IEEE Access
Multidisciplinary | Rapid Review | Open Access Journal

Received 10 February 2023, accepted 3 March 2023, date of publication 13 March 2023, date of current version 17 March 2023.

Digital Object Identifier 10.1109/ACCESS.2023.3256519

SURVEY

A Systematic Literature Mapping on Using Blockchain Technology in Identity Management

T. T. TRAM NGO, T. ANH DANG, V. VUONG HUYNH, AND T. CONG LE
Viettel Solutions, Viettel Group, Hanoi 100000, Vietnam

Corresponding author: T. T. Tram Ngo (tramntt3@viettel.com.vn)

This work was supported by Viettel Solutions, Viettel Group.

ABSTRACT Although blockchain is an emerging technology, it has been applied in a lot of domains by leveraging its features. Traditional identity management systems have many issues regarding security and privacy of personal data. Blockchain has the potential to mitigate and avoid such issues by creating trust among the parties involved in the system while reducing reliance on third-party authorities. The first blockchain-based identity management solutions were launched in 2016. Since then, due to high demand, numerous primary and experimental studies, and intatives have been carried out to provide solutions to this research topic. Along with that, there are also a lot of secondary studies to overview the current state of research on this topic. However, the number of systematic research articles is still limited and each research has its limitation. Through this study, we provide a novel systematic literature including categorization of studies into predefined categories (domain, research type, place of publication), analysis of publication frequency, co-authorship, number of papers citing each paper of all studied papers. Comparing to other systematic literature mapping studies, our paper provides a more comprehensive view of the studied articles. In particular, we analyze the number of citations, which no study has ever done. In this research, we studied 361 papers published from January 2009 to April 2022 in four big databases (IEEE Explore, ACM Digital Library, ScienceDirect, Springer Link), the largest number of articles studied compared to previous researches. The obtained results show that most of the articles under validation research type (providing solution and implementing that solution but not in real-world scenarios) propose solutions/systems, models/schemes and architectures to address general problems. We also find that the majority of authors works alone or collaborate in a separate group and co-work in only one paper. This shows that there is no long term collaboration in blockchain-based identity management, and thus subsequent publications presenting real-world blockchain-based identity management products do not exist.

INDEX TERMS Blockchain, identity management, decentralization, self-sovereign identity, systematic mapping.

I. INTRODUCTION

The identity is a mean to diffirenciate a holder (citizen, business, administration) from any other. In this increasingly digital-led world, most people have at least one digital identity that helps them to prove electronically that they are who they claim to and thus get access to services. Instead of using traditional physical document (such as a passport, a driver's license or a government-issued ID), the digital identity verifies that an identity matches their real-world identity using e-mail adress, username – password …The digital identity has its advantages in eliminating use of physical documents, but it has also some disadvantages that come from the fact that it is mostly stored in central repositories and managed by third-party entity. Centralized storage is risky and a target for hackers. Data managed by third-party entity leads to privacy issues. Therefore, it is neccesaire to introduce new strong Identity Management (IdM) solutions to deal with these issues.

Identity management (IdM), also known as identity and access management (IAM) allows only authorized people to have access to the services provided to them. In an IAM

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

system, there are two principal actors: users and service providers (SP). Each user is provided an account and the means to demonstrate to SP that he is the owner of that account. There is an issue in managing identity of user as each user usually has a lot of digital identities corresponding to diffirent SPs. It means that users must memorize many username/password couples or they use same password many accounts. It is unsecure and influences the users' privacy. There have been scandals about the security lack and leakage of users' personal data due to hacking or as companies holding the user's identity sell or use it for purposes not authorized by the user. To overcome problems of existing IdM systems, it is neccessaire to have solutions applying new technologies that minimize, even eleminate central storage and do not depend on third-party entity. This is where blockchain - distributed ledger technology comes into play.

Blockchain-based IdM solutions have been around since 2016. Since then, there has been a lot of primary research on this topic [1], [2], [3], [4], [5], [6]. Along with that, there are also a lot of secondary studies to overview the current state of research on this topic ([7], [8], [9], [10], [11], [12], [13], [14]). However, the number of systematic research articles is still limited ([15], [16], [17]). Through this study, we provide a systematic mapping study including categorization of studies into predefined categories (domain, research type, place of publication), analysis of publication frequency, co-authorship of all the identified studies. In this research, we studied 361 papers published from January 2009 to Avril 2022 in four big databases (IEEE Explore, ACM Digital Library, ScienceDirect, Springer Link).

The remainder of this paper is structured as follows. In section II, some basic concepts of IdM system and blockchain are presented. Section III presents related work regarding secondary studies that are most related to our work as well as highlights differences of our work in comparison to them. In Section IV, we describe the research methodology in details, and respective results are presented by anwsering the research question in Section V. Discussions with in-depth analysis about the results will be given in Section VI. In the last section, we present our conclusions.

II. PRELIMINAIRES

In this section, we will introduce some basic concepts that contribute to a blockchain-based IdM system: definition of IdM, IdM models, IdM system requirements, building blocks of blockchain, blockchain types as well as applications of blockchain.

A. IDENTITY MANAGEMENT

Identity and access management (IAM), also known as identity management (IdM), is a combined term used to create, manage digital and electronic user identities, and regulate user access to on-premises and in-cloud assets of an organization [18]. IAM and IAM tools work to secure systems and sensitive data. They do this through: Password management; two-factor and multi-factor authentication; provisioning software; reporting and monitoring applications; biometrics; behavior analytics [18].

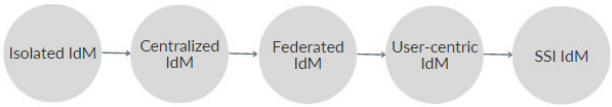

FIGURE 1. The evoluation of IdM models.

IdM - an interesting topic of research - is increasingly attracting attention in today's digital world where the majority of the population has a digital identity. Nowadays IdM system plays an important role, therefore, there are many standards, frameworks, criteria that help ensure right operations of this kind of system. We may list here somes such as: the Security Assertion Markup Language (SAML) [19], the Web Services Federation (WS-Fed) [20], the Identity Federation Framework (ID-FF) [21], and the Identity Web Services Framework (ID-WSF) [22], the Open Authentication (OAuth) [23], and the OpenID [24]. In spite of these standards, frameworks and criteria, traditional IdM systems have inherent issues when users have to memorize a lot of passwords while using many IdM systems. To address these issues, there have been many IdM models proposed ([25], [26]). We can classify them into five categories: Isolated IdM; Centralized IdM; Federated IdM; User-centric and Self-Sovergein Identity (SSI). The evoluations of this five models is presented in Fig. 1.

1) IdM SYSTEM MODELS

- **Isolated IdM:** In this model, user identity data belongs to each service provider. It means that the identities of this service provider cannot be used in other service providers. This model is very simple to implement. However, it has some following limitations: (1) it cannot scale when number of SPs increases and (2) the users need to remember their identity information for every single SP, or face the risk of insecurity when using the same identity information.
- **Centralized IdM:** There is only one common identity provider in the trusted domain in this model. This means that in the same trusted domain, the user utilizes only one identifier and credential to access to all service providers. Therefore, it should be careful to select the identifier.
- **Federated IdM:** In this type of model, there is a trusted model and a federation including multiple identity providers. This model enables their users to use the same identity information for all service providers within the federation. For example, a user of Facebook can choose to sign in to another website using either their identity information for the website or their Facebook account information.
- **User-centric IdM:** This type of model empowers users to control their own digital identities. Users have the right to select their credentials when responding to an authentication or attribute requester and it gives users

more rights and responsibility over their identity information [27].

- **SSI:** In the self-sovereign Identity model, the ownership of data is given to users in order to enable them to control their personal data and increase transparency of the system. The benefit of using this model for users is possibility to control their information without depending on third parties. This avoids data lost or misuse of sensitive information.

2) IdM SYSTEM REQUIREMENTS

To build a good IdM system, there are several requirements to satisfy [28]. In this section we enlist some of them and explain each requirement very briefly.

- **Security:** An IdM system manages access to different services such as social network activities, blogging, and emailing, Government services, online banking, e-commerce activities, etc. For each service, there are different levels of security. Therefore, to ensure right operations for each service, a minimum security is required.
- **Privacy:** Nowadays, it is very important to protect the privacy of user, user identity. Configuring a IdM with mechanisms by which privacy can be guaranteed (such as Privacy Enhancing Technologies) should allow protecting user privacy and user identity.
- **Interoperability:** If any IdM system can well interoperate with other existing systems, it should be a very good system.
- **Truthworthiness:** A successful IdM system needs to demonstrate to users its truthworthiness in order for users to trust it. From the user's point of view, they must also trust the system to provide sensitive personal information.
- **Affordability:** Price is a crucial factor in attracting users for a new system. Therefore, the price of a new system should not be higher than that of existing systems. In addition, providing new features is also appreciated for a new system.

B. BLOCKCHAIN TECHNOLOGY

Blockchain was an emerging technology introduced in 2009 by Satoshi Nakamoto with its first whitepaper about "Bitcoin" [29]. A blockchain is a distributed database or ledger that is shared among the nodes of a computer network [30]. Blockchain is a peer-to-peer network and makes transactions transparent through its consensus mechanism [29]. Transactions after including in blockchain will be never deleted or modified. By leveraging this feature and consensus mechanism of blockchain, this technology can be used to eliminate participation of central authorities and used for decentralized solutions.

To understand more about blockchain, we will describle terms that are most mentioned while talking about blockchain: block, node, consensus, Merkle tree, mining, smart contract, incentive.

- **Block:** is a building block of blockchain - a set of transactions happened in the peer-to-peer network. It's also considered as a page of the distributed ledger of blockchain. A block is added to the blockchain after processing a mechanism called "consensus".
- **Node:** is a computer representitng the owner of transactions [31], and participates to validate and store the complete history of transactions on the network.
- **Consensus:** is utilized to preserve agreement among the nodes in the network [32]. Through this, consensus algorithms establish reliability and trust in the Blockchain network. Most popular consensus of blockchain enlisted are: proof-of-work, proof-of-stake, Practical Byzantine Fault Tolerance…
- **Mining:** Mining is the process by which new block is created and added to the blockchain [33]. The node who is responsible for this process is called "miner". Mining also serves to secure the blockchain system against fraudulent transactions or transactions spending the same amount of bitcoin more than once, known as a double-spend [33].
- **Merkle tree:** is a efficient and secure structure to encode data about transactions in blockchain. It also allows for efficient and secure verification of content in a large body of data.
- **Smart contract:** A "smart contract" is simply a program that runs on a blockchain. It's a collection of code (its functions) and data (its state) that resides at a specific address on the blockchain [34].
- **Incentive:** when a miner completes mining a new block of blockchain, he gains some forms of incentives.

III. RELATED WORKS

In order to deal with issues of traditional IdM systems (central storage and reliance on third-party authorities), blockchain technology has been applied in this field. By leveraging the concepts of distributed immutable ledgers and consensus mechanism of blockchain, it is easy to implement distributed identity by providing a trusted online storage of digital identities, credentials, and revocation registries [78].

Although blockchain-based IdM is still a new research topic, there is already a lot of primary research on the topic. Along with that, there have also been many secondary studies analyzing and synthesizing them to give an overview of this research topic [15], [16], [17], [31], [36], [37], [38], [39], [40], [41], [42]. Of the secondary papers mentioned above, only [15], [16], [17], [41], [42] presented search strategies. And to the best knowledge of the authors, there are few secondary studies [15], [16], [17] that perform Systematic Mapping Study (SMS) with description about their search strategy.

Rathee and Singh [15] provided a systematic mapping of 30 primary stuties published from 2009 to 2021. The aim of

this research are: 1) find out the research trends in IdM using blockchain, 2) understand the challenges in IdM and report whether block-chain can solve the IdM challenges, 3) scrutinize and understand how the different frameworks of IdM would deal with security, integrity, and privacy problems, 4) know about initiatives taken for IdM using blockchain, 5) which consensus algorithms are popular among blockchains, 6) know about the research projects going on in the field of IdM using blockchain. They concluded that blockchain technology has possibility to address inherent issues of conventional IdM systems with some challenges about privacy and interoperability to overcome in the future with more researches.

In [16], a systematic mapping of 120 studies from 2009 to 2021 was adopted to provide a coarse-grained overview of decentralized and Self-Sovereign Identity. In addition, this study structures the research area by identifying, analyzing, and classifying the research papers according to predefined parameters (their contribution, application domain, IT field, research type, research method, and place of publication). They also provided insights into trends, demographics, challenges, gaps, and opportunities for future research. The results of this stydy show that the research articles mainly provide new solutions and models, which are only researched and implemented in test environment, not many studies have put them into practice. Most articles focus on general rather than a specific domain.

Reference [17] presents a rigorous systematic mapping and systematic literature review covering theoretical and practical advances in Self-Sovereign Identity of 57 studies from 2016 to 2021. In order to construct a classification scheme of identified studies, the authors defined and answered four research questions. This classification scheme was used to categorize and review publications. They also disscussed about open challenges of SSI.

