IEEE Access
Multidisciplinary ⋮ Rapid Review ⋮ Open Access Journal

Received August 25, 2021, accepted September 22, 2021, date of publication October 4, 2021, date of current version October 15, 2021.

Digital Object Identifier 10.1109/ACCESS.2021.3117588

Decentralized and Self-Sovereign Identity: Systematic Mapping Study

ŠPELA ČUČKO AND MUHAMED TURKANOVIĆ
Faculty of Electrical Engineering and Computer Science, University of Maribor, 2000 Maribor, Slovenia

Corresponding author: Špela Čučko (spela.cucko@um.si)

This work was supported in part by Slovenian Research Agency (Research Core Funding) under Grant P2-00577, and in part by the European Union's Horizon 2020 Research and Innovation Program [Digital Europe for All (DE4A)] under Agreement 870635.

ABSTRACT Self-Sovereign Identity is an emerging, user-centric, decentralized identity approach utilizing some form of decentralized technology. It provides a means for digital identification without reliance on any external authority, enabling entities to control their identity and data flow during digital interactions while enhancing security and privacy. With the rise of blockchain technology, Self-Sovereign Identity is gathering momentum in academia and industry while the number of research papers increases rapidly. However, Self-Sovereign Identity is still a young unstructured field in its early stages of research. Thus, a systematic mapping methodology was adopted to provide a coarse-grained overview of decentralized and Self-Sovereign Identity and structure the research area by identifying, analyzing, and classifying the research papers according to predefined parameters, which is to say according to their contribution, application domain, IT field, research type, research method, and place of publication. Furthermore, the nature and scope of the research were determined, while existing research topics, gained insights into trends, demographics, challenges, gaps, and opportunities for future research were also presented. The results suggest that validation research and solution proposals prevail, addressing decentralized identity in a general matter. Papers mainly propose systems/solutions, architectures, and frameworks, focusing on authentication, security, privacy, and trust, while there are hardly any studies researching usability, user experience, patterns, and good practices.

INDEX TERMS Blockchain, decentralized, identifier, identity, self-sovereign, self-sovereign identity, SSI.

I. INTRODUCTION

There is a growing interest in decentralized technology, especially blockchain, and its application in different domains, including identity management [1], [2]. In the spring of 2015 [3], the identity community recognized blockchains' potential for utilizing an identity layer on the internet as its underlying infrastructure can facilitate an exchange of assets and enable trust in relationships between entities without the need for a centralized intermediary. Although blockchain initialized developments in the field of decentralized identity, it is not always required for implementation, as peer decentralized identifiers (peer DIDs) can standalone and present a method that is entirely off-ledger.

Unlike centralized systems, where control and power are in the hands of central authority, decentralization entails the distribution of control among the participants in the system, thus, represents a shift of power from central authorities to entities, e.g. users/identity holders, enabling user-centric systems. The latter is crucial, especially in the field of identity management, where currently sensitive, Personal Identifiable Information (PII) is stored in centralized repositories, posing a threat to privacy and security. Due to personal data misuse and data breaches that have led to countless concerns, such as PII leaks and identity thefts, the decentralized identity approach, more narrowly Self-Sovereign Identity (SSI), is gathering momentum and interest in academia and industry. In addition, it is being considered by many organizations and governments around the world [4]. Moreover, it is being standardized by World Wide Web Consortium (W3C) [5], [6] and Decentralized Identity Foundation (DIF) [7], striving to establish a new decentralized identity ecosystem. Another important initiative worth mentioning is the European Commission's framework proposal for trusted, secure, and widely usable European Digital Identity, which will enable all Europeans to digitally prove their identity and

The associate editor coordinating the review of this manuscript and approving it for publication was Chunming Gao.

This work is licensed under a Creative Commons Attribution 4.0 License. For more information, see https://creativecommons.org/licenses/by/4.0/

provide certain personal attributes, to access digital services across the Union. Meanwhile, it will empower users to be in control of their data through identity wallets [8].

As the field is gaining momentum and becoming popular in academia and industry, the number of research articles, initiatives, and solution proposals is increasing rapidly. Yet, there is still some ambiguity, misunderstanding, and disagreement about key principles and concept definitions. The core of the decentralized identity, precisely the Self-Sovereign Identity concept, lies behind the objectives to provide a means for digital identification, with minimizing or even eliminating reliance on a central authority, eliminating a single point of failure. Allowing entities to create identifiers independently of any external party, gather identity claims from various sources, securely and autonomously store, manage and distribute/share them while remaining in full control of identifiers and associated identity data. Furthermore, with the use of decentralized technologies and cryptographic primitives, security and privacy are enhanced, and transparency and data minimization can be achieved. However, SSI is still a young unstructured field in its early stages of research, with many research opportunities and challenges that need to be tackled. Thus, this study aims to gain a broad insight into existing knowledge by conducting a Systematic Mapping Study, classifying research papers into pre-defined categories, providing a coarse-grained overview, and structuring the research area. Furthermore, we aim to identify research trends, demographics, and potential research gaps, that can serve as a starting point for further research.

The remainder of this paper is structured as follows. In section II, the general concepts of decentralized and Self-Sovereign Identity are outlined. Section III presents related work regarding secondary studies and highlights the differences to our work. The research methodology is described in Section IV, and respective results are presented in Section V. Section VI discusses the results of the systematic mapping study concerning the research question. Last but not least, Section VII presents conclusions and future work.

II. DECENTRALIZED IDENTITY

The decentralized identity model is enabled by the emergence of decentralized technologies, providing the ability to eliminate intermediaries. Therefore, the goal of decentralization is to minimize or even fully eliminate a single point of compromise or failure by minimizing or even removing a central authority [9] that serves as an identity provider (IdP) and is responsible for identity administration and management. In traditional identity management systems, personal data, i.e. identity attributes, are centrally stored under the control and management of IdP. Influenced by IdPs' internal privacy and security policies that greatly affect data usage and its safety. Meanwhile, requesting parties as well as entities themselves must trust the IdP regarding the availability, integrity, and confidentiality of attributes. Alternatives to maintaining centralized storage are decentralized approaches [10]. Some are similar to traditional identity solutions, where existing trusted credentials from third parties are used for identity verification or authentication. However, the central IdP is accompanied by decentralized storage, where validated attestations are stored on a distributed ledger for later validation, presenting the main differentiation [11].

On the other hand, decentralized approaches do not rely on any centralized IdP. In contrast with traditional, centralized, and federated approaches that are account-based or digital certificate-based and require entities, e.g. users to trust and rely on identity providers, the latter is based on peer-to-peer relationships between interacting parties. Hence, the ecosystem consists of various entities that enact roles formerly performed by a central authority [9]. It enhances decentralization, transparency, and user control [12] in transactions involving identity information. It usually relies on some form of decentralized ledger technology (DLT), blockchain, distributed file system, or another decentralized system, such as Hashgraphes and Tangle [13]. Open-source Hyperledger projects can also be used, as Hyperledger Indy was specifically built for the implementation of decentralized identities. Thus, it can be used standalone or with other blockchains [14], [15]. The use of blockchain is the most popular, however not mandatory for the implementation of decentralized identity as it can also be achieved with mentioned alternatives [13]. Nevertheless, blockchain may facilitate the implementation of decentralized identity, and it coincides with some desirable properties of Self-Sovereign Identity [16].

A. SELF-SOVEREIGN IDENTITY

Self-Sovereign Identity (SSI) is an emerging, decentralized identity approach that enables entities (e.g. individuals, organizations, and objects) to fully control their digital identity without reliance on any external authority, eliminating a single point of failure. SSI presents a paradigm shift, a shift in power and control, from identity and service providers to users, who must be central to the administration of identity and information flow during digital interactions [17], [18]. Therefore, SSI is user-centric [19], allowing users to generate and manage unique decentralized identifiers (DID) independent of any third party [20] and acquire identity attributes from third-party issuers. Moreover, identifiers and associated personal data can be securely stored by them and presented freely when proof of identity is required. That way, personal data is no longer kept in third-party databases, enhancing security and privacy, and reducing risk, connected to data leakage and other identity-related cybercrimes [21].

This can be enabled by an ecosystem (i) facilitating the acquisition and storage of verifiable claims and credentials containing identity attributes, (ii) facilitating the sharing of verifiable presentations, including zero-knowledge proofs and data minimization, (iii) allowing the verification of claims and identities, and (iv) establishing trust among entities (i.e. trust triangle), or issuers, identity holders, and verifiers that interact with each other and can encompass various roles, depending on the situation.

The paradigm is still in its infancy, and there is no consensus on an exact definition of SSI. However, initiatives to describe [20] and formally define the concept [22], essential architectural components [19], and principles [23] that are important for its implementation exist.

The position paper presented by Wagner *et al.* [20] involves cooperation between experts from different institutions and companies, addressing SSI and showing agreement on the future directions regarding standardization, interoperability, regulation, privacy, and security.

Mühle *et al.* [19] provided a high-level overview of SSI architecture and key components of the SSI system, mainly identification, authentication, verifiable claims, and attribute storage. Ferdous *et al.* [22] have mathematically formalized the concept of SSI, using mathematical notions and properties, and have presented various envisioned flows.

Allen [23] proposed ten guiding principles of SSI, laying out the requirements for an SSI system, highlighting the importance of independent existence, user control, data access, transparency, persistence, portability, interoperability, consent, data minimization, and protection. The Sovrin Foundation grouped Allen's principles into three categories security, controllability, and portability [19], while Toth and Anderson-Priddy [24] validated them and suggested five additional principles, namely usability, counterfeit prevention, identity verification, identity assurance, and secure transactions. Furthermore, Ferdous *et al.* [22] analyzed existing definitions, extracted properties, and classified them into five categories, foundational, security, controllability, flexibility, and sustainability.

The aforementioned principles can be viewed as a set of objectives that SSI systems should achieve. Thus, SSI is not dependent on a specific technology and implementation but can be realized in various ways. However, it can be best achieved by utilizing decentralized ledger technology (DLT), usually blockchain technology [17], decentralized identifiers (DID) [5], and verifiable credentials (VC) [6] standardized by The World Wide Web Consortium (W3C).

DLT provides a cryptographic root of trust [21] and serves as a trustless, decentralized public-key infrastructure (DPKI) [25]. It acts as a replacement for a centralized registration authority in traditional identity management systems, where the pairing of identifier and authentication method is maintained [19].

DIDs are globally unique decentralized identifiers, providing a means for authentication using cryptographic proofs. Allowing entities to prove control over them, without requiring permission from any third party [5], [13]. VCs are digital credentials issued by the issuer to a holder, whereby the issuers attest to certain attributes, containing information related to identity subject, issuing authority, type of credential, asserted attributes or properties, constraints of identity, and evidence related to its derivation [6]. DIDs and VCs are directly managed and controlled by the identity holder. They are stored in the user-controlled off-chain storage and can be presented to any relying party when needed [19].

Several distinctions between decentralized and Self-Sovereign Identity can be drawn from the literature and existing implementations. Usually, there are differences in the method of registration, precisely identifier registration, and identity attribute aggregation.

1) Decentralized identity can be derived from existing government-issued identity documents and is provided by services performing identity proofing based on existing third-party trusted credentials, such as passports, driving licenses, etc. After verifying, validated identity attestations are recorded on a distributed ledger for later verification by third parties [11], [18], [26]. On the other hand, SSI does not rely on any existing documents. Each entity can create an unlimited number of identities without relying on documents, as identity information can be self-attested or preferably obtained later by gathering credentials from different issuers.
2) In some decentralized proposals [27], [28], a single identity is allocated for every entity and stored in the blockchain for authentication purposes. Otherwise, SSI allows for the generation of an unlimited number of identifiers depending on the situation and requirements. These solutions are common, especially for IoT implementations, where devices can authenticate each other without a central authority.
3) The decentralized identity system does not meet the requirements of SSI regarding control, or other important criteria relating to controllability, portability, security, or the other principles addressed above.

III. RELATED WORKS

Several secondary studies dealing with aspects of decentralized and Self-Sovereign Identity (SSI) have been published over the years.

Rouhani and Deters [29] have presented a review of five studies related to the application of smart contracts in the field of decentralized identity, and categorized them into seven groups: (i) healthcare, (ii) IoT, (iii) identity management, (iv) record keeping, (v) supply chain, (vi) BPM, and (ii) voting.

Maesa and Mori [2] have surveyed six applications of blockchain, specifically (i) electronic voting, (ii) healthcare records, (iii) identity management, (iv) access control, (v) decentralized notary, and (vi) supply chain. For each, they have analyzed the problem, provided blockchain-based proposals, and presented existing solutions from the literature. As for identity management, an SSI system was brought to the forefront, and its properties were discussed in the context of blockchain-based implementation. The former explored a broader field of blockchain applicability and argued that desired SSI properties can be satisfied by blockchain-based implementation, [30], [31] focused on the domain of healthcare, while also recognizing blockchain's potential for implementing an identity system.

