to consider when implementing SSI solutions [34]. In the self-sovereign identity solution, these principles are aimed at user control besides providing the differences between the seven laws. Stokkink and Pouwelse (2018) used these ten self-sovereign identity principles to test blockchain-based SSI solutions: Sovrin and uPort. They included an additional property in the evaluation list that involves claims to be provable [58].

The problem with the current identity solution is identified as the individual is not the real owner of their identity. Besides, this problem can be overcome with the growth of the SSI solution. A DNS-Idm blockchain-based identity management system is developed using a smart contract to improve protection and privacy features [59]. In [43], the author compares various blockchain identity management systems and identifies challenges like trust, security, and privacy issues. Also, he discussed various trust, security, and privacy-based schemes that can be utilized to improve the blockchain-based identity nmangennet system. Shuaib et al.

(2022) compare the identity model, namely, centralized, federated, user-centric, and SSI based on laws of digital identity and suggested the SSI solution to be used for blockchain-based land registry system [60, 61]. Finally, a comparison of the available SSI solution, i.e., uPort, Sovrin, and Shocard, is made with the developed DNS-Idm using security and privacy criteria like ownership, user control and consent, human integration, privacy-friendly, and directed precise identity.

Dunphy and Petitcolas (2018) made a comparison between blockchain solutions that used SSI based on the seven laws of identity [62], where they used trusted, decentralized identity where identity proofing relies on trustable existing credentials. They concluded that the usability (human integration) feature needs further improvement [63].

Similarly, Panait et al. (2020) evaluated ten current blockchain identity management solutions using SSI focusing on the implementation of the platform and long-term validity [64]. He emphasizes the need to improve the cryptography and usability aspect of the SSI's current identity management solution. On the other hand, Van Bokkem et al.(2019) evaluated the seven blockchain-based self-sovereign identity solutions based on the eleven identity principles outlined by [34] alongside the provable property notion [65]. In [66], a comparative study of the popular identity management system is done using SSI like ShoCard, UPort, and Sovrin based on the seven laws of identity by [62].

Liu et al. (2020) compared blockchain identity systems that use SSI, namely, uPort, Sovrin, and Shocard, based on aspects like control, security, and privacy. Liu et al. compared the existing blockchain-based self-sovereign identity system such as UPort, ShoCard, and Sovrin [43] using the principles of self-sovereign identity given by [34].

The three self-sovereign identity solutions, namely, Everest, Evernym, and uPort, are analyzed using the SSI principle using the desk research and interview with company blockchain experts [19]. As the "consent" principle in developing countries is difficult to adopt, so it has been removed with the "Inclusion" principle.

4.2.2. Our Evaluation Criteria. The SSI requires the basic principle of identity given by [2]. The principle of SSI in an article by Allen is examined that provides an additional view on the digital identity liked to the seven identity principles given by Cameron. The ten essential principles for SSI are portability, access, transparency, persistence, control, transparency, existence, interoperability, protection, and minimization [34]. A similar classification of principle for SSI is given in (Ferdous et al., 2019), containing three properties: acceptance, zero cost, and controllability. Further, these principles were classified in [29], where the SSI principle is divided into three main groups: controllability, security, and portability. Additionally, the seven principles, namely, availability, approval, tenacity, approval, authority, autonomy, and confidentiality, were used to compare SSI solutions [11].

None of these classifications is complete since several properties are still missing. However, it appears that some principles under one group can be irrelevant, as described in [29], where they highlighted that the principle of persistence and existence in the context of controllability are mismatched. This study introduces the principle of "Inclusion" and the elimination of "Existence," which is essential for implementation in developing countries. The "usability" principle was also incorporated in the assessment model, as customer service's role is crucial in creating a better digital identity system. Therefore, a new taxonomy is categorized based on the classifications given by [11, 30] to compare the SSI solutions in SSI compliance principles. Figure 3 gives a mapping of principles of identity with the SSI principles. Based on all these classifications, new criteria for evaluating the SSI solutions have been proposed. The proposed principles to compare the SSI based solution in our study are described as follows:

(1) *Inclusion*. Everyone possesses an individual identity and should have an identity from birth to death

(2) *User Control and Consent*. Users must have ownership over their identity and can refer, update, trace, and access their personal data. Online data sharing of personal data should only be accomplished with user consent

(3) *Privacy and Protection*. The user's "right to privacy" should be secured on the protocol level

(4) *Portability*. The identities should be available as long as the identity owner desires. The identity information will be portable, allowing users to access and control their identity, increasing identity persistence over time

(5) *Persistence*. The identity system will be long-lasting, where identity owners can recover private keys and passwords if their primary device is damaged or stolen

(6) *Transparency*. The system used to manage the identity network must be transparent in its processes, management, and updates

(7) *Interoperability*. User identities are universally acceptable across various international boundaries and systems

(8) *Human Integration*. The system interface meets the user's needs where identity owners will add user experience in upcoming technology and services

4.3. RQ3: What Is the Evaluation Result of Various Blockchain-Based Self-Sovereign Identity Solutions? Secure user authentication and authorization are significant challenges for a reliable identity solution that needs to be addressed. SSI is a possible solution for resolving current identity models' issues and providing permanent identity while providing full user control. Blockchain is an innovative technology to implement SSI solutions. The use of blockchain technology in the identity management system presents a possible solution for storing data on the blockchain. The stored data is secured using cryptographic tools and makes them immutable. The blockchain-based SSI solution foster trust among participants within the network without disclosing