In [41], a systematic review of 36 research efforts and patents that introduce SSI applications was conducted by Liu et al. In particular, authentication, privacy, and trust aspects were assessed. The results show that some issues and implications still exist after integrating blockchain technology. Issues arise when users lose their blockchain identities and when they need to change them and the cost of SSI integration and existing systems.

In [42], a systematic review of 43 blockchain-based SSI market offerings was presented. However, the authors did not describe how to select them. In this revieu, these 43 offerings were assessed using 75 criteria including compliance and liability, end-user experienct, technology, implementation, integration and operation criteria. The results of the review show that no reviewed application meets all criteria and no SSI solution has the maturity of conventional IAM offerings; a production-level integration standard (such as OAuth [23] and SAML [19]); and OS-level integration.

In [38], a survey about traditional and blockchain-based IdM systems for IoT devices was presented by Zhu and Badr. This survey identified solutions and challenges focusing on authentication, privacy, trust and performance. The authors concluded that SSI solutions are necessary for IoT devices by it nature and it should be careful to use public blockchain while storing and maintaining in IoT devices, therefore we could use private blockchain as an altenative.

There are three surveys that produced similar outputs [31], [37], [40]. The all three did not describe their search strategy. They all focused on the blockchain framework and the type of the blockchain network (public, private, permissionless, permissioned, cortium) that are used in the surveyed works. In particular, 8 SSI offerings were reviewed by Gilani et al. [31]. The review presented in detail about which offering support selective disclosure of personal information. It detailed also the way to manage cryptographic keys and blockchain-specific details (how to store credentials, on or off ledger). Besides, Kaneriya and Patel [37] reviewed 6 SSI systems as well as proposed enhancements for each system to perform in the future. Lastly, in [40], 15 applications were reviewed by Lim et al. The applications are for-profit and non-profit company-made, government-related, and open-source ones. The authors emphasized that it is ideal to apply SSI solutions to proper user-centric, secure and cost-effective IAM.

Another work [36] does not specify the way to select the reviewed works. It reviewed 10 SSI systems using blockchain by analysing their attendance to the ten principles of SSI [43]. They analysed in details which principle each paper satisfies.

In [39], Mühle et al. proposed ‘‘four basic components of SSI’’: identification, authentication, verifiable claims and attribute storage. As a result, they conducted a discussion about how research works and market offerings try to provide solutions for each of four components.

Among all the secondary studies mentioned above, the studies [15], [16], [17] are the most related to our research. Based on them, we combined the strengths and eliminated disadvantages of each study to create our own. Our study covers more papers than all the three studies (361 papers compared to 30, 120 and 57 relatively). Comparing to [15] and [17], our research provides more information about demographics and a classification of research papers into predefined categories (application domain, contribution, research type and identity type). [16] does not include co-authorship network and not analyse number of citations.

IV. RESEARCH METHODOLOGY

As far as, there are a lot of primary studies on identity management using blockchain. As mentioned in the previous section, although there are few secondary studies on this topic, there are only three systematic mapping studies ([16], [17], [15]). Each has its own limitations that need to be improved. In order to provide a novel coarse-grained overview that could complete the gaps of previous researches, the author follows a popular method called ‘‘systematic mapping’’ presented by Peterson et al. [44]. In detail, we perform the following steps:

1) Defining the objectives of research (section IV-A)
2) Determining research questions (section IV-B)
3) Constructing search strategy and conducting a search in order to identify revelant papers (section IV-C)
4) Defining selection criteria (inclusion and exclusion) to filter only relevant papers (section IV-D)
5) Constructing a classification scheme (section IV-E)
6) Presenting classification results using maps (section V)
7) Discus in detail of all results (section VI)

The steps are decribed in details in the following sections.

A. RESEARCH OBJECTIVES

As mentioned above, this research's purpose is to obtain a novel coarse-grained overview and a approriate classification of existing research papers in the literature. Besides, this research also provides insights about trends, demographics, relationship between authors and co-reference network of the identified papers.

B. RESEARCH QUESTIONS

According to the objectives defined in the previous section, we obtain the research questions (RQ) and sub-questions as followings:

- RQ1: What are the trends and demographics of research papers?
  - RQ1.1: How many papers are published each year?
  - RQ1.2: Where are they published (conferenece / journal ...)?
  - RQ1.3: Which countries invest the most in this topic based on the organizational affiliation of the researchers?
  - RQ1.4: What is the co-authorship network of the identified papers?
  - RQ1.5: How does the community pay attention to the all the identified papers (reflected in the number of articles that cite these articles)?
- RQ2: What do the papers focus on?
  - RQ2.1: What are main contributions of research papers in identity manangement?
  - RQ2.2: In which domain are blockchain-based identity management solutions applied?
- RQ3: What are the research types and identity types of the papers?
  - RQ3.1: In which type of research should each paper be classified?
  - RQ3.2: What is the ratio between SSI and decentralized identity among all identified papers?

C. SEARCH STRATEGY

According to the objectives defined in the previous section, we propose a research strategy.

First of all, a database to collect research papers is provided. Among a lot of scientific databases in the field of computer science, we decided to select four biggest ones, IEEE Xplore, ACM, Science Direct, and Springer Link.

To obtain research papers dealing with identity management using blockchain technology, we defined the following keywords: ''blockchain identity'', ''self sovereign identity'', ''self sovereignty'', and their variants.

Each database has it own specific search engine, so we conducted an appropriate search string for each one. We limited our search in papers using English from January 2009 to April 2022.

Table 1 describes search string and number of papers found for each database.

D. SELECTION CRITERIA

Selecting relevant papers from the brut results obtained in section C is a mandatory step. To do that, we applied a set of inclusion and exclusion criteria. These criteria are presented in details in Table 2.

We removed papers that did not meet the inclusion and exclusion criteria described in Table 2 by firstly year and type of publication, and then screening title, abstract, keywords, and full-text of papers.

By doing that, we finally got 361 papers that fulfill all criteria.

E. CLASSIFICATION SCHEME

In order to anwser the research questions described in Section B, we defined a classification scheme that classifies

studied papers into several categories: 1) contributions, 2) domain, 3) place of publication, 4) type of research, 5) year of research, 6) state of author.

There are some sub-categories in each category. These relationships are described in Table 3. These categories are almost similar to ones in [16] with some little adjustments in **domain** and **contribution**. Although, in [16], the authors did not describe them in details so that readers cannot know how the identified papers were classified. In this research, we will fill this gap to help readers and other researchers have a clearer view in this point.

It is very clear to understand most of categories, except ''contribution'' and ''type of research''. We explain briefly here how to categorize papers into different sub-categories basing on it contribution.

- **Architecture, platform, pattern, model/schem, framework, protocol, system/solution:** papers propose a new architecture, platform, pattern, model/ scheme, framework, protocol, system/solution of IdM system respectively.
- **Specifications:** papers give specifications for a IdM system.
- **Method/Methodology:** papers present a method/ methodology to propose solutions for IdM system, or method/methodology of research.
- **Existing solutions:** mostly review, survey papers give an evaluation about existing solutions for IdM system.

TABLE 1. Search string and number of papers found in each database.

Database	Search string	Sub-total	Total
IEEE	("**Abstract**":"blockchain" OR "self-sovereign" OR "block-chain" OR "selfsovereign" AND "identity") OR ("**Document Title**":"blockchain" OR "self-sovereign" OR "block-chain" OR "selfsovereign") AND "identity") OR ("**Author Keywords**":"blockchain" OR "self-sovereign" OR "block-chain" OR "selfsovereign" AND "identity") AND ("**Index Terms**":"identity")	736	742
	("**Document Title**":"self-sovereign identity" OR "self sovereign identity" OR "self-sovereignty" OR"self sovereignty") OR ("**Abstract**":"self-sovereign identity" OR "self sovereign identity" OR "self-sovereignty" OR "self sovereignty") OR ("**Author Keywords**":"self-sovereign identity" OR "self sovereign identity" OR "self-sovereignty" OR "self sovereignty") AND ("**Index Terms**":identity)	97	
ACM	**Keywords**: "blockchain" OR "block-chain" OR "selfsovereign" OR "self-sovereign" AND "identity"	72	72
Science Direct	**Title, abstract or author-specified keywords**: ("blockchain" OR "self-sovereign" OR "block-chain" OR "selfsovereign") AND "identity"	109	109
Springer Link	identity AND blockchain AND (blockchain OR self-sovereign OR block-chain OR selfsovereign) **Title contains**: identity	136	257
	self-sovereign identity OR self sovereign identity OR self-sovereignty OR self sovereignty	138	

TABLE 2. Selection criteria.

Inclusion criteria	Exclusion criteria
• Papers mentioning identity management using blockchain • Papers written in English • Papers published between January 2009 and April 2022 • Papers are in conferences, journals, magazines, symposiums, workshops, forums, congresses and summits • Primary and second studies	• Studies in a book • Mentioning identity management not using blockchain • Papers in form of summary, poster and powerpoint presentations

TABLE 3. Categories and sub-categories for classification scheme.

Contribution	Domain	Place of publication	Type of research	Year of research	State of author
Architecture Platform Pattern Model/Scheme Framework Protocol System/solution Specifications Methode/Methodology Existing solutions Use of decentralized identity Definition/Concepts Challenges and opportunities Other	Education Government Healthcare Smart city Banking and financial Industry IoT Supply chain Transport General Oher	Conference Journal Symposium Magazine Workshop Summit Forum Congress	Conceptual research Solution proposal Validation research Evaluation research Opinion paper Experiential paper	From 2009 to 2022	All states in the world

- **Use of decentralized identity:** papers mention use of decentralized identity, application of decentralized identity in different domains.
- **Definition/Concepts:** papers present new definitions/concepts of IdM systems.
- **Challenges and opportunities:** papers discuss about challenges and opportunities of integrating blockchain to IdM systems.

For ''Type of research'', we followed the classification proposed in [16] and [45] which defined six types of research papers: Conceptual research, Solution proposal, Validation research, Evaluation research, Opinion paper, and Experiential paper.

- **Conceptual research:** focus on concepts and include a new way of looking and thinking. They usually contain proposals for new perspectives on a theoretical level.

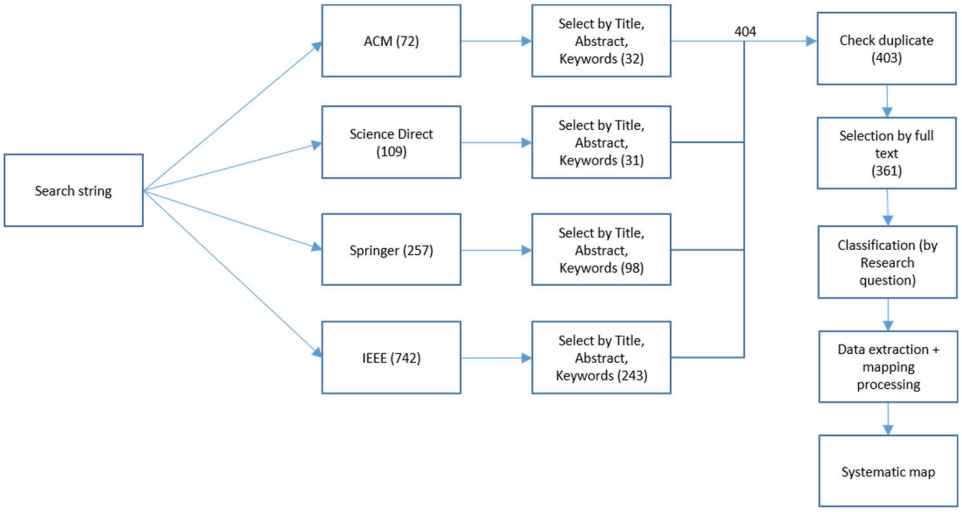

FIGURE 2. Research process with number of papers in each step.

- **Solution proposal:** 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
- **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.
- **Evaluation research:** is firstly the proposed solution implemented and tested in real-world scenarios. In addition, unlike [16], we slightly modified by classifying papers that evaluate existing solutions in this type.
- **Opinion paper:** contain the author's personal viewpoint on a given subject, either positive or negative
- **Experiential paper:** 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.

Depending on its nature, one paper may be classified into one or more categories and sub-categories as long as it satisfies the requirements.

The next section will present the results of this classification of all identified papers.

The research process with number of papers obtained after processing each step is described in Fig. 2.

V. RESULTS AND SYSTEMATIC MAPS

Applying all steps of the research process presented in Section IV, we obtained all relevant papers that meet all criteria and classified them into respective categories and subcategories described in Table 3. Besides, we also constructed co-authorship network of all identified papers to have an insight about the relationship between authors.

In next sections, we present obtained results by anwsering the three research questions mentioned in the previous section.

