International Journal of Research in Engineering, Science and Management
Volume 6, Issue 12, December 2023
https://www.ijresm.com | ISSN (Online): 2581-5792

Decentralized Identity and Access Management (IAM) and Self-Sovereign Identity

Sudip Kumar Roy*
Department of Electronics and Communication Engineering, Jaypee Institute of Information Technology, Noida, India

***Abstract*: Self-Sovereign Identity (SSI) represents a ground breaking, user-focused approach to digital identity management. This paradigm shifts the control of personal data back to the user, diverging from traditional centralized models that depend on third-party verification. SSI is gaining significant momentum, particularly in the blockchain sphere, where its principles align seamlessly with decentralized technologies. This growing interest is reflected in the increasing volume of scholarly articles and industry discussions on the topic. As SSI is still an emerging area, its landscape is continuously evolving. To provide a detailed and structured overview of the field, researchers have employed systematic mapping techniques. This method involves an in-depth examination and categorization of academic papers, focusing on various dimensions such as the type of contribution, application areas, related IT fields, research methodologies, and publication venues. This structured approach aids in understanding the depth and breadth of current research, highlighting prevalent themes, demographic trends, and potential areas for future investigation. The analysis reveals a dominant focus on validation research and the development of solutions for decentralized identities. Most studies present new systems, designs, and conceptual frameworks. These primarily address key aspects like authentication processes, enhancing security and privacy measures, and establishing trust. However, there is a notable gap in research related to the user aspect of SSI, such as its usability, user experience, design patterns, and best practices. This indicates a significant area for future research, emphasizing the need to balance technical advancement with user-centric design in the evolving landscape of Self-Sovereign Identity.**

***Keywords*: blockchain, decentralized, identifier, identity, self-sovereign, self-sovereign identity, SSI.**

1. Introduction

The burgeoning interest in decentralized technology, especially blockchain, is influencing various sectors, with identity management emerging as a key area [1]. This trend became prominent in the spring of 2015, when the identity community identified the potential of blockchain to create an identity layer on the internet. Such an infrastructure could enable asset exchanges and build trust in relationships between entities without a central intermediary. While blockchain has been pivotal in advancing decentralized identity concepts, it is not the only method for implementation. Peer Decentralized Identifiers (peer DIDs) offer a ledger-free alternative, functioning independently of blockchain technology.

This independence from blockchain allows peer DIDs to offer a unique approach to identity management. They provide a flexible and adaptable solution, especially in environments where blockchain may not be suitable or required. Peer DIDs facilitate the direct and efficient management of digital identities, proving particularly beneficial in situations demanding quick identity verification and heightened data privacy [2]. This method expands the possibilities within the realm of decentralized identity technologies, presenting a versatile and secure option in the rapidly evolving domain of digital identity [3].

Decentralization marks a shift from centralized systems, where a single authority holds control, to a more distributed model that spreads control among its participants [4]. This transformation is particularly significant in the realm of identity management, where it empowers users or identity holders, fostering user-centric systems. The centralized storage of Personal Identifiable Information (PII) in current systems raises serious concerns regarding privacy and security [5]. The emergence and growing popularity of decentralized identity models, especially Self-Sovereign Identity (SSI), are driven by increasing worries about the misuse of personal data, data breaches, PII leaks, and identity thefts [6].

This movement towards decentralized identity is not just academic but also industrial, receiving attention and efforts towards standardization from major organizations like the World Wide Web Consortium (W3C) and the Decentralized Identity Foundation (DIF) [7]. These entities aim to create a new ecosystem for decentralized identity. Another significant step in this direction is the European Commission's proposal for a trusted European Digital Identity, which includes the concept of identity wallets, giving users more control over their data [8]. This evolution represents a fundamental change in how personal identity is managed and secured, underscoring a societal shift towards greater data sovereignty and personal privacy.

As interest in decentralized identity systems intensifies, the volume of related research articles, innovative initiatives, and proposed solutions is rapidly increasing. Yet, there exists a certain level of confusion and debate regarding the fundamental principles and definitions within this domain. Central to the concept of decentralized identity, particularly Self-Sovereign Identity (SSI), is the goal of enabling digital identification in a manner that reduces or entirely removes dependence on central

*Corresponding author: rajveersinha694@gmail.com

authorities, thereby eliminating single points of failure. This approach entails the independent creation of identifiers by entities, the aggregation of identity claims from diverse sources, and the secure management and dissemination of these claims, all under the entity's complete control.