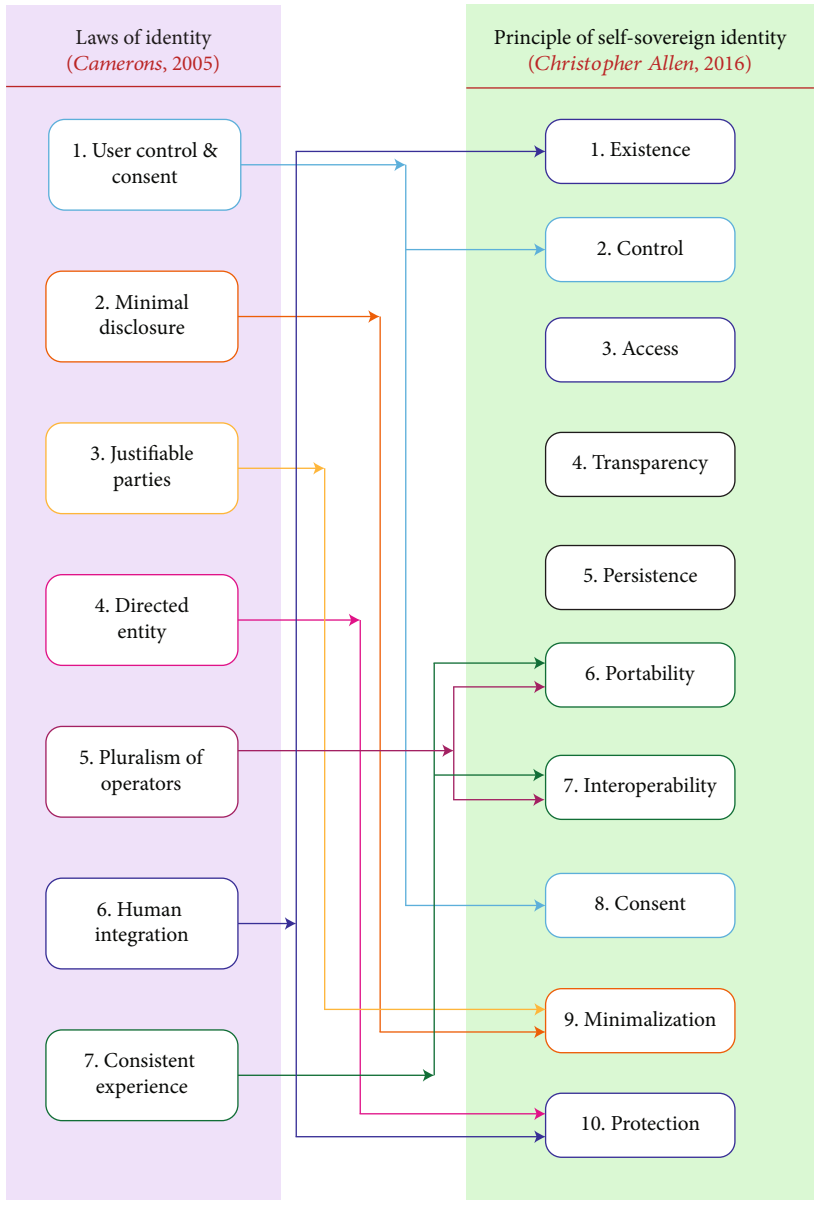

Figure 3: Mapping of principles of identity with the SSI principles.

the actual data. Various blockchain-based SSI solutions will be discussed and compared in this section based on the criteria defined in Section 4.2.2. The comparative analysis of the existing SSI solutions has been given in Table 4.

(1) *Selfkey* [26]. It has been created based on an SSI network where users can store data on personal devices [67]. Selfkey is a digital identity self-sovereign network [68] where user information is stored on a user-operated device, providing user ownership. If a third party needs to access identity data, the user will present information stored in the blockchain. SelfKey ensures that zero-knowledge proof gathers only a minimal amount of data, meeting acceptance and minimization requirements. It uses censorship-resistant and force-resistant algorithms to verify the identity where individuals can ascertain the identity claims of a customer. The portability in Selfkey is achieved using UPort. A significant weakness of Selfkey is a third-party dependency where no specific information about a trusted third party is available. Other inadequacies of Selfkey include lack of human integration and persistent identifier attributes that can last for a particular time [69]

(2) *Shocard* [27]. The ShoCard offers a digital identity authentication platform designed based on the public blockchain. Identity owner authentication is achieved using a centralized database containing cryptographic hashes of digital identity users. The individual is responsible for initiating interaction with third parties to check identity. Data is

Table 4: Different evaluation criteria for comparing SSI solutions.