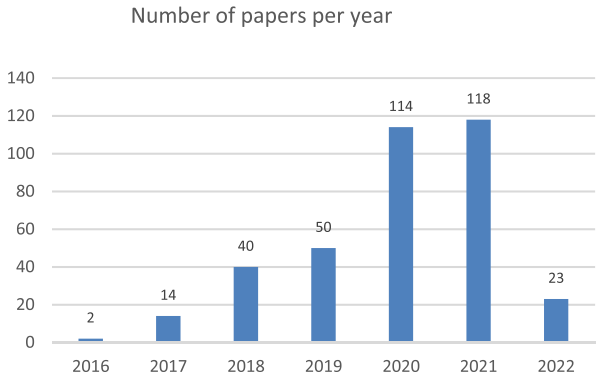

FIGURE 3. Number of papers over years.

A. DEMOGRAPHY

Fig. 3 presents the number of papers published in each year from 2016 (RQ1.1). No papers dealing identity management using blockchain in our four databases is found before this time. We can see that number of papers increases year by year form 2 papers in 2016 to 118 papers in 2021. This shows that this topic of research is interesting and attracts researchers.

In order to answer RQ1.2, we got information about place of publication of each paper then classified it into one of eight type (Conference, Journal, Symposium ...). The results are showed in Fig. 4. And Fig. 5 presents number of papers in each place of publicaction (we only show top fourteen places with the most papers). For a short conclusion, most papers were published in conferences and journals, majority of IEEE database.

To address RQ1.3, we counted number of papers for each active states based on the organizational affiliation of the authors. The obtained results are presented in Fig. 6 where we can see that China, India, and USA invest most in this field.

For RQ1.4, we need to have the authors' name of all identifier papers. It's quite hard to construct a co-authorship

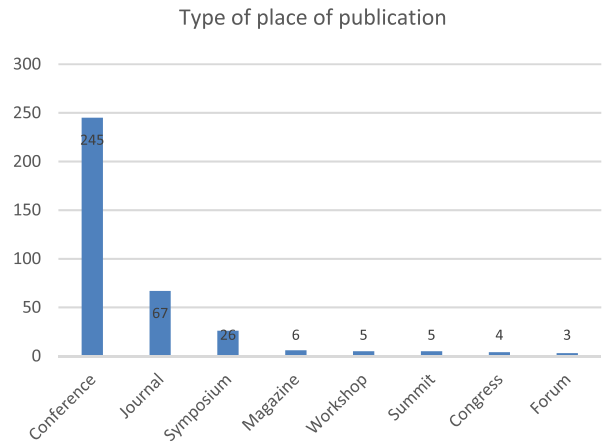

FIGURE 4. Number of papers by type of place of publication.

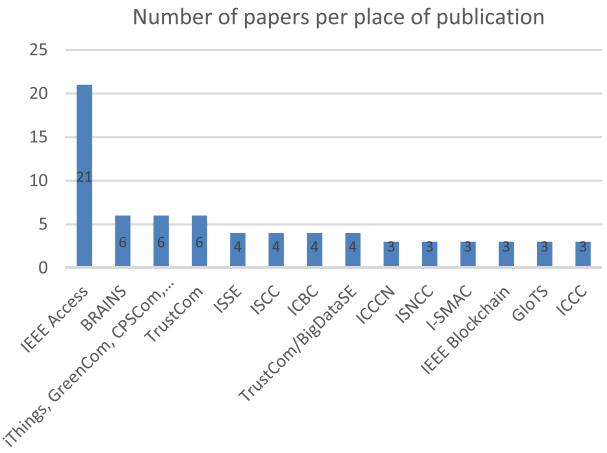

FIGURE 5. Number of papers per place of publication.

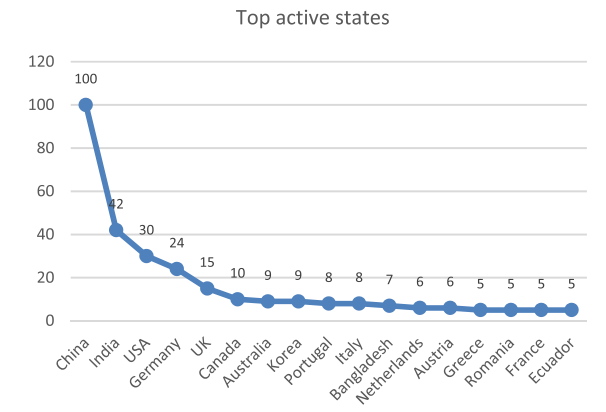

FIGURE 6. Number of papers of the top active states, according to authors' affiliation.

network [46] of 361 papers. As it would result in a tangled and hard-to-see network. So, we devided their authors in two

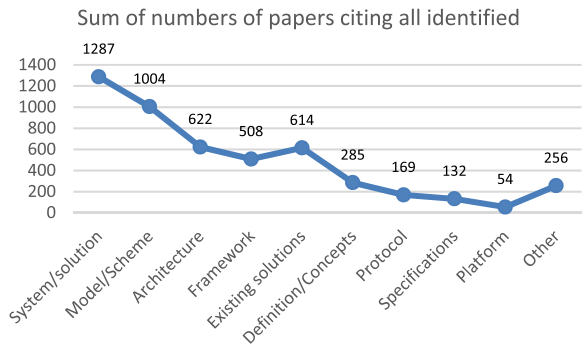

FIGURE 7. Sum of numbers of citing all identified papers by contribution.

set. The first one contains all authors who cooperate together within only one paper. The resulting network graph of this case is showed in Fig. 13 using Gephi [47]. The second one contains the remaining authors who co-work in at least two papers or at least one author of one paper co-works with other authors in one other paper. Fig. 14 presents results of this case. Authors and co-works between them are represented by vertex and edges respectively. In this weighted undirected graph, the weight of edges is proportional to number of co-works between two authors. The results obtained show that mainly groups of authors still work individually (alone or a separate group) and co-work in only one paper.

It is interesting and useful for readers to know how the community pays attention to the selected articles (Q1.5) as at least it can be an instruction for them to choose which publication to read and publish their research paper in IdM based on blockchain. To have the information about that, we have to know how many other papers refer to each article. To do that, we analyse the papers that are cited by from 50 other papers as they are able to reflect the overall of 361 papers. We focus only on the following aspect: contribution, domain, states based on the organizational affiliation of the authors, database and placce of publication of the selected papers. The results obtained are shown in Fig. (7-12). For a short conclusion, we can see that papers providing new systems/solutions and models/schemes as well as papers dealing with general issues gain the greatest interest of readers and IEEE is the best place to read and publish papers in this topic of research. More discussion in details will be presented in Section VI.

B. SUBJECT OF INTEREST

This section will answer RQ2 and its sub-questions, focus on the subject of interest of the studied papers.

In order to address RQ2.1 and RQ2.2 relating main contributions and application domains of all the identified papers, firstly we need to classify them into categories defined in Table 3. Then we constructed a classification maps (Fig. 15 and Fig. 17) that represent the relationship between contributions and domains.

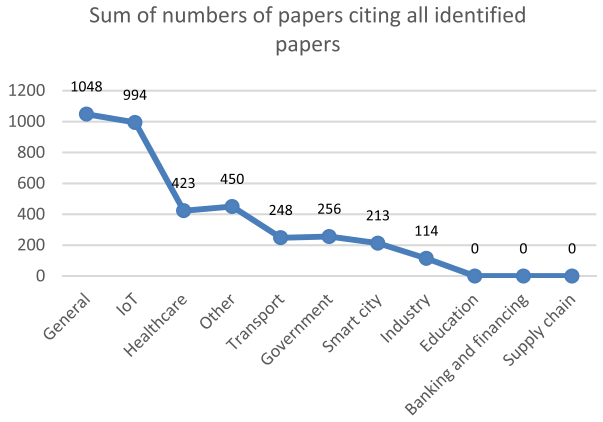

FIGURE 8. Sum of numbers of citing all identified papers by domain.

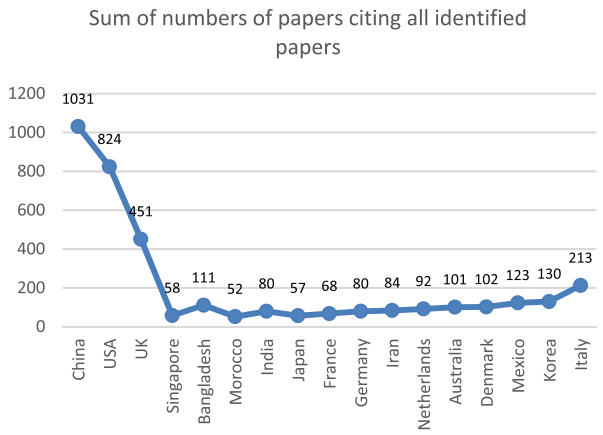

FIGURE 9. Sum of numbers of citing all identified papers by state of author.

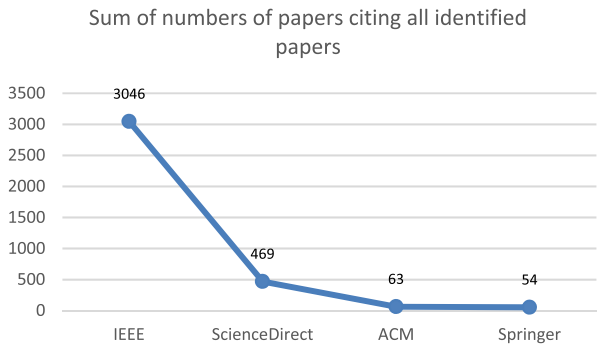

FIGURE 10. Sum of numbers of citing all identified papers by database.

The results in Fig. 11 show that articles mainly provide new system/solution, architecture, framework and model/scheme. It is shown also that most papers deal with general issues not focusing on a specific domain. Besides, IoT gains also momentum when there are 61 papers in this domain

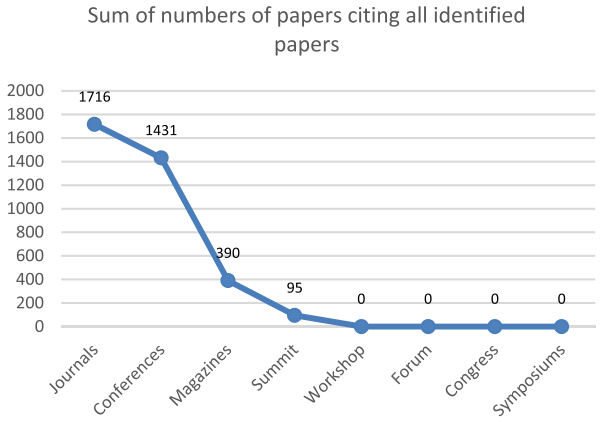

FIGURE 11. Sum of numbers of citing all identified papers by place of publication.

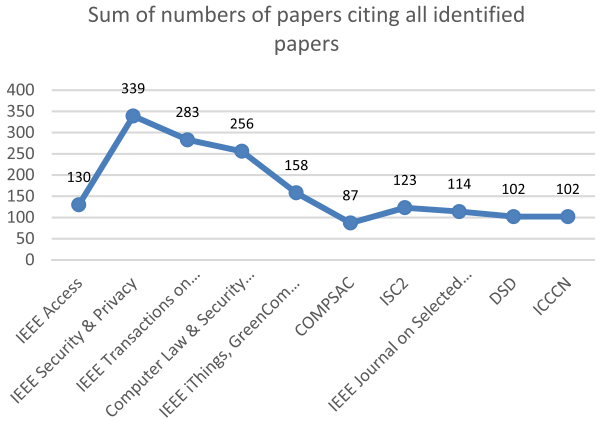

FIGURE 12. Sum of numbers of citing all identified papers by title of publication.

C. RESEARCH TYPES AND IDENTITY TYPES

Similarly, to anwser RQ3.1 about research type, we presented the results of classification in Fig. 16 and Fig. 18.

Regarding the ratio between decentralized identity solutions and SSI solutions among all studied papers (RQ3.2), the classification map is presented in Fig. 16 and Fig. 19.

For Fig. 17 - 19, instead of just counting the number of papers corresponding to each cell, we show which paper is in which cell. This helps readers and other researchers have more information in details.

VI. DISCUSSION

In the previous section, we presented several results that help us anwser the research questions described in Section IV-B. This section, we will analyse these results in details.

