Decentralized ID and Self-Sovereign Identity Solutions Using Blockchain: A Systematic Literature Review

Irene Priscila Cedillo Orellana
Department of Computer Sciences/Universidad de Cuenca
Cuenca, Ecuador *priscila.cedillo@ucuenca.edu.ec*

Andrea Paulina Rodriguez Zuñiga
Department of Computer Sciences/Universidad de Cuenca
Cuenca, Ecuador *andreap.rodriguez@ucuenca.edu.ec*

Alberto Carlo Soriano Eusebio
Department of Computer Sciences/Universidad de Cuenca
Cuenca, Ecuador *alberto.soriano@ucuenca.edu.ec*

Elizabeth Viviana Cabrera Avila
Department of Computer Sciences/Universidad de Cuenca
Cuenca, Ecuador *vcabrera@dca.ufrn.br*

Paúl Esteban Cárdenas Delgado
Department of Computer Sciences/Universidad de Cuenca
Cuenca, Ecuador *paul.cardenasd@ucuenca.edu.ec*

Abstract

Today users do not have control over their digital identities. To access and validate them, they must authenticate through a third party which they must trust. This is a problem that researchers have addressed with the blooming of new paradigms such as Decentralized Identifiers (DIDs) and Self-Sovereign Identity (SSI). In this context, blockchain appears as a new path that ensures traceability to all transactions. Although there are several primary studies related to this topic, there needs to be more contributions that condense all the information of research groups in a secondary study, which summarizes the techniques and trends of DIDs and SSI. Therefore, this paper presents a systematic literature review to identify research trends, challenges, and solutions to DID and SSI using blockchain. Twenty-three papers published from 2014 to October 2022 were selected following inclusion and exclusion criteria. The investigation points out how most DIDs and SSI solutions are set in the general domain as academic postulations that could be released in the commercial field.

Keywords: decentralized ID, self-sovereign, DID, SSI, blockchain

1. Introduction

Within a world where subjects have started to lose trust in centralized models that look deprecated and have lost effectiveness, concepts such as Decentralized Identifiers (DIDs) and Self-Sovereign Identity (SSI) have gained a role play in the security field. This is because DIDs and SSI relate payloads with a subject after verification processes without any intermediary actor like the government. Similarly, blockchain has appeared as a new path to transparency with its non-repudiation features that ensure traceability to all transactions. Therefore, it is unsurprising that DIDs and SSI solutions have adopted implementations over blockchain technologies. Thus, it is a fact that DIDs and SSI are proximate topics, so often taken as equals, that the differences between them could be shown as merely conceptual and with many research opportunities and challenges that need to be taken. In this paper, we conducted a systematic literature review to identify research trends and challenges to DIDs and SSI blockchain-based solutions while searching for gaps in the field that can serve as a starting point for further research.

A systematic review identifies, analyzes, and interprets unbiasedly all the evidence on a specific topic presented in relevant primary studies; it uses a structured approach to minimize bias and maximize objectivity [5]. Several primary studies have been carried out in this context, but the information that provides insights to researchers is scattered in several digital libraries and databases. Besides, there are no secondary studies that perform a summary of the research state in this field. Then, it is necessary to have a study that joins all the information in a systematic review that shows research gaps and the proposed solutions condensed.

We obtained twenty-three papers collected in the digital libraries ACM, IEEE Xplore and Springer Link, which were selected after applying the inclusion and exclusion criteria.

The remainder of this paper is structured as follows. Section 2 outlines general concepts of DIDs and SSI, including a discussion about existing systematic literature reviews in the field. The research methodology is described in Section 3, and individual results are presented in Section 4. Section 5 discusses the relevance and contributions of the systematic literature review. A validation of the systematic review is presented in Section 6. and last but not least, Section 7 presents conclusions and future work.

2. Background

This section explains concepts related to DIDs, SSI, and blockchain technologies to readers so they can understand the field where this investigation occurred.

Decentralized ID

According to Sporny et al. [12], Decentralized Identifiers (DIDs) are a new class of subject identifiers that enable verifiable decentralized digital identities. A subject can be a person, organization, thing, or data model. Unlike typical federated identifiers, DIDs can be decoupled from centralized registries, identity providers, and certificate authorities. DIDs are Uniform Resource Identifiers (URIs) that associate a DID subject with a DID document, allowing reliable interaction with a subject; they are designed to enable individuals and organizations to use systems they trust to generate their credentials.

Self-Sovereign Identity

Related to Self-Sovereign, a subject that owns more than one DID can present claims or related credentials without needing an intermediary. Then, Self-Sovereign does not allow individuals or organizations to control all aspects of their identity that are provided by external parties such as, for example, the government [14].

