Hindawi
Wireless Communications and Mobile Computing
Volume 2022, Article ID 5670714, 17 pages
https://doi.org/10.1155/2022/5670714

Review Article

Identity Model 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] Deepika Koundal,[4] Arwa Mashat,[5] and Assaye Belay[6]

[1]*Razak Faculty of Technology and Informatics (RFTI), Universiti Teknologi Malaysia (UTM), Kuala Lumpur, Malaysia*
[2]*College of Computer Science & IT, Jazan University, Jazan, Saudi Arabia*
[3]*King Faisal University, Department of Information Systems, College of Computer Sciences and Information Technology, Al Hofuf, Saudi Arabia*
[4]*University of Petroleum & Energy Studies, Department of Systemics, Dehradun, India*
[5]*King Abdulaziz University, Faculty of Computing and Information Technology, Jeddah, Saudi Arabia*
[6]*Mizan-Tepi University, Department of Statistics, Tepi, Ethiopia*

Correspondence should be addressed to Assaye Belay; abstat23@gmail.com

Received 6 January 2022; Accepted 27 January 2022; Published 15 February 2022

Academic Editor: Deepak Kumar Jain

The land registry system is one of the essential components of any governance model required to ascertain the ownership records uniquely. This paper reviews the existing literature and provides a detailed literature review consisting of 3 stages based on three research questions (RQ) that highlight the step by step evaluation and analysis. We selected 48 primary articles out of 477 extracted from different scientific databases based on criteria and RQ defined in the research method section. The majority of these papers focus on assessing the identity issues related to the land registry system and reviewing the existing identity models to find the best possible identity model to resolve the identified identity problems in the land registry. This paper examines the current land registry model and its shortcomings. It explains the various blockchain types and their characteristics. It further evaluates the usability of blockchain technology in different aspects of the land registry. Identity management is one of such weaknesses in the blockchain-based land registry model that has been assessed in detail. Identity issues of blockchain-based models have been further evaluated on defined criteria. The paper ends with a discussion on possible identity models and their comparative analysis to ascertain the most suitable identity model to resolve the identity issues of land registry systems.

1. Introduction

The land registry system is a process of transferring land ownership that protects stakeholders' rights, increasing trust and confidence among the people. Due to poor coordination between various departments, the verification of land title requires a physical visit, *m* making it time-consuming and often encouraging bribery [1]. About 70% of the world's population does not have access to the formal land registration system, where bribery is a common occurrence; around $700 million is said to be given as bribe in the land registry office in India [2]. Furthermore, per the World Bank study from 2007, two-thirds of court cases in the country are pertinent to land disputes related to property title [3]. The paper-based land registry system poses several issues such as high time complexity, centralised control, physical visit to property site for verification, high transaction cost, vulnerability to human errors, corruption, fraud, lack of transparency, third-party involvement, reduced reliability, lack of effectiveness, and ownership issue [4] Blockchain technology I a popular case of distributed ledger technology (DLT) that emerged as a ground-breaking technology, especially in the case of transaction and record management. It supports several attributes like immutability, security, integrity, authentication, and traceability, which is very much essential for every land registry system. Several scholars working on the land registry system suggested that the use of blockchain technology in land registration enhances security and transparency, thus improving the efficiency of the existing land registration system [5]. Also, it will reduce the cost and time for the land transaction without involving a third party. The benefits of using blockchain in the land registry system can be summarised as increased transparency, increased trust, increased predictive capability, reliability, increased control, cost reduction, reduced energy consumption, security, ease of access, privacy, reducing corruption, and error reduction [6–15].

However, the use of blockchain in land registry systems has some limitations concerning the identity that needs attention while designing a blockchain-based land registry system. These concerns are compliance with identity principles [16–21], need for identity solution [22–24], legal validity [23,25,26], user control [27–29], and independent verification [18,20,23,27,30]. To achieve efficient implementation of blockchain technology in the land-registry system and to counter the limitations, it is necessary to address these issues. Numerous studies have confirmed that a digital identity is essential to carry out a reliable property transaction and verification. ID verification for transactional parties is also crucial in preventing cyber frauds and crimes, as stated in Money laundering directive 2018/843 [31]. Currently, the land registry system does not have a specified digital identity solution that authorises users to control their personal information and data. Various researches and reports emphasised the need for such a digital identity solution to provide users with control and ownership over this identity [21,26,30]. Moreover, using digital identity in the land registry system will reduce the time involved, the risk of fraud, and prevent information loss [32]. The issue with the current use of blockchain for identity management is related to compliance with the "principles of identity" [18].

The digital identity model is categorised into four different levels by Christopher Allen in the year 2016, namely, as centralised identity, federated identity, user-centric identity, self-sovereign identity (SSI) model [33,34]. Any identity model must assure that users' personal information is being safely protected from data breaches and unauthorised dissemination [35]. This paper reviews the different identity models and tries to identify the best possible model for identity, specifically for the use case of land registry applications. This paper examines these aspects based on three research questions (RQs) and validates the proposed solutions. All other identity models are controlled by identity providers and not by the users themselves except SSI. The self-sovereign identity model satisfies the identity principles allowing users to control and manage their personal data independently and enable minimal disclosure of personal information [33,36].

This article contains five sections. Section 2 explains the background information like the land registry system basics, including types and limitations, blockchain technology, characteristics of blockchain, and digital identity. Section 3 describes the research method, research questions, data sources, and extraction mechanism. It is followed by Section 4, which explains and discusses the outcomes of the review extracted from literature based on research questions. Finally, Section 5 concludes the paper based on the findings.

2. Background

This section provides a brief description of the domain and technologies used in the study.

2.1. Land Registry System. Land registry is a method by which a government agency registers and records land ownership and rights. These records validate land title, facilitate land transactions, and avoid corruption. The existing land registry models have slowed down valid land transactions and ownership verification. In some of the worst situations, land misrepresentation may be allowed [37]. Land registry is a system in which government bodies document the property rights and changes in land ownership in compliance with the existing laws and regulations to safeguard landowners' rights and make land management easier [38–40]. The land is characterised by immovability, scarcity, and high value. Land is the most significant and essential matter of property. Land registration refers to the registration of land and all properties on the ground [41].

Currently, land registration methods are generally established in western countries. It is usually classified into three types: contract registration, right registration, and Torrens registration. Zhang Wei compares and relates land registry systems in France, Germany, the United Kingdom, and Australia [42]. The authors in Refs. [43,44] explicitly mentioned three types of Torrens registration, rights registration, and contract registration modes. In Ref. [45], a comparative study of Japan and Hong Kong land registry systems has been done, and suggestions are given. In Ref. [46], the authors emphasise the development process, problems, and suitable recommendations for the Chinese land registry system. The Comparative analysis of the land registry bodies in Canada, Korea, Taiwan, and the USA has been done in Ref. [47].

2.2. Types of Land Registry System. Commonly, there are two types of land registry systems: (1) title registry system, which records land ownership, and (2) deed registry system, where only deeds are registered, and ownership must be presumed.

(i) Deeds Registry System: a deed is a record of a particular land transaction that proves a specific agreement. The deed is registered in the deed registration system. Nevertheless, the deed does not serve as evidence for legal rights between the involved parties in the land transaction [48,49].

(ii) Title Registration System: it registers and records land ownership, land rights, and title, thereby establishing legal rights and consequences. Using a title registration system, people can see the legal owner and point to the land's actual coordinates. The registered information is the ultimate authority for validating claims and transactions [48,49].

2.3. Limitation of Land Registry System. The government faces difficulties in maintaining land records and providing up-to-date data. The various departments keep and update land records at the district and village levels. Also, poor coordination between departments leads to nonsynchronised information, leading to inconsistency and mismatch. The limitations of the current land registry are discussed below.

(i) High time complexity: in a traditional property registry, the process to deal with property involves different logical phases, such as housing evaluation, document compilation, document execution, execution of the main contract, money transfer and registration, making the whole process more complicated and costly [10].

(ii) Centralised control: land registry authorities' central structure encourages corruption and fraud. Every land registry department functions independently, making a record-update in one department outdated for another department [11].

(iii) Physical property site visit and verification: a buyer checks the physical location, coordinates, and the previous property loan. This entire process is performed manually, making the process more complicated and vulnerable to fraud and information loss [30,50,51].

(iv) More transaction cost: the transaction cost in the real estate market is due to information irregularities of knowledge concerning the hidden cost of property objects [10,52], and regulations [53].

(v) Lack of efficiencies: the land registry system has irregularities such as incomplete records, difficulty in navigation, and challenges to locate [6,54]. These irregularities result in a lack of transparency in the land registry system [8].

(vi) Less secure: the centralised architecture of the land registry raises issues of attack and corruption. It contains unreliable, vulnerable, and vital documents resulting in difficulty to control the system [10,51]. The authenticity of the land registry is a serious concern because records are not appropriately synchronised [14].