As shown in Fig. 3, we can observe that the number of annual publications (RQ1.1) increases greatly year by year (from 2 studies in 2016 to 118 studies in 2021). Although the search is limited to publications since 2009, the actual results

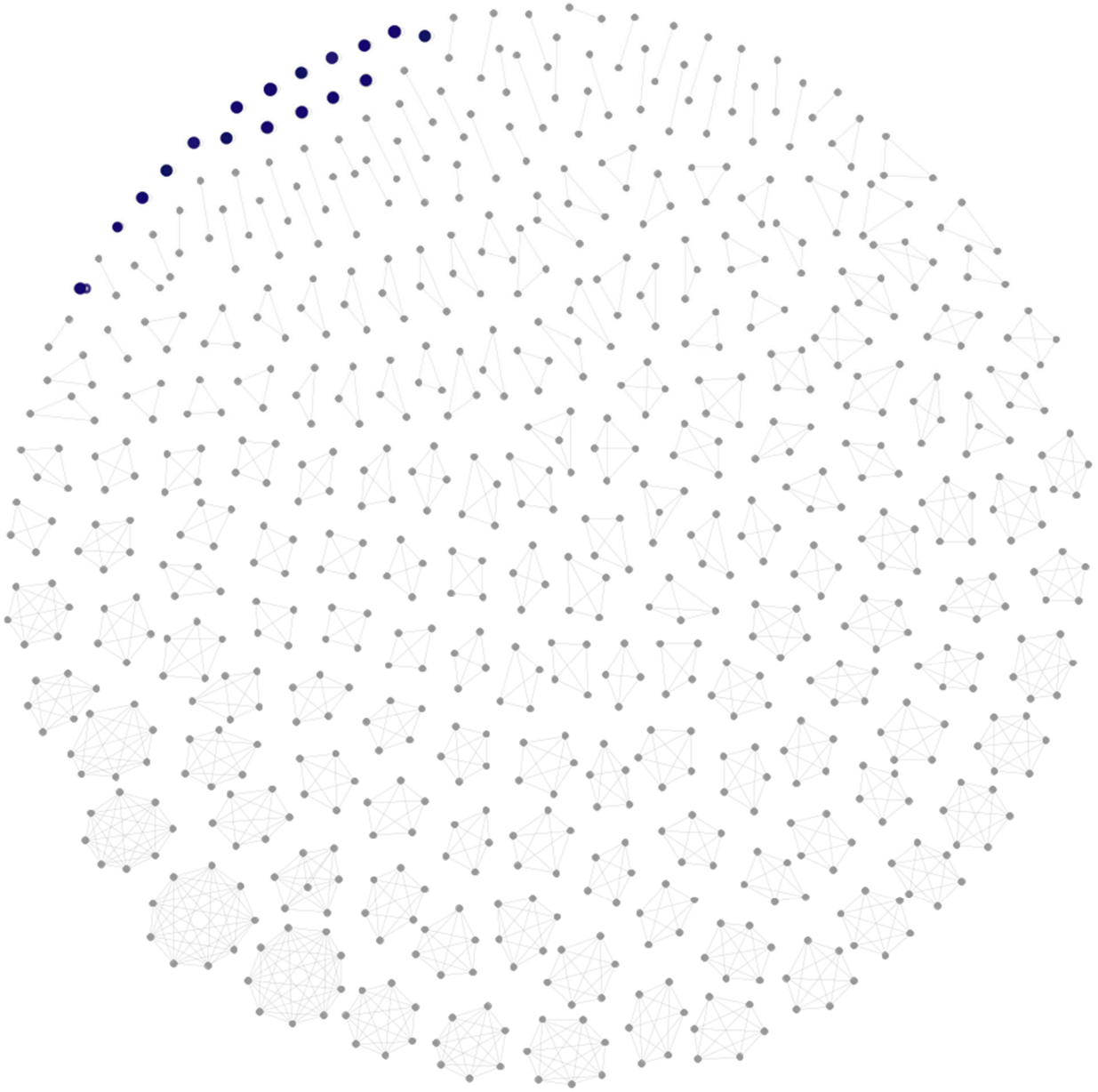

FIGURE 13. Co-authorship network graph where there is no relationship between groups of authors.

show that IdM using blockchain has attracted attention and development since 2016.

The number of articles in 2016 was only 2. By 2017 the number of articles was up to 14, increased 7 times; from 2017 to 2018 increased from 14 to 40; 2018 to 2019 from 40 to 50. In 2020 increased dramatically from 50 to 118. The number of articles in 2020 and 2021 is nearly equal, possibly due to the outbreak of the Covid-19 pandemic in 2020, IdM using blockchain is of outstanding interest. Paper number 2022 is less than 2021 due to limited search to April 2022.

Regarding the distribution of articles among databases, we have: 235 papers come from IEEE Explore (65.1%); 73 papers from Springer Link (20.22%); 28 papers ACM (7.76%), and the remaining 25 papers from ScienceDirect (6.95%). For question RQ1.2, the majority of articles were published in the proceedings of the conferences (245 papers, 67.86%); 67 papers in journals (18.56%); 26 papers in symposium (7.2%), and the rest are distributed among magazines, workshops, forums, summits, congresses. As for the place of publication, these 361 papers were published in 252 publications. Specifically, in the publications, IEEE Access has the

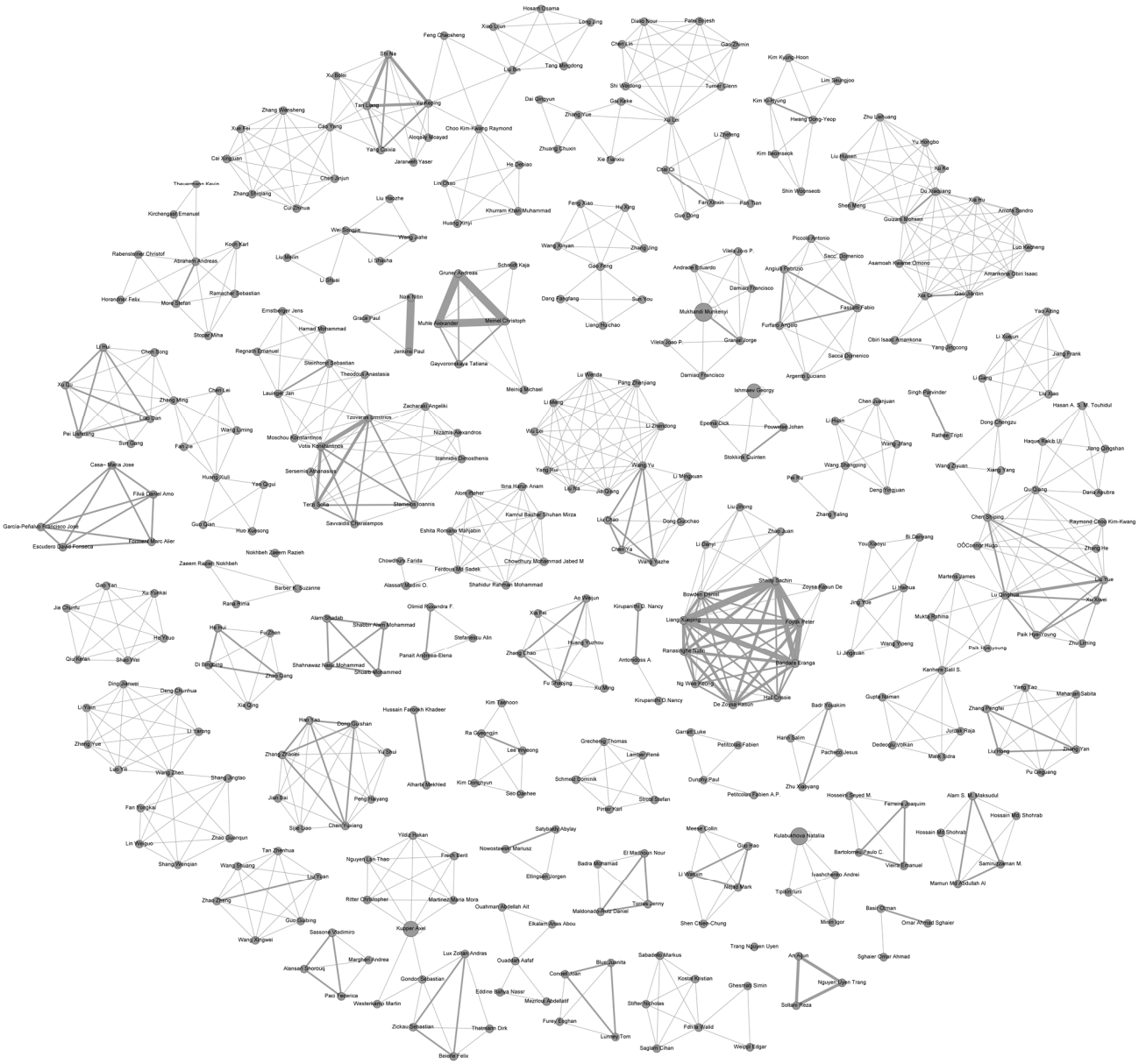

FIGURE 14. Co-authorship network graph, where vectors represent authors and edges the co-authorship of one or more works.

highest number of papers (21 papers, equivalent to 5.82%). For the remaining publications, the number of papers published is 6 or less. Specifically, there are 3 publications with 6 papers; 4 publications have 4 papers; 12 publications with 3 articles; the rest mostly consists of 2 papers and 1 papers. This distribution is shown in Fig. 5 with the top 14 publications with the most articles. Due to the large number of publications (252 publications) but limited research length, we cannot list all of them.

As in section V, we commented that China, India, and USA are the countries (RQ1.3) with the most blockchain-based IdM research according to our search results. In which, China leads with 100 papers (27.7%), followed by India with 42 papers (11.6%), USA with 30 papers (8.3%), Germany (24 papers, 6.6%), and UK (15 papers, 4.2%). For the remaining remaining countries, each country contributed less than 10 papers. The full list of contributing countries is listed in Table 4.

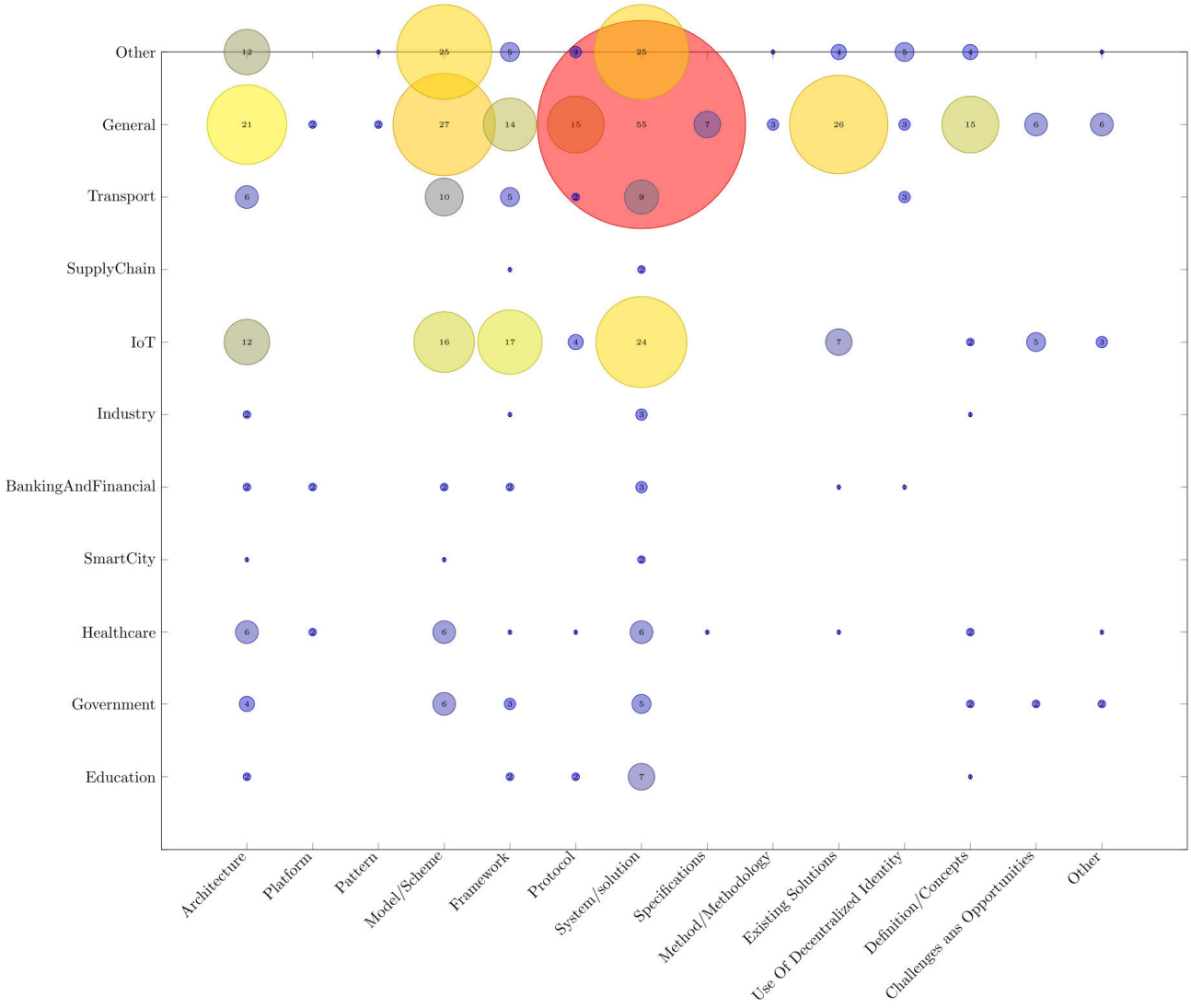

FIGURE 15. Classification map, representing the intersection between papers' contribution and domain.