Leveraging decentralized technologies and cryptographic methods, SSI aims to bolster security and privacy, fostering an environment of transparency and minimal data usage. Despite its growing popularity, SSI is still in its nascent stages as a research field, unstructured and ripe with both opportunities and challenges. This study's objective is to offer a thorough understanding through a Systematic Mapping Study. It aims to categorize existing research, highlight current trends and demographic data, and pinpoint areas that warrant further investigation, thereby laying a groundwork for future research endeavours in this exciting and evolving field. The core of decentralized identity, particularly the Self-Sovereign Identity concept, lies the objective of providing a means for digital identification while minimizing or eliminating reliance on a central authority and eradicating a single point of failure. This involves entities independently creating identifiers, gathering identity claims from various sources, securely managing and distributing them, all while retaining full control of identifiers and associated identity data. The use of decentralized technologies and cryptographic primitives enhances security and privacy, achieving transparency and data minimization. Despite the growth, SSI remains a young, unstructured field in its early research stages, presenting numerous opportunities and challenges. This study aims to provide a comprehensive overview through a Systematic Mapping Study, classifying research papers, identifying trends, demographics, and potential research gaps as a foundation for future exploration.

2. Decentralized Identity

The advent of decentralized technologies has catalyzed the development of decentralized identity models, which seek to reduce dependency on intermediaries. The cornerstone of decentralization is the elimination of a single point of failure or vulnerability, achieved by minimizing reliance on central authorities [9], typically identity providers (IdPs) responsible for managing identities. In conventional identity management systems, IdPs centrally store and control personal data, or identity attributes. This centralized model, governed by the IdP's own privacy and security policies, has a profound impact on the security and utilization of personal data. Trust in the IdP becomes a critical factor for both entities requesting data and the data subjects themselves, in terms of the availability, integrity, and confidentiality of these attributes.

Decentralized identity approaches [10] offer an alternative to this centralized storage, mirroring traditional identity systems that use credentials issued by trusted third parties for identity verification or authentication. However, the distinguishing feature of these decentralized systems is their use of distributed ledger technology. This technology enables the storage of validated attestations on a distributed ledger, allowing for their subsequent validation without relying on a central authority [11]. This paradigm shift in identity management not only enhances data security but also empowers individuals with greater control over their personal information.

Decentralized identity approaches mark a departure from traditional models by eliminating the reliance on centralized identity providers (IdPs). Unlike the account-based or digital certificate-based systems of traditional and federated identity models, decentralized approaches are rooted in direct, peer-to-peer interactions. In this framework, various entities assume roles traditionally handled by a central authority [9], fostering an environment of decentralization, transparency, and enhanced user control over identity transactions [12]. These decentralized systems commonly utilize technologies like decentralized ledger technology (DLT), blockchain, distributed file systems, or other novel decentralized structures such as Hashgraphs and Tangle [13].

Open-source initiatives, particularly those under the Hyperledger umbrella like Hyperledger Indy, play a crucial role in the development of decentralized identities. These projects can be implemented independently or in tandem with other blockchain technologies [14], [15]. While blockchain is a commonly used technology in this context, it is not an exclusive requirement for decentralized identity systems. Alternative technologies, as previously mentioned, can effectively fulfill the same purpose [13]. However, blockchain's inherent characteristics often align well with the principles of Self-Sovereign Identity, making it a favorable choice in many implementations [16]. This flexibility in technology choice underscores the adaptability and innovative potential of decentralized identity models in reshaping digital identity management.

Self-Sovereign Identity (SSI) is a pioneering concept in the realm of decentralized identity models, granting entities like individuals, organizations, and even objects, the power to manage their digital identities autonomously, without the need for external authorities. This approach is instrumental in mitigating the risk of a single point of compromise or failure, thereby shifting the balance of power from traditional identity and service providers to the users themselves [17], [18]. At its core, SSI is inherently user-centric [19], enabling users to create and control their own decentralized identifiers (DID) without the intervention of third parties [20].

In the SSI framework, users can obtain identity attributes from third-party issuers, securely maintain their identifiers and associated personal data, and present them as needed for identity verification. This shift away from centralized third-party data storage bolsters security and privacy, substantially reducing the threats of data breaches and identity theft [21]. By placing users at the centre of the identity management process, SSI not only enhances individual data sovereignty but also fosters a more secure and resilient digital ecosystem. This evolution in identity management underscores the potential of SSI to redefine digital interactions in an increasingly interconnected world.

This transformative shift towards Self-Sovereign Identity is underpinned by an ecosystem designed to streamline the acquisition, storage, and sharing of verifiable credentials and claims. This system supports the creation of verifiable

presentations, including zero-knowledge proofs and techniques for minimizing data exposure, while also facilitating the verification of claims and identities. Central to this ecosystem is the concept of the trust triangle, encompassing issuers, identity holders, and verifiers, each playing critical and interchangeable roles based on the context.