Both conducted a survey on blockchain-based SSI solutions. Houtan *et al.* [31] collected solutions from academia and industry and classified them into five categories, namely (i) data control and protection, (ii) digital identity, (iii) social insurance, (iv) social data governance, (i) healthcare and patient data. They investigated the potential of blockchain technology and concluded that its characteristics are suitable, or even beneficial, when realizing a standardized, interoperable healthcare ecosystem that supports SSI and allows patients to regain control over their data, which has been gathered from various sources, while simultaneously remaining in the center of the ecosystem. The authors also highlighted some challenges regarding security and privacy, lack of standardized implementation methods, and the fact that existing solutions are mostly in beta or test stages, not ready for real-world use. Shuaib *et al.* [30] have also stated several requirements for adopting SSI in healthcare and have presented some advantages and a use case involving different stakeholders.

Mundhe *et al.* [32] conducted a survey, studying various authentication and privacy-preserving techniques in VANETS, including decentralized blockchain-based schemes, and providing scheme classification, strengths, and weaknesses. The study revealed that most of the existing schemes require centralized entities, e.g. trusted authorities who assign identity or certificates to vehicles and store them in the blockchain.

Zhu and Badr [33] conducted a survey on traditional and blockchain-based identity management systems focusing on IoT, identifying solutions and challenges including access control, privacy, trust, and performance. Bartolomeu *et al.* [34] also focused on the IoT and provided a review of use-cases, technology, and challenges of SSI, including a discussion regarding technical challenges, best practices, and standardization.

Gilani *et al.* [35] and Kaneriya *et al.* [36] described and analyzed existing blockchain-based identity management solutions that claim to fulfil self-sovereignty. Gilani *et al.* [35] recognized a lack of evaluation criteria, e.g. a scale for solution assessment. While many solutions have been compared and evaluated based on the law of identity [18], [25], [37] or SSI taxonomy [22], [38], they performed a technical evaluation, disclosing differences in design and implementation, such as a network or blockchain type and data storage, key management, selective disclosure, smart contracts, and GDPR compliance. They also discussed the key concepts and architecture of SSI and pointed out research gaps and challenges. Challenges and future research directions were also discussed by Bernabe *et al.* [21], who surveyed the current state of the art on privacy-preserving solutions, providing an overview of privacy and blockchain concepts in general. The authors also presented identity management systems, which is to say SSI on the blockchain. They analyzed and compared existing solutions, their features, and privacy aspects with an emphasis on GDPR. Providing a comparison of compliance with GDPR principles, such as lawfulness, fairness, transparency, data minimization, integrity, and confidentiality.

Kuperberg [39] has conducted a systematic survey of existing blockchain-based identity and access management solutions and provided an evaluation framework consisting of 75 criteria for the evaluation of decentralized and SSI management systems. The criteria were applied to 43 offerings, which were analyzed in detail and evaluated in terms of end-user functionality, mobility, overhead aspects, compliance, regulations, standardization, and integration.

Liu *et al.* [25] reviewed three solutions, namely Sovrin, uPort, and ShoCard, and compared them based on Cameron's law of identity. They also provided a comprehensive review of 50 existing blockchain-based identity management papers and patents published between May 2017 and January 2020 across various academic databases (ACM Digital Library, IEEE Explore, ScienceDirect, and Springer Link) and Google Scholar. The study focuses on classifying research papers into three main categories: authentication, privacy, and trust. Throughout the analysis, they identified research gaps and opportunities and highlighted few identity-related challenges that include identity wallet leakage and identity changes.

Rathee and Singh [40] carried out an extensive systematic literature mapping of identity management using Blockchain technology. They identified and analyzed 30 primary studies published between 2009 and 2020 with the objective of (i) finding out research trends (ii) and challenges, (iii) scrutinizing identity management frameworks, (iv) identifying initiatives and (v) research projects that use blockchain in the field of identity management, and (v) determining popular consensus algorithms. Once again, they concluded that the integration of blockchain has the potential to overcome the limitations of conventional identity management. Hence, some privacy and interoperability challenges remain.

In contrast to the aforementioned studies, our research includes a larger set of papers, provides more extensive classification and data visualization. It includes both blockchain-based and non-blockchain-based implementations while excluding papers that rely on a central authority for identity registration.

Although all the secondary studies presented above are connected to our research to some extent, the studies [25], [40] are the most related. However, they do not: (i) include non-blockchain-based implementations, (ii) distinguish between decentralized and Self-Sovereign Identity, (iii) classify papers based on their contributions, domain, IT field, and research type.

IV. RESEARCH METHODOLOGY

Most studies presented in the previous section performed a Survey or Systematic Literature Review (SLR), the aim of which is to analyze primary studies on a given research topic in detail and provide an overview of a specific research area. Unlike SLR, in order to get a coarse-grained overview and gain insights into the trends and demographics of existing

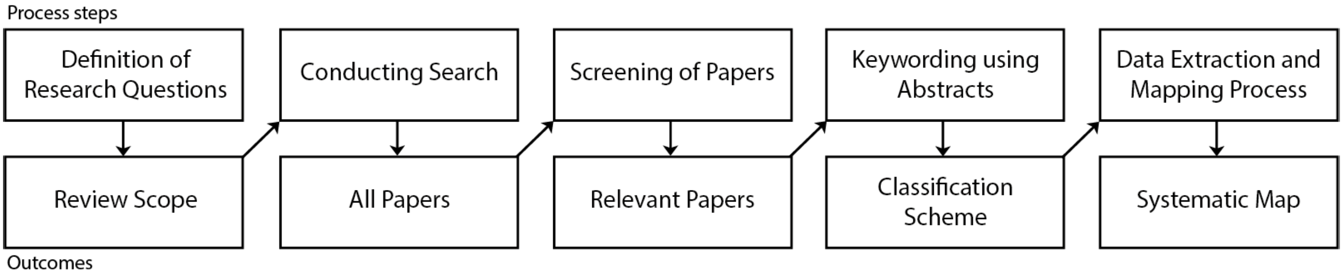


FIGURE 1. **Systematic mapping process [41].**

studies on a broader research topic, a Systematic Mapping Study (SMS) can be performed [41], [42].

Its objective is to (i) structure a field of interest and research type of identified studies, (ii) build a classification scheme, (iii) categorize existing studies within the field, (iv) display frequencies of publications for classification categories and (v) provide result visualization with classification maps. Thus, the main result of the SMS process are classification maps that map identified studies according to research questions and determine coverage in a certain category.

Since decentralized identity, precisely Self-Sovereign Identity, is still in its infancy, the research field is not structured yet. A lot of research has to be done in the future before its wide acceptance can be considered. At this point, we believe SMS is desirable and useful to identify gaps and provides opportunities for further research. Moreover, it can also serve as a starting point for further investigations. Therefore, we decided to follow the guidelines provided by Petterson *et al.* [41], [42] and conducted an SMS process, performing the following steps:

1) defining research questions (section IV-A and IV-B),
2) determining the search strategy and conducting a search (section IV-C and IV-D),
3) paper screening (section IV-D),
4) keywording and constructing classification scheme (section IV-E),
5) data extraction, classification, and mapping of the studies (section V).

Each step results in an outcome, displayed in Fig. 1, and is described in detail in the following sections.

A. RESEARCH OBJECTIVES

This SMS aims to gain a broad insight into existing knowledge/studies in the field of decentralized and Self-Sovereign Identity. The goal is to provide a coarse-grained overview of research papers and classify them according to predefined parameters. Additionally, the hope was to determine the nature and scope of the research and get insights into trends, demographics, challenges, and gaps in the field of decentralized and Self-Sovereign Identity. The main research objectives that should be achieved at the end of the study are:

(i) identify a research subject of interest regarding decentralized and Self-Sovereign Identity.
(ii) identify types of contributions of existing primary and secondary papers.
(iii) identify the number of decentralized identity solutions that employ the principles of Self-Sovereign Identity.
(iv) identify types of research conducted and research methodology used in relevant research papers.
(v) identify domains and IT fields addressed in relevant research papers.
(vi) identify literature demographics and research trends over the years.

The latter is reflected in the formulated research questions and sub-questions (RQs) in subsection IV-B.

B. RESEARCH QUESTIONS

Based on the literature review, and previously defined research objectives, we have defined the research questions (RQ) and sub-questions listed below.

RQ1: What is the subject of interest in research papers dealing with decentralized and Self-Sovereign Identity? What does the research encompass?

1) Which contributions have been introduced in the field of decentralized identity? In which categories can research on decentralized identity be classified based on its contribution? (RQ1.1)
2) From the pool of decentralized identity solutions, how many employed the principles of Self-Sovereign Identity? (Ratio between SSI and decentralized identity). (RQ1.2)
3) What type of research has been conducted in relevant research papers? (RQ1.3)
4) In which domains were decentralized identity solutions studied/applied? (RQ1.4)
5) In which categories can be decentralized identity solutions classified based on the IT field? (RQ1.5)

RQ2: What are the trends and literature demographics in the field of decentralized identity?

1) How many scientific papers were published in the field of decentralized identity each year? (RQ2.1)
2) Where have the studies in the field of decentralized identity been published (according to the number of published papers)? (RQ2.2)

TABLE 1. Inclusion and exclusion criteria.

Inclusion criteria	Exclusion criteria
• papers addressing decentralized or Self-Sovereign Identity, • papers published after 2012, • papers written in English, • papers accessible electronically (in IEEE Xplore or Science Direct database), • papers published in journals, magazines, conferences (proceedings), workshops, symposiums, congresses, forums, and summits, • papers from the computer science research area, • primary and secondary studies.	• papers addressing centralized or/and federated identity, • papers addressing decentralized identity but relying on the certificate or trusted authority for identity registration, • studies published in a book, • papers published in the form of summary, Poster, or PowerPoint presentations.

3) From the perspective of the organizational affiliation of the researchers, what countries have contributed the most in the field of decentralized identity? (RQ2.3)

In the following section, the research strategy is presented. It includes a selection of scientific databases, identification of keywords, and construction of search strings. Afterward, a search for relevant papers was conducted.

C. SEARCH STRATEGY

After defining the research questions, we identified the keywords and formed a search string. The latter was structured in a way that allows a broad overview of the entire research space.

1) KEYWORDS

The identified keywords are Self-Sovereign Identity, Self Sovereign Identity, decentralized identity, decentralised identity, blockchain identity, block-chain identity, blockchain based identity, block-chain based identity, decentralized identifier.

2) THE FINAL SEARCH STRING USED IS

(“SELF-SOVEREIGN” OR “SELF SOVEREIGN” OR “DECENTRALI*ED” OR “BLOCKCHAIN” OR “BLOCK-CHAIN”) AND (IDENTITY OR IDENTIFIER).

We have limited our search to two of the biggest and most important scientific databases in the field of computer science, IEEE Xplore and the Science Direct. The decision on limitation is based on sole interest in (peer-reviewed) scientific papers, trying to distance ourselves from expert and common/popular papers. Furthermore, Scopus includes papers from IEEE Xplore and Science Direct.

Another thing worth noting regarding search strategy is search string adjustment. Since Science Direct does not allow wildcards, we had to switch DECENTRALI*ED to DECENTRALIZED. However, other aspects of the string remain the same in both databases.

The search string was then used in selected databases while taking into account the results (i) in the field of computer science, (ii) and the period between 2012 and 2021. The second can be justified by the fact that decentralized and Self-Sovereign Identity have only become a general topic of discussion since 2015. Due to growing interest in decentralized technology, especially blockchain, the Internet Identity Workshop (IIW) started a discussion about blockchain identity in the spring of 2015. Recognizing its potential in the field of identity management [3] as blockchain can facilitate some desired features of digital identity, solving some problems that traditional IdM systems entail. Therefore, we decided to consider papers published after 2012, taking a two year buffer time.

3) LIMITATIONS

The study was limited to (i) two databases, (ii) English papers (iii) published between January 2013 and January 2021. Relevant papers were identified exclusively by searching databases. Thus, another limitation is that we (iv) did not utilize the snowballing effect nor add additional resources while studying the full text.

D. INCLUSION AND EXCLUSION CRITERIA

To filter out relevant papers, obtained from the previous step, a set of inclusion and exclusion criteria have been defined (Table 1).

The screening process was carried out gradually, as presented in Fig. 2. Firstly, papers were obtained based on (i) the search string application in defined databases. Then, eliminated based on (ii) year and publication type, (iii) title, abstract, and keywords, and finally, based on (iv) full-text screening.

Following the application of the criteria, 120 studies were collected in the final phase and are listed in the appendix.

E. CLASSIFICATION SCHEME

While screening research papers, a classification scheme was defined based on key concepts extracted from the titles, keywords, and abstracts. Screening allowed us to determine the context of individual research and gain a broader insight into the research field. We focused on several aspects that reflect pre-defined research questions and serve as representative categories, namely: (i) contributions, (ii) domains,

TABLE 2. Classification scheme with representative categories.