Blockchain Technology

Blockchain is a shared and unalterable ledger that facilitates the process of recording transactions and tracking tangible or intangible assets in a business network. It is a distributed ledger technology to which all network participants have access. Furthermore, it is distinguished for its unalterable transaction log; thus, transactions are recorded only once, guaranteeing no one can modify them [15].

Existing systematic reviews for DID and SSI

Several searches were conducted in the IEEE Xplore, ScienceDirect, and ACM Digital Library to establish the existence of other systematic reviews related to that presented in this paper. The following search string was used: *(decentrali* OR self-sovereign OR self sovereign) AND (id OR identi*) AND (blockchain OR block chain OR block-chain) AND (systematic) AND (review)*. However, only two results were found: an SSI systematic and mapping review [9] in 2021 and a DID and SSI mapping review [11] in 2020.

The nearest study to our systematic review is [11]; however, as it is a systematic mapping, the authors are centered on classifying studies without a deep understanding and analysis of each one. On the other hand, the study presented in [9] analyzes theoretical and practical advances in Self-Sovereign Identity. This work proposes different extraction criteria from our review; its main criteria seek to examine: i) what practical problems associated with SSI have been introduced and solved, ii) How SSI is formally specified, and iii) what concept/idea is introduced or refused.

Schardong and Custódio [9] have systematically mapped and classified theoretical and practical advances in Self-Sovereign Identity, including both peer-reviewed and non-peer-reviewed literature that expanded the conceptual discussion on what SSI is. Also, it introduced mathematical formulation to define SSI-related problems, presented a novel pragmatic problem related to the SSI ecosystem, and presented a solution to it. Čučko and Turkanovi [11] published a mapping review analyzing 120 research papers concerning six criteria: i) contribution, ii) domain, iii) IT Field, iv) research type, v) research method, and vi) place of publication. The results show that research in the DIDs and SSI field had increased by 96.7 % from 2017 to 2021.

In the literature, it has been found several secondary studies (not systematic or mapping literature reviews) released in the DID and SSI field, including or not blockchain as their implementation technology. Some of these studies are detailed below.

Gilani et al. [4] provide an overview of challenges, research gaps, and trade-offs of the current state of the art on privacy-preserving solutions in decentralized systems using blockchain; that paper shows central concepts of SSI, including the components of identity proofing and authentication solutions for different solutions such as uPort, Blockstack, SelfKey, Civic, and Shocard. Bartolomeu et al. [1] reduce the scope and discuss SSI's use cases, technologies, and challenges in the IoT field; this study also analyzes some popular self-sovereign identity frameworks: Hyperledger Indy, uPort, Blockstack, Veres One, and Jocolom, comparing them respecting seven characteristics: main goal, development, verifiable credentials, distributed ledger, transactions per second, transaction delay, and transaction cost. Every mentioned framework leverages blockchain technology. Kuperberg [6] has surveyed a wide array of blockchain-based solutions providing an evaluation framework for decentralized and SSI management systems; it included an extensive set of requirements covering ecosystem aspects, end-user functionality, mobility and overhead aspects, compliance/liability, EU regulations, standardization, and integration.

In contrast to [1], our review includes papers about DID and SSI fields. Also, our study is diverse from [6] as our focus is the domain incursion and solutions trends in those domains while considering security assets (access control policies, authentication method, and encryption type). Finally, at this final issue, our investigation differs from [4] because our scope is broader; both SSI and DID solutions are covered and include applications, architectures, prototypes, schemes, and frameworks, while [4] only analyzes commercial applications associated with SSI.

3. Research Method

A systematic review is developed using a rigorous, reliable, repetitive, and extended methodology. This review follows the steps presented by Kitchenham methodology [5]: i) planning the review, ii) conducting the review, and iii) reporting the review.

3.1. Planning the review

This systematic review aims to obtain and analyze the trends, challenges, and solutions for assessing SSI and DIDs paradigms based on blockchain technology, primarily inner domains. The study will identify gaps and new research areas for future investigation.

Considering the chosen methodology, in this section, we present the research questions, identify the sources for the search, present the exclusion and inclusion criteria for selecting the

Table 1. Inclusion and Exclusion Criteria

Inclusion Criteria	Exclusion Criteria
Studies presenting usages to Decentralized ID in a specific domain. Studies presenting solutions applying Decentralized ID. Studies presenting usages of Self-sovereign Identity in a specific domain. Studies presenting solutions applying Self-sovereign Identity	Duplicate reports in different sources. Short papers with less than five pages. Papers not written in English. Introductory papers for special issues, books, workshops, or posters.

primary studies, establish the strategy for extracting the information, and define the synthesis strategy.