(vii) Lack of transparency: the current land registration process lacks transparency for transactions, such as leasing, purchasing, and selling, and does not achieve data security and authenticity [14].

(viii) Ownership issue: there is no structured regulatory system for land registries between the multiple departments. The land record is maintained at the level of districts or villages and needs synchronisation. There are various discrepancies between documents and actual reality. Also, many users claim ownership for the same piece of land [4,55,56].

(ix) Third-party involvement: during the traditional land registry process, many individuals, such as brokers, land inspectors, lawyers, notaries, and authorities, participate in the process, resulting in high costs, complexity, and delay [50,55].

3. Blockchain

Blockchain is an innovative technology for storing records, contracts, and transactions [57]. The blockchain is an example of DLT, initially established for Bitcoin cryptocurrency. It is an immutable ledger that groups and stores a set of records in a block. Each block is generated using cryptographic hash functions and connected in the form of a chain.

Blockchain is a decentralised ledger spread through a network of connecting nodes, which records all transactions among peers operating on the same protocol. Blockchain records transactions without a trusted third party. It is a way of monitoring transaction information, contracts, and anything independently registered and verified. It guarantees there is only one owner and no replication of the same object or component [21,58].

3.1. Types of Blockchain. Researchers have classified blockchain into three types, namely, public, private, and hybrid (federated) blockchain [59–61].

(i) Public blockchain: it enables anyone to create, modify, and validate the block by recording and updating data using transactions between entities involved [62]. It allows every node to participate in the consensus process [63]. Therefore, every block has equal authority in creating a new node if they have the same set of resources.

(ii) Private blockchain: it allows only authorised participants in the network to make, modify, and create transactions inside the ledger [64]. It means that only a small group of nodes can be allowed in the consensus process, and a few can only generate the new block. This type of blockchain can be used in financial institutions and other organisations where general users can participate in some sort of consensus with limited authorised persons.

(iii) Hybrid (federated) blockchain: it is a hybrid of public and private blockchain models that balances all features. Each node can participate in the consensus process, and only a few can create a new node. If the current land registry system uses a hybrid blockchain, then all registrars, notaries, and other parties will be involved in submitting official land registry documents.

3.2. Characteristics of Blockchain. The blockchain concept contains the following characteristics.

(i) Shared database: one source and one backup database are commonly used in the land registry system. The blockchain is a decentralised ledger that is shared across multiple databases.

(ii) Several writers: each transaction is stored in a blockchain inside each copy of the database. The land registry system records the land transaction and updates into one system; this copy is recorded into the backup system.

(iii) Disintermediation: anyone can keep a copy of the database and make a transaction on it. In the current land registry systems, reliable third parties also update a registration.

(iv) Timestamping: in the blockchain, record or transaction creation and the modification time are securely controlled. Nobody, not even the document's owner, can change the document after it is registered, ensuring the credibility of the timestamping facility.

(v) Transaction validity: blockchain can check whether the transaction is valid to prevent unauthorised transactions. The trusted third party checks transaction validity in conventional land registry systems.

(vi) Validation: blockchain records any sequence of authenticated transactions. It is a public ledger that is unalterable. All transactions are part of a ledger in current land registry systems and can be validated through an audit trail.

(vii) Scalability: blockchain can be extended easily. Anyone who wants to upload a transaction can do it.

4. Digital Identity

Digital identity is a substitute for the present notion of a user's true identity [65]. It contains digital information that identifies the person's uniqueness and provides the same level of trust as provided in a face-to-face transaction, producing a particular attribute that is deposited in databases that differentiate users in a similar system [66].

4.1. Digital Identity Lifecycle.

4.1. Digital Identity Lifecycle. The usage and prerequisite process of digital identity is a series of cyclic events which can be elaborated in the lifecycle model, as presented in Figure 1.

(i) Registration: the initial stage of the digital identity lifecycle is partitioned into claiming and verification. (1) In the first step, the identity attribute is inserted on the identity provider's web or mobile application to give the identity to the owner. (2) Based on the selected security level by the user, a suitable authentication method can be established by a user. (3) The finalised application is provided to the service provider.

(ii) Verification: in the verification stage, (4) the identity owner confirms the verification of his or her identity data provided by the identity provider. (5) The identity provider verifies the identity based on the presented data. An official government ID is required for verification.

(iii) Issuance: after the successful identity verification, (6) the identity provider processes the application of identity owner and (7) assigns the identity credential employing the digital identity.

(iv) Authentication: to use online services, such as accessing a web portal for making flight reservations, the identity owner uses a digital identity. (9) The trusted third party may request to verify the identity owner. (10) The identity owner chooses the identity provider and provides one of the identity credentials to verify their identity (12) and gives consent to the trusted third party to access identity attributes on a timely basis. (13) After providing consent, the trusted third party receives the data to authenticate the owner identity.

(v) Authorisation and service delivery: in step (14), the trusted third party reviews the rights linked with the owner's digital identity. If the review result is positive, the transaction is authorised. (15) Then, the service requested by the identity owner is provided.

5. Research Method

The Kitchenham Guidelines [4] have been adopted to make a straightforward, repeatable, systematic literature review to select the most appropriate identity model for blockchain-based land registries. The organisational plans are developed to recognise the need for review and to formulate a review plan. Furthermore, the review results are published by identifying the research, selecting the samples, assessing the performance, and extracting and synthesising the data. The research method used in this research study contains the research questions and data sources. The search terms used for retrieving papers is given in Table 1, and the exclusion and inclusion criteria for searching relevant articles is defined in Table 2.

5.1. Research Questions. The first stage of systematic literature review (SLR) is to identify research questions (RQs) that allow for a broad overview [67]. The main aim of this study is to answer the following research questions:

RQ: how to select the most appropriate identity model for the blockchain-based land registry?

To answer the main research question, we have defined three guiding questions:

RQ1: what are the identity issues in the blockchain-based land registry?

RQ2: how to comply with digital identity principles?

RQ3: which method can be used to compare the most appropriate identity model?

To address the above guiding questions, we used the guidelines given by Kitchenham et al. for a systematic review [67] and the standard procedure for selecting the literature for research.

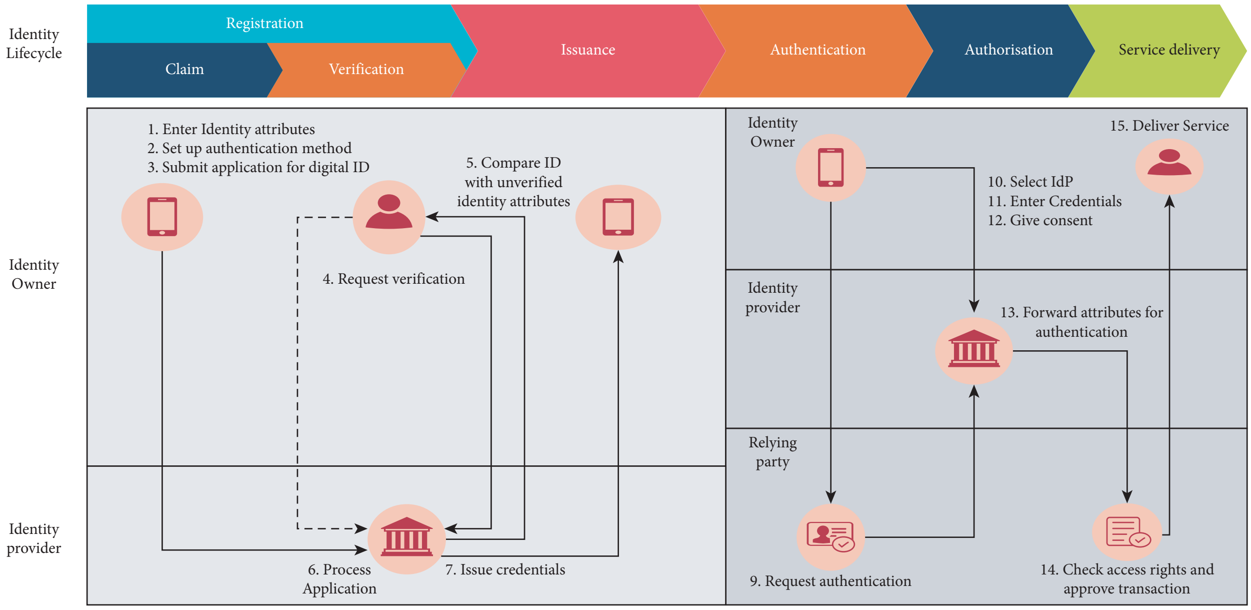

Figure 1: Digital identity lifecycle.