Contribution	Domain	IT field	Research type	Research method	Place of publication
Architecture Pattern Model/Scheme Framework Protocol System/solution Specifications Method/Methodology Existing solutions Use of decentralized identity Definition/Concepts Challenges and opportunities Other	Education Government Healthcare Retail and eCommerce Banking and financial Industry Supply chain Transport General Other	IoT Security Privacy Trust DPKI Authentication IT architecture Patterns UX and Usability	Validation research Evaluation research Solution proposal Conceptual paper Opinion paper Experiential paper	Analysis and Synthesis Comparison Descriptive method Mathematical method Survey (Literature review) SLR SMS Questionnaire Experiment Prototyping Case study Simulation	Journal Conference Symposium Congress Forum Summit Magazine Workshop

Internet of Things (IoT)
Decentralized Public Key Infrastructure (DPKI)
Information Technology architecture (IT architecture)
UX (User Experience)

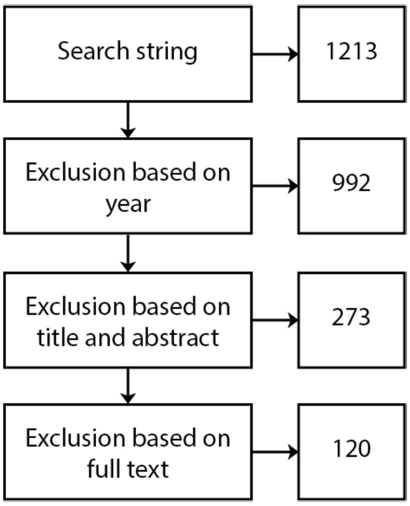

Search string
1213
Exclusion based on year
992
Exclusion based on title and abstract
273
Exclusion based on full text
120

FIGURE 2. Gradual reduction of the number of papers through the screening process.

(ii) IT fields, (iv) place of publication, (v) type of research, and (vi) research methods used. Categories and subcategories were then used as a basis for paper classification and result visualization (systematic maps) and can be seen in Table 2. Each identified paper was classified into one or more categories, respectively.

Research papers included can introduce several contributions in the field of decentralized identity (novel system/solution, architecture, model, scheme, framework, method, etc.) and can focus on different IT fields (IoT, security, privacy, and trust, usability, user experience, etc.) in various domains (education, healthcare, transport, supply chain, banking, and finance, etc.). Based on identified research activities, and the researched methods used (analysis and synthesis, prototyping, experiment, survey, etc.), papers can be categorized according to the classification proposed by Wieringa *et al.* [43], which have proposed the classification of research papers with evaluation criteria extension. They have identified six types of research papers: Solution proposal, Validation research, Evaluation research, Philosophical/conceptual papers and Experience/experiential papers.

1) Solution proposals contain a proposal for a novel or significantly improved solution, like architecture, model, framework, etc., without full-blown validation or implementation of the proposed solution.
2) Validation research contains validation of the proposed solution, either by prototyping, conducting an experiment, simulation, mathematical analysis, mathematical proof of properties, etc., but has not been used in real-world scenarios.
3) Evaluation research, unlike validation research, contains the proposed solution that solves a problem and has been implemented and tested in real-world scenarios.
4) Philosophical/conceptual papers focus on concepts and include a new way of looking and thinking. They usually contain proposals for new perspectives on a theoretical level. Unlike Wieringa *et al.* [43], we slightly modified evaluation criteria. Since primary and secondary papers were included in our research, surveys, SLRs, and SMS were mainly classified into this category.
5) Opinion papers contain the author's personal viewpoint on a given subject, either positive or negative.
6) Experience/experiential papers consist of lessons learned and a description of the author's personal experience in using, for instance, a framework, a tool, a system, or other solutions.

By analyzing papers, we were able to classify them accordingly.

V. RESULTS AND SYSTEMATIC MAPS

After obtaining papers that meet the inclusion criteria and after classification scheme definition, we have begun with

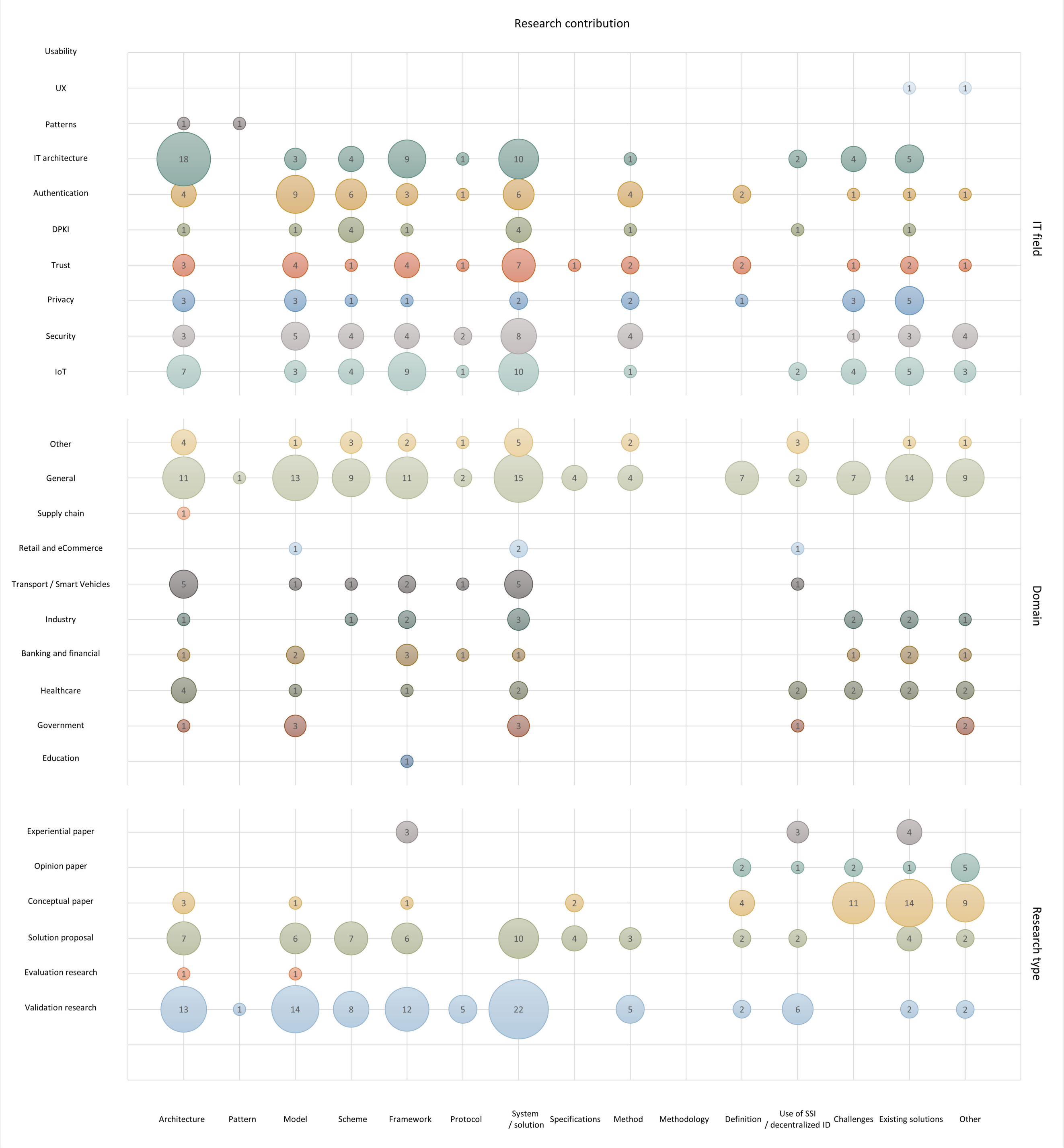


FIGURE 3. Classification map, representing the intersection between papers' contributions and the IT field, domain, and research type.

information extraction and categorization of papers according to their contribution type, domain, IT field, research type, research method, and place of publication. We also recorded whether the article addresses SSI or whether it was merely a decentralized identity and noted if it mentioned the term Self-Sovereign Identity, decentralized identifier, and verifiable credentials.

A. CONTRIBUTION

Finally, we carried out a systematic mapping process which resulted in several maps and visualizations addressing different research perspectives. The final classification map shown in Fig. 3 gives an overview of the number of studies regarding contribution research type, domain, and IT field. It shows which contributions have been introduced in the field of

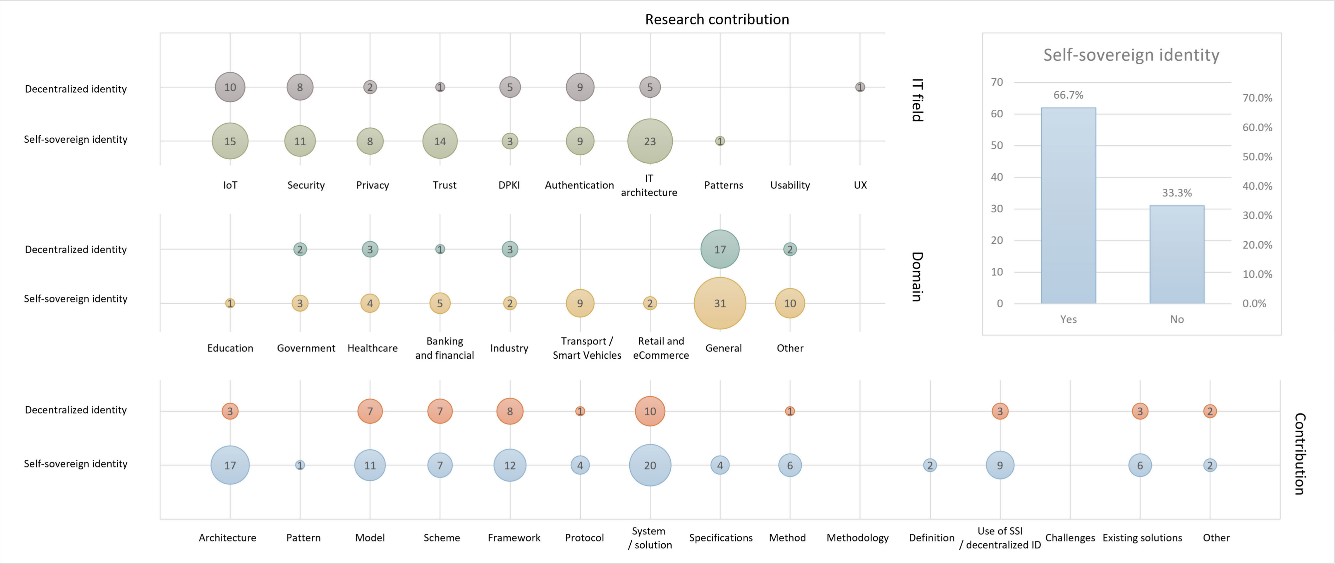


FIGURE 4. Classification map focusing on the demarcation between decentralized and Self-Sovereign Identity, regarding contribution, domain, and IT field, as well as a representation between papers addressing decentralized versus Self-Sovereign Identity.

decentralized identity (RQ1.1), what type of research has been conducted in relevant research papers (RQ1.3), in which domains were decentralized identity studied/applied (RQ1.4) and which IT fields are the most often addressed regarding decentralized identity (RQ1.5). Therefore, the result of the classification map answers the first research question, except for the second sub-question (RQ 1.2.), which addresses the ratio between Self-Sovereign Identity and decentralized identity solutions proposed or validated. The latter is displayed in the classification map in Fig. 4.

B. DEMOGRAPHY

To answer RQ2.1, the number of papers published each year has been counted and is displayed in Fig. 6. To address RQ2.3., we have also recorded active countries, according to the organizational affiliation of the authors. The results of the analysis are displayed in Fig. 7.

In order to answer RQ2.2, regarding relevant papers dissemination, we recorded the publication title for each analyzed study and categorized them as journal, magazine, conference, symposium, summit, forum, workshop, or congress. Fig. 8 shows the share of published papers in each category and mapping between papers contribution and its place of publication is presented in 5.

VI. DISCUSSION

By analyzing and visualizing the results obtained from the SMS, we can draw some conclusions and answer the research questions defined earlier.

The number of included papers (RQ2.1.) regarding decentralized identity has increased over the years. Exponential growth can be observed in Fig. 6. However, note that the search was conducted in January 2021. Therefore, there were less papers published in 2021. Consequently, we assume that new papers have been added to the databases as we continued the SMS process.

From 2017 to 2018, the number increased by 83.3%, from 2018 to 2019 by 58.6% and from 2019 to 2020 by 50.0%. If we consider overall growth, from 2017 to 2021, the number of papers grew by 96.7%.

The distribution between databases is as follows. Overall, 120 papers were identified and included in this study, 108 papers (90%) from IEEE Xplore, and 12 papers (10%) from the Science Direct database. 68 papers (56.7%) have been published in conference proceedings, 29 (24.2%) in journals, and 10 in Symposiums (8.3%). The rest were published in summits, magazines, forums, workshops, and congresses, respectively, as displayed in Fig. 8 (RQ2.2).