To meet the review's objectives, this review answers the following research questions:

RQ1: Which IT fields have had Decentralized ID or Self-Sovereign Identity solutions?

RQ2: Which tools addressing Decentralized ID or Self-Sovereign Identity are there in the academy?

RQ3: Which security challenges have been addressed in Decentralized ID or Self-Sovereign solutions Identity?

Identification of data sources and searches strategy

To obtain the primary studies, the digital libraries of the most relevant organizations in the Software Engineering community were consulted: IEEE Xplore, ACM Digital Library, and Springer Link. We also applied a snowball search method in the first level to obtain more possible papers addressing the topic. The search covered the period from 2014 to October 2022. This period has been chosen due to 2014 was the year in which the Credentials Community Group was formed, hosted by the World Wide Web Consortium (W3C), a community that has worked in the area of SSI and DIDs since then [5].

The research included conferences and journal papers. The search string used was: *(decentrali* OR self-sovereign OR self sovereign) AND (id OR identi*) AND (blockchain OR block chain OR block-chain).* We considered the titles and abstracts of the papers for searching. The search string notation was adapted for each digital library since each uses a different syntax.

Selection criteria for primary studies

The automatic search of papers in digital libraries, using the search string, includes articles that differ from the topic addressed in this study, even though they have the words of the string when reading titles and abstracts. Therefore, for the consistent inclusion or exclusion of articles, at this stage, we rely on the inclusion and exclusion criteria detailed in Table 1; studies that meet at least one of the following criteria will be accepted or rejected as appropriate.

Data Extraction Strategy

We divided the research questions into several criteria to extract the data from the set of selected primary studies. Appendix A summarizes the data extraction criteria for classifying the collected solutions and applications. Each data extraction criterion and its options are explained as follows:

- **Criterion 1: Information Technology(IT) field.** This and the second criterion indicate the current scope of the academic solutions to DIDs and SSI using blockchain. This criterion classifies the solutions in one of nine IT fields adopting the classification proposed in [11]: IoT, Security, Privacy, Trust, User Experience (UX) and Usability, Patterns, IT Architecture, Decentralized Public-Key Infrastructure (DPKI).

- **Criterion 2: Domain**. The solutions were classified using the suggested domains in [11]: Education, Government, Health care, Retail and eCommerce, Banking and Financial, Industry, Supply chain, Transport, General, and Others.
- **Criterion 3: Blockchain Type**. To discover which types of blockchain is used to apply each solution, it was established the following classification: Public, Hybrid, Consortium, and Private.
- **Criterion 4: Software pricing**. This criterion identifies whether the application has any monetary cost to the user. There are three categories: i) Free, ii) Paid and iii) Test phase (if the product is in the testing phase or is a prototype).
- **Criteria 5: Solutions and Application**. Solutions and Applications can be divided according to their nature into Architecture, App, Methodology, Prototype, and Others [2]. Garnica-Bautista et al. [3] consider three primary types of applications: Website, Desktop and Mobile Application; all papers with this kind of solutions are included in the category App.
- **Criterion 6: Control Access Model**. This criterion determines the approach to applying policies and deciding on resource access. Stalling and Brown [13] present some models: Attributes-Based Access Control (ABAC), Role Based Access Control (RDAC), Mandatory Access Control (MAC), and Discretionary Access Control (DAC).
- **Criterion 7: Authentication method**. This criterion refers to the process carried out by a user to access a system or resource, according to [13] the authentication methods are: Password-based, Token-based, Biometric Authentication, and Remote User.
- **Criterion 8: Cryptographic algorithms**. If a solution or infrastructure has a tool using symmetric encryption algorithms, it is classified as private key; otherwise, if it uses asymmetric encryption it is a public key.

3.2. Conducting the review

The search to identify primary studies in digital libraries was conducted in October 2022. The process resulted in ninety-seven papers being obtained from those digital libraries. Some papers were duplicated due to their appearance in at least two digital libraries. Also, nine papers were added from a manual search.

The papers were selected following inclusion and exclusion criteria. The most significant aspect of this selection was that many of the papers from digital libraries were included as potential papers because their titles and abstracts contained the search string; however, once the titles and abstracts had been read, even after scanning the full paper we discovered that the topic of the paper was different to that of our investigation. So then, twenty-three papers were selected for our study. Fig 1 shows the number of papers found in each digital library, the papers screened at each stage, and the total number of studies included in the review.