In this ecosystem, the flexibility of roles allows for dynamic interactions among the entities. For example, an entity that acts as an issuer in one scenario could assume the role of a verifier in another. This adaptability enhances the robustness of the identity management process, ensuring that trust and security are maintained across different contexts and interactions. The integration of advanced cryptographic techniques, like zero-knowledge proofs, further reinforces privacy and security, enabling entities to verify credentials without exposing sensitive information. This holistic approach not only empowers users but also lays the foundation for a more secure and trust-based digital environment.

The Self-Sovereign Identity (SSI) concept, still in its developmental stages, has seen considerable efforts towards defining its structure, key components, and foundational principles necessary for its implementation [20], [22], [19], [23]. Wagner et al. [20] contributed significantly with a position paper that established a consensus on critical areas such as standardization, interoperability, regulatory concerns, privacy, and security. Mühle et al. [19] offered a comprehensive view of the SSI architecture, while Ferdous et al. [22] introduced a mathematical formalization, providing clarity with precise mathematical expressions and process flows.

The ten guiding principles of SSI, as outlined by Christopher Allen [23] and further categorized by the Sovrin Foundation into themes of security, controllability, and portability [19], have been instrumental in steering the ongoing discourse in this field. Additionally, Toth and Anderson-Priddy [24] expanded this framework by proposing five more principles, enriching the understanding of SSI's core values. Ferdous et al. [22] took a different approach, analyzing and extracting key properties from existing definitions of SSI, thereby categorizing them for a more structured analysis. These collective efforts represent a significant stride in conceptualizing and materializing the SSI framework, laying a solid foundation for its future development and application..

Self-Sovereign Identity (SSI) is a concept not confined to a single technology but often materializes through the use of decentralized ledger technology (DLT), blockchain, decentralized identifiers (DID), and verifiable credentials (VC), with standardization efforts led by The World Wide Web Consortium (W3C). DLT serves as a trustless, decentralized infrastructure for public-key cryptography, establishing a cryptographic foundation of trust [21]. DIDs are distinct, globally recognized identifiers that enable authentication without the need for third-party authorization [5], [13], while VCs are digital attestations issued by issuers, directly governed and managed by the identity owner [6]. In comparing decentralized identity with Self-Sovereign Identity, the literature and practical applications reveal noticeable differences, particularly in terms of identifier creation and the accumulation of identity attributes. Whereas decentralized identity systems often utilize existing, government-issued documents for identity establishment, SSI enables the creation of multiple identities, independent of such documents. SSI offers the capability to produce a vast array of identifiers, an attribute that proves highly beneficial in contexts like the Internet of Things (IoT). In contrast, decentralized identity frameworks might not fully align with the SSI principles concerning control, portability, security, and other key aspects previously mentioned. This distinction underlines the unique attributes and broader applicability of SSI in the evolving landscape of digital identity management [19].

3. Related Works

Numerous secondary research publications have explored various facets of decentralized and Self-Sovereign Identity (SSI) over time. Among these, Rouhani and Deters [29] conducted a comprehensive analysis of five studies that focus on the integration of smart contracts within decentralized identity systems. Their review categorizes the application of decentralized identity into seven key sectors: (i) healthcare, (ii) Internet of Things (IoT), (iii) identity governance, (iv) documentation and record management, (v) logistics and supply chain management, (vi) Business Process Management (BPM), and (vii) electoral processes.

This segmentation highlights the versatility and broad applicability of decentralized identity systems across various industries and domains. In each sector, decentralized identity offers unique benefits, such as enhancing security in healthcare, streamlining operations in supply chains, and introducing transparency in voting systems. The diversity in applications underscores the adaptability of decentralized and Self-Sovereign Identity frameworks, making them a pivotal component in the evolution of numerous industries.

In their comprehensive study, Maesa and Mori [2] examined six distinct applications of blockchain technology, focusing on areas such as (i) digital voting systems, (ii) medical record management, (iii) identity governance, (iv) access management, (v) decentralized authentication services, and (vi) logistics and supply chain oversight. Their detailed analysis involved pinpointing challenges within these domains and proposing blockchain-centric solutions, while also referencing established literature for each application area. Particularly in identity governance, they underscored the importance of Self-Sovereign Identity (SSI) frameworks, examining their characteristics in the context of blockchain deployment. While Maesa and Mori's research spanned a variety of blockchain applications, other studies like those referenced in [30] and [31] specifically zoomed in on the healthcare sector, acknowledging the transformative potential of blockchain in developing robust identity management systems.