Ref	Year	Evaluation criteria (self-sovereign identity principle)										
		Control	Consent	Minimization	Protection	Interoperability	Access	Portability	Existence	Persistence	Transparency	Other criteria
[59]	2019	User control and consent, privacy-friendly	Protected ownership		Directed precise identity		Human integration					
[58]	2018	Control	Consent	Minimization	Protection	Interoperability	Access	Portability	Existence	Persistence	Transparency	Provable
[19]	2018	Control	Consent	Minimization	Protection	Interoperability	Access	Portability	Inclusion	Persistence	Transparency	
[63]	2018	Control	Justifiable parties	Minimal disclosure	Directed identity	Pluralism	Human integration	Contexts				
[66]	2019	Control	Justifiable parties	Minimal disclosure	Directed identity	Pluralism	Human integration	Contexts				
[65]	2019	Control	Consent	Minimization	Protection	Interoperability	Access	Portability	Existence	Persistence	Transparency	Provable
[43]	2020	Control	Justifiable parties	Minimal disclosure	Directed identity	Pluralism	Human integration	Contexts				
Our study		User control and consent			Privacy and protection	Interoperability	Human integration	Portability	Inclusion	Persistence	Transparency	

ultimately stored in a protected data envelope that receivers can only decrypt. ShoCard was founded in 2015 and can include five million records within 30 minutes in a verified public blockchain [27, 63]

It enables users and organizations to create identities secure and verified where end-users control personal information access and 3rd party sharing. The third party or ShoCard will not access the data without first sharing useful information. The blockchain network is used to store the identities, but it does not hold the user's identity data. Additionally, ShoCard does not have decentralized login data storage, a target of hacking where the central servers are intermediaries among users and trusted third parties [63]. The partially centralized status of ShoCard creates instability in the existence of ShoCard ID. If ShoCard servers stop running, identity holders will not be able to use their own digital IDs and credentials [70].

Additionally, the cryptographic key management does not support users since ShoCard stores the identities on the public blockchain, which provides open access and transparency. Users will secure the private key in their personal device, where the service provider uses a public key to verify the ShoCard ID. Organizations may use a software development kit to integrate ShoCard technology with its current application or website. ShoCard supports multiple authentication and verification, such as KYC, encryption, traceable authorizing, and credential certification, besides offering an authentication mechanism using a phone app. The method of authentication involves downloading the application to establish its ShoCard ID. It requires a user to take a snapshot of a legitimate government-issued identity through which ShoCard gathers personal information. The user can then validate the details, create a password, or ask for a biometric scan.

(3) *Civic* [24]. Civic is based on a blockchain-based identity authentication ecosystem where a third party wallet creates key pairs, storing identification information in the user's computer. Civic and blockchain only accept data hashes stored on the Ethereum network as ERC20 Tokens. Civics support three independent groups in the network: consumers, validators, and service providers, based on the Ethereum blockchain and uses smart contracts to track the proof of attestation

The Civic identity utilizes the validated identity for websites and mobile development without requiring the username and passwords for multiparty authentication. Users monitor their protected data and must only share information in which they are willing. The Civic app is used to store identity information on a mobile device in an encrypted form. The hash value of attached identity information is stored in the Merkel tree and collected in the blockchain. The Merkle tree sections can be exposed selectively, increasing user control by enabling identity owners to disclose personal details selectively. The Civic allows trustworthy identity authentication providers known as validators to participate and sign transactions in public blockchain nodes. It reconfigures the centralization function and provides an interactive open system for the validator, but it is not entirely decentralized.

Nevertheless, it has the same consensus mechanism as the Sovrin. The authenticator can revoke identity records. For instance, when a user changes their last name, the authenticating agency cancels the blockchain's previous/invalid last name. Therefore, Civic users depend on authentication authorities to establish a protected digital identity, resulting in a lack of portability [71]. Civic is a transparent system that utilizes a permission-less blockchain and does not have software or infrastructure for its network [72].

The benefits of the Civic ecosystem include a strong relationship among financial institutions, public agencies, and utilities as it intends to build a market among banks, utility organizations, local, state or federal governments, etc., verifying individual or business identity attributes in a blockchain. The validators can price identity authentication and sell the identity to stakeholders using smart contracts. The Civic system remains effective, as it plays a vital role in its ecosystem and uses validators to verify identity data accessible through mobile apps. Civic also plans to launch the Civic wallet. By integrating identification with other applications, users can interact more securely and efficiently using standard cryptocurrency applications compared to other wallets. However, the development of this project is at an early stage.

(4) *Sovrin* [27]. The Sovrin foundation started using blockchain to store distributed identities to formalize and create an SSI network. Theoretically, anyone can verify or issue the identity. The Sovrin is used to build identities, using centralized CA to create a trust model network, and using permissioned blockchain and Stewards nodes to achieve consensus. The Sovrin Foundation is a nonprofit organization with a board of twelve trustees, including the governance council

Sovrin allows a user to have complete control over digital identities where the user can choose which information to be shared and with whom. This selective disclosure uses a unique technique, ZKPs. Additionally, Sovrin provides pair-named DIDs [73] and public keys to protect user privacy without compromising functionality. Since the Sovrin network only has central authority, users rely on agencies and stewards where trust and accountability are managed through stewards' confidence, integrity, and noncollusion system. User data is stored in the user's personal computer and cannot be stored in the network service provider's database. Sovrin aims to establish a market for customers to incorporate data portability and restore private key loss using cryptographic accumulators. Semantic graphs, like JSON-LD, are often used to provide portability among providers.