4. Results and Analysis of the Systematic Review

The systematic review found twenty-three primary studies. In these papers, we gathered information about twenty-three different DIDs and SSI solutions (each one addressed in one paper) implemented by blockchain technology, these papers is displayed in Appendix B. A summary of the most relevant results obtained from the extraction criteria phase is presented in Table 2. To the criteria EC1, EC2, and EC7 the percentage add surpasses the 100% because the solutions analyzed could be placed in more than one item of the criterion: the criteria do not have exclusive items. Each data extraction criterion and the obtained results are discussed.

- **Criterion 1. IT field**. In general. “Patterns” (0%) and “UX and Usability” (0%) are the domains in which the investigations present a gap that could be assessed.
- **Criterion 2. Domain**. The results in this criterion indicate a marked contrast between the solutions presented. Most of the solutions (65%) were implemented in the “General”

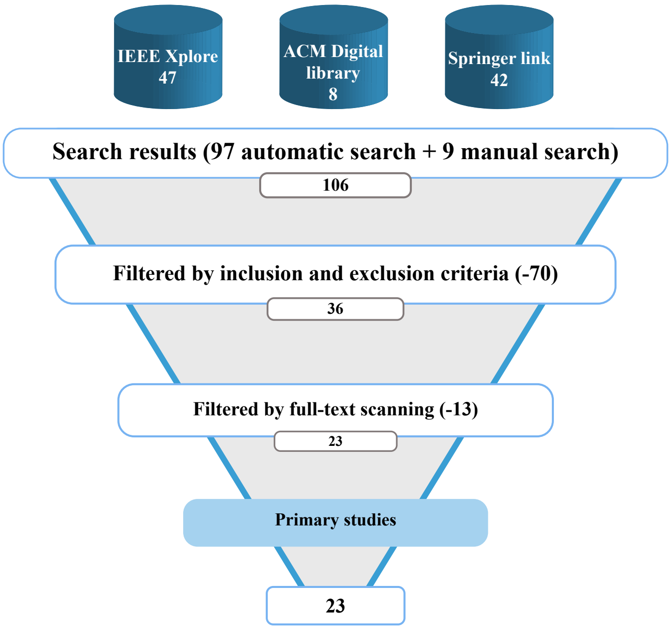
IEEE Xplore
47
ACM Digital library
8
Springer link
42
Search results (97 automatic search + 9 manual search)
106
Filtered by inclusion and exclusion criteria (-70)
36
Filtered by full-text scanning (-13)
23
Primary studies
23

Fig. 1. Diagram of the papers selection procedure.

domain (S01, S02, S04, S06, S07, S08, S10, S11, S12, S13, S14, S18, S20, S21, S22); the remaining domains present a gap that could be assessed.

- **Criterion 4. Software pricing**. Most of the reviewed papers were categorized within the “test phase” because they are architectures, frameworks or schemes that can be used to generate a solution (S02, S03, S04, S05, S07, S09, S10, S12, S13, S15, S17, S18, S19, S20, S21, S22, S23). No applications have been presented in a paid way to the public; we found that only one tool called "uPor" has been freely available to the public (S08). It is an open-source identity management system oriented to common people or organizations, users can securely publish their identity, transfer their credentials, sign transactions and control their keys and data. It could be used as a web application on desktop and mobile platforms.
- **Criterion 5. Solutions and applications**. The results indicate that little over half of the solutions were implemented in the “Others” category, in this group are systems, schemas, protocols and frameworks (65%; S01, S03, S04, S06, S07, S11, S12, S13, S14, S16, S18, S20, S21, S22, S23).
- **Criterion 6. Access control models**. The results indicate that 26% of the solutions have not considered or discussed access control when proposing their solutions (S07, S15, S16, S17, S22, S23). Of the remaining papers, 48% prefer the “ABAC” model to access control (S03, S04, S05, S06, S09, S10, S14, S18, S19, S20, S21). The strength of the ABAC approach is its flexibility and expressive power [13]. Using ABAC the "DIAM-IoT" framework grants device owners to define user-specific rules for control of their device data.

4.1. Trends of DIDs and SSI Blockchain-based solutions

In this subsection, we present the study’s contribution that responds to the research questions about trends that exist when a solution is designed in the DIDs and SSI fields.