These comprehensive studies were primarily dedicated to examining blockchain-based Self-Sovereign Identity (SSI) solutions in various contexts. In their work, Houtan et al. [31] divided such solutions sourced from academic and industrial research into five distinct categories: (i) management and safeguarding of data, (ii) digital identity systems, (iii) social

insurance frameworks, (iv) governance of social data, and (v) management of healthcare and patient-specific data. They aimed to harness the unique features of blockchain to create an interconnected healthcare ecosystem that empowers patients to manage their personal health data. While recognizing the potential of these solutions, their analysis also brought to light several challenges, including issues related to security, privacy, and the nascent stage of these technologies, highlighting their limited practical application in the real world. In a similar vein, Shuaib et al. [30] outlined the essential criteria necessary for the successful implementation of SSI in the healthcare sector. They explored the advantages of SSI and presented a practical use case that involved a variety of stakeholders, thus illustrating the practical implications and benefits of SSI in healthcare.

Furthermore, Mundhe et al. [32] embarked on an exhaustive survey that focused on authentication and privacy maintenance methods in Vehicular Ad Hoc Networks (VANETs), encompassing decentralized approaches that utilize blockchain technology. Their research meticulously categorized various schemes, shedding light on their respective advantages and limitations. A notable observation in their study was that the majority of the schemes they reviewed were dependent on centralized frameworks. This dependence on central authorities for the allocation of identities and the storage of certificates contradicted the fundamental decentralized ethos. This reliance underscores a critical challenge in the integration of decentralized principles within VANETs, pointing towards the need for more autonomous and decentralized solutions in the field of vehicular network security and identity management.

In their detailed analysis, Zhu and Badr [33] explored both conventional and blockchain-powered identity management systems, with a particular emphasis on their application in the Internet of Things (IoT). Their survey highlighted various solutions and pinpointed key challenges such as access management, privacy concerns, trustworthiness, and system performance. Similarly, Bartolomeu et al. [34] concentrated on the IoT domain, offering a comprehensive review of use-cases, technological aspects, and challenges associated with Self-Sovereign Identity (SSI). Their discussion extended to addressing technical hurdles, identifying effective practices, and the importance of standardization in the field of SSI. These studies underscore the growing significance of SSI and blockchain technologies in the IoT sphere, emphasizing the need for continuous innovation and standardization to overcome existing challenges and fully leverage the benefits of these emerging technologies.

Gilani et al. [35] and Kaneriya et al. [36] provided in-depth analyses of various blockchain-based identity management systems, particularly those purporting to support the principles of self-sovereignty. Gilani et al. [35] identified a notable absence of standardized evaluation criteria for these systems. Assessments and comparisons of different solutions often utilize varied criteria. Some have based their evaluations on principles such as the law of identity [18], [25], [37] or on the taxonomy of SSI [22], [38]. These evaluations are primarily technical in nature, focusing on distinctive elements in design and implementation, including network or blockchain types, methods of data storage, key management strategies, selective disclosure capabilities, the use of smart contracts, and compliance with GDPR.

In their exploration of SSI concepts and architectures, they uncover various research gaps and challenges. Bernabe et al. [21] took a deep dive into solutions that prioritize privacy preservation, addressing the intersection of privacy, blockchain technology, and identity management systems, particularly those based on SSI. Their analysis of existing solutions included a comprehensive examination of features and privacy concerns, with a special emphasis on GDPR compliance. This collective body of work highlights the complexity and diversity of blockchain-based identity management systems, underscoring the need for continued research and development in this field to fully realize the potential of SSI in a privacy-conscious world.

Kuperberg [39] undertook a systematic assessment of blockchain-based identity and access management systems, developing a comprehensive evaluation framework that encompasses 75 distinct criteria. This framework was utilized to scrutinize 43 different solutions, examining them across a range of factors. These factors included the functionality available to end-users, the adaptability and mobility of the solutions, system overhead, adherence to compliance and regulatory standards, the extent of standardization, and the ease of integration with existing systems. This meticulous analysis by Kuperberg provides a detailed and nuanced understanding of the current landscape of blockchain-based identity and access management solutions, offering valuable insights into their capabilities, limitations, and areas for potential improvement.

Liu et al. [25] embarked on a thorough review and comparison of blockchain-based identity solutions like Sovrin, uPort, and ShoCard, applying Cameron's law of identity as a foundational framework. Their extensive research included a deep dive into academic databases and patents, resulting in a categorization of relevant papers into three key areas: authentication, privacy, and trust. They pinpointed significant research gaps and challenges, particularly focusing on issues related to identity, such as data breaches and modifications in identity wallets.

Similarly, Rathee and Singh [40] performed a detailed literature mapping of blockchain-based identity management, examining 30 primary studies published from 2009 to 2020. Their investigation aimed to uncover research trends, identify challenges, and examine various frameworks, initiatives, and projects that utilize blockchain in identity management, including an analysis of popular consensus algorithms. While they acknowledged the immense potential of blockchain technology in addressing the drawbacks of traditional identity management systems, they also highlighted ongoing issues related to privacy and interoperability, indicating areas in need of further exploration and development in the field.