Based on the analysis, 82 publications were identified, while the following are only publications in which three or more relevant studies were published (Fig. 9): (i) IEEE Access, (ii) Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS) (iii) 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), (iv) IEEE International Conference On Trust, Security And Privacy In Computing And Communications/International Conference On Big Data Science And Engineering (TrustCom/BigDataSE), (v) International Symposium on Networks, Computers and Communications (ISNCC), (vi) IEEE Communications Standards and (vii) Global Internet of Things Summit (GIoTS). A list of all identified publications is available in the Appendix.

From the perspective of the organizational affiliation of the researchers (RQ2.3), the country that has contributed the most in the field of decentralized identity is the United States

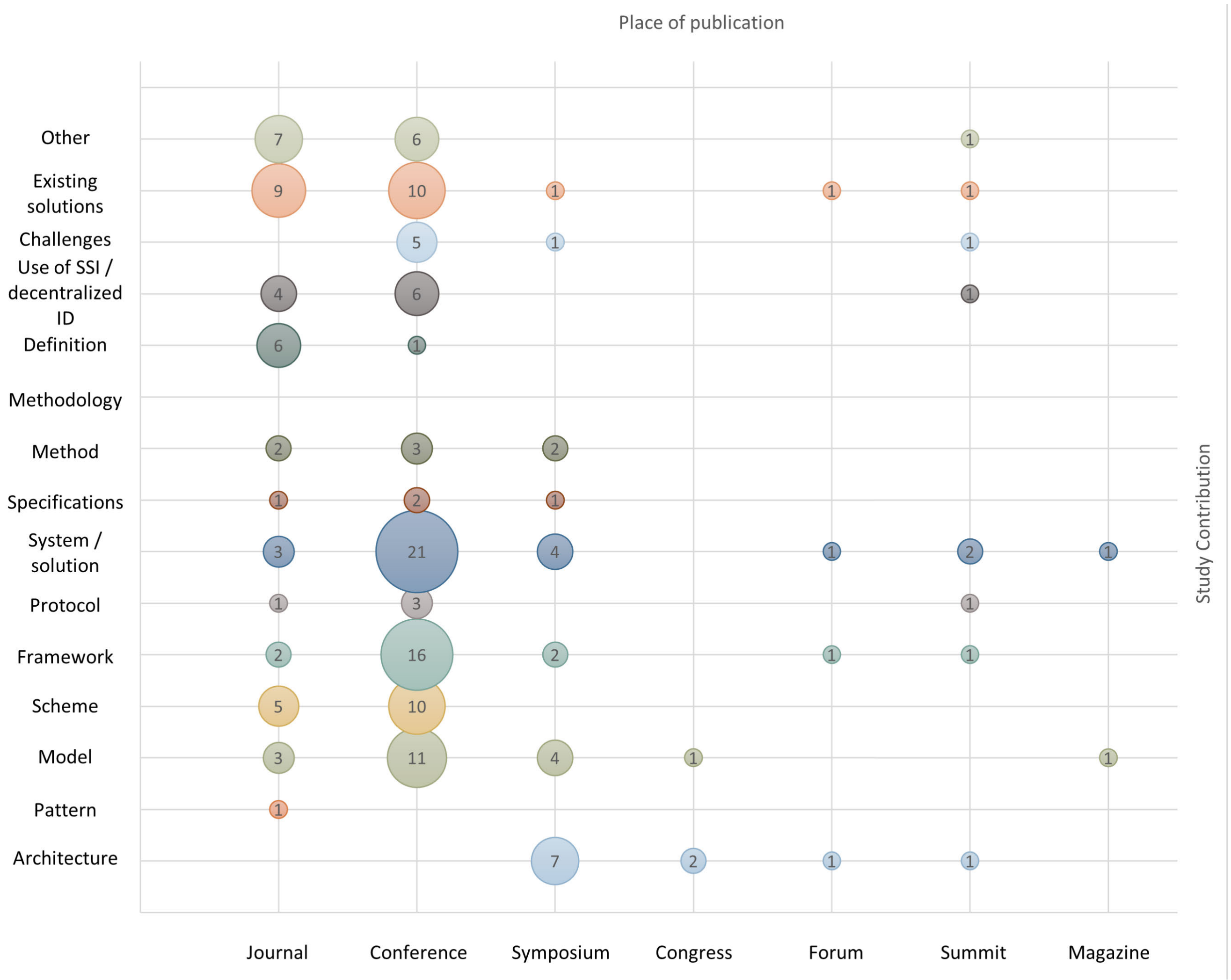


FIGURE 5. Classification map, representing the intersection between papers' contributions and its place of publication.

of America (23 studies – 19.2%). It is followed by China (16 studies – 13.3%), the United Kingdom and Germany (14 studies each – 11.7%), Canada (12 studies – 10.0%), France (8 studies – 6.7%), India (7 studies – 5.8%), Greece and Saudi Arabia (5 studies each – 4.2%), the United Arab Emirates, Portugal, Japan and Australia (4 studies each – 3.3%), Switzerland, and Malaysia (3 studies – 2.5%). The states listed above contributed more than two studies, while in the Appendix, a list of all countries is provided.

As previously mentioned, Fig. 3 indicates the study's contribution intersecting the IT field, domain, and research type.

By analyzing the papers' contributions to the field of decentralized identity (RQ1.1.), it can be concluded that the largest amount of primary studies proposed system/solution (32 studies – 26.7%), architecture (22 studies – 18.3%) and framework (22 studies – 18.3%). On the other hand, there are just a few papers addressing methods and defining the concept (7 studies – 5.8%), protocols (5 studies – 4.2%), specifications i.e. evaluation criteria (4 – 3.3%) and just one paper that proposed patterns (1 study – 0.8%). Secondary papers mostly compare or evaluate existing solutions (22 studies – 18.3%), provide an overview of the field (among the results in the other category) ether in a systematic on the non-systematic way, and present challenges, opportunities, and future research directions.

From the pool of papers that have conducted validation research, evaluation research, or proposed solutions, 66.7% of papers addressing SSI while 33.3% of papers are decentralized but not self-sovereign (RQ1.2). On the other hand, among all papers, secondary and primary ones, 82 papers (68.3%) used the term "Self-Sovereign Identity", while 68 papers (56.7%) discussed the use of decentralized identifiers (DIDs) and/or verifiable credentials (VCs), indicating the recognition of the concept and the potential of DIDs and VCs for the implementation of SSI.

Besides the differentiation between decentralized and Self-Sovereign Identity, across the examined research, different levels of decentralization were also observed. For example,

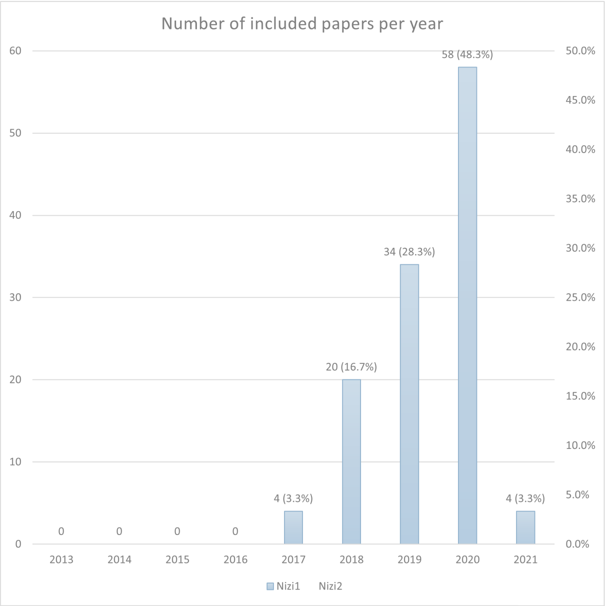


FIGURE 6. The number of papers published over the years.

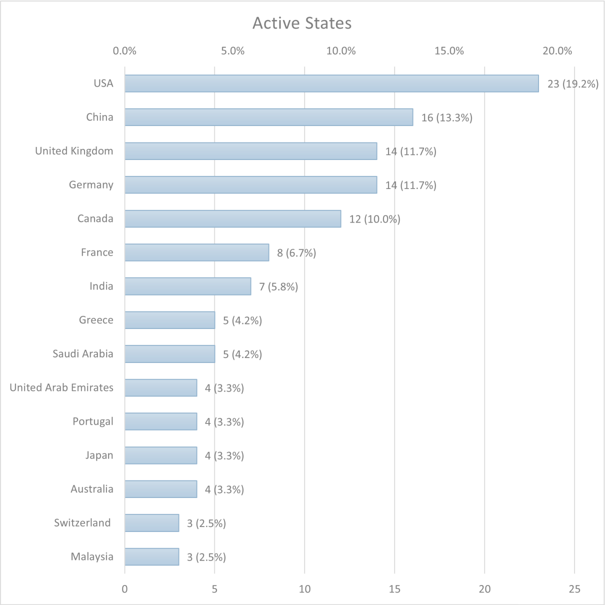
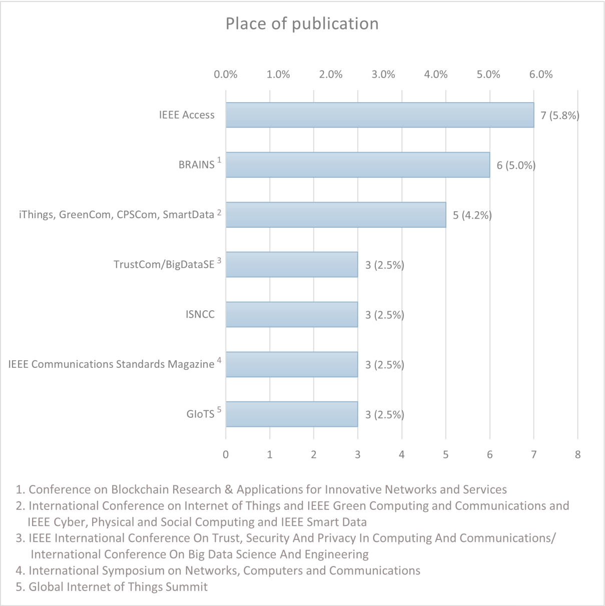


FIGURE 7. Active states, regarding authors' affiliation.

the solution proposed by [44] uses a central server for storing key-pairs, while [45] mentioning an approach to key backup and recovery using trusted third-party repositories. Some solutions rely on gateways that can introduce centralization to a certain extent [46], [47] and some utilize centralized servers that are responsible for mediating between involved entities and serve as intermediaries for storing encrypted identity attributes [18]. Moreover, solutions use different types of blockchains and vary in the number of nodes, therefore possessing different levels of decentralization.



1. Conference on Blockchain Research & Applications for Innovative Networks and Services
2. International Conference on Internet of Things and IEEE Green Computing and Communications and IEEE Cyber, Physical and Social Computing and IEEE Smart Data
3. IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ International Conference On Big Data Science And Engineering
4. International Symposium on Networks, Computers and Communications
5. Global Internet of Things Summit

FIGURE 8. The most common places of publication.

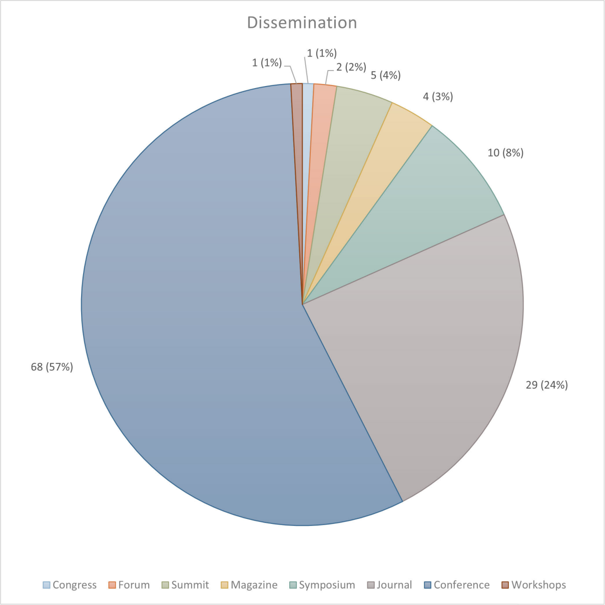


FIGURE 9. Dissemination of papers addressing decentralized identity.

As far as the IT field (RQ1.5.), a great interest around IoT is observed (29 studies – 24.2%). Numerous papers are proposing IT architectures (30 studies – 25.0%) or conducting studies regarding decentralized identity security (22 studies – 18.3%), trust (19 studies – 15.8%), and privacy (16 studies – 13.3%). Decentralized public-key infrastructure (DPKI) (8 studies – 6.7%) and authentication (22 studies – 18.3%) are also recognized as important research topics. While there are hardly any studies addressing usability (0 studies), user experience (1 study – 0.8%), patterns, and good practices (2 studies – 1.7%). The results indicate that the concept

TABLE 3. List of active states.