Table 1: 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"	8	9	5	8	2
"Identity management" AND "law of identity", "identity principle"	6	21	8	24	11
Total with duplicates	**41**	**135**	**99**	**145**	**60**

Table 2: Inclusion/exclusion criteria.

Selection criteria	Details
Exclusion	(i) Non-English journal (ii) Duplication (iii) Paper not related to the scope of our study (iv) Papers that were older versions of studies that were already considered
Inclusion	(i) Papers with research scope of blockchain technology in land registry and sub-scope identity model and identity principles (ii) Published between 2008 and 2022

5.2. Data Sources. Our study performs the search manually through five databases: Scopus, IEEE Xplore, ACM Digital Library, Science Direct, and Web of science. Grey's literature is also included, for example, the related government project reports, working papers, and appraisal documents. Blockchain implementation in the land register is a new field of study. The inclusion of grey literature extends both state of the art and the latest research sources in the area by utilising more comprehensive research sources.

5.3. Primary Study Search terms and Search Strings. The next step was to search for all related papers. A final search was carried out on January 19, 2022, covering publications from 2008 to 2022. The search consists of journals, workshops and conferences proceedings, government project reports, working papers, review documents, and book sections. The searched terms are "blockchain," "land registry," "Identity model," "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 utilised only the real estate and blockchain keywords.

In addition, 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 1 shows the search string and the results from scholarly databases.

5.4. Search for Relevant Papers. Not all the reported published papers match our study's scope, so the next step was to determine the actual relevance of the publications received against the specified search terms and search strings from research databases. It is accomplished by setting the inclusion and exclusion criteria shown in Table 2. These criteria have been used for all titles, abstracts, and keywords of previously acquired publications to identify documents to match with our research questions.

5.5. Searching Process and Finer Selection. In some instances, titles and abstracts were inadequate to better match the research questions with the chosen articles. The full paper reading is done to ensure the inclusion and exclusion criteria compactness. A total of 480 papers were found in the initial keyword searches from the selected scholarly databases (for conformity, grey literature has been excluded from the descriptive analysis). It was reduced to 458 after removing duplication by inserting it into the Mendeley software. After analysing the article under the inclusion/exclusion criteria, 73 articles were left for reading. Then, 73 papers were read in full and reapplied with the inclusion and exclusion criteria. Then, 37 papers were left. In addition, the 14 reports are selected from the grey literature search, which results in the final number of papers for this study as 51. Figure 2 shows the procedure followed for the selection process.

6. Results and Discussion

The descriptions and results of the research issues are listed in Table 3. This section is further divided into three subsections (A, B, C). Section A presents the identity challenges in the blockchain-based land registry system. Section B describes how the identity model complies with identity principles. Section C shows the different methods of comparison and analysis to select the appropriate identity model for the blockchain-based land registry system.

7. RQ1. What Are the Identity Issues Associated with Blockchain-Based Land Registry Systems?

Many blockchain-based land registry systems have been implemented to counter the limitations of the existing land registry systems. In this section, various blockchain implementations in the field of the land registry were reviewed. A brief discussion of the identity issues associated with the blockchain implementation land registry is discussed below:

7.1. Need for an Identity Solution. ID verification for transactional parties is also crucial in preventing crime, as stated in article 22 Money laundering directive 2018/843 [31]. Currently, the land registry system does not have a digital identity solution that authorises users to control their personal information and data. A blockchain-based framework was proposed to minimise the issues in the current system [22]. The blockchain is a new technology, and using it for e-ID needs to satisfy the existing laws and ID principles to protect user privacy. In an analysis to find implementation challenges concerning the current authorised framework, the author stressed the need for creating a digital identity solution to prevent criminal activity where it should comply with the regulation in providing mandatory control in obtaining the identity [23]. The blockchain is deemed as a tool to reduce land disputes in the Cyprus land registration system. However, the implementation of blockchain technology faces an issue in providing digital identity to users [24]. In Ref. [70], the author discusses several use cases of blockchain technology in countries such as Ghana, Georgia, and Sweden, highlighting the importance of a digital identity solution to use the blockchain-based land registry system in these countries. The blockchain is a new technology; it may appear that more people are involved and that things are more transparent, but it may also lead to greater inclusion and the permanent removal of plural ownership, use rights, and centralised land management in cases where statute law does not adequately represent the majority of land users.

7.2. Independent Verification. Independent identity verification is essential to validate and verify its association with a genuine user. In Ref. [18], the issue is related to the need for independent verification and the necessity to disclose network participants' identity. Also, the lengthy process of providing digital identity will lead to forged digital identity from false, incorrect, and stolen documents [23]. In addition, the issue of the unknown identity of the user and transaction data to be revealed in a permissionless blockchain is also a challenge [20]. In the Turkish blockchain land registry system, there is also the issue of ID verification and the land record data placement in the blockchain system [27]. As the process of verification of property and identity is tedious, the use of digital identity protects the user's personal data and reduces the time, fraud, and loss of information [30].

7.3. Compliance with Identity Principles. The legal and regulatory concerns are computed using, How to protect the data collected by the digital identity system? How to protect the privacy of personal information data? How to draft new rules to prevent a user from obtaining services that increase the cost of getting the certificates?

The blockchain technology application in the land registry would increase efficiency and provide greater security. A SWOT analysis of using blockchain technology in record-keeping found that it may violate the laws for personal data protection. Blockchain technology needs to meet the data protection and privacy required to execute personally identifiable information (PII) [16]. A new digital identity solution in compliance with identity principles or e-IDAS regulation contributes significantly and improves the area [17]. In the analysis for the use of blockchain in land registry systems in Georgia and Sweden, the study pointed out the various issues of noncompliance with identity principles, like disclosing the identity of the associated party

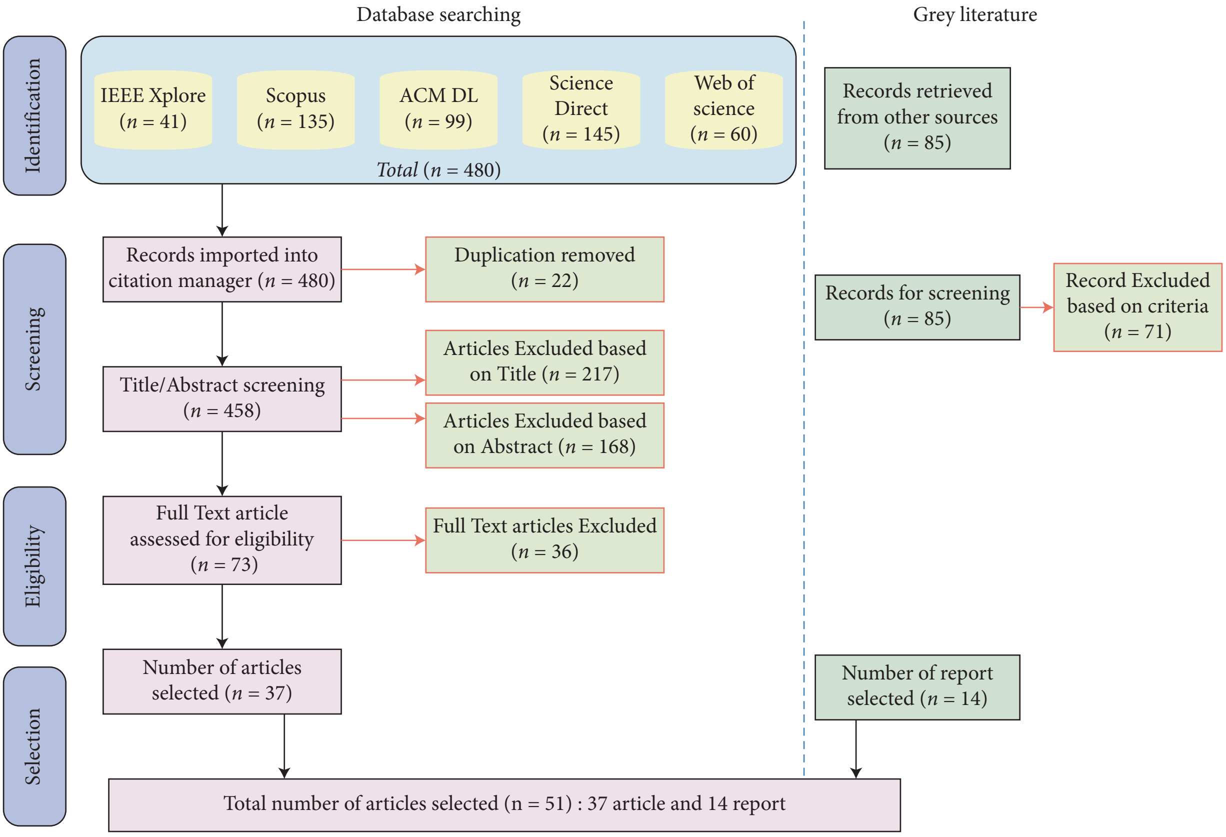
Database searching
Grey literature
Identification
IEEE Xplore (n = 41)
Scopus (n = 135)
ACM DL (n = 99)
Science Direct (n = 145)
Web of science (n = 60)
Total (n = 480)
Records retrieved from other sources (n = 85)
Screening
Records imported into citation manager (n = 480)
Duplication removed (n = 22)
Records for screening (n = 85)
Record Excluded based on criteria (n = 71)
Title/Abstract screening (n = 458)
Articles Excluded based on Title (n = 217)
Articles Excluded based on Abstract (n = 168)
Eligibility
Full Text article assessed for eligibility (n = 73)
Full Text articles Excluded (n = 36)
Selection
Number of articles selected (n = 37)
Number of report selected (n = 14)
Total number of articles selected (n = 51) : 37 article and 14 report

FIGURE 2: Study selection procedure.