These investigations, in contrast to earlier ones, focus on a range of technical and regulatory factors in their assessment of blockchain-based identity management systems. They offer a detailed critique of the challenges and opportunities in this

field. Our research encompasses a broader collection of studies, providing a more thorough classification and enhanced data visualization techniques. Uniquely, it considers both blockchain and non-blockchain implementations, deliberately omitting studies that depend on a centralized authority for identity registration.

While the secondary studies previously mentioned relate to our research in various ways, studies [25], [40] are particularly relevant. However, these studies have certain limitations: they do not (i) incorporate non-blockchain implementations into their analysis, (ii) clearly differentiate between decentralized identity and Self-Sovereign Identity models, (iii) classify papers according to their specific contributions, application domains, IT fields, or types of research conducted. Our study addresses these gaps, providing a more comprehensive and multi-dimensional view of the current state of identity management research.

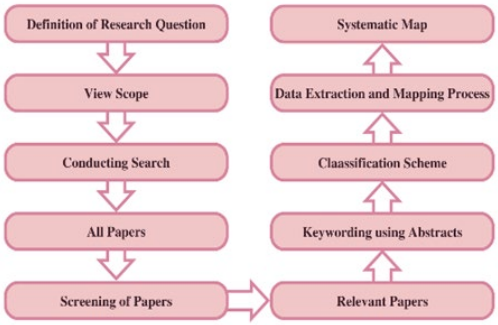

Fig. 1. Systematic mapping process

4. Research Methodology

To further elaborate on the methodology discussed in the previous section, it's important to note that while several studies have adopted survey methods or Systematic Literature Reviews (SLR) for in-depth examination of primary research within specific areas, the application of a Systematic Mapping Study (SMS) is pivotal for gaining a more expansive insight. This approach is particularly effective in identifying broader trends and demographic information across extensive research areas [41], [42]. The SMS process is designed to: (i) systematically structure and define the research field of interest, (ii) create a robust classification scheme, (iii) sort and categorize the collected studies, (iv) analyse and display the frequency of publications across various classification categories, and (v) visualize the results through detailed and informative classification maps. These maps serve as a pivotal outcome of the SMS, providing a visual interpretation of the studies in relation to specific research questions and offering an insight into the depth of coverage across different research categories.

Considering the nascent stage of decentralized identity, especially Self-Sovereign Identity (SSI), which currently lacks a well-structured research framework, it's evident that extensive future research is required for its broader adoption. In this context, a Systematic Mapping Study (SMS) is invaluable for identifying existing research voids and highlighting areas ripe for further exploration. This approach, aligning with the methodologies proposed by Petterson et al. [41], [42], is instrumental in laying the groundwork for future scholarly work. The SMS process encompasses several key steps:

i. Formulating Research Questions (Sections IV-A and IV-B).
ii. Developing a Search Strategy and Executing the Search (Sections IV-C and IV-D).
iii. Selection and Screening of Papers (Section IV-D).
iv. Keyword Analysis and Development of a Classification Framework (Section IV-E).
v. Gathering Data, Classifying, and Mapping the Studies (Section V).

Each phase plays a critical role in achieving the final results, which are visually represented in Fig. 1 and detailed in the subsequent sections of the study.

The primary goal of this SMS is to thoroughly understand the current state of knowledge and research in the realms of decentralized and Self-Sovereign Identity. The aim is to present a broad-brush overview of research papers, categorizing them based on established criteria. Furthermore, this study seeks to ascertain the extent and nature of existing research, uncovering trends, demographic patterns, prevailing challenges, and unexplored areas in the field of SSI. The overarching objectives of this research include:

i. Delving into a research subject of interest within the realm of decentralized and Self-Sovereign Identity.
ii. Identifying the diverse types of contributions made within both primary and secondary literature.
iii. Quantifying the prevalence of decentralized identity solutions that adhere to the principles of Self-Sovereign Identity.
iv. Analysing the various research methodologies and types of research conducted in the pertinent research papers.
v. Determining the domains and IT fields addressed in the relevant body of research.
vi. Uncovering the demographics of the literature and tracing the evolving research trends over time.

These objectives are meticulously crafted to align with the formulated research questions and sub-questions (RQs), ensuring a comprehensive and systematic exploration of the decentralized and Self-Sovereign Identity domain.

5. Research Questions

In line with the insights derived from our extensive literature survey and the pre-established research objectives, we have developed a set of research inquiries (RI) along with related sub-inquiries:

RI1: What is the central theme in scholarly articles addressing decentralized and Self-Sovereign Identity systems? What is the scope of this research?