Active state	Frequency	Percentage
USA	23	19.2%
China	16	13.3%
Germany	14	11.7%
United Kingdom	14	11.7%
Canada	12	10.0%
France	8	6.7%
India	7	5.8%
Saudi Arabia	5	4.2%
Greece	5	4.2%
Australia	4	3.3%
Japan	4	3.3%
Portugal	4	3.3%
United Arab Emirates	4	3.3%
Malaysia	3	2.5%
Switzerland	3	2.5%
Taiwan	2	1.7%
Turkey	2	1.7%
Bangladesh	2	1.7%
Brazil	2	1.7%
Austria	1	0.8%
Brussels	1	0.8%
Ecuador	1	0.8%
Iran	1	0.8%
Ireland	1	0.8%
Jordan	1	0.8%
Morocco	1	0.8%
Myanmar	1	0.8%
Netherlands	1	0.8%
New Zealand	1	0.8%
Romania	1	0.8%
Russia	1	0.8%
South Korea	1	0.8%
Sri Lanka	1	0.8%
Tunisia	1	0.8%

of decentralized and Self-Sovereign Identity is well known. However, implementation independence is reflected in the absence of precisely defined architecture. Therefore, many studies propose and present proofs-of-concept for different IT architectures. However, the best implementation is still a matter of research, circumstances, and the application domain. The absence of studies addressing user experience (UX) and usability in decentralized identity systems is not surprising. Before tackling the latter, a strong foundation with an emphasis on security and privacy is needed. Without strong fundamentals and good architecture, there cannot be patterns and good practices.

Most of the included papers have studied decentralized identity in general (69 studies – 57.5%), not focusing on a specific domain (RQ1.4.). We believe the generalization is a consequence of the novelty. Within any new research field, it is necessary to first objectively and generally define basic principles, concepts, and architecture. Only then can the findings be applied to other areas and be explored further. However, application in some domains is already happening. There are a few studies in the field of transport and smart vehicles (10 studies – 8.3%), healthcare (9 studies – 7.5%), banking and finance (8 studies – 6.7%), government, retail and ecommerce, supply chain and industry (each 7 studies – 5.8%), and education (1 study – 0.8%).

With the COVID-19 outbreak, the potential and the need for decentralized and Self-Sovereign Identities was further recognized [48]–[52]. Especially as it can be used for the identification of individuals who have already been vaccinated or tested negatively within a stipulated time and can mitigate the spread of the virus. Furthermore, it can ensure privacy and security of personal information, and therefore quickly gain trust within a society. Shuaib *et al.* [48] reviewed the aspects of SSI application. Meanwhile, Gans *et al.* [49] focused on SSI possibilities for undocumented individuals during the pandemic. Hasan *et al.* [50] designed, implemented, and evaluated digital medical passports with immunity certificates for COVID-19 test-takers, employing Self-Sovereign Identity. Similarly, Xin [51] introduces GreenPass, a solution utilizing DLT, decentralized identity, verifiable credentials, and distributed storage. Bandara *et al.* [52] developed Connect, an identity wallet

TABLE 4. List of identified places of publication.

Place of publication	Frequency	Percentage
IEEE Access	7	5.8%
Conference on Blockchain Research & Applications for Innovative Networks and Services (BRAINS)	6	5.0%
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)	5	4.2%
Global Internet of Things Summit (GIoTS)	3	2.5%
IEEE Communications Standards Magazine	3	2.5%
International Symposium on Networks, Computers and Communications (ISNCC)	3	2.5%
IEEE International Conference On Trust, Security And Privacy In Computing And Communications/ IEEE International Conference On Big Data Science And Engineering (TrustCom/BigDataSE)	3	2.5%
IEEE Symposium Series on Computational Intelligence (SSCI)	2	1.7%
IEEE International Conference on Blockchain (Blockchain)	2	1.7%
IEEE Annual Consumer Communications & Networking Conference (CCNC)	2	1.7%
IEEE International Conference on Blockchain and Cryptocurrency (ICBC)	2	1.7%
IEEE/CIC International Conference on Communications in China (ICCC Workshops)	2	1.7%
International Conference on Computer Communication and Networks (ICCCN)	2	1.7%
IEEE Internet Computing	2	1.7%
IEEE Security & Privacy	2	1.7%
IEEE Transactions on Engineering Management	2	1.7%
IEEE Transactions on Vehicular Technology	2	1.7%
TEQIP III Sponsored International Conference on Microwave Integrated Circuits, Photonics and Wireless Networks (IMICPW)	2	1.7%
Information Processing & Management	2	1.7%
IEEE International Symposium on Systems Engineering (ISSE)	2	1.7%
IEEE World Forum on Internet of Things (WF-IoT)	2	1.7%
IEEE / ITU International Conference on Artificial Intelligence for Good (AI4G)	1	0.8%
IEEE Conference on Application, Information and Network Security (AINS)	1	0.8%
Canadian Journal of Electrical and Computer Engineering	1	0.8%
IEEE Conference on Business Informatics (CBI)	1	0.8%
IEEE Canadian Conference of Electrical and Computer Engineering (CCECE)	1	0.8%
Iberian Conference on Information Systems and Technologies (CISTI)	1	0.8%
IEEE Conference on Communications and Network Security (CNS)	1	0.8%
International Conference on Advanced Communication Technologies and Networking (CommNet)	1	0.8%
Annual Computer Software and Applications Conference (COMPSAC)	1	0.8%
Computer Communications	1	0.8%
Computer Law & Security Review	1	0.8%
Computer Science Review	1	0.8%
IEEE Asia-Pacific Conference on Computer Science and Data Engineering (CSDE)	1	0.8%
Crypto Valley Conference on Blockchain Technology (CVCBT)	1	0.8%
IEEE/CVF Conference on Computer Vision and Pattern Recognition Workshops (CVPRW)	1	0.8%
International Conference on Cyber-Enabled Distributed Computing and Knowledge Discovery (CyberC)	1	0.8%
IEEE International Conference on Decentralized Applications and Infrastructures (DAPPCON)	1	0.8%
IEEE Intl Conf on Dependable, Autonomic and Secure Computing, Intl Conf on Pervasive Intelligence and Computing, Intl Conf on Cloud and Big Data Computing, Intl Conf on Cyber Science and Technology Congress (DASC/PiCom/CBDCom/CyberSciTech)	1	0.8%
IEEE Eurasia Conference on IOT, Communication and Engineering (ECICE)	1	0.8%
IEEE European Technology and Engineering Management Summit (E-TEMS)	1	0.8%
IEEE International Conference on Emerging Technologies and Factory Automation (ETFA)	1	0.8%
IEEE European Symposium on Security and Privacy Workshops (EuroS&PW)	1	0.8%
Future Generation Computer Systems	1	0.8%
IEEE Globecom Workshops (GC Wkshps)	1	0.8%
IEEE International Symposium on Technologies for Homeland Security (HST)	1	0.8%
International Conference on Advanced Information Technologies (ICAIT)	1	0.8%
International Conference on Cloud and Autonomic Computing (ICCAC)	1	0.8%
IEEE International Conference on Consumer Electronics (ICCE)	1	0.8%
International Conference on Emerging Technologies in Computer Engineering: Machine Learning and Internet of Things (ICETCE)	1	0.8%
International Conference on Emerging Trends in Information Technology and Engineering (ic-ETITE)	1	0.8%

TABLE 4. ***(Continued.)*** **List of identified places of publication.**

IEEE International Conference on Healthcare Informatics (ICHI)	1	0.8%
International Conference on Information Systems and Computer Aided Education (ICISCAE)	1	0.8%
International Conference on Intelligent Sustainable Systems (ICISS)	1	0.8%
International Conference on Computing, Networking and Communications (ICNC)	1	0.8%
IEEE International Conference on System Engineering and Technology (ICSET)	1	0.8%
IEEE Communications Surveys & Tutorials	1	0.8%
IEEE Industrial Electronics Society	1	0.8%
IEEE Internet of Things Magazine	1	0.8%
IEEE Software	1	0.8%
International Joint Conference on Neural Networks (IJCNN)	1	0.8%
International Conference on Internet of Things: Systems, Management and Security (IOTSMS)	1	0.8%
International Conference on Intelligent Systems (IS)	1	0.8%
IEEE Symposium on Computers and Communications (ISCC)	1	0.8%
IEEE International Conference on Intelligence and Security Informatics (ISI)	1	0.8%
IEEE Computer Society Annual Symposium on VLSI (ISVLSI)	1	0.8%
Journal of King Saud University - Computer and Information Sciences	1	0.8%
Journal of Network and Computer Applications	1	0.8%
Journal of Parallel and Distributed Computing	1	0.8%
IEEE Conference on Local Computer Networks (LCN)	1	0.8%
IEEE International Conference on Mobile Cloud Computing, Services, and Engineering (Mobile-Cloud)	1	0.8%
International Symposium on Network Computing and Applications (NCA)	1	0.8%
Network Security	1	0.8%
IEEE Power & Energy Society General Meeting (PESGM)	1	0.8%
Procedia Computer Science	1	0.8%
Annual Conference on Privacy, Security and Trust (PST)	1	0.8%
IEEE International Conference on Smart Computing (SMARTCOMP)	1	0.8%
SoutheastCon	1	0.8%
International Conference on Smart and Sustainable Technologies (SpliTech)	1	0.8%
IEEE Vehicular Technology Conference (VTC2020-Spring)	1	0.8%
IEEE/WIC/ACM International Conference on Web Intelligence (WI)	1	0.8%
International Conference on Wireless Networks and Mobile Communications (WINCOM)	1	0.8%

for storing digital identities and activity trace data on the blockchain utilizing Self-Sovereign Identity proofs.

Concerning research type (RQ1.3), the emphasis is mainly on validation research (57 studies – 47.5%) and solution proposals (36 studies – 30.0%) providing new solutions. On the other hand, there is very little evaluation research (1 study – 0.8%), which could be linked to the fact that decentralized and Self-Sovereign Identity is still in its early stages of research. Conceptual papers (22 studies – 18.0%) provide overviews of the research area and/or describe and analyze existing decentralized solutions while providing a list of opportunities and challenges that need to be addressed in the future.

VII. CONCLUSION

Decentralized identity, narrowly Self-Sovereign Identity (SSI) is a new, user-centric approach to digital identity on the internet that has emerged with the rise of decentralized technologies. It is gathering momentum in academia and industry, as it can solve some of the problems of traditional identity management approaches, primarily related to the aspects of security and privacy. It provides a means for digital identification while enabling users to remain in control of their identifiers and associated identity data by minimizing their reliance on third parties.

With the rise of blockchain technology and its application in different domains, the identity community recognized its potential as blockchain features coincide with some desired properties of digital identity. Thus, since the first discussions in 2015, the number of research papers addressing decentralized and Self-Sovereign Identity has increased rapidly, accumulating knowledge and paving the way for a new era of digital identity. However, the field is still new, unstructured, in the early stages of research, with many research opportunities and challenges.

Therefore, this study presented a systematic mapping study with the aim of structuring the research area, identifying existing research topics, gaps, challenges, and opportunities for future research. It provides a broader insight into the field of decentralized and Self-Sovereign Identity by gathering, analyzing, and classifying the research papers according to their contribution, application domain, IT field, research type, and method, as well as a place of publication.

An analysis of the results suggests that the number of papers has been growing exponentially over the years, while distribution in conference proceedings predominates (56.7%)

and is followed by distribution in journals (24.2%) and symposiums (8.3%). Most papers were published in the journal IEEE Access (5.8%) and the most active state, according to the authors' organizational affiliation, is the United States of America (19.2%).

Validation research (47.5%) and solution proposals (30.0%) prevail, with the prototyping method, generating proofs-of-concept, predominating (40.0%). The identified papers mainly propose systems/solutions (26.7%), architectures (18.3%), and frameworks (18.3%), some compare existing studies (18.3%), while just a few papers address the methods, protocols, patterns and specifications, i.e. the evaluation criteria to determine if a decentralized identity solution is SSI or not.

According to the IT field, numerous papers propose IT architectures (25.0%), address authentication (18.3%), security (18.3%), trust (15.8%), and privacy (13.3%), while there are hardly any studies researching usability, user experience, patterns and good practices.

In most cases, research is conducted generally (57.5%), not focusing on a specific domain. Despite this, the potential in various areas, such as transport, healthcare, banking and finance, government, is also recognized.

With (i) the increased number of research, (ii) solid definition/understanding of the concept, architecture, and its individual components, and (iii) all efforts towards standardization, in the future, we can expect more narrowly focused research, i.e. specializations for each area with specifics accessed. Moreover, it would be useful to (i) differentiate research according to the type of entities involved in the interactions, such as individuals, organizations, things, etc. and (ii) precisely define which properties the system should utilize to be recognized as self-sovereign, while (iii) investigating the extent to which decentralization is possible at all and (iv) analyze the usability and user experience of SSI. Thus, our future research might focus on conducting an SLR or analyzing the impact of usability and user experience on SSI adoption.