The bubbles diagrams in Figs 2 and 3, relate the extraction criteria to generate conclusions and results from these investigations. In Fig 2, the x-axis represents EC5: the Type of Solution of the tool, while on the y-axis, we have the Domain and the IT field. It shows that most DID

Table 2. Data extraction criteria results

Extrac. Criteria	Possible answers	#	%	Extrac. Criteria	Possible answers	#	%
EC1 **IT field**	IoT	4	17	**EC2** **Domain**	Education	0	0
	Security	12	52		Government	1	4
	Privacy	14	61		Health Care	1	4
	Patterns	0	0		Retail and eCommerce	1	4
	Authentication DPKI	8	35		Banking and Financial	1	4
	IT	3	13		Industry	3	13
	Architecture	3	13		Supply chain	0	0
	Trust	10	43		Transport	5	22
	UX and Usability	0	0		General	15	65
					Others	1	4
EC3 **Blockchain type**	Public	13	57	**EC4** **Software pricing**	Free	1	4
	Private	3	13		Paid	0	0
	Hybrid	1	4		Test phase	17	74
	Consortium	1	4		No App	5	22
	Not mentioned	5	22				
EC5 **Solution and applications**	Architecture	3	13	**EC6** **Control access model**	ABAC	11	48
	App	5	22		RDAC	1	4
	Methodology	0	0		MAC	3	13
	Prototype	0	0		DAC	2	9
	Others	15	65		Not Mentioned	6	26
EC7 **Authentication method**	Password-based	6	26	**EC8** **Cryptographic algorithms**	Private key	0	0
	Token-based	2	9		Public key	21	91
	Biometric	5	22		Not mentioned	2	9
	Remote user	13	57				
	Not mentioned	2	9				

and SSI solutions are set in the General domain and can be adapted to others as Education or Supply chain. Within the General domain, architectures and applications have been developed; however, the most significant number of solutions are schemes, systems, protocols and frameworks (categorized in others). It proves the DID and SSI blockchain solutions are still in a child phase with a vast spectrum to be fulfilled.

Although the solutions are in the general domain, they have penetrated more equally into IT Fields. Attractive solutions addressing IT Architecture, Security, and Privacy fields are presented. Schanzenbach et al. (S10) developed “reclaimID”, an architecture that allows users to reclaim their digital identities by securely sharing identity attributes without needing a centralized service provider. Similarly, Stokkink and Pouwelse (S09) show a blockchain-based digital identification solution to provide identity in a situation of mutual mistrust. Their solution is based on a general model of proven claims, for which verifications of the veracity from outside sources must be gathered. Moreover, for COVID-19 test takers, Hasan et al. (S15) implemented a solution with digital medical passports (DMP) and immunity certificates. It describes smart contracts successfully tested and designed to maintain test-takers’ digital medical identities and enable rapid responses from the appropriate medical authorities. Definitely, we believe that the solutions categorized within general postulations should be implemented in a specific area such as health care, education, government, or industry, so that solutions that are not currently commercial products can be used by the general public.

The systems (S03, S07, S21, S22), schemas (S11, S12, S18), protocols (S01, S14), and frameworks (S04, S13, S16, S20) developed using blockchain technology represent 65% of analyzed papers (15); however, they are not yet practical tools available to the public ("Test Phase"). This fact could change if these solutions progress quickly and get released as Web services, Desktop or Mobile applications. IMEI Database (S02), NEXTLeap (S05), or reclaimID (S10) are examples of potential future applications; now, they have created only test applications to validate their proposed approaches.

Regarding blockchain, Public blockchains (e.g; Hyperledger Indy and Ethereum) are the trend to apply DID and SSI applications (57%). We observed there are vast possibilities to grow