- What advancements have been made in the field of decentralized identity, and how can these studies be classified in terms of their contributions? (RI1.1)
- In the sphere of decentralized identity solutions, what proportion adheres to the concepts of Self-Sovereign

Identity? (Assessing the ratio of SSI to decentralized identity) (RI1.2)
- What kinds of research methods have been utilized in pertinent scholarly papers? (RI1.3)
- What sectors have seen the application or study of decentralized identity solutions? (RI1.4)
- How can decentralized identity solutions be segmented according to their role in the information technology sector? (RI1.5)

RI2: What are the evolving patterns and demographic characteristics of the literature in the decentralized identity arena?
- Annually, how many academic articles concentrating on decentralized identity have been released? (RI2.1)
- In terms of the volume of publications, in which forums have studies on decentralized identity been disseminated? (RI2.2)
- Reflecting on the institutional connections of the authors, which nations have made significant contributions to the decentralized identity field? (RI2.3)

In the following segment, we outline our research methodology, which includes choosing appropriate academic databases, pinpointing key terms, and crafting search queries. Subsequently, we elaborate on the process of conducting a thorough search to locate pertinent studies that align with our defined research inquiries.

6. 6. Search Strategy

Upon establishing our research inquiries, we proceeded to select relevant key terms and construct a detailed search phrase. This phrase was carefully designed to provide a thorough overview of the entire scope of our research topic, ensuring a wide-ranging investigation of the area.

A. Key Terms

The chosen key terms include: "Self-Sovereign Identity," "decentralized identity," "identity via blockchain," and "decentralized digital identifier."

B. Refined Search Phrase

Our refined search phrase is: ("SELF-SOVEREIGN" OR "SELF SOVEREIGN" OR "DECENTRALIZED" OR "BLOCKCHAIN" OR "BLOCK CHAIN") AND (IDENTITY OR IDENTIFIER).

We limited our search to two leading academic databases in the computer science domain, IEEE Xplore and Science Direct, to focus on (peer-reviewed) scholarly articles and avoid non-specialist and popular media sources. Additionally, we included Scopus in our research scope, as it aggregates works from both IEEE Xplore and Science Direct.

A key component of our search methodology involved tailoring the search phrase to align with Science Direct's specific requirements. The platform's constraints on wildcard usage necessitated altering 'DECENTRALI*ED' to 'DECENTRALIZED'. Nonetheless, the primary composition of our search phrase was maintained uniformly across both databases.

Employing this adjusted search phrase, we executed our search within the chosen databases, ensuring that the results were pertinent to the field of computer science and covered the period from 2012 to 2021.

Our decision to focus on literature from 2012 onwards stems from the rise in prominence of decentralized and Self-Sovereign Identity concepts, which notably began to gain significant attention around 2015. The discussion of blockchain-based identity systems notably intensified during the Internet Identity Workshop (IIW) in the spring of 2015, highlighting the increasing interest in decentralized technologies, especially blockchain, for their potential to transform identity management [3]. Blockchain technology, with its inherent features, offers considerable advantages for digital identity solutions and addresses various limitations found in conventional Identity Management (IdM) systems.

Therefore, to cover the crucial period of development and recognize the uptick in dialogues and technological progress, our selection included publications from 2012 forward. This approach provided a two-year margin to guarantee an extensive and thorough inclusion of relevant literature.

C. Limitations

Our research encountered various constraints. Initially, it was limited to (i) two particular databases, (ii) articles written in English, and (iii) papers published from January 2013 to January 2021. The process of locating relevant articles depended exclusively on searches within these databases, overlooking possible external sources and not employing the snowballing technique during the analysis of the full-text articles.

D. Inclusion and Exclusion Criteria

To effectively filter the gathered papers, we developed specific criteria for inclusion and exclusion, as outlined in Table 1. The selection process was conducted in stages, as illustrated in Fig. 2. Initially, papers were retrieved through (i) applying the search phrase in the selected databases. They were then excluded based on (ii) year and type of publication, (iii) the analysis of the title, abstract, and keywords, and ultimately, (iv) an in-depth review of the complete text.

7. Classification scheme

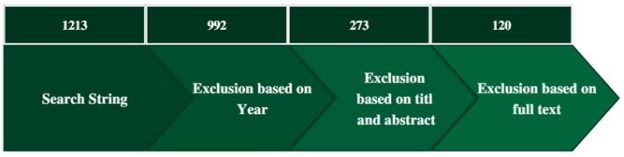

Fig. 2. Gradual reduction of the number of papers through the screening process

In the process of evaluating the research papers, we devised a categorization system by extracting essential ideas from titles, keywords, and abstracts. This structure allowed us to understand the essence of each study and acquire a holistic grasp of the research area. Our attention was concentrated on diverse elements corresponding to our predetermined research

questions, serving as crucial categories, namely: (i) contributions and (ii) application areas.