Sovrin protocol uses open-source software licenses built based on the Hyperledger Indy [74]. The Sovrin trust system will regulate the Sovrin network of digital identity, security, policies, and stewards [75]. Sovrin network contains stewards worldwide, including various financial institutions, start-ups,

charities, and authority for personal information. Sovrin foundation requires systems to comply with other digital identity systems where the user's interaction is not clearly defined. Since Sovrin is in the early stage of development, developers and providers entering the identity ecosystem need to extensively discuss user experience [74].

(5) *uPort* [23]. The uPort uses an open ID system that enables customers to enrol their identities securely, sign transactions, send and request identity keys, as well as, accessing keys and data [76]. The identity owner appoints trustees to produce a public key through a controller for key recovery purposes. The controller consensus is achieved by replacing the missing public key when executing a proxy with a newly created key. Built using the Ethereum blockchain, the UPort connects attributes and stores them as a basic JSON structure [77]. The identity owner will obtain the ecosystem's credentials without performing identity proofing when using the uPort framework. Users control UPortID and share personal information with third parties where users' personal data is always available and stored on-chain or off-chain using IPFS. In uPort, the user has more responsibilities and authority over uPort IDs

UPort identifiers can be created without disclosing personal information since the missing inherent connection between the UPort identities contributes to system robustness. The registry user's JSON information is publicly available, which may violate user privacy. Users can claim ownership over uPort IDs without depending on a centralized entity. UPort also contains several centralized components such as transfer messaging service, push notification centre, and program manager attributes which are means for machine control or compliance. UPort allows users to store identity data, credentials, and keys in the self-sovereign wallet while the personal user key is stored on user devices. The key recovery protocol allows users a persistent digital identity in case of mobile loss or theft. The software also supports faster authentication singular-sign-on support for Dapps and other apps besides establishing a Decentralized Identity Foundation for a uniform user experience. Furthermore, The QR code-scanning functionality allows communication with the other party [78]. Nevertheless, users consider UPort's key protocol to recover and preserve personal data complex and lack comprehensibility [77].

(6) *Blockstack* [25]. Blockstack is a decentralized network of computers that handles identity and perhaps even users' data. Blockstack ID is a decentralized user ID that connects decentralized applications (DApps). Blockstack public benefit corporation (PBC) is an open-source organization interested in developing core Blockstack protocols and applications [79]

The application developed on Blockstack provides users control over their own identities and eliminates failure reference points. The user's used data credentials cannot be stored at a centralized server where content sharing is carried out using encryption. However, the collection of profiles can be seen and tracked globally through a blockchain which may leak information and endangers users' privacy. Blockstack business logic and data processing works on a computer rather than on centralized servers hosted by service providers. The decentralized storage current scheme, Gaia [80], ensures that users own and operate private data lockers. Cloud users may use these lockers as additional data storage platforms.

In Blockstack, the key recovery protocol is unavailable; thus, users cannot reset their keys in the event of failure or stolen ID, thereby noncompliance with the persistence principle. Conceptually, Blockstack operates on the top of the Bitcoin network and is an open-source repository offering programming libraries on a variety of platforms. The portable nature of Blockstack allows developers to adapt and integrate other technologies. Blockstack involves a full-stack approach that provides all layers required to build decentralized applications besides allowing customers with a single username to operate across all applications without passwords. Nevertheless, the Blockstack environment is in its initial development stage and only offers desktop versions of the Blockstack browser [81].

(7) *LifeID* [82]. LifeID is an open digital identity platform that allows users to create a personal online identity. Users verify every online real-world transaction where authentication is required without third-party companies or government organizations. LifeID is often used combined with a biometric smartphone and app [83]. Only the user accepts the information request from third parties that need user consent. LifeID uses zero-knowledge proof where data is recorded on the user's computer, and the necessary information is released whenever identity verification is needed. The LifeID Identity is backed up and recovered using three different methods: cold storage backup, trusted relatives or associates, and a reputable organization, combating theft by momentarily disabling or restoring identities

(8) *Evernym* [84]. Evernym was established in 2013 by Jason Law, and Timothy Ruff is a well-known player and aims to facilitate SSI introduction within various industries [84]. Sovrin was explicitly designed for identity, and the company describes itself as the world's first professionally authenticated and verifiable public service provider. The mobile application, Connect Me wallet, enables users to create private, peer-to-peer communication with other people. It also allows users to control digital keys and verifiable credentials of their digital identity

Evernym achieves universal accessibility by using Sovrin to claim that SSI is a global public utility to meet everyone's

Table 5: Comparative study of the Blockchain-based self-sovereign identity solutions.

SSI principles (evaluation criteria)	Blockchain-based self-sovereign identity solutions								
	Sovrin	ShoCard	Selfkey	uPort	Civic	Blockstack	LifeID	Evernym	EverID
Inclusion	✓	✓	✓	✓	✓	✓	✓	✓	✓
User control and consent	✓	✓	x	✓	✓	✓	✓	x	✓
Privacy and protection	✓	x	✓	x	✓	x	x	✓	x
Portability	✓	x	✓	✓	x	✓	✓	✓	✓
Persistence	✓	x	x	✓	x	x	✓	✓	x
Transparency	✓	✓	✓	✓	✓	✓	✓	✓	x
Interoperability	✓	✓	✓	✓	✓	✓	✓	x	✓
Human integration	x	✓	x	✓	✓	x	x	x	✓