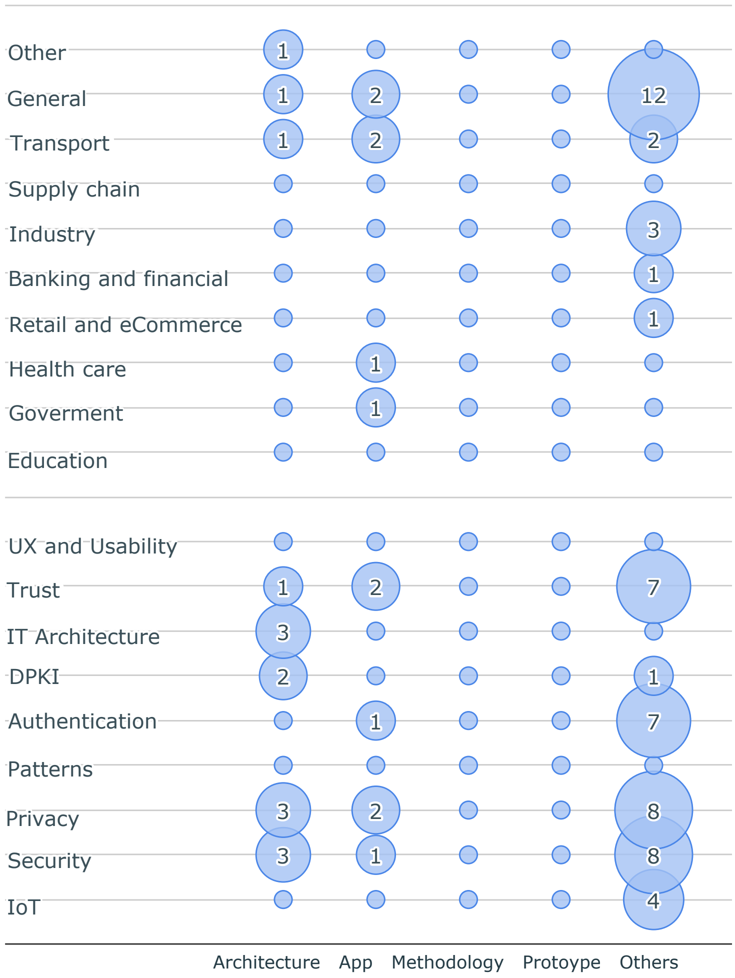

Fig. 2. Comparison between EC5: Solutions and Applications with EC1: IT Field and EC2: Domain.

the contributions of DIDs and SSI in the academic and industrial fields.

This research also raises how much security criteria (RQ3) are currently considered to propose solutions. Fig 3 shows that ABAC is primarily used to guarantee access control, and the most used authentication method is Remote-user (57%). Moreover, for encryption, all public blockchains use public-key algorithms to access.

We found exciting proposals addressing security criteria, such as those in S06, S09, and S20. In the first study, a proof of concept of a Decentralized OpenID Connect Provider is performed relying on an auth encrypted, that is, an authenticated public key encrypted and signed by DID; in the second paper, the authors expose a blockchain-based digital identity solution without relying on any single trusted third-party, achieving legally valid identity at the passport level; and the latest proposal introduces a blockchain-based identity framework for IoT correlation device signatures (low-level identities) and owners identify themselves to use in authentication credentials and ensure that any IoT entity usually behaves.

4.2. Challenges faced by DID and SSI Blockchain-based solutions

DID and SSI are starting to show their potential; consequently, they are technologies facing challenges. Two studies have pointed out crucial features to have in mind when doing an inves-

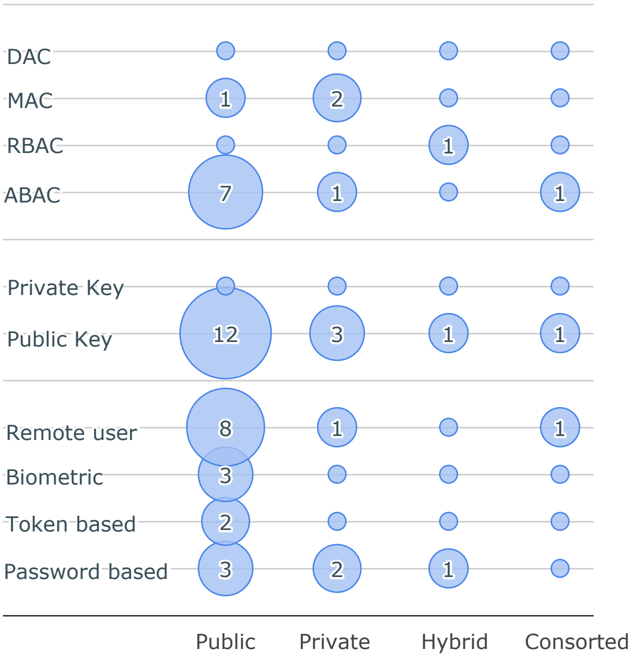

Fig. 3. Comparison between EC6: Access Control Model with EC7: Authentication method, EC8: Cryptographic algorithms, and EC3: Blockchain type criteria.

tigation in this fields[1] [4]; our systematic review remarks on areas in need of future work:

- **Scalability**: currently, many proposed novel DIDs and SSI blockchain-based solutions are either: prototypes, architectures, frameworks, or schemas with implementation promising scalability in the industrial field. For this reason, releasing applications into the market is needed.
- **User experience**: users have poor knowledge of the concepts of DIDs and SSI, but also about Public-Key Infrastructures (PKIs) and private keys management. This situation limits the scope of getting non-technical users to try the solutions.
- **Patterns**: among the solutions analyzed, there are no proposed patterns when developing schemes, architectures, or frameworks. Patterns are essential as future systems and applications can be developed easier if they follow a proven basis and have good practices to apply.
- **Security criteria**: related to access control criteria, it should be considered deeply in more studies to propose solutions for generating trust in the user who uses a solution and preventing them from vulnerabilities. The 26% of analyzed studies in this review do not consider access control when proposing solutions.