In the process of screening the papers, we established a categorization framework by deriving key themes from titles, keywords, and abstracts. This approach facilitated a thorough grasp of each study and offered a deeper insight into the wider research field. Our examination focused on various facets corresponding to our established research inquiries, serving as key categorizations, specifically: (i) contributions, (ii) application sectors, (iii) information technology areas, (iv) publication venues, (v) nature of research, and (vi) methodologies employed. These classifications and their subcategories formed the foundation for sorting papers and illustrating findings through structured maps, as depicted in Table 2. Every selected paper was categorized into one or more relevant groups.

The selected research papers contributed variously to the field of decentralized identity, including new systems, approaches, architectures, models, methods, and frameworks, along with various IT aspects such as IoT, cybersecurity, data privacy, trust mechanisms, functionality, and user interaction. These works spanned a range of sectors, encompassing education, healthcare, transport, logistics, banking, and financial services. We classified these papers according to the typology suggested by Wieringa et al. [43], which identifies six types of research contributions:

1. Solution Proposals: These papers introduced new or significantly improved solutions (like an architecture, model, or framework) but lacked extensive validation or practical implementation.
2. Validation Research: This type included the substantiation of proposed solutions through prototypes, experiments, simulations, mathematical proofs or analyses, yet without real-world deployment.
3. Evaluation Research: This category involved solutions that were applied and tested in real scenarios, demonstrating problem-solving effectiveness.
4. Philosophical/Conceptual Papers: These focused on theoretical constructs, offering fresh viewpoints and theoretical models. Our evaluation criteria slightly diverged from Wieringa et al. [43], incorporating primary and secondary papers, categorizing surveys, Systematic Literature Reviews (SLRs), and Systematic Mapping Studies (SMS) within this segment.
5. Opinion Papers: These presented the authors' subjective stances on specific topics, either endorsing or critiquing them.
6. Experience Papers: These shared practical insights and experiences in applying various frameworks, tools, systems, or other solutions.

Our methodology facilitated accurate categorization of the papers under these defined types.

8. Results and Systematic Maps

Following the selection of articles that satisfied our inclusion criteria and the creation of a categorization framework, we began extracting data and organizing the papers according to their respective contributions, application domains, IT fields, types of research, research methodologies, and contexts of publication. Furthermore, we documented whether the studies explicitly focused on Self-Sovereign Identity (SSI), decentralized identity, or related concepts such as Self-Sovereign Identity, decentralized identifiers, and verifiable credentials.

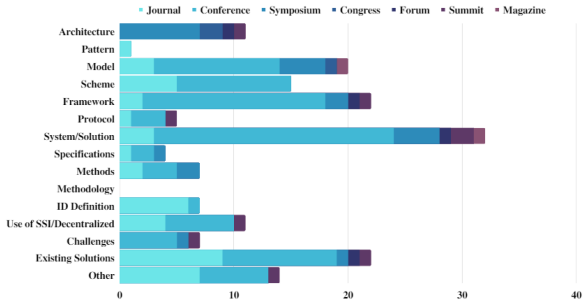

Fig. 3. Classification map, representing the intersection between papers

A. Contribution

The systematic mapping procedure resulted in a variety of maps and visual representations that encapsulate a range of research viewpoints. The main classification map, shown in Fig. 3, offers a comprehensive view of research focusing on contributions, types of research, domains, and IT areas within the decentralized identity sphere. This map illustrates the array of contributions found in decentralized identity research, outlines the nature of research undertaken in the relevant studies, highlights the fields where decentralized identity has been researched or implemented, and identifies the most commonly addressed IT areas. Importantly, this map addresses our first research question (RQ1.1), exploring the kinds of contributions and domains investigated. The specific proportion of Self-Sovereign Identity to decentralized identity solutions proposed or verified (RQ 1.2) is depicted in Fig. 3.

B. Demography

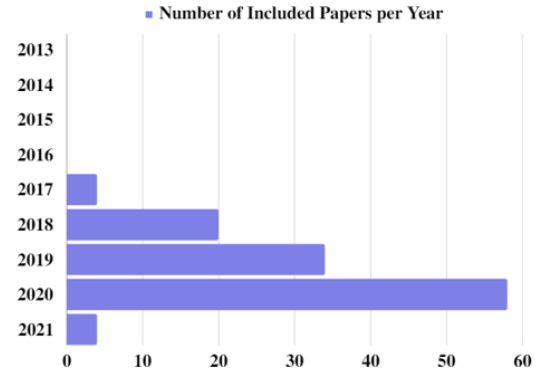

Fig. 4. Number of papers published over the years

To address Research Question 2.1 (RQ2.1), concerning the annual frequency of publications, we charted the number of papers published each year, as visually depicted in Figure 4.

Moreover, in exploring the dissemination channels of pertinent papers (Research Question 2.2, RQ2.2), we classified

the publications into various formats, such as journal articles, magazines, conference proceedings, symposia, summits, forums, workshops, and congresses. Figure 5 illustrates the distribution of these papers among these diverse publication formats.