APPENDIX. ACTIVE STATES

See Table 3.

APPENDIX. PUBLICATIONS

See Table 4.

APPENDIX. INCLUDED PAPERS

REFERENCES

[1] Y. Liu, Q. Lu, H.-Y. Paik, X. Xu, S. Chen, and L. Zhu, "Design pattern as a service for blockchain-based self-sovereign identity," *IEEE Softw.*, vol. 37, no. 5, pp. 30–36, Sep. 2020.

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

[3] R. Soltani, U. T. Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1129–1136.

[4] M. Takemiya and B. Vanieiev, "Sora identity: Secure, digital identity on the blockchain," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2018, pp. 582–587.

[5] A. Gruner, A. Muhle, and C. Meinel, "An integration architecture to enable service providers for self-sovereign identity," in *Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA)*, Sep. 2019, pp. 1–5.

[6] S. K. Gebresilassie, J. Rafferty, P. Morrow, L. Chen, M. Abu-Tair, and Z. Cui, "Distributed, secure, self-sovereign identity for IoT devices," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–6.

[7] N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in *Proc. 8th IEEE Int. Conf. Mobile Cloud Comput., Services, Eng. (MobileCloud)*, Aug. 2020, pp. 90–95.

[8] A. Othman and J. Callahan, "The Horcrux protocol: A method for decentralized biometric-based self-sovereign identity," in *Proc. Int. Joint Conf. Neural Netw. (IJCNN)*, Jul. 2018, pp. 1–7.

[9] R. Soltani, U. T. Nguyen, and A. An, "Practical key recovery model for self-sovereign identity based digital wallets," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervas. Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 320–325.

[10] Z. A. Lux, F. Beierle, S. Zickau, and S. Gondor, "Full-text search for verifiable credential metadata on distributed ledgers," in *Proc. 6th Int. Conf. Internet Things, Syst., Manage. Secur. (IOTSMS)*, Oct. 2019, pp. 519–528.

[11] N. Naik and P. Jenkins, "UPort open-source identity management system: An assessment of self-sovereign identity and user-centric data platform built on blockchain," in *Proc. IEEE Int. Symp. Syst. Eng. (ISSE)*, Oct. 2020, pp. 1–7.

[12] N. Naik and P. Jenkins, "Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems," in *Proc. IEEE Int. Symp. Syst. Eng. (ISSE)*, Oct. 2020, pp. 1–6.

[13] S. L. Ribeiro and I. A. de Paiva Barbosa, "Risk analysis methodology to blockchain-based solutions," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 59–60.

[14] Q. Stokkink and J. Pouwelse, "Deployment of a blockchain-based self-sovereign identity," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1336–1342.

[15] G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. Calcina Ccori, W. T. Pereira, and M. K. Zuffo, "Self-sovereign identity for IoT environments: A perspective," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2020, pp. 1–6.

[16] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, "Self-sovereign identity: Use-cases, technologies, and challenges for industrial IoT," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2019, pp. 1173–1180.

[17] M. P. Bhattacharya, P. Zavarsky, and S. Butakov, "Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–7.

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

[19] K. C. Toth and A. Anderson-Priddy, "Self-sovereign digital identity: A paradigm shift for identity," *IEEE Secur. Privacy*, vol. 17, no. 3, pp. 17–27, May 2019.

[20] P. Tambe and D. P. Tambay, "Reducing modern slavery using AI and blockchain," in *Proc. IEEE/ITU Int. Conf. Artif. Intell.Good (AIG)*, Sep. 2020, pp. 22–27.

[21] H. Gulati and C.-T. Huang, "Self-sovereign dynamic digital identities based on blockchain technology," in *Proc. SoutheastCon*, Apr. 2019, pp. 1–6.

[22] A. Abraham, K. Theuermann, and E. Kirchengast, "Qualified eID derivation into a distributed ledger based IdM system," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1406–1412.

[23] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90478–90494, 2020, doi: 10.1109/ACCESS.2020.2994090.

[24] J. Kaneriya and H. Patel, "A comparative survey on blockchain based self sovereign identity system," in *Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2020, pp. 1150–1155.

[25] Z. A. Lux, D. Thatmann, S. Zickau, and F. Beierle, "Distributed-Ledger-based authentication with decentralized identifiers and verifiable credentials," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 71–78.

[26] A. Gruner, A. Muhle, T. Gayvoronskaya, and C. Meinel, "A quantifiable trust model for blockchain-based identity management," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1475–1482.

[27] S. E. Haddouti and M. D. Ech-Cherif El Kettani, "Analysis of identity management systems using blockchain technology," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Apr. 2019, pp. 1–7.

[28] A. Gruner, A. Muhle, and C. Meinel, "Using probabilistic attribute aggregation for increasing trust in attribute assurance," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Dec. 2019, pp. 633–640.

[29] D. Hardman, L. Harchandani, A. Othman, and J. Callahan, "Using biometrics to fight credential fraud," *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 39–45, Dec. 2019.

[30] R. Soltani, U. T. Nguyen, and A. An, "Decentralized and privacy-preserving key management model," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–7.

[31] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based solution for COVID-19 digital medical passports and immunity certificates," *IEEE Access*, vol. 8, pp. 222093–222108, 2020.

[32] A.-E. Panait, "Is the user identity perception influenced by the blockchain technology?" in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Nov. 2020, pp. 1–3.

[33] P. C. Bartolomeu, E. Vieira, and J. Ferreira, "Pay as you go: A generic crypto tolling architecture," *IEEE Access*, vol. 8, pp. 196212–196222, 2020.

[34] K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A survey on blockchain-based identity management and decentralized privacy for personal data," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 97–101.

[35] M. Luecking, C. Fries, R. Lamberti, and W. Stork, "Decentralized identity and trust management framework for Internet of Things," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 1–9.

[36] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the Internet of Things," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1568–1573.

[37] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger, and S. Steinhorst, "Towards a blockchain-based identity and trust management framework for the IoV ecosystem," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2020, pp. 1–6.

[38] M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnell, and D. Reed, "The trust over IP stack," *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 46–51, Dec. 2019.

[39] P. Dunphy, L. Garratt, and F. Petitcolas, "Decentralizing digital identity: Open challenges for distributed ledgers," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2018, pp. 75–78.

[40] J. Liu, A. Hodges, L. Clay, and J. Monarch, "An analysis of digital identity management systems—A two-mapping view," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 92–96.

[41] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020.

[42] D. Pennino, M. Pizzonia, A. Vitaletti, and M. Zecchini, "Binding of endpoints to identifiers by on-chain proofs," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Jul. 2020, pp. 1–6.

[43] J. Xu, K. Xue, H. Tian, J. Hong, D. S. L. Wei, and P. Hong, "An identity management and authentication scheme based on redactable blockchain for mobile networks," *IEEE Trans. Veh. Technol.*, vol. 69, no. 6, pp. 6688–6698, Jun. 2020.

[44] W. Xin, "Fighting COVID-19 and helping economy reopen by using blockchain technology," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC Workshops)*, Aug. 2020, pp. 102–105.

[45] K. Wittek, L. Lazzati, D. Bothe, A. Sinnaeve, and N. Pohlmann, "An SSI based system for incentivized and selfDetermined customer-to-business data sharing in a local economy context," in *Proc. IEEE Eur. Technol. Eng. Manage. Summit (E-TEMS)*, Mar. 2020, pp. 1–5.

[46] A. S. Sani, D. Yuan, K. Meng, and Z. Y. Dong, "Idenx: A blockchain-based identity management system for supply chain attacks mitigation in smart grids," in *Proc. IEEE Power Energy Soc. Gen. Meeting (PESGM)*, Aug. 2020, pp. 1–5.

[47] M. Htet, P. T. Yee, and J. R. Rajasekera, "Blockchain based digital identity management system: A case study of Myanmar," in *Proc. Int. Conf. Adv. Inf. Technol. (ICAIT)*, Nov. 2020, pp. 42–47.

[48] D. W. Chadwick, R. Laborde, A. Oglaza, R. Venant, S. Wazan, and M. Nijjar, "Improved identity management with verifiable credentials and FIDO," *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 14–20, Dec. 2019.

[49] M. A. R. Tonu, S. Hridoy, M. A. Ali, and S. A. Azad, "Block–NID: A conceptual secure blockchain based national identity management system model," in *Proc. IEEE Asia–Pacific Conf. Comput. Sci. Data Eng. (CSDE)*, Dec. 2019, pp. 1–7.

[50] S. Ganta, B. Rebekka, N. Gunavathi, and B. Malarkodi, "Unique identity management scheme for distributed NFV market place using Ethereum," in *Proc. TEQIP III Sponsored Int. Conf. Microw. Integr. Circuits, Photon. Wireless Netw. (IMICPW)*, May 2019, pp. 454–457.

[51] Y. Liu, G. Sun, and S. Schuckers, "Enabling secure and privacy preserving identity management via smart contract," in *Proc. IEEE Conf. Commun. Netw. Secur. (CNS)*, Jun. 2019, pp. 1–8.

[52] P. J. Windley, "Multisource digital identity," *IEEE Internet Comput.*, vol. 23, no. 5, pp. 8–17, Sep. 2019.

[53] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan, and S. Wang, "An identity management system based on blockchain," in *Proc. 15th Annu. Conf. Privacy, Secur. Trust (PST)*, Aug. 2017, pp. 44–4409.

[54] X. Zhu, Y. Badr, J. Pacheco, and S. Hariri, "Autonomic identity framework for the Internet of Things," in *Proc. Int. Conf. Cloud Autonomic Comput. (ICCAC)*, Sep. 2017, pp. 69–79.

[55] A. S. Omar and O. Basir, "Decentralized identifiers and verifiable credentials for smartphone anticounterfeiting and decentralized IMEI database," *Can. J. Electr. Comput. Eng.*, vol. 43, no. 3, pp. 174–180, 2020.

[56] K. Inoue, D. Suzuki, T. Kurita, and S. Imai, "Process scheduling of personal identity verification on decentralized trust," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 184–191.

[57] D. Maldonado-Ruiz, J. Torres, and N. El Madhoun, "3BI-ECC: A decentralized identity framework based on blockchain technology and elliptic curve cryptography," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 45–46.

[58] H. Niavis, N. Papadis, V. Reddy, H. Rao, and L. Tassiulas, "A blockchain-based decentralized data sharing infrastructure for off-grid networking," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2020, pp. 1–5.

[59] H. Halpin, "Nym credentials: Privacy-preserving decentralized identity with blockchains," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Jun. 2020, pp. 56–67.

[60] X. Fan, Q. Chai, Z. Li, and T. Pan, "Decentralized IoT data authorization with pebble tracker," in *Proc. IEEE 6th World Forum Internet Things (WF-IoT)*, Jun. 2020, pp. 1–2.

[61] B. Alzahrani, "An information-centric networking based registry for decentralized identifiers and verifiable credentials," *IEEE Access*, vol. 8, pp. 137198–137208, 2020.

[62] S. Terzi, C. Savvaidis, K. Votis, D. Tzovaras, and I. Stamelos, "Securing emission data of smart vehicles with blockchain and self-sovereign identities," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 462–469.

[63] S. Patil and L. Ragha, "Deployment and decentralized identity management for VANETs," in *Proc. 3rd Int. Conf. Emerg. Technol. Comput. Eng., Mach. Learn. Internet Things (ICETCE)*, Feb. 2020, pp. 202–209.

[64] E. Kim, Y.-S. Cho, B. Kim, W. Ji, S.-H. Kim, S. S. Woo, and H. Kim, "Can we create a cross-domain federated identity for the industrial Internet of Things without Google?" *IEEE Internet Things Mag.*, vol. 3, no. 4, pp. 82–87, Dec. 2020.

[65] N. Priya, M. Ponnavaikko, and R. Aantonny, "An efficient system framework for managing identity in educational system based on blockchain technology," in *Proc. Int. Conf. Emerg. Trends Inf. Technol. Eng. (ic-ETITE)*, Feb. 2020, pp. 1–5.

[66] S. R. Niya, B. Jeffrey, and B. Stiller, "KYoT: Self-sovereign IoT identification with a physically unclonable function," in *Proc. IEEE 45th Conf. Local Comput. Netw. (LCN)*, Nov. 2020, pp. 485–490.

[67] R. Rana, R. N. Zaeem, and K. S. Barber, "An assessment of blockchain identity solutions: Minimizing risk and liability of authentication," in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell.*, Oct. 2019, pp. 26–33.

[68] M. Westerkamp, S. Gondor, and A. Kupper, "Tawki: Towards self-sovereign social communication," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastructures (DAPPCON)*, Apr. 2019, pp. 29–38.

[69] Y. Zheng, Y. Li, Z. Wang, C. Deng, Y. Luo, Y. Li, and J. Ding, "Blockchain-based privacy protection unified identity authentication," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Oct. 2019, pp. 42–49.