TABLE 3: Identity issues in blockchain-based land registry system.

Ref	Description	Year	Limitations
[14]	Evaluated the use of blockchain in the land transaction by analysing the three blockchain-based solutions to record transfer and land ownership	2017	1. User's rights can be violated when the blockchain will show the personal identity information (PII) to the public user
[16]	Performed a SWOT analysis to use blockchain technology for land record-keeping	2017	1. Lack of user control over the identity
			2. Violates data laws for personally identifiable information
[17]	Done analysis of the application and finding issues of using blockchain in real estate by doing a case study in Germany	2017	1. Lack of digital identity and standards
			2. Right to the privacy of the individual personal data
[18]	Study to use and issues of applying blockchain technology in the land registry system of Georgia and Sweden	2019	1. Disclosing the identity of the associated party without consent 2. Lack of independent verification 3. Lack of disclosure of network participant identity
[19]	An overview of the use case of blockchain in real estate and explored the potentials and its limitations of blockchain in different sectors	2020	1. Lack of compliance with the regulatory requirement of identity for PII
[20]	Analyses the implementation issues of data protection and privacy regulation in the blockchain land registry system	2018	1. Lack of data protection and privacy regulation
			2. Issue of unknown identification
[21]	To find the technical and legal obstacles in the adoption of blockchain technology in land governance	2018	1. The need for a robust identity management system that satisfies the identity principle
[22]	Studied the application and issues of blockchain in Ghana land registry and also proposed a blockchain-based framework for land registration to minimise the current system's problems	2020	1. Need to satisfy the existing laws and ID principles for e-ID

Table 3: Continued.

Ref	Description	Year	Limitations
[23]	An analysis of different blockchain land registry systems was done to find implementation challenges for the current authorised framework	2019	1. Need for creating a digital identity solution 2. Digital identity compliance with the regulation to provide control for obtaining the identity 3. A lengthy process of providing the digital identity 4. Implication challenge for the new law to the current governance
[24]	To reduce the issue of land disputes and the problems with the traditional and present land registration system in Cyprus using blockchain	2020	1. The need for a digital Id solution
[25]	Minimises the issue of transaction costs and time consumption by using blockchain and identity management systems in Swedish land registry transfers	2018	1. The validity of a digital signature
[26]	To analyse various blockchain-based land registry systems in Sweden, Georgia, England, and Wales. And, to find the causes of delay in the adoption of blockchain technology for the real estate sector	2019	1. Unable to provide the identity to involved parties 2. Standardisation of the digital data 3. Unable to satisfy the legality framework and provide transparency
[27]	Study the issues in the Turkish land registry system and suggest the use of blockchain technology in the Turkish land registry system to provide tamper-proof record-keeping	2019	1. Lack of privacy for personal user data 2. The validity of the electronic signature 3. Verification of ID and placing the land record in the system
[28]	Identified the constraints and benefits of using blockchain for real estate and property rights	2020	1. The need for methods for privacy preservation of user data 2. The anonymity of providing digital identity
[29]	Identified the advantages and shortcomings of implementing the blockchain as a technological solution in land administration	2019	1. Lack of data protection and privacy of personal user data.
[30]	Studied the problem of the real estate industry like time consumption, manual process, and ownership issues by utilising blockchain technology	2019	1. The need for digital identity and the protection of personal data
[32]	Discusses the challenges, limitations, and opportunities in the real estate sector and explores the implementation challenges of blockchain technology	2020	1. Lack of ID verification for prevention of illegal activity and money laundering 2. The ID needs to satisfy the identity principle
[68]	Explains the working of Swedish land registry authority in collaboration with the chromaway and Telia company using blockchain and emphasises the need for a secure ID solution for personal identity information	2016	1. Lack of secure ID solution
[69]	The study proposes a blockchain-enabled framework for small land acquisition in Ghana to solve the country's economically opaque and poorly managed land administration procedures, which encourage multiple sales of the same lands and other land tenure security challenges. In Ghana, this blockchain-enabled framework improves transparency, accountability, and land record keeping	2021	1. Lack of validity of land ownership document
[70]	The article looks at how blockchain can be used in land administration in Ghana, Georgia, and Sweden. Blockchain land registries may prolong zones of dispossession based on colonial histories and current inequality	2021	1. The need for a digital Id solution
[71]	It proposes a scalable land registry system based on blockchain technology, which enables efficient, decentralised, and transparent data sharing and storage	2021	1. Lack of data protection and privacy of personal user data 2. Lack of searching mechanism for huge user data

for publicity function without user consent [18]. The use of blockchain technology in the real estate sector and its limitations, such as the digital identity compliance with the regulatory requirement of identity for PII, is presented in Ref. [19]. In Ref. [20], the issues in implementing data protection and privacy regulation, which increases the concern of money laundering activities and knowing your customer (KYC), has been discussed. A review to find the technical and legal obstacle in the adoption of blockchain technology in land governance, and analysis to identify the need for a robust identity management system that satisfies the identity principle of the user for providing identity to the involved parties, parcels, and property is presented in Ref. [21].

7.4. Legal Validity. The process of adopting digital technology requires the legal validity of digital documentation to make them legally binding. The legal framework varies from country to country, and cross-border transactions have to be defined by some legal framework. The uses of blockchain will hasten the identification of the property, and provide security, trust, and accuracy of land transfer by digital tracking of transactions. Nevertheless, the validity of digital signatures across borders remains a challenge [25].

In implementing the smart contract in the current land registry system, there are also issues related to the implication of the new law in contemporary governance [23]. Oxford University conducted various interviews with startup companies and technical experts that revealed the difficulties of standardising digital identity and blockchain in satisfying the legality framework and providing transparency [26]. In reviewing the Turkish land registry system, the author suggested using blockchain technology for tamper-proof record-keeping, which can be recovered in the case of disasters. However, there is a need for the legal validity of electronic signatures [27]. Further in Ref. [69], the author also examined alternate approaches for enhancing property rights in the land sector in Ghana and internationally, in addition to the current significant emphasis on the titling and lease registration, For example, if alternate solution paperwork, such as tamper-proof blockchain-based land allocation notes, becomes widely accepted as a legal validation of land ownership, the dependence on chiefs and government servants for leases and land title certificates, or even other papers to safeguard leases and title certificates, will be significantly reduced.

7.5. User Control. Managing digital identity: where the user creates a digital identity for online services and remembers the user ID and password, a centralised party controls the identity and users have no control over their identity, raising the issue of how users' personal data are used and protected and shared. The weakness of adopting blockchain in record-keeping is that it lacks sufficient user control over verification of transactions as the government or organisation controlling the blockchain may reverse the approved transaction [16]. The privacy of the users' data is at risk when the principles of publicity are applied [27]. Personal data protection is also at stake as blockchain is an open source, enabling everyone to view transaction data and logs [28]. The open nature of blockchain also concerns data protection and privacy, such as personal ID [29]. There should be some prerequisites for employing blockchain, such as the lack of a generic and consistent blockchain architecture to secure the user's digital data. The analysis should be carried out in these directions. As the population grows, the number of people who use the blockchain land registry systems will also grow. So there is a concern related to securing the users' personal data. It means data on the blockchain scheme will keep increasing. Storing and protecting such massive amounts of data in blockchain requires rapid search operations as well as effective privacy mechanisms [71].

8. RQ2: How to Comply with Digital Identity Principles?

Cameron examined identity models to find the cause of their failure and market adaptability, and he established that some guiding principles needed to build a successful Identity model [72]. These laws also act as a guiding principle for organisations and researchers working in the area of identity management. The Internet lacks a layer of identity's necessary capabilities and describes an identity metasystem that the author believes might provide the Internet with essential capabilities.

The law of identity consists of seven principles that provide several guidelines on how to manage and disclose a user's identity and how to identify various entities with different types of identification.