5. Discussion

In this section, the relevance and contribution of the results of the systematic review are discussed pointing out strengths and weaknesses of the evidence collected. Since our systematic review's validity has been considered a relevant aspect, this section also discusses its possible limitations and how they can be addressed.

5.1. Strengths and Weaknesses

The main strengths are related to the IoT field addressed by the papers analyzed and the type of solutions evaluated. Concerning the IoT field, the systematic review gathered many solutions considering several fields, meaning how many solutions pointed out that DID and SSI systems could get involved transversally in IoT technologies. However, there is still the position that all the fields need more investigation, considering even more parameters presented in this investigation, such as Authentication, DPKI, and UX and Usability.

5.2. Implications for research and practice

The contributions of this paper have implications for both research and practice. The review shows the current state of the art with a certain level of guaranteed quality in the results. Knowing the state of the art will help the community detect deficiencies and identify new lines of research. For researchers and practitioners, the result of this systematic review is a catalog of different solutions. The results permitted discovering which domains and fields are a trend when implementing solutions. It has been possible to know what type of blockchain technology and the security criteria must be applied in a specific case. Finally, some challenges in the DID and SSI areas were detected.

We consider it appropriate to include solutions presented in white papers such as those described by Bartolomeu et al. [1]; it would be important to know the alternatives presented in the industrial field and contrast them with those presented by the academy.

6. Validation of the systematic review

We attempted to select the research string that permits collecting studies whose information helps to answer the research questions. Acronyms like DID or SSI were not part of the string because they can refer to concepts different to used in this investigation (e.g., DID could be found in so many papers as the DO verb in past tense). The papers included in this review were limited from 2014 to October 2022, guaranteeing that the information is current. Only documents with a minimum of five pages were considered to ensure the papers provide sufficient detail and analysis. Finally, the search discarded documents that were not in English.

6.1. Validation of selection of primary studies

To validate the two reviewers' correct selection of the primary studies and the accurate description of the inclusion and exclusion criteria, we randomly selected ten papers and the reviewers labeled each one as excluded or included (according to the criteria). The results were analyzed through Cohen's Kappa coefficient, a statistical used to assess the reliability of classifications made by two raters into two or more categories; its value ranges from -1 to 1, with 1 indicating perfect agreement. Cohen's Kappa coefficient for agreement on inclusion in the review was 0.882 for two raters. According to Landis and Koch, there exists an almost perfect deal [7].

6.2. Validation of data extraction criteria and classification

The inconveniences about the extraction criteria and classification are related to errors in defining the criteria and a lousy category. Regarding the first aspect, the established extraction criteria are clear and understandable; they do not give rise to confusion that triggers problems in the classification. A process similar to that applied in validating the selection of primary studies was followed to validate the paper's classification. We randomly selected five studies included in the review (each study is analyzed with forty-one measures). The two reviewers categorized the studies using the extraction criteria and the results were analyzed using Cohen's Kappa coefficient. The coefficient was 0.80 interpreted as substantial agreement.

6.3. Quality assessment of the primary studies

To evaluate the quality of the papers, we analyze their relevance considering the importance of the journals or conferences where they were published. The articles were classified into three categories: “very relevant,” “relevant” and “not so relevant.” This aspect was rated by considering the CORE Conference Ranking (A*, A, B, and C) and the Scimago Journal and Country Rank (SJR)(Q1, Q2, Q3 or Q4). The primary studies were classified as follows:

- **Very relevant:** papers published in conferences rated as A* or A in the CORE classification or published in journals rated as Q1 or Q2 in the SJR classification. Also in this category are papers from conferences that don’t have a Core Ranking but publish relevant papers about Decentralized Identifiers, Self-Sovereign Identity and blockchain. All papers included have a score of 10 points.
- **Relevant:** papers published in conferences rated as B or C in the CORE classification or as Q3 or Q4 in the SJR classification. Also, include papers published in journals excluded from the SJR list. The papers received a score of 5 points.
- **Not relevant:** paper published in conferences not included in the CORE classification. They have a null score (0 points).

  Each paper received a rating based on the detailed criteria; the average value of this quality assessment was 8.2 points. This indicates that the selected papers were published in relevant conferences or journals.