[70] L. Bathen, G. H. Flores, G. Madl, D. Jadav, A. Arvanitis, K. Santhanam, C. Zeng, and A. Gordon, "SelfIs: Self-sovereign biometric IDs," in *Proc. IEEE/CVF Conf. Comput. Vis. Pattern Recognit. Workshops (CVPRW)*, Jun. 2019, pp. 2847–2856.

[71] W. L. Sim, H. N. Chua, and M. Tahir, "Blockchain for identity management: The implications to personal data protection," in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2019, pp. 30–35.

[72] Z. Zhao and Y. Liu, "A blockchain based identity management system considering reputation," in *Proc. 2nd Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE)*, Sep. 2019, pp. 32–36.

[73] A. Jamal, R. A. A. Helmi, A. S. N. Syahirah, and M.-A. Fatima, "Blockchain-based identity verification system," in *Proc. IEEE 9th Int. Conf. Syst. Eng. Technol. (ICSET)*, Oct. 2019, pp. 253–257.

[74] N. Nchinda, A. Cameron, K. Retzepi, and A. Lippman, "MedRec: A network for personal information distribution," in *Proc. Int. Conf. Comput., Netw. Commun. (ICNC)*, Feb. 2019, pp. 637–641.

[75] S. Friebe, I. Sobik, and M. Zitterbart, "DecentID: Decentralized and privacy-preserving identity storage system using smart contracts," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./ 12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 37–42.

[76] M. Schanzenbach, G. Bramm, and J. Schütte, "Reclaimid: Secure, self-sovereign identities using name systems and attribute-based encryption," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 946–957.

[77] M. Alessi, A. Camillo, E. Giangreco, M. Matera, S. Pino, and D. Storelli, "Make users own their data: A decentralized personal data store prototype based on Ethereum and IPFS," in *Proc. 3rd Int. Conf. Smart Sustain. Technol. (SpliTech)*, Jun. 2018, pp. 1–7.

[78] A. S. Omar and O. Basir, "Identity management in IoT networks using blockchain and smart contracts," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Jul. 2018, pp. 994–1000.

[79] D. Chakravarty and T. Deshpande, "Blockchain-enhanced identities for secure interaction," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Oct. 2018, pp. 1–4.

[80] P. Coelho, A. Zuquete, and H. Gomes, "A propose for a federated ledger for regulated self-sovereignty," in *Proc. 13th Iberian Conf. Inf. Syst. Technol. (CISTI)*, Jun. 2018, pp. 1–4.

[81] M. Tavares, A. Guerreiro, C. Coutinho, F. Veiga, and A. Campos, "WalliD: Secure your ID in an ethereum wallet," in *Proc. Int. Conf. Intell. Syst. (IS)*, Sep. 2018, pp. 714–721.

[82] D. Li, W. Peng, W. Deng, and F. Gai, "A blockchain-based authentication and security mechanism for IoT," in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–6.

[83] H. Anada and S. Arita, "Anonymous authentication scheme with decentralized multi-authorities," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, May 2017, pp. 1–6.

[84] A. Dixit, W. Asif, and M. Rajarajan, "Smart-contract enabled decentralized identity management framework for industry 4.0," in *Proc. 46th Annu. Conf. IEEE Ind. Electron. Soc. (IECON)*, Oct. 2020, pp. 2221–2227.

[85] Y. Chu, J. M. Kim, Y. Lee, S. Shim, and J. Huh, "SS-DPKI: Self-signed certificate based decentralized public key infrastructure for secure communication," in *Proc. IEEE Int. Conf. Consum. Electron. (ICCE)*, Jan. 2020, pp. 1–6.

[86] C.-H. V. Lin, C.-C. J. Huang, Y.-H. Yuan, and Z.-S. S. Yuan, "A fully decentralized infrastructure for subscription-based IoT data trading," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Nov. 2020, pp. 162–169.

[87] I. Agudo, M. Montenegro-Gomez, and J. Lopez, "A blockchain approach for decentralized V2X (D-V2X)," *IEEE Trans. Veh. Technol.*, vol. 70, no. 5, pp. 4001–4010, May 2021.

[88] A. Papageorgiou, A. Mygiakis, K. Loupos, and T. Krousarlis, "DPKI: A blockchain-based decentralized public key infrastructure system," in *Proc. Global Internet Things Summit (GIoTS)*, Jun. 2020, pp. 1–5.

[89] K. Yang, H.-M. Liao, L.-H. Zhao, S.-Z. Zheng, and H.-W. Li, "Research on network security protection technology of energy industry based on blockchain," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC Workshops)*, Aug. 2020, pp. 162–166.

[90] Y. Ren, R. Xie, F. R. Yu, T. Huang, and Y. Liu, "Potential identity resolution systems for the industrial Internet of Things: A survey," *IEEE Commun. Surveys Tuts.*, vol. 23, no. 1, pp. 391–430, 1st Quart., 2021.

[91] R. Laborde, A. Oglaza, S. Wazan, F. Barrere, A. Benzekri, D. W. Chadwick, and R. Venant, "A user-centric identity management framework based on the W3C verifiable credentials and the FIDO universal authentication framework," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–8.

[92] B. Yilmaz, E. Barak, and S. Ozdemir, "Improving webRTC security via blockchain based smart contracts," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Oct. 2020, pp. 1–6.

[93] N. Prakash, D. G. Michelson, and C. Feng, "CVIN: Connected vehicle information network," in *Proc. IEEE 91st Veh. Technol. Conf. (VTC-Spring)*, May 2020, pp. 1–6.

[94] H. Wang, Y. Yao, Q. Hou, X. Wang, L. Zeng, W. Qiu, D. He, and Q. Wang, "Design of work ticket system and scheduling algorithm based on blockchain," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Dec. 2020, pp. 858–863.

[95] F. Fotopoulos, V. Malamas, T. K. Dasaklis, P. Kotzanikolaou, and C. Douligeris, "A blockchain-enabled architecture for IoMT device authentication," in *Proc. IEEE Eurasia Conf. IoT, Commun. Eng. (ECICE)*, Oct. 2020, pp. 89–92.

[96] R. Laborde, A. Oglaza, S. Wazan, F. Barrere, A. Benzekri, D. W. Chadwick, and R. Venant, "Know your customer: Opening a new bank account online using UAAF," in *Proc. IEEE 17th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Jan. 2020, pp. 1–2.

[97] C. Patsonakis, K. Samari, A. Kiayias, and M. Roussopoulos, "Implementing a smart contract PKI," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1425–1443, Nov. 2020.

[98] F. Harer and H.-G. Fill, "Decentralized attestation of conceptual models using the ethereum blockchain," in *Proc. IEEE 21st Conf. Bus. Informat. (CBI)*, Jul. 2019, pp. 104–113.

[99] A. S. Omar and O. Basir, "Smart phone anti-counterfeiting system using a decentralized identity management framework," in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2019, pp. 1–5.

[100] R. Ansey, J. Kempf, O. Berzin, C. Xi, and I. Sheikh, "Gnomon: Decentralized identifiers for securing 5G IoT device registration and software update," in *Proc. IEEE Globecom Workshops (GC Wkshps)*, Dec. 2019, pp. 1–6.

[101] Y. Liang, "Identity verification and management of electronic health records with blockchain technology," in *Proc. IEEE Int. Conf. Healthcare Informat. (ICHI)*, Jun. 2019, pp. 1–3.

[102] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions for blockchain: Review and challenges," *IEEE Access*, vol. 7, pp. 164908–164940, 2019.

[103] M. El-Hajj, A. Fadlallah, M. Chamoun, and A. Serhrouchni, "Ethereum for secure authentication of IoT using pre-shared keys (PSKs)," in *Proc. Int. Conf. Wireless Netw. Mobile Commun. (WINCOM)*, Oct. 2019, pp. 1–7.

[104] S. Rouhani and R. Deters, "Security, performance, and applications of smart contracts: A systematic survey," *IEEE Access*, vol. 7, pp. 50759–50779, 2019.

[105] V. S. Rathina, B. Rebekka, N. Gunavathi, and B. Malarkodi, "Novel NFV entities managing scheme for telecom providers using proof of concept blockchain," in *Proc. TEQIP III Sponsored Int. Conf. Microw. Integr. Circuits, Photon. Wireless Netw. (IMICPW)*, May 2019, pp. 288–292.

[106] P. Cui and U. Guin, "Countering botnet of things using blockchain-based authenticity framework," in *Proc. IEEE Comput. Soc. Annu. Symp. VLSI (ISVLSI)*, Jul. 2019, pp. 598–603.

[107] H. Orman, "Blockchain: The emperors new PKI?" *IEEE Internet Comput.*, vol. 22, no. 2, pp. 23–28, Mar. 2018.

[108] E. Bandara, X. Liang, P. Foytik, S. Shetty, C. Hall, D. Bowden, N. Ranasinghe, and K. De Zoysa, ''A blockchain empowered and privacy preserving digital contact tracing platform,'' *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102572.

[109] T. Dursun and B. B. Üstündağ, ''A novel framework for policy based on-chain governance of blockchain networks,'' *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102556.

[110] T. Rathee and P. Singh, ''A systematic literature mapping on secure identity management using blockchain technology,'' *J. King Saud Univ. Comput. Inf. Sci.*, pp. 1–15, Mar. 2021.

[111] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, ''A survey on essential components of a self-sovereign identity,'' *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018.

[112] R. Seifert, ''Digital identities–self-sovereignty and blockchain are the keys to success,'' *Netw. Secur.*, vol. 2020, no. 11, pp. 17–19, Nov. 2020.

[113] M. Shuaib, S. Alam, M. S. Alam, and M. S. Nasir, ''Self-sovereign identity for healthcare using blockchain,'' *Mater. Today, Proc.*, pp. 1–5, Mar. 2021.

[114] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, ''Blockchain-based identity management systems: A review,'' *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102731.

[115] C. Sullivan and E. Burger, ''E-residency and blockchain,'' *Comput. Law Secur. Rev.*, vol. 33, no. 4, pp. 470–481, 2017.

[116] D. Di Francesco Maesa and P. Mori, ''Blockchain 3.0 applications survey,'' *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Apr. 2020.

[117] A. A.-N. Patwary, A. Fu, S. K. Battula, R. K. Naha, S. Garg, and A. Mahanti, ''FogAuthChain: A secure location-based authentication scheme in fog computing environments using blockchain,'' *Comput. Commun.*, vol. 162, pp. 212–224, Oct. 2020.

[118] B. Qin, J. Huang, Q. Wang, X. Luo, B. Liang, and W. Shi, ''Cecoin: A decentralized PKI mitigating MitM attacks,'' *Future Gener. Comput. Syst.*, vol. 107, pp. 805–815, Jun. 2020.

[119] S. Sahmim, H. Gharsellaoui, and S. Bouamama, ''Edge computing: Smart identity wallet based architecture and user centric,'' *Proc. Comput. Sci.*, vol. 159, pp. 1246–1257, 2019.

REFERENCES

[1] A. I. Sanka, M. Irfan, I. Huang, and R. C. C. Cheung, ''A survey of breakthrough in blockchain technology: Adoptions, applications, challenges and future research,'' *Comput. Commun.*, vol. 169, pp. 179–201, Mar. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0140366421000268, doi: 10.1016/j.comcom.2020.12.028.

[2] D. Di Francesco Maesa and P. Mori, ''Blockchain 3.0 applications survey,'' *J. Parallel Distrib. Comput.*, vol. 138, pp. 99–114, Apr. 2020. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S0743731519308664, doi: 10.1016/j.jpdc.2019.12.019.

[3] A. Preukschat and D. Reed, *Self-Sovereign Identity: Decentralized Digital Identity and Verifiable Credentials*. Shelter Island, NY, USA: Manning Publications, 2021.

[4] EBSI. *EBSI Documentation*. Accessed: Aug. 18, 2021. [Online]. Available: https://ec.europa.eu/cefdigital/wiki/display/CEFDIGITAL/ebsi

[5] W3C. *Decentralized Identifiers (DIDS) V1.0. Core Architecture, Data Model, and Representations*. Accessed: Jul. 21, 2021. [Online]. Available: https://www.w3.org/TR/did-core/

[6] W3C. *Verifiable Credentials Data Model 1.0. Expressing Verifiable Information on the Web*. Accessed: Jul. 6, 2021. [Online]. Available: https://www.w3.org/TR/vc-data-model/

[7] DIF. *DIF—Decentralized Identity Foundation*. Accessed: Jul. 8, 2021. [Online]. Available: https://identity.foundation/

[8] European Commission. *Commission Proposes a Trusted and Secure Digital Identity for All Europeans*. Accessed: Jul. 8, 2021. [Online]. Available: https://ec.europa.eu/commission/presscorner/detail/en/ip_21_2663

[9] P. Dunphy, L. Garratt, and F. Petitcolas, ''Decentralizing digital identity: Open challenges for distributed ledgers,'' in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops (EuroS&PW)*, Apr. 2018, pp. 75–78, doi: 10.1109/EuroSPW.2018.00016.