Regarding the collaboration of authors of the papers included in the study (RQ1.4), based on Fig. 13 and Fig. 14, we can see that mainly groups of authors still work individually (alone or a separate group) and co-work in only one paper. Specifically, in Fig. 13, there are 22 authors working alone; 44 groups of 2 authors; 42 groups of 3 authors; 50 groups of 4 authors; 34 groups of 5 authors; 17 groups of 6 authors; 5 groups of 7 authors; 1 group of 8 authors, and 2 groups of 9 authors.

From Fig. 14, we can see that the authors with the most papers is Naik Nitin and Jenkins Paul with 7 papers, of which 6 are the co-works of two authors and one paper shared by two people together with Grace Paul. Besides, there is another group of authors who also have 7 papers, which are Gruner Andreas, Muhle Alex, and Meinel Christophe. They co-worked in all 7 papers including 2 with Gayvoron Skaya and one with Schmidt Kaja, one with Meinig Michael. The authors have published 6 papers including Liang Xueping and Shetty Sachin, of which both authors collaborated in all six papers and 5 papers were the co-works of the two authors with Bandara Eranga. Next, two authors jointly published 4 papers, namely Votis Konstantinos and Tzovaras Dimitrios. Lu Quinghua also published 4 papers, of which 3 papers were made with Liu Yue and combined with many other authors to create a large network. Similarly, Yu Keping also published 4 papers in which 3 papers were combined with Shi Na and Tan Liang, and combined with other authors to create a complex web. The trio of An Aijun, Nguyen Uyen Trang, and Soltani Reza combined in 3 papers.

In Fig. 14, some nodes are larger in size as the authors do some papers alone.

Regarding to the interest of reseachers in blockchain-based IdM (RQ1.5), we analyse number of papers refering the identified papers in each category. We focus the papers with

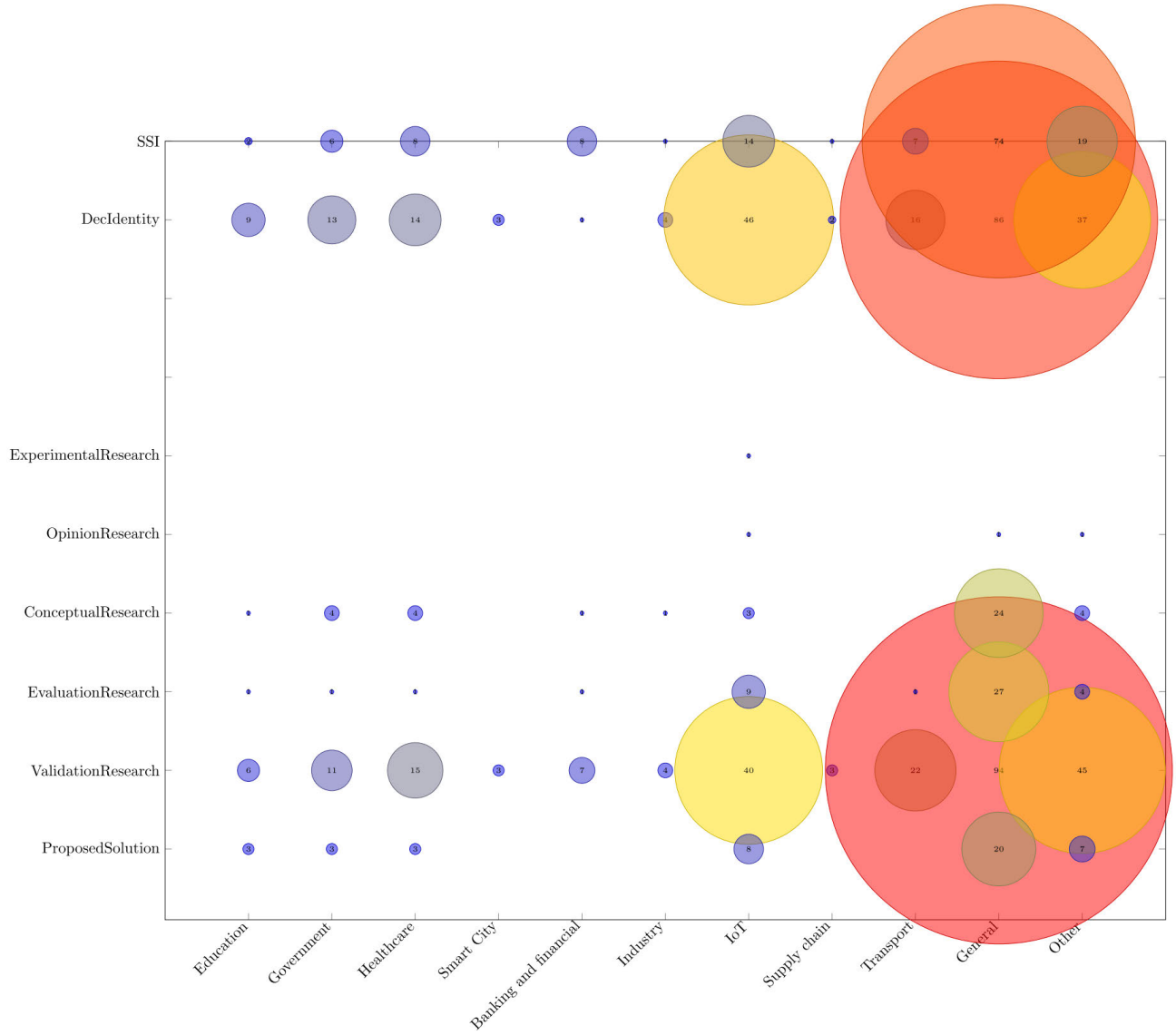

FIGURE 16. Classification map, representing the intersection between papers' domain and research type and identity type.

more than 50 citations. They are [4, 13, 14, 42, 48, 49, 60, 63, 67, 70, 79, 92, 105, 113, 123, 124, 133, 139, 146, 165, 166, 201, 206, 207, 209, 213, 227, 236, 263, 317, 319, 325, 330, 380, 386]. A summary of ten most cited articles is presented in Table 5. Observing Fig. 7, we can see that the greatest interest is for articles providing new systems/solutions (cited in 1287 articles in total), followed by articles providing new models/schemes (1004 times), architecture (622 times), framework (508 times), existing solutions (614 times). Readers seem to pay less attention to the remaining categories: Definition/Concepts (285 times), Protocol (169 times), Specifications (132 times), Platform (54 times), Other (256 times). Concerning the domain of the identified papers, through Fig. 8, we can find out that the papers mention general issues attract the most interest of researchers as they are cited in 1048 papers. Another domain that also attracts many articles referencing it is IoT (994 times). With Fig. 9, we can observe that the papers of the authors from China, USA, and UK gain the greatest appeal of readers with with the number of articles referencing them, respectively 1031, 824, 451. Observing Fig. 10, we can see that IEEE seems to be the best and the biggest database for readers and rerearchers of blockchain-based IdM when papers published in IEEE are cited by 3043 papers in 3659 papers. Fig. 11 shows that papers published in conferences, journals, and magazines gain most attraction from readers. Last but not least, observing Fig. 12, we can see that publications of IEEE make up the majority of the top publications with the most referencing papers, especially IEEE Access, IEEE Security & Privacy, and IEEE Transactions on Services Computing.

Concerning the contribution of the identified papers (RQ2.1), observing Fig. 15 and Fig. 17, it can be seen that

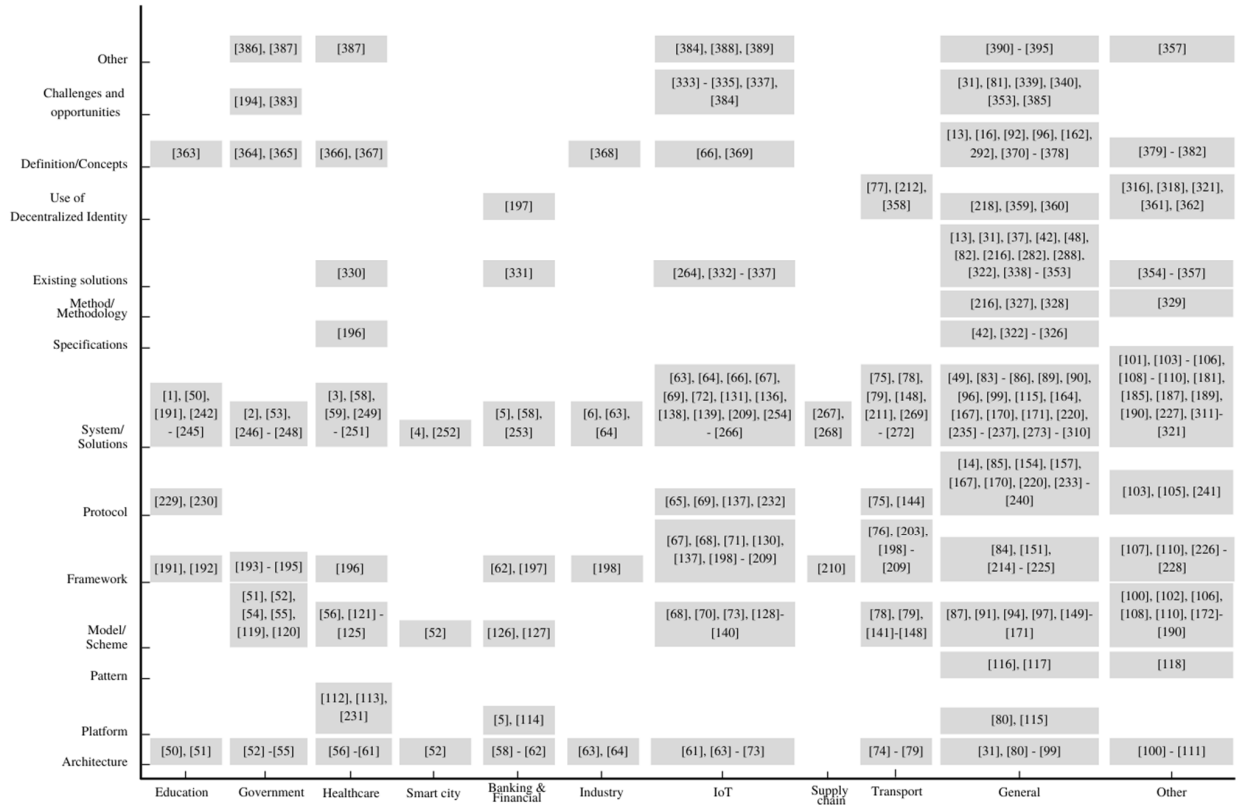

FIGURE 17. Classification map for papers' contributions and domain.

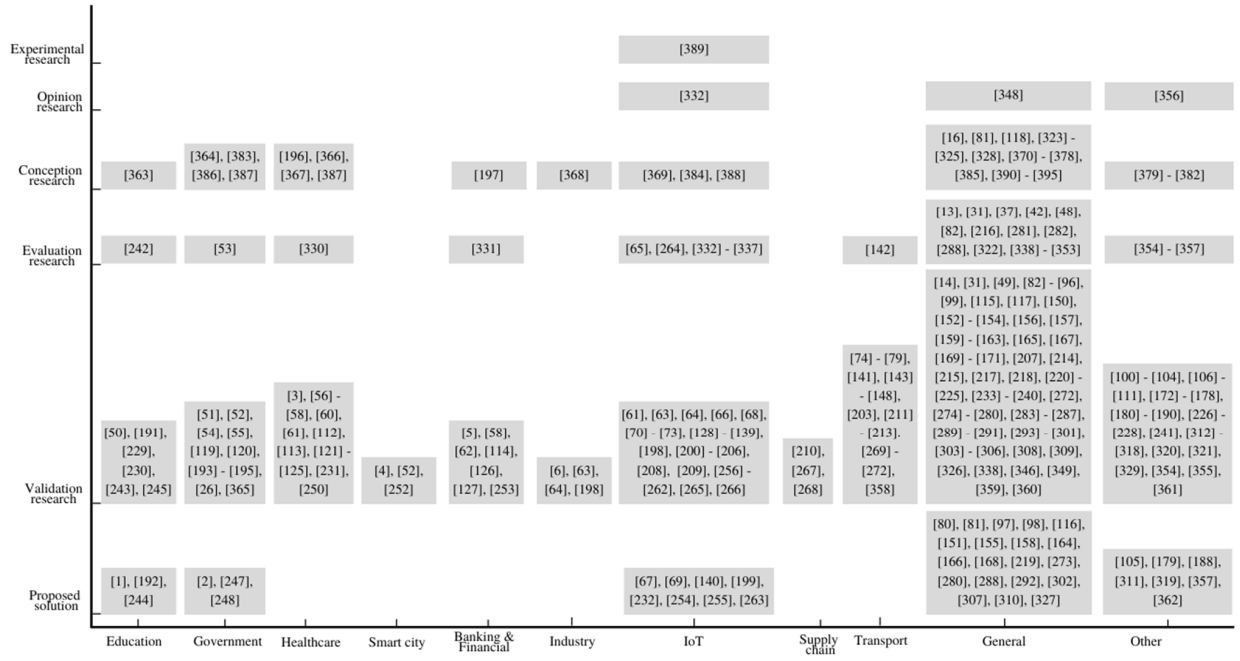

FIGURE 18. Classification map for papers' domain and research type.