identity needs. The firm will handle an identity on behalf of a vulnerable person or anyone else incapable of managing their digital wallet. Evernym can store all personal information on the customer's smartphone while control in an Evernym solution is enabled by biometry, using the default biometrics on a particular device. The Evernym solution provides an easy way to import/import a private key and handle an SSI. An individual may usually import a private key into a digital wallet through a text file or QR code scanning. Using Sovrin, Evernym will have a concept of "guardian," a trusted third party to protect an exposed individual's identity. Evernym uses a hybrid open-source framework that provides access to a permission ledger where guardian organizations must behave according to the criteria set out in the Sovrin Trust Framework. The INF or Sovrin Foundation management and the secure implementation of blockchain may reduce the abuse of digital identity and personal identity information. Evernym observed that the Sovrin network architecture, management, and operation could provide members with the possible portability of their public and private data in compliance with other principles. Evernym connections within the Sovrin network will be connected by comparing a "fairly-pseudonymous identification," or a single DID in each relation. The Evernym system is unable to provide flexibility which results in a lack of interoperability. Also, a small amount of information is available for the user control of the issuer's credential [72].

In Evernym's Connect. Me DApp, user biometrics is necessary to access a given identity and the related details in all situations. Individuals may also be expected to provide biometric information to establish peer-to-peer contact networks with other individuals and organizations in accepting credentials from an issuer to exchange credentials.

(9) *EverID* [85]. EverID is a user-centric-based SSI and transitional solution built on blockchain [85]. The decentralized framework of EverID includes data, documents, and biometrics to store and validate user identities. EverID provides multiple third-party user verification and enables the secure transfer of value between network members [86]. The decentralized architecture provider ownership of personal data, which can be accessed only by the user. The individual's personal details are stored so that the individual controls how with whom and for how long these details are shared (persistence). The EverID system is operated on a number of network supernodes. Such supernodes are the blockchain host

Additionally, it hosts the bridge service to allow data transfer to an API server where SDK-enabled devices perform these transactions, making it portable. EverID differs from other approaches, as the user does not need a device because the digital computer identity (a combination of biometrics, government identification and third-party confirmations) is being saved on the cloud. However, EverID noncompliance with the minimization property as the data is required for a claim to be checked where the user must fully reveal it. For example, if the user is over 18, the user can choose to show his complete birthday or not. EverID is also not open-source; thus, the statements in the whitepapers cannot be provable. Its implementation details are also not available in the public domain, raising concerns about compliance with transparency [65].

Additionally, it hosts the bridge service to allow data transfer to an API server where SDK-enabled devices perform these transactions, making it portable. EverID differs from other approaches, as the user does not need a device because the digital computer identity (a combination of biometrics, government identification and third-party confirmations) is being saved on the cloud. However, EverID noncompliance with the minimization property as the data is required for a claim to be checked where the user must fully reveal it. For example, if the user is over 18, the user can choose to show his complete birthday or not. EverID is also not open-source; thus, the statements in the whitepapers cannot be provable. Its implementation details are also not available in the public domain, raising concerns about compliance with transparency [65].

5. Discussion

Based on the detailed analysis of available SSI solutions that can be used in the land registry environment, Table 5 provides a review of these selected SSI solutions. It shows that

ShoCard is not complying with the principle of privacy, portability, and persistence due to its partial dependence on a centralized server for attribute validation. Selfkey lacks user control and consent, which is a significant weakness, persistence, and human integration. Civic does not comply with portability and persistence due to its reliance on a third party. Evernym does not comply with the principles of user control and interoperability. EverID does not comply with the principles of privacy, persistence, and transparency. LifeID has a significant issue of privacy and security. Blockstack does not comply with privacy, persistence, and human integration principles. Among these available SSI solutions, Sovrin and UPort are the SSI models that comply with maximum SSI principles but noncompliance with human integration and privacy principles, respectively. The above assessment shows that none of the available SSI solutions fully comply with SSI principles.

6. Conclusion

This paper highlights the limitations of existing identity solutions, advantages of SSI, and its application in the blockchain-based land registry system. This paper uses a systemic literature review (SLR) based on three defined research questions highlighting the role of SSI in solving the issue of noncompliance with identity principles, evaluation criteria for evaluating existing SSI solutions, and suggesting the best possible SSI solution in the case of Blockchain-based Land registry system. This SLR has selected 251 papers based on criteria and 65 articles from grey literature and finally used a total of 43 articles for review. A detailed study of SSI principles and evaluation criteria for existing SSI solutions have been defined. Based on the defined evaluation criteria, an extensive review of the existing SSI solutions has been done. This study highlights the strengths, limitations, and functioning of each SSI solution, and it concludes that none of the existing SSI solutions complies with all the SSI principles. Based on the defined evaluation mechanism, Sovrin is the best possible solution among the existing SSI solutions. It complies with most of the SSI principles but lacks the scale of human integration. It is the best possible SSI solution that can be applied in the case of a Blockchain-based land registry system. As the Sovrin lacks a human integration factor that is essential for ease of use and high adaptability, it provides a scope for further improvement and future research.

Data Availability

Data is available on reasonable request.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] J. Dempsey and M. Graglia, *Case study: property rights and stability in Afghanistan*, New America, 2017.

[2] K. Cameron, "The laws of identity," August 2005, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf.