Compliance with these laws is essential to build a successful Identity model; else, it creates a sequence of side effects that will gradually weaken the subsequent technology. In 2005, Kim Cameron wrote the Law of Identity as an identity and access architect at Microsoft Corporation [72]. These identity laws describe several objective dynamics that specify a digital identity metasystem, generally accepted as an online distributed computer framework.

Furthermore, Table 4 explains how identity models comply with identity principles. These laws of identity are briefly described 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 recognise omnidirectional identifiers for public entities and unidirectional identifications for private entities, simplifying discovery and preventing unnecessary correlation disclosures.

Table 4: Identity model compliance with identity principles.

Law no.	Digital identity principles	How identity model compliance with identity principles.
1	User control and consent	The identity model must only be configured to view identity data in compliance with the user's control and consent. If a transaction is to reveal the identity data of the user, then user consent is necessary to allow users for making decisions and to control their personal identity information (PII).
2	Minimum disclosure	An identity model should disclose less personal identification information (PII) and restrict usage until it is appropriate for the transaction to be carried out. Therefore, only a minimal number of PII is then stored
3	Justifiable parties	An identity model could reveal minimal identifying details to parties who have the essential and justifiable position in the identity relationship
4	Directed identification	An identity model should encourage the use of global identities for private use by public and local identities
5	Pluralism of operators and technology	An identity model should be robust enough to represent identities in a standard format for the identification and validation even in different administrative domains
6	Human integration	To ensure adequate security against identity attacks (e.g., impersonations and phishing), an identity model must provide a safe link between users and machines
7	Consistent experience across contexts	An identity model should offer the user a simple, consistent experience by providing support to various operators and technologies

(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.

9. RQ3: WHICH Method Can Be Used to Compare the Most Appropriate Identity Model?

9.1. Methods and Criteria for Comparison of Identity Model. The digital identity model is categorised into four different levels by Christopher Allen in the year 2016 [33,34] as centralised, federated, user-centric, and self-sovereign identity models.

A comparative study has been performed on three identity models (centralised, federated, and user-centric) based on standards. The standards selected for the comparison are complexity, implementation, scalability, user's requirement, and single sign-on (SSO) [34]. A comparison of the personal identity models (domain and user-centric identity models) was performed based on the criteria needed to provide identity management functionality. The criteria selected are user control and consent, anonymity, reputation, trust making a decision, identity discovery, multiple ids & identity providers, and SSO [73]. A survey on the technology used in the identity model is conducted on the core design principles of the identity model [74].

A state of the art comparison of various initiatives of identity model to support future networks is performed [75]. A two-way mapping view analysis of the identity model provides useful future research directions. The analysis is performed on identity and attribute mapping, the connection among operations and general design consideration [76]. In Ref. [77], a comparison of the current identity model according to the Cameron identity principles ("laws of identity") [72] was performed to determine the appropriate identity model for the identity metasystem.

Traditional identity systems are centralised (as well as federated models) depending on mobile wallet applications. At the same time, these identity models have improved usability [78]. Various digital identity management models are compared to ascertain the usability requirement to provide high-level analysis to adapt identity management in a heterogeneous environment. The usage requirements for identity management discussed by the author are management, usability, interoperability, scalability, functionality, trustworthiness, security, privacy, liability, and human integration [79]. In addition, the identity models and methods are mapped to these identity management requirements [80].

The analysis of the identity models based on Cameron identity principles ("laws of identity") [72] is performed to make a roadmap for managing and migration of identity in heterogeneous environments [81]. To identify the trust problems in the identity models, the author defined the trust requirement by focusing on the trust issues and comparing various available identity models based on these trust requirements [82]. Table 5 provides a tabular representation of these research works in literature for evaluating the identity models.

The primary purpose of our study is to identify the identity challenges in blockchain-based land registry system that mainly highlights the lack of compliance with identity principles that have been already defined in Table 3.

Table 5: Methods and criteria for comparison of the identity model.

		Criteria							
Ref	Method used	User control and consent	Minimum disclosure	Justifiable parties	Directed identity	Pluralism of operators and technology	Human integration	Consistent experience across contexts	Additional
[34]	Identity management standard					Scalability	User's requirement	SSO	Complexity, implementation
[73]	Identity management functionality	User control and consent	Anonymity	Trust making decisions, reputation	Identity discovery	Multiple IDs and IdPs		SSO	
[74]	Core design principle	User control and consent, privacy, protection				Cross-domain access			
[75]	Features of the identity model	Privacy	Anonymity			Interoperability	Security	Mobility	
[76]	Two-way mapping					Connections among the operations		identity mapping, attribute mapping	General design considerations
[77]	Identity principles	Control	Minimal disclosure	Justifiable parties	Directed identity	Pluralism	Human integration	Contexts	
[79]	Usability requirements		Pseudonymity			Interoperability, scalability	Security	Portability	Recovery (persistence)
[80]	Identity requirement			Trustworthiness		Interoperability, scalability	Usability, integration, security	Portability, functionality	Management, liability
[81]	Identity principles	Control	Minimal disclosure	Justifiable parties	Directed identity	Pluralism, scalability	Human integration	Contexts	
[82]	Trust requirements	Privacy, authentication	Adhere to privacy policy for PII	Identity mapping between SPs	Client authentication by the service provider	Scalability	Personal authentication device is tamper-resistant	Client credentials handing	

Therefore, it is imperative to define the criteria for evaluation and select the best appropriate identity model for the land registry system. Table 5 provides a comparative study of various methods used by different researchers to compare identity models. We have selected compliance with the identity principle to compare the identity model as it is the most comprehensive criteria and provides a defined structure to evaluate the models.

In the following section, we present a short description of each identity model with respective pros and cons and further compare these identity models according to compliance with each law defined by Cameron. Table 6 summarises the results of this comparison and highlights the laws that each model addresses.

9.2. Type of Identity Model. The identity models have been classified into four categories: centralised, federal, user-centric, and self-sovereign. These identity models have been explained in this section.

(i) Centralised identity model: the centralised identity model contains an individual organisation that controls identity. It consists of one identity and identifier within a trusted domain. It runs on a client-server model and has a separate function for service provider and identity provider (IDP). The identity provider provides the user authentication and identity function utilised by every service. The service provider then sends a direct request to the central identity provider to verify the user [74]. Centralised identity can manage a vast number of users and is applied in various ways such as a single sign-on [83], identifier, and a meta identifier domain [82]. The different identity management systems use a central identity system like PKI [84] and Kerberos [85].

(ii) Nevertheless, storing all identities in one IDP is an inefficient way to provide user privileges and access to a different domain. At the same time, centralised identity proves to possess inadequate privacy protection. Users have to store or memorise a range of passwords as they have to verify separately with each company. Organisations must use large hardware and high costs to secure user verification, passwords, and data [82].

(iii) Federal identity model: multiple identity providers agree and function under a shared trust framework in the federated identity model. This model distributes users' digital information to multiple identity providers rather than being centralised in one. This association of identity providers is commonly known as a federation and usually a unique user identifier for every user. However, the user usually will not utilise this model. Access is granted through a single service provider. Various protocol and identity management systems are implemented, such as security mark-up language [86,87] and the liberty alliance framework [88]. The key difference between the federal identity model and centralised and third-party approaches is that the federal model uses many to many identity management approaches. In contrast, centralised and third-party approaches can be viewed as one to one [5,89]. Nevertheless, there are challenges, including inaccurate identity usage, absence of uniformity, and lack of information accuracy [82,90,91].

(iv) User-centric identity model: the user-centric identity is proposed to solve the weakness of adopting user participation. The federal identity consists of numerous organisations and domains where the user has to memorise a large number of passwords and identity credentials [92]. The user-centric method is designed by mapping the hardware used to store the data on a personal device [93]. A personal device may be with and without a keyboard and require authentication like a password. In the user-centric model, the user keeps passwords and certificates from different service providers inside a personal computer. Therefore, the user is in control of his or her data. It is the first model to implement a framework that supports user identity management. Instead of handling multiple identities, a user has a personal device that contains several identities and passwords provided by the different identity providers. This personal device serves as an IdP selector. It includes a collection of credentials from various IdPs. After the authentication of a user by the IdP, the user can experience a single sign-on experience without the communication and agreement among identity providers.

(v) Self-sovereign identity model: the user is the main administrator of the identity in the self-sovereign identity model (SSI), and they have much greater control over data and information than others. Unlike centralised, user-centric, and federated models, the self-sovereign identity does not require a person to manage the identity of individuals [35,94]. It also provides the recording and transfer of identity information and trust among entities [95]. The function of an identity provider is restricted to as an issuer of identity only. It is a relatively new concept in online identity management that enables users to control and manage identity information (e.g. attributes, identifiers, and credentials) [96]. The SSI stores the identity information locally on the user's personal device. However, placing personal details on the ledger is not the right approach since the ledger is immutable; data written in the ledger cannot be modified or deleted. Therefore, SSI uses the distributed ledger to share claims, proof, and attestations instead of sharing current attributes. SSI is based on Zero-Knowledge Proof (ZKP), which allows one user to prove that they know some information or fulfill a specific requirement without providing the factual information that supports the proof [97].