the articles mainly provide new system/solution (139 papers, 38.5%), architecture (64 papers, 17.73%), framework (49 papers, 13.57%), and model/scheme (92 papers, 25.48%). This result was similarly reflected in paper [16]. For the remaining categories, there are less papers focusing on: platform, pattern, protocol, specifications, method/methodology,

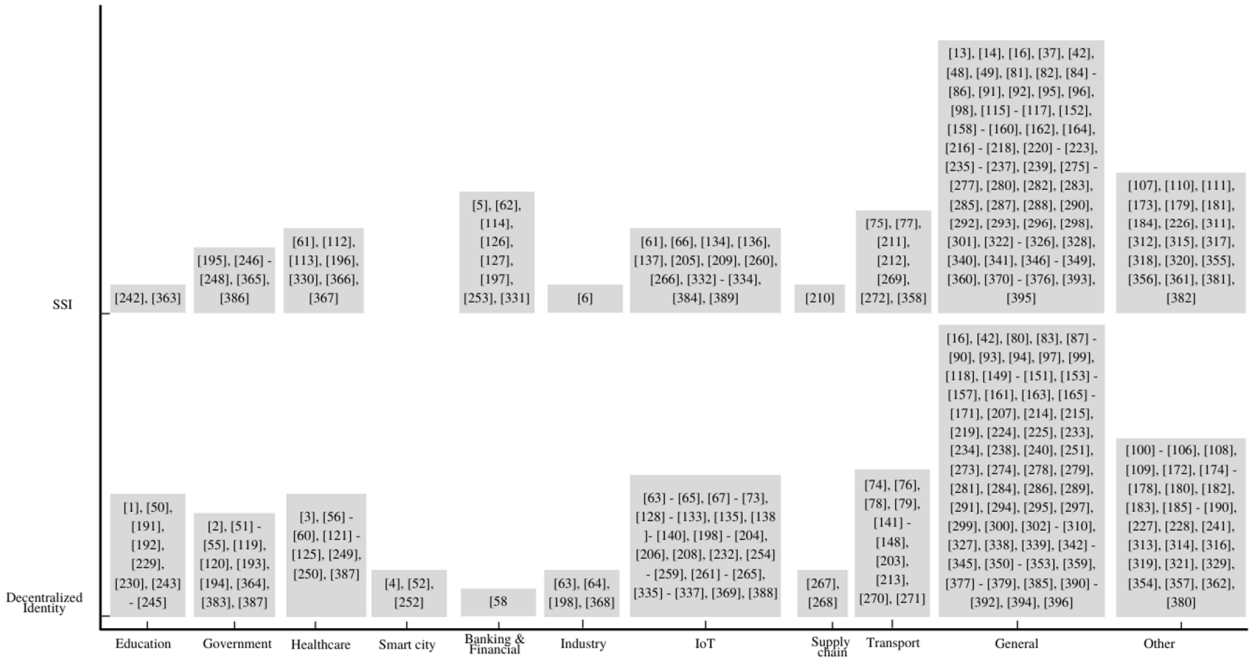

FIGURE 19. Classification map for the type of identity (decentralized or SSI) on which papers focus, regarding domain.

TABLE 4. List of states in each database (with SD standing for ScienceDirect, SL for Springer Link, Per. for Percentage).

States	SD	SL	ACM	IEEE	Total	Per.
China	10	22	11	57	**100**	27.7%
India	1	12	1	28	**42**	11.6%
USA	3	6	3	18	**30**	8.3%
Germany	2	4		18	**24**	6.6%
UK	0	1	1	13	**15**	4.2%
Canada				10	**10**	2.7%
Australia	1	3		5	**9**	2.5%
Korea				9	**9**	2.5%
Italy	1	3		4	**8**	2.2%
Portugal			3	5	**8**	2.2%
Bangladesh		2		5	**7**	1.9%
Netherlands		3	1	2	**6**	1.7%
Austria		3		3	**6**	1.7%
Greece		0	1	4	**5**	1.4%
Romania		2	1	2	**5**	1.4%
France		1		4	**5**	1.4%
Ecuador				5	**5**	1.4%
Morocco			1	3	**4**	1.1%
Japan		1		3	**4**	1.1%
Malaysia	1	0		3	**4**	1.1%
Saudi Arabia	2			2	**4**	1.1%
Northern Ireland				3	**3**	0.8%
Brazil		1		2	**3**	0.8%
Spain		0	2	1	**3**	0.8%
Denmark	1	1		1	**3**	0.8%
Switzerland			1	2	**3**	0.8%

States	SD	SL	ACM	IEEE	Total	Per.
Sweden		1	1	1	**3**	0.8%
UAE	1			1	**2**	0.6%
Belgium		1		1	**2**	0.6%
Myanmar		1		1	**2**	0.6%
Singapore				2	**2**	0.6%
Turkey	1			1	**2**	0.6%
Taiwan	1			1	**2**	0.6%
Norway		1	1		**2**	0.6%
Russia		2			**2**	0.6%
Slovenia				1	**1**	0.3%
Egypt				1	**1**	0.3%
Mexico				1	**1**	0.3%
Algeria				1	**1**	0.3%
Qatar				1	**1**	0.3%
Iran				1	**1**	0.3%
Sri Lanka				1	**1**	0.3%
Pakistan				1	**1**	0.3%
Senegal				1	**1**	0.3%
Luxembourg				1	**1**	0.3%
Thailand				1	**1**	0.3%
Ireland				1	**1**	0.3%
Indonesia				1	**1**	0.3%
Serbia				1	**1**	0.3%
Iraq				1	**1**	0.3%
Rwanda		1			**1**	0.3%
New Zeland		1			**1**	0.3%

use of decentralized identity, challenges and opportunity. Secondary studies mainly review and survey in order to compare and evaluate existing solutions of this research topic. In addition, they also provide views and perspectives on the

TABLE 5. Summary of ten most cited articles from 361 selected articles.

Article	Summary
[48]	The article introduce the emerging landscape of DLT-based IdM and evaluate three representative proposals-uPort, ShoCard, and Sovrin-using the analytic lens of a seminal framework that characterizes the nature of successful IdM schemes.
[133]	In this paper, a blockchain based multi-WSN authentication scheme for IoT is proposed. The nodes of IoT are divided into base stations, cluster head nodes and ordinary nodes according to their capability differences, which are formed to a hierarchical network. A blockchain network is constructed among different types of nodes to form a hybrid blockchain model, including local chain and public chain. In this hybrid model, nodes identity mutual authentication in various communication scenarios is realized, ordinary node identity authentication operation is accomplished by local blockchain, and cluster head node identity authentication are realized in public blockchain. The analysis of security and performance shows that the scheme has comprehensive security and better performance.
[386]	In December 2014, Estonia became the first nation to open its digital borders to enable anyone, anywhere in the world to apply to become an e-Resident. Estonian e-Residency is essentially a commercial initiative. The application of blockchain to e-Residency has the potential to fundamentally change the way identity information is controlled and authenticated. This paper examines the legal, policy, and technical implications of this development.
[4]	The platforms supporting the smart city applications are rarely implemented from scratch by a municipality and/or totally owned by a single company, but are more typically realized by integrating some existing ICT infrastructures thanks to a supporting platform, such as the well known FIWARE platform. This work proposes a novel solution for distributed management of identity and authorization policies by leveraging on the blockchain technology to hold a global view of the security policies within the system, and integrating it in the FIWARE platform. A detailed assessment is provided to evaluate the goodness of the proposed approach and to compare it with the existing solutions.
[70]	In this paper, BlendCAC, a blockchain-enabled decentralized capability-based access control is proposed for the security of IoTs. The BlendCAC aims at an effective access control processes to devices, services, and information in large scale IoT systems. Based on the blockchain network, a capability delegation mechanism is suggested for access permission propagation. A robust identity-based capability token management strategy is proposed, which takes advantage of a smart contract for registration, propagation, and revocation of the access authorization. In the proposed BlendCAC scheme, IoT devices are their own master to control their resources instead of being supervised by a centralized authority. Implemented and tested on a Raspberry Pi device and on a local private blockchain network, the experimental results demonstrate the feasibility of the proposed BlendCAC approach to offer a decentralized, scalable, lightweight, and fine-grained AC solution to IoT systems.
[319]	This paper focuses on utilizing blockchain technology to introduce a new ID as a service (IDaaS) for digital identity management. The proposed blockchain-based ID as a service (BIDaaS) is explained with one practical example that shows how the proposed BIDaaS works as an identity and authentication management infrastructure for mobile users of a mobile telecommunication company.
[380]	This research is a systematic mapping review with the goal of collecting all relevant existing research of Digital Identity on Blockchain technology implemented in a smart city environment. The objective of this paper is to understand the current research topics, challenges, and future directions of these areas from the technical point of view. It is expected that this paper can stimulate interest in theory and practice to further discussions and research in these areas.
[63]	To preserve the privacy of devices in Industrial Internet of Things (IIoT), this paper designs an identity management mechanism, which can realize that devices being authenticated remain anonymous. Besides, session keys between two parties are negotiated, which can secure the subsequent communications. Extensive experiments have been conducted to show the effectiveness and efficiency of the proposed mechanism.
[13]	This paper aims to achieve the first formal and comprehensive step toward an academic investigation of self-sovereign identityby providing the first-ever formal and rigorous treatment of the concept of self-sovereign identity using a mathematical model. This paper examines the properties that a self-sovereign identity should have and explores the impact of self-sovereign identity over the laws of identity. It also highlights the essential life-cycles of an identity management system and inter-relates how the notion of self-sovereign identity can be applied in these life-cycles. In addition, the paper illustrates several envisioned flows involving a self-sovereign identity leveraging blockchain technology covering different aspects of an identity management system.
[123]	This paper proposes a system for identity and access management using blockchain technology to support authentication and authorization of entities in a digital system. A prototype demonstrates the application of blockchain in identity and access management using the Hyperledger Fabric framework. It provides a proof of concept based on a use case concerning Electronic Health Records from the healthcare domain where an immutable and auditable history is desired for data concerning patients. Basic authentication and authorization operations are able to execute in 2-3 seconds with an initial size of blockchain of about 3.8 MB covering physicians in Denmark.

challenges and opportunities of applying blockchain to IdM. Also in Fig. 15 and Fig. 17, we see that most papers deal with general issues with 156 papers (43.21%), not focusing on a specific domain (RQ2.2). This is really reasonable as with a new research topic like blockchain-based IdM, it is necessary to have a general knowledge and research to lay the foundation for application in specific domains. The obtained results show that IoT attracts a lot of attention from researchers (61 papers, 16.9%). This may be as IoT is a growing domain and device identification is gaining strong interest. In addition, transport is also researched together with healthcare. Some other domains gather also momentum such as: education, government, smart city, banking, supply chain, industry.

For RQ3.1, observing Fig. 16 and Fig. 18 shows that the majority of papers are validation research (241 papers, 66.76%), proposed solution (44 papers, 12.19%), evaluation research (44 papers, 12.19%), and conceptual research (40 papers, 11.08%). There are very few papers of other types of research (experimental research, opinion research). This seems obvious as blockchain-based IdM is still a nascent topic, with few real-world applications yet.

For RQ3.2, different from the results in paper [16], the number of articles mentioning decentralized identity (223 papers, 61.77%) is greater than ones mentioning SSI (140 papers, 38.78%). The results are obviously seen in Fig. 16 and Fig. 19.

Notice that the total of all percentages does not equal 100% as there are some papers that discuss about more than one sub-category.

VII. CONCLUSION

In today's digital world, identity management is of great interest as almost everyone owns several digital identities. Traditional identity management systems expose many disadvantages in terms of security and privacy of personal data. Users are increasingly aware of these weaknesses, and they expect solutions that allow them to be autonomous in controlling their identities and reduce their reliance on third parties.

Blockchain was born in 2009. With its own characteristics, it has been applied in many fields of technology and life. Therefore, the application of blockchain to identity management was also discussed in 2015 and has attracted more and more research and development. With the increasing amount of research as primary papers, it is essential to have secondary articles that analyze and synthesize them in order to have a systematic view on this research topic.