[3] K. Mintah, K. T. Baako, G. Kavaarpuo, and G. K. Otchere, "Skin lands in Ghana and application of blockchain technology for acquisition and title registration," *Journal of Property, Planning and Environmental Law*, vol. 12, no. 2, pp. 147–169, 2020.

[4] B. Bundesverband, *Blockchain Opportunities and Challenges of a New Digital Infrastructure for Germany*, Blockchain Bundesverband, Berlin,Germany, 2017, https://jolocom.io/wp-content/uploads/2018/07/Blockchain-Opportunities-and-challenges-of-a-new-digital-infrastructure-for-Germany-_-Blockchain-Bundesverband-2018.pdf.

[5] M. Kaczorowska, "Blockchain-based land registration: possibilities and challenges," *Masaryk University Journal of Law and Technology*, vol. 13, no. 2, pp. 339–360, 2019.

[6] N. Mehdi, "Blockchain: an emerging opportunity for surveyors?," 2020, https://www.rics.org/globalassets/blockchain_insight-paper.pdf.

[7] G. Sylvester, *E-Agriculture in action: blockchain for agriculture opportunities and challanges*, Food and agriculture organization of the united nations and the international telecommunication union, Bangkok, 2018th edition, 2019.

[8] J. Torres, M. Nogueira, and G. Pujolle, "A survey on identity management for the future network," *IEEE Communication Surveys and Tutorials*, vol. 15, no. 2, pp. 787–802, 2013.

[9] H. Ning, X. Liu, X. Ye, J. He, W. Zhang, and M. Daneshmand, "Edge computing-based ID and nID combined identification and resolution scheme in IoT," *IEEE Internet of Things Journal*, vol. 6, no. 4, pp. 6811–6821, 2019.

[10] M. Laurent, J. Denouël, C. Levallois-Barth, and P. Waelbroeck, "Digital identity," *Digital Identity Management*, pp. 1–45, 2015.

[11] M. A. Bouras, Q. Lu, F. Zhang, Y. Wan, T. Zhang, and H. Ning, "Distributed ledger technology for eHealth identity privacy: state of the art and future perspective," *Sensors*, vol. 20, no. 2, p. 483, 2020.

[12] M. Schaffner, *Analysis and Evaluation of Blockchain-Based Self-Sovereign Identity Systems*, Technical University of Munich, Munich, Germany, 2020.

[13] I. T. Javed, F. Alharbi, B. Bellaj, T. Margaria, N. Crespi, and K. N. Qureshi, "Health-ID: a blockchain-based decentralized identity management for remote healthcare," *Health*, vol. 9, no. 6, p. 712, 2021.

[14] A. S. Podda and L. Pompianu, "An overview of blockchain-based systems and smart contracts for digital coupons," in *ICSEW'20: Proceedings of the IEEE/ACM 42nd International Conference on Software Engineering Workshops*, pp. 770–778, Jun 2020.

[15] D. Pavithran, J. N. Al-Karaki, and K. Shaalan, "Edge-based blockchain architecture for event-driven IoT using hierarchical identity based encryption," *Information Processing and Management*, vol. 58, no. 3, p. 102528, 2021.

[16] Y. Panfil and C. Mellon, *The credential highway: how self-sovereign identity unlocks property rights for the bottom billion*, New America Weekly, 2019.

[17] K. Panetta, *5 trends drive the gartner hype cycle for emerging technologies, 2020*, Gartner, 2020, https://www.gartner.com/smarterwithgartner/5-trends-drive-the-gartner-hype-cycle-for-emerging-technologies-2020/.

[18] M. Van Wingerde, *Blockchain-Enabled Self-Sovereign Identity*, Tilburg University, Tilburg, Netherland, 2017.

[19] M. Graglia, C. Mellon, and T. Robustelli, "The nail finds a hammer self-sovereign identity, design principles, and property rights in the developing world," New America Weekly, 2018.

[20] serkan senturk, *Future of property rights: self-sovereign identity and property rights*, New America Weekly,, America, 2019.

[21] Q. Shang and A. Price, "A blockchain-based land titling project for the Republic of Georgia," *Innovations*, vol. 12, no. 3/4, pp. 72–78, 2019.

[22] Sovrin Foundation, *Sovrin™: A Protocol and Token for Self-Sovereign Identity and Decentralized Trust*, Sovrin Foundation, 2018.

[23] C. Lundkvist, R. Heck, J. Torstensson, and Z. Mitton, *Uport: A Platform for Self-Sovereign Identity*, ConsenSys, 2016.

[24] Civic Technologies Inc, "Civic whitepaper," 2017, https://tokensale.civic.com/CivicTokenSaleWhitePaper.pdf..

[25] M. Ali, R. Shea, J. Nelson, and M. J. Freedman, "Blockstack: a new internet for decentralized applications," 2017, http://blockstack.org.

[26] Self Key Foundation, "Self-sovereign identity for more freedom and privacy-self key," 2017, https://selfkey.org/.

[27] S. Card, "Sho Card," 2020, https://shocard.com/wp-content/uploads/2019/02/ShoCard-Whitepaper-2019.pdf.

[28] A. Nagy, K. A. Nyante, A. Peter, and Z. Hattyasy, Eds., *Secure Identity Management on the Blockchain*, University of Twente, 2018.