Table 6: Comparison of identity model based on identity principles.

Law no.	Digital identity principle	Identity models			
		Centralised	Federal	User-centric	SSI model
1	User control and consent	**x**	**x**	x	✓
2	Minimum disclosure	**x**	✓	✓	✓
3	Justifiable parties	**x**	**x**	✓	✓
4	Directed identification	**x**	✓	✓	✓
5	Pluralism of operators and technology	**x**	✓	✓	✓
6	Human integration	✓	✓	✓	✓
7	Consistent experience across contexts	**x**	**x**	✓	✓

9.3. Comparison of Identity Model Based on Identity Principles. In this section, analysis of identity models has been done based on their compliance with seven laws of identity. Table 6 provides a comparative study of this analysis of identity models based on identity laws.

(i) Law 1: user control and consent: the identity model must provide an easy, convenient way to manage user identity. This identity model can gain user trust by supporting the user in managing digital identities and publishing information. The user-centric and self-sovereign identity models operate on this principle, but the user-centric identity model does not entirely meet it. A user-centric model also includes a third-party identity provider to store identity information. It means a third-party IdP is still required to control the identity.

(ii) Law 2: minimum disclosure: the Identity model is vulnerable to identity attacks. The best way to mitigate this issue is to acquire only the details that a provider "needs to know" and retain only the information that needs to be preserved." Thus, by following these processes, minimal harm can be ensured in the event of an identity attack [72]. In short, except for the centralised model, all models have their way to manage limited disclosure. The federated model integrates the alias, which enables recognisable data shown to the federation of third-party identity providers. The user identity information is unreachable without contacting the IdP who created the identity. The user-centric model aims to solve this type of identity attack but still has multiple identities linked to their personal identity provider. The identity information always depends on a third-party IdP, which is vulnerable to identity attacks. In the self-sovereign model, users can never place identity data on the ledger; it uses a zero-knowledge strategy, which significantly reduces the amount of information exposed to data breaches since it never discloses the actual identity information.

(iii) Law 3: justifiable parties: the identity model should notify users of the party or parties it interacts with when the information is exchanged. It, therefore, sets out the main concepts of the user-centric and self-sovereign identity model. The user-centric and self-sovereign model helps users to find the preferred identity provider and share the identity information.

(iv) Law 4: directed identification: to manage the identities in a hyper-related environment, the identity model needs to establish an identity relation to create a meaning for a given environment. Consequently, the identity model needs to support two separate identity connections: "omnidirectional" and "unidirectional." Public entities (e.g. identity and service providers) should have symmetric, well-known identifiers. Where the customer wishes to exchange information with other entities based on the principle of minimal disclosure, a short-term agreement shall be drawn up, showing the least identifiable information that provides a "unidirectional" identifying connection.

(v) Law 5: pluralism of operators and technology: the identity model must allow multiple identity providers to interact with different technologies. The identity model should also promote the coexistence of various technologies. All models have resources to work in a different domain, except for a centralised model. The federation model defines a set of rules and agreements that allow for identity sharing between various models with different strategies for multiple organisations. Personal IdP offers interoperability to various identity providers in the user-centric model. For example, in Ref. [98], an identity provider module is implemented that allows users to send authentication messages from one direction to another. In the model of self-sovereignty, the possibility of sharing identity claims adopted by different domains is in line with the law of pluralism.

(vi) Law 6: human integration: the identity model should consider the user as a part of the system. It must also have security protection to communicate with human devices to defend against identity attacks. In addition to preliminary identity authentication, a person must have different means of proving his or her identity. This aspect of human integration relates to the method of authentication. For example, implementing multi-factor authentication allows user authentication to take place only if more than one form of identity verification is provided. All identity models offer multi-factor authentication to achieve human integration at a certain level.

(vii) Law 7: consistent experience across contexts: the identity model allows a user to connect with the identity and define the identity elements to be exchanged. The interaction of the user must also be integrated into the identity model. Identity approval is a core aspect of the user-centric and self-sovereign identity model. The user-centric model allows the user to determine which identity information is exchanged between the IdPs. Also, in a self-sovereign identity model, when the consumer manages his or her identity, he or she decides which identity claim to be shared.

The SSI model can offer users complete control over their identities to reduce management costs, increase efficiency, and overcome the shortcomings of existing other identity models. Only the necessary information will be revealed to third parties that are known as selective disclosure [99,100]. Issuing identity credentials built on the trusted network among two parties is the main objective of the self-sovereign identity model. SSI can create a convenient communication method using an easy, automated process and standard format. Furthermore, new standards like decentralised identifiers (DIDs) have been developed as the backbone of the SSI environment. Self-sovereign identity must be accessible for use across multiple systems.

10. Conclusion

This paper reviews the fundamental aspects of blockchain application in the land registry system and issues related to identity. First, it provides a background study that highlights the land registry systems, problems, blockchain, and concepts of digital identity. This paper uses a systemic literature review (SLR) based on three defined research questions highlighting the identity issues with the blockchain-based land registry, compliance with identity principles, and review of existing identity models to resolve identity issues of land registry. This SLR has selected 477 papers based on criteria and 85 articles from grey literature and finally used a total of 48 articles for review. Firstly, it highlights the issues associated with digital identity in compliance with the identity principles. Then, it explores how identity models comply with the digital identity principles and elaborates on the laws of digital identity. Finally, it explores the different comparison criteria for comparing identity models. This paper has further described and evaluated different models of digital identity, namely, centralised, federal, user-centric, and SSI models. All these four identity models have been compared based on seven identity principles. The comparison highlights that the centralised identity model lacks most of the identity principles, and the federal model covers only three principles. The user-centric model covers most of the identity principles but lacks user control and consent criteria, which is an important aspect of digital identity. This study concludes that the SSI model complies with all the identity principles. It is the most suitable model for providing digital identity to users and resolving the identified issues related to the blockchain-based land registry system.

Data Availability

It is a review article and thus there is no underlying data set used, although the article contains the detailed analysis of the previous researches done in the field.

Conflicts of Interest

The authors declare that they have no conflicts of interest.

References

[1] US Agency for International Development, *Investor Survey on Land Disputes: Perceptions and Practices of the Private Sector on Land and Resource Tenure Risks*, US Agency for International Development, Washington, DC, USA, 2018.

[2] F. v. Weizsäcker, S. Eggler, and E. Atarim, *Land Registries on a Distributed Ledger*, Deutsche Gesellschaft fürInternationale Zusammenarbeit (GIZ) GmbH, Berlin, Germany, 2019, https://www.giz.de/de/downloads/giz2019-en-distributed-land-registry.pdf.

[3] A. Tapscott, *India Land Registry on Blockchain*, Research Institute Lighthouse, Toronto, Canada, 2018, https://www.blockchainresearchinstitute.org/project/indias-land-registry-on-blockchain/.

[4] V. Thakur, M. N. Doja, Y. K. Dwivedi, T. Ahmad, and G. Khadanga, "Land records on blockchain for implementation of land titling in India," *International Journal of Information Management*, vol. 52, pp. 101940–101949, 2020.

[5] G. Eder, "Digital transformation: blockchain and land titles," in *OECD Global Anti Corruption and Integrity Forum*, pp. 1–12, OECD (Organisation for Economic Co-Operation and Development), Paris, France, 2019, https://www.oecd.org/corruption/integrity-forum/academic-papers/Georg%20Eder-%20Blockchain%20-%20Ghana_verified.pdf.

[6] J. A. T. Fairfield, "BitProperty," *Southern California Law Review*, vol. 88, no. 5, pp. 805–874, 2015.

[7] A. Gervais, G. O. Karame, K. Wüst, V. Glykantzis, H. Ritzdorf, and S. Capkun, "On the security and performance of proof of work blockchains," in *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, vol. 24–28, pp. 3–16, Vienna, Austria, October 2016.

[8] V. Hoxha and S. Sadiku, "Study of factors influencing the decision to adopt the blockchain technology in real estate transactions in Kosovo," *Property Management*, vol. 37, no. 5, pp. 684–700, 2019.

[9] M. Kempe, *The Land Registry in the Blockchain*, A Development Project with Lantmäteriet, Sweden, 2016.

[10] D. K. D. Mehendale, "Implications of block chain in real estate industry," *International Journal of Recent Technology and Engineering*, vol. 8, no. 1, pp. 500–503, 2019.