[10] M. Schanzenbach, G. Bramm, and J. Schütte, ''ReclaimID: Secure, self-sovereign identities using name systems and attribute-based encryption,'' in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 946–957, doi: 10.1109/TrustCom/BigDataSE.2018.00134.

[11] R. Rana, R. N. Zaeem, and K. S. Barber, ''An assessment of blockchain identity solutions: Minimizing risk and liability of authentication,'' in *Proc. IEEE/WIC/ACM Int. Conf. Web Intell. (WI)*, Oct. 2019, pp. 26–33.

[12] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, ''Blockchain-enabled decentralized identify management: The case of self-sovereign identity in public transportation,'' *Blockchain, Res. Appl.*, pp. 1–40, May 2021, Art. no. 100014. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2096720921000099, doi: 10.1016/j.bcra.2021.100014.

[13] M. Davie, D. Gisolfi, D. Hardman, J. Jordan, D. O'Donnell, and D. Reed, ''The trust over IP stack,'' *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 46–51, Dec. 2019, doi: 10.1109/MCOMSTD.001.1900029.

[14] The Linux Foundation. *Hyperledger Indy*. Accessed: Aug. 18, 2021. [Online]. Available: https://www.hyperledger.org/use/hyperledger-indy

[15] *Hyperledger Indy*. Accessed: Aug. 18, 2021. [Online]. Available: https://hyperledger-indy.readthedocs.io/en/latest/

[16] D. van Bokkem, R. Hageman, G. Koning, L. Nguyen, and N. Zarin, ''Self-sovereign identity solutions: The necessity of blockchain technology,'' 2019, *arXiv:1904.12816*. [Online]. Available: http://arxiv.org/abs/1904.12816

[17] O. Avellaneda, A. Bachmann, A. Barbir, J. Brenan, P. Dingle, K. H. Duffy, E. Maler, D. Reed, and M. Sporny, ''Decentralized identity: Where did it come from and where is it going?'' *IEEE Commun. Standards Mag.*, vol. 3, no. 4, pp. 10–13, Dec. 2019, doi: 10.1109/MCOMSTD.2019.9031542.

[18] P. Dunphy and F. A. P. Petitcolas, ''A first look at identity management schemes on the blockchain,'' *IEEE Security Privacy*, vol. 16, no. 4, pp. 20–29, Jul./Aug. 2018, doi: 10.1109/MSP.2018.3111247.

[19] A. Mühle, A. Grüner, T. Gayvoronskaya, and C. Meinel, ''A survey on essential components of a self-sovereign identity,'' *Comput. Sci. Rev.*, vol. 30, pp. 80–86, Nov. 2018. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013718301217, doi: 10.1016/j.cosrev.2018.10.002.

[20] K. Wagner, B. Némethi, E. Renieris, P. Lang, E. Brunet, and E. Holst. (2018). *Self-Sovereign Identity: A Position Paper on Blockchain Enabled Identity and the Road Ahead*. [Online]. Available: https://jolocom.io/wp-content/uploads/2018/10/Self-sovereign-Identity-_-Blockchain-Bundesverband-2018.pdf

[21] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, ''Privacy-preserving solutions for blockchain: Review and challenges,'' *IEEE Access*, vol. 7, pp. 164908–164940, 2019, doi: 10.1109/ACCESS.2019.2950872.

[22] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, ''In search of self-sovereign identity leveraging blockchain technology,'' *IEEE Access*, vol. 7, pp. 103059–103079, 2019, doi: 10.1109/ACCESS.2019.2931173.

[23] C. Allen. (2016). *The Path to Self-Sovereign Identity*. Accessed: Aug. 16, 2021. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[24] K. C. Toth and A. Anderson-Priddy, ''Self-sovereign digital identity: A paradigm shift for identity,'' *IEEE Secur. Privacy*, vol. 17, no. 3, pp. 17–27, May 2019, doi: 10.1109/MSEC.2018.2888782.

[25] Y. Liu, Q. Lu, H.-Y. Paik, X. Xu, S. Chen, and L. Zhu, ''Design pattern as a service for blockchain-based self-sovereign identity,'' *IEEE Softw.*, vol. 37, no. 5, pp. 30–36, Sep. 2020, doi: 10.1109/MS.2020.2992783.

[26] W. L. Sim, H. N. Chua, and M. Tahir, ''Blockchain for identity management: The implications to personal data protection,'' in *Proc. IEEE Conf. Appl., Inf. Netw. Secur. (AINS)*, Nov. 2019, pp. 30–35, doi: 10.1109/AINS47559.2019.8968708.

[27] D. Li, W. Peng, W. Deng, and F. Gai, ''A blockchain-based authentication and security mechanism for IoT,'' in *Proc. 27th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Jul. 2018, pp. 1–6, doi: 10.1109/ICCCN.2018.8487449.

[28] A. S. Omar and O. Basir, ''Smart phone anti-counterfeiting system using a decentralized identity management framework,'' in *Proc. IEEE Can. Conf. Electr. Comput. Eng. (CCECE)*, May 2019, pp. 1–5, doi: 10.1109/CCECE.2019.8861955.

[29] S. Rouhani and R. Deters, ''Security, performance, and applications of smart contracts: A systematic survey,'' *IEEE Access*, vol. 7, pp. 50759–50779, 2019, doi: 10.1109/ACCESS.2019.2911031.

[30] M. Shuaib, S. Alam, M. S. Alam, and M. S. Nasir, ''Self-sovereign identity for healthcare using blockchain,'' *Proc. Mater. Today*, pp. 1–5, Mar. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214785321021027, doi: 10.1016/j.matpr.2021.03.083.

[31] B. Houtan, A. S. Hafid, and D. Makrakis, "A survey on blockchain-based self-sovereign patient identity in healthcare," *IEEE Access*, vol. 8, pp. 90478–90494, 2020, doi: 10.1109/ACCESS.2020.2994090.

[32] P. Mundhe, S. Verma, and S. Venkatesan, "A comprehensive survey on authentication and privacy-preserving schemes in VANETs," *Comput. Sci. Rev.*, vol. 41, Aug. 2021, Art. no. 100411. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1574013721000514, doi: 10.1016/j.cosrev.2021.100411.

[33] X. Zhu and Y. Badr, "A survey on blockchain-based identity management systems for the Internet of Things," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1568–1573, doi: 10.1109/Cybermatics_2018.2018.00263.

[34] P. C. Bartolomeu, E. Vieira, S. M. Hosseini, and J. Ferreira, "Self-sovereign identity: Use-cases, technologies, and challenges for industrial IoT," in *Proc. 24th IEEE Int. Conf. Emerg. Technol. Factory Automat. (ETFA)*, Sep. 2019, pp. 1173–1180, doi: 10.1109/ETFA.2019.8869262.

[35] K. Gilani, E. Bertin, J. Hatin, and N. Crespi, "A survey on blockchain-based identity management and decentralized privacy for personal data," in *Proc. 2nd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Sep. 2020, pp. 97–101, doi: 10.1109/BRAINS49436.2020.9223312.

[36] J. Kaneriya and H. Patel, "A comparative survey on blockchain based self sovereign identity system," in *Proc. 3rd Int. Conf. Intell. Sustain. Syst. (ICISS)*, Dec. 2020, pp. 1150–1155, doi: 10.1109/ICISS49785.2020.9315899.

[37] S. E. Haddouti and M. D. E.-C. El Kettani, "Analysis of identity management systems using blockchain technology," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Apr. 2019, pp. 1–7, doi: 10.1109/COMMNET.2019.8742375.

[38] R. Soltani, U. T. Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," in *Proc. IEEE Int. Conf. Internet Things (iThings), IEEE Green Comput. Commun. (GreenCom), IEEE Cyber, Phys. Social Comput. (CPSCom), IEEE Smart Data (SmartData)*, Jul. 2018, pp. 1129–1136, doi: 10.1109/Cybermatics_2018.2018.00205.

[39] M. Kuperberg, "Blockchain-based identity management: A survey from the enterprise and ecosystem perspective," *IEEE Trans. Eng. Manag.*, vol. 67, no. 4, pp. 1008–1027, Nov. 2020, doi: 10.1109/TEM.2019.2926471.

[40] T. Rathee and P. Singh, "A systematic literature mapping on secure identity management using blockchain technology," *J. King Saud Univ.-Comput. Inf. Sci.*, pp. 1–15, Mar. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S1319157821000690, doi: 10.1016/j.jksuci.2021.03.005.

[41] K. Petersen, R. Feldt, S. Mujtaba, and M. Mattsson, "Systematic mapping studies in software engineering," in *Proc. 12th Int. Conf. Eval. Assessment Softw. Eng.*, vol. 17, Jun. 2008, pp. 1–10.

[42] K. Petersen, S. Vakkalanka, and L. Kuzniarz, "Guidelines for conducting systematic mapping studies in software engineering: An update," *Inf. Softw. Technol.*, vol. 64, pp. 1–18, Aug. 2015.

[43] R. Wieringa, N. Maiden, N. Mead, and C. Rolland, "Requirements engineering paper classification and evaluation criteria: A proposal and a discussion," *Requir. Eng.*, vol. 11, no. 1, pp. 102–107, Mar. 2006, doi: 10.1007/s00766-005-0021-6.

[44] M. Takemiya and B. Vanieiev, "Sora identity: Secure, digital identity on the blockchain," in *Proc. IEEE 42nd Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Jul. 2018, pp. 582–587, doi: 10.1109/COMPSAC.2018.10299.

[45] R. Soltani, U. T. Nguyen, and A. An, "Practical key recovery model for self-sovereign identity based digital wallets," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervas. Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr. (DASC/PiCom/CBDCom/CyberSciTech)*, Aug. 2019, pp. 320–325, doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.

[46] A. Gruner, A. Mühle, and C. Meinel, "An integration architecture to enable service providers for self-sovereign identity," in *Proc. IEEE 18th Int. Symp. Netw. Comput. Appl. (NCA)*, Sep. 2019, pp. 1–5, doi: 10.1109/NCA.2019.8935015.

[47] A. Abraham, K. Theuermann, and E. Kirchengast, "Qualified eID derivation into a distributed ledger based IdM system," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng. (TrustCom/BigDataSE)*, Aug. 2018, pp. 1406–1412, doi: 10.1109/TrustCom/BigDataSE.2018.00195.

[48] M. Shuaib, S. Alam, M. S. Nasir, and M. S. Alam, "Immunity credentials using self-sovereign identity for combating COVID-19 pandemic," *Proc. Mater. Today*, pp. 1–5, Mar. 2021. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S2214785321021155, doi: 10.1016/j.matpr.2021.03.096.

[49] R. B. Gans, J. Ubacht, and M. Janssen, "Self-sovereign identities for fighting the impact of COVID-19 pandemic," *Digit. Government, Res. Pract.*, vol. 2, no. 2, pp. 1–4, Mar. 2021, doi: 10.1145/3429629.

[50] H. R. Hasan, K. Salah, R. Jayaraman, J. Arshad, I. Yaqoob, M. Omar, and S. Ellahham, "Blockchain-based solution for COVID-19 digital medical passports and immunity certificates," *IEEE Access*, vol. 8, pp. 222093–222108, 2020, doi: 10.1109/ACCESS.2020.3043350.

[51] W. Xin, "Fighting COVID-19 and helping economy reopen by using blockchain technology," in *Proc. IEEE/CIC Int. Conf. Commun. China (ICCC Workshops)*, Aug. 2020, pp. 102–105, doi: 10.1109/ICCCWorkshops49972.2020.9209939.

[52] E. Bandara, X. Liang, P. Foytik, S. Shetty, C. Hall, D. Bowden, N. Ranasinghe, and K. De Zoysa, "A blockchain empowered and privacy preserving digital contact tracing platform," *Inf. Process. Manage.*, vol. 58, no. 4, Jul. 2021, Art. no. 102572. [Online]. Available: https://www.sciencedirect.com/science/article/pii/S030645732100073X, doi: 10.1016/j.ipm.2021.102572.

ŠPELA ČUČKO received the master's degree in informatics and technology of communication from the Faculty of Electrical Engineering and Computer Science, University of Maribor, where she is currently pursuing the Ph.D. degree in computer science. She is currently a Young Researcher with the Institute of informatics and a member of the Research and Development Group named Blockchain Lab:UM. Her current research interests include digital, decentralized, and self-sovereign identities.

MUHAMED TURKANOVIĆ is currently the Head of research and development at Blockchain Lab:UM, Maribor, Slovenia; an Assistant Professor at the Faculty of Electrical Engineering and Computer Science, Institute of Informatics, University of Maribor (UM), Slovenia; the Head of operations at Digital Innovation Hub UM; and the UM's coordinator of the H2020 Project DE4A—Digital Europe for All. He was a Managing Director and a CTO of an IT Company, from 2013 to 2016. His current research interests include advanced database technologies, cryptography, digital identities, and blockchain.