Therefore, in this study, we want to provide a systematic mapping to provide a comprehensive systematic view of blockchain-based IdMs through classifying them by contribution, application domain, identity type, and research type. In addition, we also provide an anthropological analysis as well as the trend of papers on this topic. To do that, we studied 361 papers from 4 databases (IEEE Explore, ScienceDirect, ACM, and Springer Link). The obtained results show that the number of studies increases greatly over the years. The year 2020 marks a breakthrough in numbers, which can be explained by the outbreak of the covid-19 pandemic which has increased the demand for decentralized identity management. Regarding the place of publication of papers, published papers are mostly concentrated in conference proceedings, journals, and symposiums. The publication with the most published articles is IEEE Access. The countries with the most research papers are China, India, and the USA. Concerning the interest of readers in the topic of blockchain-based IdM, the most interesting papers are the paper proposing model/solution and model/scheme, papers dealing with general solution and IoT. Papers published in conferences and journals, majority in IEEE attract most readers were most cited.

The papers mainly belong to validation research and solution proposal types. The papers focus on general solutions, not specific to any specific domain. For specific domains, there is more prominence in IoT, transport as well as healthcare. Most of the papers focus on proposing solutions, architecture, framework, model / scheme.

From the results of this work, in the future, we may focus on analysing SSI and decentralized identity solutions and models for IoT devices in expecting to conduct insights of this narrow research domain. As according to our research results, IoT is increasingly gain momentum in this period.

CONFLICTS OF INTEREST

No Conflict of interest.

REFERENCES

[1] M. A. Forment, D. A. Filvà, F. J. García-Peñalvo, D. F. Escudero, and M. J. Casañ, "Learning analytics' privacy on the blockchain," in *Proc. 6th Int. Conf. Technol. Ecosyst. Enhancing Multiculturality*, Oct. 2018, pp. 294–298, doi: 10.1145/3284179.3284231.

[2] A. Jha, R. K. Bhattacharjee, M. Nandi, and F. A. Barbhuiya, "A framework for maintaining citizenship record on blockchain," in *Proc. ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, Jul. 2019, pp. 29–38, doi: 10.1145/3327960.3332389.

[3] J.-S. Lee, C.-J. Chew, J.-Y. Liu, Y.-C. Chen, and K.-Y. Tsai, "Medical blockchain: Data sharing and privacy preserving of EHR based on smart contract," *J. Inf. Secur. Appl.*, vol. 65, Mar. 2022, Art. no. 103117, doi: 10.1016/j.jisa.2022.103117.

[4] C. Esposito, M. Ficco, and B. B. Gupta, "Blockchain-based authentication and authorization for smart city applications," *Inf. Process. Manage.*, vol. 58, no. 2, Mar. 2021, Art. no. 102468, doi: 10.1016/j.ipm.2020.102468.

[5] E. Bandara, X. Liang, P. Foytik, S. Shetty, N. Ranasinghe, K. De Zoysa, and W. K. Ng, "Promize—Blockchain and self sovereign identity empowered mobile ATM platform," in *Intelligent Computing*, vol. 284, K. Arai, Ed. Cham, Switzerland: Springer, 2021, pp. 891–911, doi: 10.1007/978-3-030-80126-7_63.

[6] N. D. Sarier, "Efficient biometric-based identity management on the blockchain for smart industrial applications," *Pervas. Mobile Comput.*, vol. 71, Feb. 2021, Art. no. 101322, doi: 10.1016/j.pmcj.2020.101322.

[7] L. Bell, W. J. Buchanan, J. Cameron, and O. Lo, "Applications of blockchain within healthcare," *Blockchain Healthcare Today*, vol. 1, pp. 1–7, Jul. 2018, doi: 10.30953/bhty.v1.8.

[8] M. Hölbl, M. Kompara, A. Kamišalić, and L. N. Zlatolas, "A systematic review of the use of blockchain in healthcare," *Symmetry*, vol. 10, no. 10, p. 470, Oct. 2018, doi: 10.3390/sym10100470.

[9] A. Dorri, S. S. Kanhere, and R. Jurdak, "Towards an optimized BlockChain for IoT," in *Proc. 2nd Int. Conf. Internet-Things Design Implement.*, Apr. 2017, pp. 173–178.

[10] O. Novo, "Blockchain meets IoT: An architecture for scalable access management in IoT," *IEEE Internet Things J.*, vol. 5, no. 2, pp. 1184–1195, Apr. 2018, doi: 10.1109/JIOT.2018.2812239.

[11] R. Azzi, R. K. Chamoun, and M. Sokhn, "The power of a blockchain-based supply chain," *Comput. Ind. Eng.*, vol. 135, pp. 582–592, Sep. 2019, doi: 10.1016/j.cie.2019.06.042.

[12] F. Longo, L. Nicoletti, A. Padovano, G. d'Atri, and M. Forte, "Blockchain-enabled supply chain: An experimental study," *Comput. Ind. Eng.*, vol. 136, pp. 57–69, Oct. 2019, doi: 10.1016/j.cie.2019.07.026.

[13] 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.

[14] 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)*, Rio de Janeiro, Brazil, Jul. 2018, pp. 1–7, doi: 10.1109/IJCNN.2018.8489316.

[15] T. Rathee and P. Singh, "A systematic literature mapping on secure identity management using blockchain technology," *J. King Saud Univ.-Comput. Inf. Sci.*, vol. 34, no. 8, pp. 5782–5796, Sep. 2022, doi: 10.1016/j.jksuci.2021.03.005.

[16] S. Cucko and M. Turkanovic, "Decentralized and self-sovereign identity: Systematic mapping study," *IEEE Access*, vol. 9, pp. 139009–139027, 2021, doi: 10.1109/ACCESS.2021.3117588.

[17] F. Schardong and R. Custódio, "Self-sovereign identity: A systematic review, mapping and taxonomy," 2021, *arXiv:2108.08338*.

[18] V. Beal. (Jun. 22, 2015). *Identity and Access Management (IAM)*. Accessed: Jul. 10, 2022. [Online]. Available: https://www.webopedia.com/definitions/iam/

[19] J. Hughes, S. Cantor, J. Hodges, F. Hirsch, P. Mishra, R. Philpott, and E. Maler, *Profiles for the Oasis Security Assertion Markup Language (SAML) V2. 0*, OASIS Standard 200503, 2005.

[20] M. Hondo, H. Maruyama, A. Nadalin, and N. Nagaratnam, "Web services federation language (WS-federation)," BEA Syst., BMC Softw., CA, USA, IBM, Layer 7 Technol., Microsoft, Novell VeriSign, USA, Version 1.1, 2006. Accessed: Mar. 13, 2023. [Online]. Available: https://schemas.xmlsoap.org/ws/2006/12/federation/ws-federation.pdf

[21] S. Cantor, J. Hodges, J. Kemp, and P. Thompson, "Liberty ID-FF architecture overview," Liberty Alliance Project, Wason Thomas, Herausgeber Liberty Alliance, Menlo Park, CA, USA, Version 1.2, 2003.

[22] C. P. Cahill, G. Whitehead, and H. Yang, "Liberty ID-WSF provisioning service specifi cation," Liberty Alliance Project, Intel Corp., CA, USA, Version 1.2, 2007.

[23] D. Hardt, *The OAuth 2.0 Authorization Framework*, document RFC6749, 2012.

[24] D. Recordon and D. Reed, "OpenID 2.0: A platform for user-centric identity management," in *Proc. 2nd ACM Workshop Digit. Identity Manage.*, Nov. 2006, pp. 11–16.

[25] A. Jøsang, M. Zomai, and S. Suriadi, "Usability and privacy in identity management architectures," in *Proc. 5th Australas. Symp. ACSW Frontiers*, vol. 68, Jan. 2007, pp. 143–152.

[26] G.-J. Ahn and J. Lam, "Managing privacy preferences for federated identity management," in *Proc. Workshop Digit. Identity Manage.*, New York, NY, USA, Nov. 2005, pp. 28–36, doi: 10.1145/1102486.1102492.

[27] G.-J. Ahn, M. Ko, and M. Shehab, "Privacy-enhanced user-centric identity management," in *Proc. IEEE Int. Conf. Commun.*, Jun. 2009, pp. 1–5.

[28] M. S. Ferdous and R. Poet, "A comparative analysis of identity management systems," in *Proc. Int. Conf. High Perform. Comput. Simulation (HPCS)*, Jul. 2012, pp. 454–461.

[29] S. Nakamoto, "Bitcoin: A peer-to-peer eletronic cash system," Bitcoin, White Paper, 2008. Accessed: Mar. 14, 2023. [Online]. Available: https://bitcoin.org/bitcoin.pdf

[30] A. Hayes. (Jun. 24, 2022). *What is a Blockchain?* Accessed: Jul. 18, 2022. [Online]. Available: https://www.investopedia.com/terms/b/blockchain.asp

[31] 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)*, Paris, France, Sep. 2020, pp. 97–101, doi: 10.1109/BRAINS49436.2020.9223312.

[32] B. Lashkari and P. Musilek, "A comprehensive review of blockchain consensus mechanisms," *IEEE Access*, vol. 9, pp. 43620–43652, 2021, doi: 10.1109/ACCESS.2021.3065880.

[33] A. M. Antonopoulos, *Mastering Bitcoin*, 1st ed. Sebastopol, CA, USA: O'Reilly, 2015.

[34] J. Douglas and N. Kumar. (Jul. 11, 2022). *Introduction to Smart Contracts*. Accessed: Jul. 18, 2022. [Online]. Available: https://ethereum.org/en/developers/docs/smart-contracts/

[35] Oracle. *What is Blockchain?* Accessed: Jul. 18, 2022. [Online]. Available: https://www.oracle.com/middleeast/blockchain/what-is-blockchain/

[36] O. Dib and K. Toumi, "Decentralized identity systems: Architecture, challenges, solutions and future directions," *Ann. Emerg. Technol. Comput.*, vol. 4, no. 5, pp. 19–40, Dec. 2020, doi: 10.33166/AETiC.2020.05.002.

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

[38] X. Zhu and Y. Badr, "Identity management systems for the Internet of Things: A survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, Dec. 2018, doi: 10.3390/s18124215.

[39] 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, doi: 10.1016/j.cosrev.2018.10.002.

[40] S. Y. Lim, P. T. Fotsing, A. Almasri, O. Musa, M. L. M. Kiah, T. F. Ang, and R. Ismail, "Blockchain technology the identity management and authentication service disruptor: A survey," *Int. J. Adv. Sci., Eng. Inf. Technol.*, vol. 8, nos. 4–2, p. 1735, Sep. 2018, doi: 10.18517/ijaseit.8.4-2.6838.

[41] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, Sep. 2020, Art. no. 102731, doi: 10.1016/j.jnca.2020.102731.

[42] 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.

[43] C. Allen. (Apr. 25, 2016). *The Path to Self-Sovereign Identity*. Life with Alacrity. Accessed: Jul. 18, 2022. [Online]. Available: http://www.lifewithalacrity.com/2016/04/the-path-to-self-soverereign-identity.html

[44] 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, doi: 10.1016/j.infsof.2015.03.007.

[45] 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.

[46] M. Savić, M. Ivanović, and L. C. Jain, "Co-authorship networks: An introduction," in *Complex Networks in Software, Knowledge, and Social Systems*, vol. 148. Cham, Switzerland: Springer, 2019, pp. 179–192, doi: 10.1007/978-3-319-91196-0_5.

[47] M. Bastian, S. Heymann, and M. Jacomy, "Gephi: An open source software for exploring and manipulating networks," in *Proc. Int. AAAI Conf. Web Social Media*, Mar. 2009, pp. 361–362, doi: 10.13140/2.1.1341.1520.

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

[49] 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)*, Halifax, NS, Canada, Jul. 2018, pp. 1336–1342, doi: 10.1109/Cybermatics_2018.2018.00230.

[50] S. V. Mukhopadhyay and S. K. Gupta, "Decentralized accreditation of educational attainments using blockchain," in *Proc. 6th Int. Conf. Converg. Technol. (I2CT)*, Maharashtra, India, Apr. 2021, pp. 1–4, doi: 10.1109/I2CT51068.2021.9418201.

[51] P. Datta, A. Bhowmik, A. Shome, and M. Biswas, "A secured smart national identity card management design using blockchain," in *Proc. 2nd Int. Conf. Adv. Inf. Commun. Technol. (ICAICT)*, Dhaka, Bangladesh, Nov. 2020, pp. 291–296, doi: 10.1109/ICAICT51780.2020.9333487.

[52] A. H. Rahat, M. R. Rumon, T. J. Joti, H. Tasnin, T. Akter, A. Shakil, and M. I. Hossain, "Blockchain based secured multipurpose identity (SMID) management system for smart cities," in *Proc. IEEE 12th Annu. Comput. Commun. Workshop Conf. (CCWC)*, Las Vegas, NV, USA, Jan. 2022, pp. 737–744, doi: 10.1109/CCWC54503.2022.9720808.

[53] 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)*, Yangon, Myanmar, Nov. 2020, pp. 42–47, doi: 10.1109/ICAIT51105.2020.9261785.