[11] H. Mukne, P. Pai, S. Raut, and D. Ambawade, "Land record management using hyperledger fabric and IPFS," in *Proceedings of the 2019 10th International Conference on Computing, Communication and Networking Technologies (ICCCNT)*, pp. 1–8, Kanpur, India, July 2019.

[12] N. Radziwill, “Blockchain revolution: how the technology behind bitcoin is changing money, business, and the world,” *Quality Management Journal*, vol. 25, no. 1, pp. 64-65, 2018.

[13] S. Underwood, “Blockchain beyond bitcoin,” *Communications of the ACM*, vol. 59, no. 11, pp. 15–17, 2016.

[14] V. L. Lemieux and V. L. Lemieux, “Evaluating the use of blockchain in land transactions: an archival science perspective,” *European Property Law Journal*, vol. 6, no. 3, pp. 392–440, 2017.

[15] G. Zyskind, O. Nathan, and S. Pentland, “Decentralising privacy: using blockchain to protect personal data,” in *Proceedings of the 2015 IEEE Security and Privacy Workshops*, pp. 180–184, San Jose, CA, USA, May 2015.

[16] V. L. Lemieux, *Blockchain Record-Keeping: A Swot Analysis*, ARMA International, Overland Park, KS, USA, Dec. 2007, https://magazine.arma.org/wp-content/uploads/simple-file-list/2017_06_IM_blockchain_recordkeeping_SWOT_lemieux.pdf.

[17] 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.

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

[19] N. Mehdi, *Blockchain: An Emerging Opportunity for Surveyors?*, London, UK, 2020, https://www.rics.org/globalassets/blockchain_insight-paper.pdf.

[20] G. Sylvester, “E-agriculture in action: blockchain for agriculture opportunities and challanges,” in *Bangkok: Food and Agriculture Organisation of the United Nations and the International Telecommunication Union*Rome, Italy, 2019, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-E_AGRICULT.03-2018-PDF-E.pdf.

[21] J. M. Graglia and C. Mellon, “Blockchain and property in 2018: at the end of the beginning,” *Innovations: Technology, Governance, Globalization*, vol. 12, no. 1-2, pp. 90–116, 2018.

[22] K. Mintah and K. Godwin, “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.

[23] M. Vega Maza, “El auge de blockchain y sus posibilidades reales de aplicación en los registros de las administraciones públicas,” *IDP. Revista de Internet, derecho y política*, vol. 28, no. 28, pp. 109–126, 2019.

[24] B. Yapicioglu and R. Leshinsky, “Blockchain as a tool for land rights: ownership of land in Cyprus,” *Journal of Property, Planning and Environmental Law*, vol. 12, no. 2, pp. 171–182, 2020.

[25] J. McMurren, A. Young, and S. Verhulst, *Addressing Transaction Costs through Blockchain and Identity in Swedish Land Transfers*, GOVLAB, Brooklyn, NY, USA, 2018, https://blockchan.ge/blockchange-land-registry.pdf.

[26] S. Andrew and B. Andrew, *The Future of Real Estate Transactions*, https://www.sbs.ox.ac.uk/sites/default/files/2019-03/FoRET-ReportSummary_0.pdf, University of Oxford Research, Oxford, UK, 2019, https://www.sbs.ox.ac.uk/sites/default/files/2019-03/FoRET-ReportSummary_0.pdf.

[27] H. S. Ekmekci, *Applicability of Blockchain Technology to Turkish Land Registry System ,Masters Thesis*, Tilburg University, Tilburg, Netherlands, 2019.

[28] O. Konashevych, “Constraints and benefits of the blockchain use for real estate and property rights,” *Journal of Property, Planning and Environmental Law*, vol. 12, no. 2, pp. 109–127, 2020.

[29] P. Krigsholm, K. Ridanpaa, and K. Riekkinen, “Blockchain as a technological solution in land administration-what are current barriers to implementation?” *Fig Peer Review Journal*, vol. XV, no. 9, pp. 14–22, 2019.

[30] K. S. Krupa and M. S. Akhil, “Reshaping the real estate industry using blockchain,” in *Lecture Notes in Electrical Engineering*, vol. 545, pp. 255–263, , no. 12, Springer, Singapore, 2019.

[31] T. Antonio and P. Lilyana, “Directive (EU) 2018/843 of the European parliament and of the council,” *Official Journal of the European Union*, vol. 648, p. 32, 2018, https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32018L0843&from=EN.

[32] G. Teruel, “Legal challenges and opportunities of blockchain technology in the real estate sector,” *Journal of Property, Planning and Environmental Law*, vol. 12, no. 2, pp. 129–145, 2020.

[33] C. Allen, “The path to self-sovereign identity,” 2016, http://www.lifewithalacrity.com/2016/04/the-path-to-self-sovereign-identity.html.

[34] Y. Liu, “Blockchain-based identity management systems: a review,” *Journal of Network and Computer Applications*, vol. 166, Article ID 102731, 2020.

[35] 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.

[36] M. Van Wingerde, *Blockchain-enabled Self-Sovereign Identity*, Tilburg University, Tilburg, Netherlands, 2017.

[37] A. Dobhal and M. Regan, “Immutability and auditability: the critical elements in property rights registries,” in *Proceedings of the Annual World Bank Conference on Land and Property: Annual World Bank Conference on Land and Property*, pp. 1–8, Washington, DC, USA, 2016.

[38] S. Alam, M. Shuaib, W. Z. Khan et al., “Blockchain-based initiatives: current state and challenges,” *Computer Networks*, vol. 198, Article ID 108395, 2021.

[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] E. Oliveira, “Land ownership and land use development: the integration of past, present, and future in spatial planning and land management policies,” *Landscape Journal*, vol. 36, no. 2, pp. 119–121, 2017.

[42] H. Lian and Y. Yu, “Reference of land registration system from countries in asia-pacific region: comparison of the United States,” *IOSR Journal of Business and Management*, vol. 18, no. 7, pp. 31–40, 2016.

[43] L. Li, R. Tan, and C. Wu, "Reconstruction of China's farmland rights system based on the "trifurcation of land rights" reform," *Land*, vol. 9, no. 2, p. 51, 2020.

[44] A.-M. Brits, C. Grant, and T. Burns, "Comparative study of land administration systems," in *Proceedings of the Regional Workshops on Land Policy Issues-Asia Program, Wollongong*, Wollongong, NSW, Australia, 2002, https://www.researchgate.net/profile/Tony-Burns/publication/238731108_LAND_TITLING_EXPERIENCE_IN_ASIA/links/5989112baca27266ada4de8b/LAND-TITLING-EXPERIENCE-IN-ASIA.pdf.

[45] R. Wu, "Implementation of land title registration system in Malaysia current offers," *The Malayan Law Journal*, vol. 1, no. 1, pp. 1–11, 2011, http://irep.iium.edu.my/29661.

[46] A. Ahmed, Z. Abubakari, and A. Gasparatos, "Labelling large-scale land acquisitions as land grabs: procedural and distributional considerations from two cases in Ghana," *Geoforum*, vol. 105, pp. 191–205, 2019.

[47] D. Grinlinton and R. Thomas, *Land Registration and Title Security in the Digital Age: New Horizons for Torrens*, Taylor & Francis, London, UK, 1st edition, 2020.

[48] E. Cooke, *The New Law of Land Registration*, Hart Publishing, London, UK, 2nd edition, 2003.

[49] E. H. Scamell, "Land law and registration," *Survey Review*, vol. 24, no. 187, pp. 235–245, 2012.

[50] A. Castellanos and R. Benbunan fich, "Digitalization of land records: from paper to blockchain," in *Proceedings of the International Conference on Information Systems 2018, ICIS*, pp. 1–9, San Francisco, CA, USA, November 2018.

[51] G. Abhishek, *Property Registration and Land Record Management via Blockchains*, Indian Institute of Technology Kanpur, Kanpur, India, 2019.

[52] N. Miller and D. Pogue, "Sustainable real estate and corporate responsibility," in *Routledge Handbook of Sustainable Real Estate*, S. S. Sara Wilkinson, T. Dixon, and N. Miller, Eds., pp. 19–36, Routledge, London, UK, 1st edition, 2018.

[53] E. Cerutti, J. Dagher, and G. Dell'Ariccia, "Housing finance and real-estate booms: a cross-country perspective," *Journal of Housing Economics*, vol. 38, pp. 1–13, 2017.

[54] N. M. Kaplanov, "Nerdy money: bitcoin, the private digital currency, and the case against its regulation," *SSRN Electronic Journal*, vol. 25, no. 1, pp. 1–65, 2012.