9. Discussion

A. Decentralized Identity Research Dynamics

The realm of decentralized identity research has experienced a significant uptick in academic focus in recent times, displaying a pattern of rapid expansion. The evolution of scholarly works on decentralized identity shows a steady increase from 2017 through 2021, marking an impressive growth of 96.7% in total publications during these years. This notable rise highlights the sustained interest and ongoing contributions in this burgeoning area. Nevertheless, it is important to consider that the study's wrap-up in January 2021 may have influenced the diminished publication count for that year, suggesting a possible continuation of this trend beyond the study's timeframe.

B. Database Representation and Publishing Venues

Upon examining the distribution of papers across various databases, it becomes evident that IEEE Xplore was the predominant repository, holding 108 papers (90%), in contrast to Science Direct's smaller share of 12 papers (10%). The research findings were primarily published through a range of platforms, with the majority appearing in conference proceedings (56.7%). Publications were also dispersed via academic journals (24.2%) and symposiums (8.3%), reflecting a diverse approach to disseminating research in this area.

C. International Participation and Geographic Distribution

The research arena showcased a wide-ranging geographical involvement from different corners of the globe. Leading this participation was the United States, representing 19.2% of the studies, with China closely trailing at 13.3%, and both the United Kingdom and Germany contributing 11.7% each. Such international representation underscores the extensive commitment and curiosity in decentralized identity research across varied geographic areas, highlighting its global importance and applicability.

D. Classification of Contributions and Key Terms

The collection of selected papers encompassed a wide spectrum of contributions. Predominantly, primary research introduced new systems or solutions (26.7%), advanced architectural designs (18.3%), and comprehensive frameworks (18.3%). On the other hand, secondary research primarily engaged in comparative analyses of existing solutions (18.3%) or provided detailed syntheses of the domain. Notably, a significant portion of these studies explored topics related to Self-Sovereign Identity (68.3%) and decentralized identifiers (56.7%), with a lesser portion (33.3%) focusing exclusively on decentralized identity, excluding self-sovereign elements (RQ1.2).

E. Investigating IT Fields and Types of Research

In our detailed analysis of Information Technology (IT) areas, significant emphasis is observed in the Internet of Things (IoT) (24.2%), complex IT frameworks (25.0%), cybersecurity (18.3%), trust mechanisms (15.8%), and data privacy (13.3%). However, areas like user functionality (0%) and experience (0.8%) received scant attention, presenting an interesting avenue for future research and innovation. Regarding the types of research conducted, validation studies (47.5%) and proposals for new solutions (30.0%) were predominant, whereas evaluation research comprised a minor segment (0.8%) of the overall research fabric.

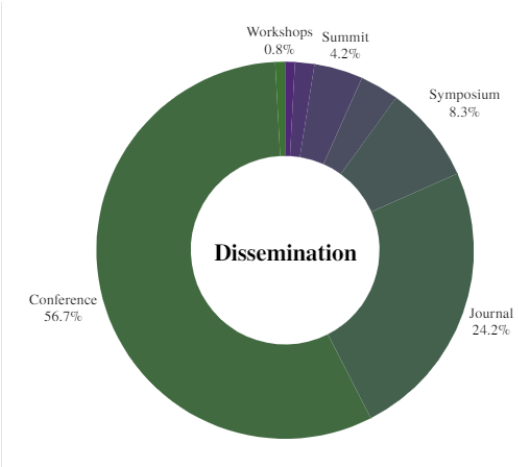

Fig. 5. Dissemination of papers addressing decentralized identity

F. Sectoral Focus and COVID-19's Impact

While a significant portion of the research (57.5%) remains broad and non-specific, targeted fields such as transportation, healthcare, financial services, governmental services, online retail, logistics and manufacturing, and education have garnered notable interest. The emergence of the COVID-19 pandemic has markedly accentuated the applicability of decentralized identity. Emerging research has proposed the use of digital health passports, immunity verification documents, and secure health data wallets, underscoring the crucial role and possibilities of decentralized identity in tackling contemporary global challenges.

10. Final Reflections and Prospective Pathways

In the realm of decentralized identity, particularly regarding Self-Sovereign Identity, there lies significant potential to address the existing limitations of traditional identity management frameworks. The ongoing increase in research publications indicates a dynamic and evolving field, which is still in the process of achieving full structure and standardization. Future research directions may include in-depth investigations into specific areas, refining the defining features of self-sovereign systems, examining the varying degrees of decentralization, and evaluating critical factors like usability and user experience for broader adoption. Efforts such as comprehensive systematic literature reviews or studies examining the impact of usability are poised to make substantial

contributions to the expanding field of decentralized identity research.

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.

[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 quantifi- able 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 manage- ment 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 Inter- net 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.