[29] A. Tobin and D. Reed, *The inevitable rise of self-sovereign identity A white paper from the Sovrin Foundation*, Sovrin Foundation, 2017, https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

[30] M. M. S. M. M. S. M. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103059–103079, 2019.

[31] P. de Marneffe, "Vice laws and self-sovereignty," *Criminal Law and Philosophy*, vol. 7, no. 1, pp. 29–41, 2013.

[32] M. H. Weik, *Computer Science and Communications Dictionary*, Springer US, Boston, MA, 2001.

[33] C. S. Wright, "Bitcoin: a peer-to-peer electronic cash system," *SSRN Electronic Journal*, 2008.

[34] C. Allen, *The path to self-sovereign identity*, Coin Desk, 2016, http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html.

[35] M. Marlinspike, *What Is 'Sovereign Source Authority'?*, Moxy Tougue, 2019, https://www.moxytongue.com/2012/02/what-is-sovereign-source-authority.html.

[36] A. Abraham, *Whitepaper: self-sovereign identity*, Graz, Austria, 2017http://www.egiz.gv.at.

[37] Q. Stokkink, D. Epema, and J. Pouwelse, "A truly self-sovereign identity system," 2020, http://arxiv.org/abs/2007.00415.

[38] F. P. Hjalmarsson, G. K. Hreioarsson, M. Hamdaqa, and G. Hjalmtysson, "Blockchain-based E-voting system," in *2018 IEEE 11th International Conference on Cloud Computing (CLOUD)*, pp. 983–986, San Francisco, CA, USA.

[39] M. Shuaib, S. M. Daud, S. Alam, and W. Z. Khan, "Blockchain-based framework for secure and reliable land registry system," *TELKOMNIKA Telecommunication, Computing, Electronics and Control*, vol. 18, no. 5, p. 2560, 2020.

[40] M. Shuaib, S. Alam, and S. M. Daud, *Improving the Authenticity of Real Estate Land Transaction Data Using Blockchain-Based Security Scheme*, Springer, Singapore, 2021.

[41] R. Joosten, *Self-sovereign identity framework and blockchain*, ERCIM NEWS, 2017, https://ercim-news.ercim.eu/en110/special/self-sovereign-identity-framework-and-blockchain.

[42] Medici, "22 companies leveraging blockchain for identity management and authentication," *MEDICI*, vol. 13, no. 21, pp. 2–5, 2017.

[43] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, "Blockchain-based identity management systems: a review," *Journal of Network and Computer Applications*, vol. 166, p. 102731, 2020.

[44] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *SAC '20: Proceedings of the 35th Annual ACM Symposium on Applied Computing*, pp. 342–345, Brno, Czech Republic, Mar 2020.

[45] R. Saia, S. Carta, D. Recupero, and G. Fenu, "Internet of entities (IoE): a Blockchain-based distributed paradigm for data exchange between wireless-based devices," *Proceedings of the 8th International Conference on Sensor Networks*, pp. , 201977–84, 2019.

[46] S. T. Siddiqui, R. Ahmad, M. Shuaib, and S. Alam, "Blockchain security threats, attacks and countermeasures," *Adv. Intell. Syst. Comput.*, vol. 1097, pp. 51–62, 2020.

[47] R. Jesse McWaters, "A blueprint for digital identity. The role of financial institutions in building digital identity," 2016, http://www3.weforum.org/docs/WEF_A_Blueprint_for_Digital_Identity.pdf.

[48] D. Sikeridis, A. Bidram, M. Devetsikiotis, and M. J. Reno, "A blockchain-based mechanism for secure data exchange in smart grid protection systems," in *2020 IEEE 17th Annual Consumer Communications & Networking Conference (CCNC)*, pp. 1–6, Las Vegas, NV, USA, Jan 2020.

[49] T. Mitani and A. Otsuka, "Traceability in permissioned blockchain," *IEEE Access*, vol. 8, pp. 21573–21588, 2020.

[50] M. Shuaib, S. Alam, M. Shahnawaz Nasir, and M. Shabbir Alam, "Immunity credentials using self-sovereign identity for combating COVID-19 pandemic," *Materials Today : Proceedings*, 2021.

[51] A. Piore, "Can blockchain finally give us the digital privacy we deserve?," 2019. https://www.newsweek.com/2019/03/08/can-blockchain-finally-give-us-digital-privacy-we-deserve-1340689.html.

[52] J. A. Ketterer and G. Andrade, "Blockchain asset registries: approaching enlightenment?- Coin Desk," Dec 2017, https://www.coindesk.com/blockchain-asset-registries-entering-slope-enlightenment.

[53] International Finance Corporation, *Secured Transactions Systems and Collateral Registries*, World Bank, 2010.

[54] M. Hendow, "Bridging refugee protection and development," 2019, https://www.researchgate.net/publication/331530630_Bridging_refugee_protection_and_development_Policy_Recommendations_for_Applying_a_Development-Displacement_Nexus_Approach.

[55] B. Kitchenham and S. Charters, *Guidelines for performing systematic literature reviews in software engineering*, EBSE, Durham, UK, 2007, https://www.elsevier.com/__data/promis_misc/525444systematicreviewsguide.pdf.

[56] McKinsey, *Infographic: what is good digital ID?*, McKinsey & Company, 2019, https://www.mckinsey.com/business-functions/mckinsey-digital/our-insights/infographic-what-is-good-digital-id.