7. Conclusions and Future Work

The systematic literature review conducted in this paper aimed to identify research trends, challenges, and solutions in the field of Decentralized Identity and Self-Sovereign Identity technologies using blockchain. In that sense, this paper has highlighted the current state of the mentioned technologies and the research in these fields. This review verified persistent challenges previously identified, which marks the necessity to spread the scope of the investigation.

Most papers focus on validation research and solution proposals; they are not yet applications that can be presented to the public. Several studies have been conducted without a specific domain. However, the potential of SSI in various areas such as Transport, Healthcare, Government, Banking and Finance has been recognized, as well as the need to include more security criteria in solutions. Access control and Authorization are the gaps when proposing solutions. In addition, future research must be done on Usability, User Experience (UX), Patterns, and good practices to fulfill quality criteria.

There is still a vast scope for further research and development in DIDs and SSI. We must continue exploring and understanding the opportunities and challenges of this technology. This review can be a basis for further research in DIDs and SSI development.

Acknowledgments

The authors would like to thank to Corporación Ecuatoriana para el Desarrollo de la Investigación y Academia - CEDIA for the financial support given to the present research, development, and innovation work through its CEPRA program, especially for the “Análisis y aplicación de formas de interacción humano-computador (HCI) en una herramienta tecnológica de Comunicación Aumentativa y Alternativa (CAA) basada en pictogramas, que ayude a las personas adultas mayores a comunicarse con su entorno" fund.

References

1. Bartolomeu, P.C., Vieira, E., Hosseini, S.M., Ferreira, J.: Self-Sovereign Identity: Use-cases, Technologies, and Challenges for Industrial IoT. IEEE International Con-

ference on Emerging Technologies and Factory Automation, ETFA. 2019-September, pp. 1173–1180 (2019)

2. Camburn, B., Viswanathan, V.K., Linsey, J.S., Anderson, D., Jensen, D., Crawford, R.H., Otto, K.N., Wood, K.L.: Design prototyping methods: state of the art in strategies, techniques, and guidelines. Des. Sci. 3 (2017)
3. Garnica-Bautista, X., Maita-Tepán, X., Mejía-Pesántez, M., Muñoz-Guillén, L.: QuizTV: A Game for Interactive Digital Television. Development Considerations Using the Ginga-NCL Middleware. In: 2018 International Conference on Information Systems and Computer Science (INCISCOS). pp. 246–253. (2018)
4. Gilani, K., Bertin, E., Hatin, J., Crespi, N.: A Survey on Blockchain-based Identity Management and Decentralized Privacy for Personal Data. In: 2020 2nd Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS). pp. 97–101. (2020)
5. Kitchenham, B., Charters, S.: Guidelines for performing Systematic Literature Reviews in Software Engineering. 2 (2007)
6. Kuperberg, M.: Blockchain-Based Identity Management: A Survey From the Enterprise and Ecosystem Perspective. IEEE Trans Eng Manag. 67 (4), 1008–1027 (2020)
7. Landis, J.R., Koch, G.G.: The measurement of observer agreement for categorical data. Biometrics. 33 (1), 159–174 (1977)
8. Lawrie, B., William, S.: Computer security: principles and practice. Pearson, Boston (2018)
9. Schardong, F., Custódio, R.: Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy. Sensors. 22 (15), (2022)
10. Serugga, J., Kagioglou, M., Tzortzopoulos, P.: Front End Projects Benefits Realisation from a Requirements Management Perspective—A Systematic Literature Review. Build. 10 (5).(2020)
11. Čučko, Š., Turkanović, M.: Decentralized and Self-Sovereign Identity: Systematic Mapping Study. IEEE Access. 9, 139009–139027 (2021)
12. Sporny, M., Longley, D., Sanadello, M., Redd, D., Steele, O. Allen, Decentralized Identifiers (DIDs) v1.0, https://www.w3.org/TR/did-core/, Accessed: April 10, 2023.
13. Stallings, W., Brown, L.: Computer Security: Principles and Practice. Prentice Hall Press, USA (2014)
14. Wagner, K., Némethi, B., Renieris, E., Lang, P., Brunet, E., Holst, E.: Self-sovereign Identity A position paper on blockchain-enabled identity and the road ahead. Identity Working Group of the German Blockchain Association (https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018.pdf). (2018)
15. What is blockchain technology?-IBM Blockchain | IBM, https://www.ibm.com/topics/blockchain, Accessed: April 10, 2023

Appendices

Appendix A

Extraction criteria. Can be accessed in:
https://bit.ly/SLR-DIDs-SSI-AppendixA

Appendix B

List of papers selected in the systematic review. Can be accessed in:
https://bit.ly/SLR-DIDs-SSI-AppendixB