[55] P. Kumar, G. A. Dhanush, D. Srivatsa, A. Nithin, and S. Sahisnu, "A buyer and seller's protocol via utilisation of smart contracts using blockchain technology," in *Communications in Computer and Information Science*, vol. 1075, pp. 464–474, Springer, Singapore, 2019.

[56] B. Agarwal, *Conclusive Land Title System for India*, Panjab University, Chandigarh, India, 2018.

[57] D. Mills, "Distributed ledger technology in payments, clearing, and settlement," *Finance and Economics Discussion Series*, vol. 2016, no. 95, pp. 971–1023, 2016.

[58] A. Anand, M. McKibbin, F. Pichel, and F. P. Bank, "Colored coins: bitcoin, blockchain, and land administration," in *Proceedings of the World Bank Conference on Land and Poverty*, pp. 1–9, March 2017, https://pdfs.semanticscholar.org/d23e/3b0fecc9f24900a3e3dd4d31dda934c6a88d.pdf.

[59] R. A. Andreev, P. A. Andreeva, L. N. Krotov, and E. L. Krotova, "Review of blockchain technology: types of blockchain and their application," *Intellekt. Sist. Proizv.*vol. 16, no. 1, p. 11, 2018.

[60] C. Cachin and M. Vukolic, "Blockchain consensus protocols in the wild," *Leibniz Int. Proc. Informatics, LIPIcs*, vol. 91, no. 1, pp. 1–24, 2017.

[61] M. Pilkington, "Blockchain technology: principles and applications," in *Research Handbook on Digital Transformations*, pp. 225–253, Edward Elgar Publishing, 2016.

[62] A. Deshpande, K. Stewart, L. Lepetit, and S. Gunashekar, *Understanding the Landscape of Distributed Ledger Technologies/Blockchain: Challenges, Opportunities, and the Prospects for Standards*, RAND Corporation, Santa Monica, CA, USA, 2020.

[63] C. S. Wright, "Bitcoin: a peer-to-peer electronic cash system," *SSRN Electronic Journal*, vol. 3440802, 2008.

[64] R. Maull, P. Godsiff, C. Mulligan, A. Brown, and B. Kewell, "Distributed ledger technology: applications and implications," *Strategic Change*, vol. 26, no. 5, pp. 481–489, 2017.

[65] C. Sullivan, "Digital identity – introduction," in *Digital Identity: An Emergent Legal Concept*, pp. 5–18, University of Adelaide Press, Adelaide, Australia, 2012.

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

[67] 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.

[68] M. Kempe, "The land registry in the blockchain," 2016, http://ica-it.org/pdf/Blockchain_Landregistry_Report.pdf.

[69] K. Mintah, F. G. Boateng, K. T. Baako, E. Gaisie, and G. K. Otchere, "Blockchain on stool land acquisition: lessons from Ghana for strengthening land tenure security other than titling," *Land Use Policy*, vol. 109, Article ID 105635, 2021.

[70] D. Rodima-Taylor, "Digitalizing land administration: the geographies and temporalities of infrastructural promise," *Geoforum*, vol. 122, pp. 140–151, 2021.

[71] A. S. Yadav, S. Agrawal, and D. S. Kushwaha, "Distributed Ledger Technology-based land transaction system with trusted nodes consensus mechanism," *Journal of King Saud University*, 2021.

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

[73] T. M. Eap, M. Hatala, and D. Gasevic, "Enabling user control with personal identity management," in *Proceedings of the IEEE International Conference on Services Computing (SCC 2007)*, pp. 60–67, Salt Lake City, UT, USA, 2007.

[74] Y. Cao, L. Yang, B. Chao, and L. Yang, "A survey of Identity Management technology," in *Proceedings of the IEEE International Conference on Information Theory and Information Security*, pp. 287–293, Beijing, China, December 2010.

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

[76] J. Liu, A. Hodges, L. Clay, and J. Monarch, "An analysis of digital identity management systems - a two-mapping view," in *Proceedings of the 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)*, pp. 92–96, Paris, France, September 2020.

[77] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the internet of things," 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), pp. 1568–1573, Halifax, Canada, July 2018.

[78] H. Farahmand, *Guidance for Decentralised Identity and Verifiable Claims*, Gartner, Stamford, CT, USA, 2020, https://www.gartner.com/en/documents/3979940/guidance-for-decentralized-identity-and-verifiable-claim.

[79] M. Allende López, *Self-Sovereign Identity: The Future of Identity: Self-Sovereignity, Digital Wallets, and Blockchain*, Inter-American Development Bank, Washington, DC, USA, 2020.

[80] D. Pöhn and W. Hommel, "An overview of limitations and approaches in identity management," in *Proceedings of the 15th International Conference on Availability, Reliability and Security*, pp. 1–10, Dublin, Ireland, August 2020.

[81] H. L'Amrani, B. E. Berroukech, Y. El Bouzekri El Idrissi, and R. Ajhoun, "Identity Management Systems: Laws of Identity for Models 7 Evaluation," in *Proceedings of the 2016 4th IEEE International Colloquium on Information Science and Technology (CiSt)*, pp. 736–740, Tangier, Morocco, October 2016.

[82] A. Josang, J. Fabre, B. Hay, J. Dalziel, and S. Pope, "Trust requirements in identity management," *Work. Grid Comput. E-Research*, vol. 44, pp. 99–108, 2005.

[83] A. Pashalidis and C. J. Mitchell, "A taxonomy of single sign-on systems," in *Lecture Notes in Computer Science*, vol. 2727, pp. 249–264, Springer, Singapore, 2003.

[84] J. Huang and D. Nicol, "A calculus of trust and its application to PKI and identity management," in *Proceedings of the 8th Symposium on Identity and Trust on the Internet - IDtrust '09*, p. 23, Gaithersburg, MD, USA, April 2009.

[85] B. Clifford Neuman and Theodore, "Kerberos: an authentication service for computer networks," *IEEE Communications Magazine*, vol. 32, no. 9, pp. 33–38, 1994.

[86] H. Lockhart, *Security Assertion Markup Language (SAML) V2: 0 Technical Overview*, vol. 2, OASIS Open, Burlington,USA, 2004http://www.oasis-open.org/committees/documents.php?wg_abbrev=security.

[87] R. L. B. Morgan, S. Cantor, S. Carmody, W. Hoehn, and K. Klingenstein, "Federated security: the shibboleth approach," *Educause Quarterly*, vol. 27, no. 4, pp. 12–17, 2004.

[88] M. Alsaleh and C. Adams, "Enhancing consumer privacy in the liberty alliance identity federation and web services frameworks," in *Lecture Notes in Computer Science*, vol. 4258, pp. 59–77, Springer, Singapore, 2006.

[89] Organisation for Economic Co-Operation and Development, *The Role of Digital Identity Management in the Internet Economy: A Primer for Policy Makers*, OECD Publishing, Paris, France, 2009.

[90] H. Alkahtani, T. H. H. Aldhyani, and M. Al-Yaari, "Adaptive anomaly detection framework model objects in cyberspace," *Applied Bionics and Biomechanics*, vol. 2020, pp. 1–14, 2020.

[91] T. H. H. Aldhyani and H. Alkahtani, "Attacks to automatous vehicles: a deep learning algorithm for cybersecurity," *Sensors*, vol. 22, no. 1, p. 360, 2022.

[92] H. Ronoh, K. Omieno, and S. Mutua, "An interoperability framework for E-government heterogeneous information systems," *IJARCCE*, vol. 7, no. 10, pp. 115–126, 2018.

[93] P. Bramhall, M. Hansen, K. Rannenberg, and T. Roessler, "User-centric identity management: new trends in standardisation and regulation," *IEEE Security and Privacy Magazine*, vol. 5, no. 4, pp. 84–87, 2007.

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

[95] F. Wang and P. De Filippi, "Self-sovereign identity in a globalised world: credentials-based identity systems as a driver for economic inclusion," *Front. Blockchain*, vol. 2, 2020.

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

[97] A. Tobin and D. Reed, *The Inevitable Rise of Self-Sovereign Identity A White Paper from the*, Sovrin Foundation, Provo, UT, USA, 2017, https://sovrin.org/wp-content/uploads/2017/06/The-Inevitable-Rise-of-Self-Sovereign-Identity.pdf.

[98] H. Koshutanski and L. Telesca, "Towards user-centric identity interoperability for digital ecosystems," *International Journal of Information Security*, vol. 1, no. 1, pp. 26–38, 2009, https://www.thinkmind.org/articles/sec_v1_n1_2008_3.pdf.

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

[100] Y. Panfil and C. Mellon, *The Credential Highway: How Self-Sovereign Identity Unlocks Property Rights for the Bottom Billion*, https://www.newamerica.org/future-land-housing/reports/ssi-credential-highway/, New America, Washington, DC, USA, 2019, https://www.newamerica.org/future-land-housing/reports/ssi-credential-highway/.