[57] W3C Credentials Community Group, "Verifiable claims task force," May 2017, https://w3c.github.io/vctf/.

[58] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *2018 IEEE international conference on internet of things (iThings) and IEEE green computing and communications (green com) and IEEE cyber, physical and social computing (CPSCom) and IEEE smart data (smart data),*, pp. 1336–1342, Halifax, NS, Canada, 2018.

[59] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, and K. Dahal, "DNS-IdM: a blockchain identity management system to secure personal data sharing in a network," *Applied Sciences*, vol. 9, no. 15, p. 2953, 2019.

[60] M. Shuaib, N. Hafizah Hassan, S. Usman et al., "Identity model for blockchain-based land registry system: a comparison," *Wireless Communications and Mobile Computing*, vol. 2022, Article ID 5670714, 17 pages, 2022.

[61] M. Shuaib, S. Alam, M. Shabbir Alam, and M. Shahnawaz Nasir, "Self-sovereign identity for healthcare using blockchain," *Materials Today: Proceedings*, 2021.

[62] K. Cameron, *The Laws of Identity*, 2005.

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

[64] A. E. Panait, R. F. Olimid, and A. Stefanescu, "Identity management on blockchain – privacy and security aspects," (2020), https://arxiv.org/abs/2004.13107.

[65] D. van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, "Self-sovereign identity solutions: the necessity of blockchain technology," (2019), https://arxiv.org/abs/1904.12816.

[66] S. El Haddouti and M. D. Ech-Cherif El Kettani, "Analysis of identity management systems using blockchain technology," in *2019 International Conference on Advanced Communication Technologies and Networking (Comm Net)*, pp. 1–7, Rabat, Morocco, Apr 2019.

[67] The Self Key Foundation, *Self Key*, Self key, 2017, https://selfkey.org/.

[68] S Foundation and Self Key Foundation, "Self key-the self key foundation," (2017), https://selfkey.org/wp-content/uploads/2019/03/selfkey-whitepaper-en.pdf.

[69] T. Koens and S. Meijer, "Matching identity management solutions to self-sovereign identity principles.pdf," vol. 2, p. 32, 2018.

[70] A.-E. Panait, R. F. Olimid, and A. Stefanescu, "Identity management on the blockchain," in *Proceedings of the Romanian Academy Series A-Mathematics Physics Technical Sciences Information Science*, pp. 45–52, 2020.

[71] M. Kuperberg, "Blockchain-based identity management: a survey from the enterprise and ecosystem perspective," *IEEE Transactions on Engineering Management*, vol. 67, no. 4, pp. 1008–1027, 2020.

[72] A. G. Nabi, *Comparative Study on Identity Management Methods Using Blockchain*, University of Zurich, 2017.

[73] D. Reed, M. Sporny, D. Longley, C. Allen, R. Grant, and M. Sabadello, "Decentralized identifiers (DIDs): data model and syntaxes for decentralized identifiers," (2019), https://w3c-ccg.github.io/did-spec/.

[74] Hyperledger Contributors, *Hyperledger Indy documentation*, Hyperledger, 2018, https://www.hyperledger.org/use/hyperledger-indy.

[75] M. Ali, R. Shea, and M. J. Freedman, *Blockstack: a new decentralized internet*, Whitepaper, 2017, http://blockstack.org.

[76] uport, *uPort*, 2019.

[77] C. Lundkvist, R. Heck, J. Torstensson, Z. Mitton, and M. Sena, *Uport: A Platform for Self-Sovereign Identity*, Sovrin Foundation, 2016.

[78] N. Nizamuddin, H. R. Hasan, and K. Salah, "IPFS-blockchain-based authenticity of online publications," in *Lecture Notes in Computer Science (including subseries Lecture Notes in Artificial Intelligence and Lecture Notes in Bioinformatics)*, vol. 10974 LNCS, pp. 199–212, 2018.

[79] O. Labazova, T. Dehling, and A. Sunyaev, "From hype to reality: a taxonomy of blockchain applications," *Proceedings of the 52nd Hawaii International Conference on System Sciences*, 2019, pp. 4555–4564, Grand Wailea, Maui, 2019.

[80] vercel, *A Decentralized Storage Architecture*, Stacks docs, 2018, https://docs.blockstack.org/storage/overview.html.

[81] M. Ali, J. Nelson, R. Shea, B. Labs, and M. J. Freedman, "Blockstack: a global naming and storage system secured by blockchains," in *usenix Annual technical conference*pp. 181–194, Denver, Colorado, 2016.

[82] I. D. Life, "Digital identity simple & secure," (2018), https://lifeid.io/.

[83] L Foundation, "Life ID-an open-source, blockchain-based platform for self-sovereign identity," p. 34, 2019.

[84] M. Nijjar, "Evernym," (2019), https://www.evernym.com/.

[85] B. Reid, B. Witteman, and W. Brad, "Ever ID whitepaper," May 2018, https://neironix.io/documents/whitepaper/6176/EverID_Whitepaper_v1.0.2_July2018.pdf.

[86] A. Aloraini and M. Hammoudeh, "A survey on data confidentiality and privacy in cloud computing," in *Proceedings of the International Conference on Future Networks and Distributed Systems*, pp. 1–7, Cambridge United Kingdom, Jul. 17.