[54] S. M. T. Toapanta, F. G. M. Quimi, M. G. T. Espinoza, and L. E. M. Gallegos, "Proposal of a model to apply hyperledger in digital identity solutions in a public organization of Ecuador," in *Proc. 3rd World Conf. Smart Trends Syst. Secur. Sustainablity (WorldS4)*, London, U.K., Jul. 2019, pp. 21–28, doi: 10.1109/WorldS4.2019.8903981.

[55] 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)*, Melbourne, VIC, Australia, Dec. 2019, pp. 1–7, doi: 10.1109/CSDE48274.2019.9162366.

[56] C. Singh, D. Chauhan, S. A. Deshmukh, S. S. Vishnu, and R. Walia, "Medi-block record: Secure data sharing using block chain technology," *Informat. Med. Unlocked*, vol. 24, Jan. 2021, Art. no. 100624, doi: 10.1016/j.imu.2021.100624.

[57] D. Peralta-Velecela, M. C. Caceres-Salamea, and V. Morocho, "Digital identity proposal for unified medical record using blockchain technology," in *Proc. IEEE 5th Ecuador Tech. Chapters Meeting (ETCM)*, Cuenca, Ecuador, Oct. 2021, pp. 1–6, doi: 10.1109/ETCM53643.2021.9590679.

[58] L. Zou, J. Chen, Q. Lan, Z. Zhou, C. Ma, and Z. Yang, "Application of blockchain digital identity technology in healthcare consumer finance system," in *Proc. IEEE 2nd Int. Conf. Power, Electron. Comput. Appl. (ICPECA)*, Shenyang, China, Jan. 2022, pp. 1212–1219, doi: 10.1109/ICPECA53709.2022.9719286.

[59] P. K. Deb, A. Mukherjee, and S. Misra, "CovChain: Blockchain-enabled identity preservation and anti-infodemics for COVID-19," *IEEE Netw.*, vol. 35, no. 3, pp. 42–47, May 2021, doi: 10.1109/MNET.011.2000669.

[60] H. Guo, W. Li, M. Nejad, and C.-C. Shen, "Access control for electronic health records with hybrid blockchain-edge architecture," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Atlanta, GA, USA, Jul. 2019, pp. 44–51, doi: 10.1109/Blockchain.2019.00015.

[61] 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, doi: 10.1109/ECICE50847.2020.9301913.

[62] K. A. M. Ahmed, S. F. Saraya, J. F. Wanis, and A. M. T. Ali-Eldin, "A self-sovereign identity architecture based on blockchain and the utilization of customer's banking cards: The case of bank scam calls prevention," in *Proc. 15th Int. Conf. Comput. Eng. Syst. (ICCES)*, Cairo, Egypt, Dec. 2020, pp. 1–8, doi: 10.1109/ICCES51560.2020.9334648.

[63] M. Shen, H. Liu, L. Zhu, K. Xu, H. Yu, X. Du, and M. Guizani, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 942–954, May 2020, doi: 10.1109/JSAC.2020.2980916.

[64] V. Vallois, A. Mehaoua, and M. Amziani, "Blockchain-based identity and access management in industrial IoT systems," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manag. (IM)*, May 2021, pp. 623–627.

[65] Y. Liu, Q. Lu, S. Chen, Q. Qu, H. O'Connor, K.-K. R. Choo, and H. Zhang, "Capability-based IoT access control using blockchain," *Digit. Commun. Netw.*, vol. 7, no. 4, pp. 463–469, Nov. 2021, doi: 10.1016/j.dcan.2020.10.004.

[66] M. Grabatin and W. Hommel, "Self-sovereign identity management in wireless ad hoc mesh networks," in *Proc. IFIP/IEEE Int. Symp. Integr. Netw. Manage. (IM)*, May 2021, pp. 480–486.

[67] D.-P. Le, H. Meng, L. Su, S. L. Yeo, and V. Thing, "BIFF: A blockchain-based IoT forensics framework with identity privacy," in *Proc. IEEE Region 10 Conf.*, Jeju, South Korea, Oct. 2018, pp. 2372–2377, doi: 10.1109/TENCON.2018.8650434.

[68] M. Chen, C. Tan, X. Zhu, and X. Zhang, "A blockchain-based authentication and service provision scheme for Internet of Things," in *Proc. IEEE Globecom Workshops*, Dec. 2020, pp. 1–6, doi: 10.1109/GCWkshps50303.2020.9367565.

[69] 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, doi: 10.1109/IOTM.0001.2000050.

[70] R. Xu, Y. Chen, E. Blasch, and G. Chen, "BlendCAC: A blockchain-enabled decentralized capability-based access control for IoTs," in *Proc. IEEE Int. Conf. Internet Things (iThings) IEEE Green Comput. Commun. (GreenCom) IEEE Cyber, Phys. Social Comput. (CPSCom) IEEE Smart Data (SmartData)*, Halifax, NS, Canada, Jul. 2018, pp. 1027–1034, doi: 10.1109/Cybermatics_2018.2018.00191.

[71] C. Huang and K. Yan, "A blockchain based fast authentication framework for IoT networks with trusted hardware," in *Proc. IEEE 22nd Int. Conf. High Perform. Comput. Commun., IEEE 18th Int. Conf. Smart City, IEEE 6th Int. Conf. Data Sci. Syst.*, Dec. 2020, pp. 1050–1056, doi: 10.1109/HPCC-SmartCity-DSS50907.2020.00141.

[72] W.-C. Liou and T. Lin, "T-auth: A novel authentication mechanism for the IoT based on smart contracts and PUFs," in *Proc. IEEE Int. Conf. Commun. Workshops (ICC Workshops)*, Montreal, QC, Canada, Jun. 2021, pp. 1–6, doi: 10.1109/ICCWorkshops50388.2021.9473808.

[73] W. Li and J. Ying, "A secure access scheme for Internet of Things devices based on blockchain," in *Proc. IEEE 12th Int. Conf. Softw. Eng. Service Sci. (ICSESS)*, Beijing, China, Aug. 2021, pp. 65–71, doi: 10.1109/ICSESS52187.2021.9522329.

[74] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets VANET: An architecture for identity and location privacy protection in VANET," *Peer-Peer Netw. Appl.*, vol. 12, no. 5, pp. 1178–1193, Sep. 2019, doi: 10.1007/s12083-019-00786-4.

[75] W. Li, C. Meese, H. Guo, and M. Nejad, "Blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof," in *Proc. 3rd Int. Conf. Hot Inf.-Centric Netw. (HotICN)*, Hefei, China, Dec. 2020, pp. 18–24, doi: 10.1109/HotICN50779.2020.9350858.

[76] S. A. George, A. Jaekel, and I. Saini, "Secure identity management framework for vehicular ad-hoc network using blockchain," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Rennes, France, Jul. 2020, pp. 1–6, doi: 10.1109/ISCC50000.2020.9219736.

[77] 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, doi: 10.1109/ACCESS.2020.3034299.

[78] D. Liu, D. Li, X. Liu, L. Ma, H. Yu, and H. Zhang, "Research on a cross-domain authentication scheme based on consortium blockchain in V2G networks of smart grid," in *Proc. 2nd IEEE Conf. Energy Internet Energy Syst. Integr. (EI2)*, Beijing, China, Oct. 2018, pp. 1–5, doi: 10.1109/EI2.2018.8582227.

[79] D. Zheng, C. Jing, R. Guo, S. Gao, and L. Wang, "A traceable blockchain-based access authentication system with privacy preservation in VANETs," *IEEE Access*, vol. 7, pp. 117716–117726, 2019, doi: 10.1109/ACCESS.2019.2936575.

[80] R. Yang, N. Liu, Z. Pang, Y. Wang, Q. Jia, W. Lu, Z. Li, M. Li, and L. Wu, "The next generation identity platform for digital era based on blockchain," in *Signal and Information Processing, Networking and Computers*, vol. 677, Y. Wang, L. Xu, Y. Yan, and J. Zou, Eds. Singapore: Springer, 2021, pp. 1035–1044, doi: 10.1007/978-981-33-4102-9_124.

[81] B. N. Eddine, A. Ouaddah, and A. Mezrioui, "Exploring blockchain-based self sovereign identity systems: Challenges and comparative analysis," in *Proc. 3rd Conf. Blockchain Res. Appl. Innov. Netw. Services (BRAINS)*, Paris, France, Sep. 2021, pp. 21–22, doi: 10.1109/BRAINS52497.2021.9569821.

[82] 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)*, Cambridge, MA, USA, Sep. 2019, pp. 1–5, doi: 10.1109/NCA.2019.8935015.

[83] I. Alom, R. M. Eshita, A. I. Harun, M. S. Ferdous, M. K. B. Shuhan, M. J. M. Chowdhury, and M. S. Rahman, "Dynamic management of identity federations using blockchain," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Sydney, NSW, Australia, May 2021, pp. 1–9, doi: 10.1109/ICBC51069.2021.9461128.

[84] D. Maldonado-Ruiz, J. Torres, N. E. Madhoun, and M. Badra, "An innovative and decentralized identity framework based on blockchain technology," in *Proc. 11th IFIP Int. Conf. New Technol., Mobility Secur. (NTMS)*, Paris, France, Apr. 2021, pp. 1–8, doi: 10.1109/NTMS49979.2021.9432656.

[85] B. C. Ghosh, V. Ramakrishna, C. Govindarajan, D. Behl, D. Karunamoorthy, E. Abebe, and S. Chakraborty, "Decentralized cross-network identity management for blockchain interoperation," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, Sydney, NSW, Australia, May 2021, pp. 1–9, doi: 10.1109/ICBC51069.2021.9461064.

[86] K. Jiang, Y. Gao, J. Xiao, and F. Zou, "Unified identity authentication system based on blockchain," in *Proc. IEEE 6th Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, Dec. 2020, pp. 2191–2200, doi: 10.1109/ICCC51575.2020.9344990.

[87] G. Dong, Y. Chen, Y. Hao, B. Jian, Z. Zhang, and L. Sijie, "A unified trust service scheme for heterogeneous identity alliance," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Haikou City, China, Dec. 2020, pp. 167–173, doi: 10.1109/NaNA51271.2020.00037.

[88] A. Furfaro, L. Argento, D. Sacca, F. Angiulli, and F. Fassetti, "An infrastructure for service accountability based on digital identity and blockchain 3.0," in *Proc. IEEE Conf. Comput. Commun. Workshops (INFOCOM WKSHPS)*, Paris, France, Apr. 2019, pp. 632–637, doi: 10.1109/INFCOMW.2019.8845092.

[89] R. T. Moreno, J. Garcia-Rodriguez, J. B. Bernabe, and A. Skarmeta, "A trusted approach for decentralised and privacy-preserving identity management," *IEEE Access*, vol. 9, pp. 105788–105804, 2021, doi: 10.1109/ACCESS.2021.3099837.

[90] A. Dua, S. S. Barpanda, N. Kumar, and S. Tanwar, "Trustful: A decentralized public key infrastructure and identity management system," in *Proc. IEEE Globecom Workshops*, Dec. 2020, pp. 1–6, doi: 10.1109/GCWkshps50303.2020.9367444.

[91] R. Mukta, J. Martens, H.-Y. Paik, Q. Lu, and S. S. Kanhere, "Blockchain-based verifiable credential sharing with selective disclosure," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun.*, Guangzhou, China, Dec. 2020, pp. 959–966, doi: 10.1109/TrustCom50675.2020.00128.

[92] 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.

[93] N. Al-Zaben, M. M. Hassan Onik, J. Yang, N.-Y. Lee, and C.-S. Kim, "General data protection regulation complied blockchain architecture for personally identifiable information management," in *Proc. Int. Conf. Comput., Electron. Commun. Eng. (iCCECE)*, Southend, U.K., Aug. 2018, pp. 77–82, doi: 10.1109/iCCECOME.2018.8658586.

[94] G. Malik, K. Parasrampuria, S. P. Reddy, and S. Shah, "Blockchain based identity verification model," in *Proc. Int. Conf. Vis. Towards Emerg. Trends Commun. Netw. (ViTECoN)*, Vellore, India, Mar. 2019, pp. 1–6, doi: 10.1109/ViTECoN.2019.8899569.

[95] M. Schanzenbach, G. Bramm, and J. Schutte, "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)*, New York, NY, USA, Aug. 2018, pp. 946–957, doi: 10.1109/TRUSTCOM/BIGDATASE.2018.00134.

[96] 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)*, Long Beach, CA, USA, Jun. 2019, pp. 2847–2856, doi: 10.1109/CVPRW.2019.00344.

[97] S. Nayak, N. C. Narendra, A. Shukla, and J. Kempf, "Saranyu: Using smart contracts and blockchain for cloud tenant management," in *Proc. IEEE 11th Int. Conf. Cloud Comput. (CLOUD)*, San Francisco, CA, USA, Jul. 2018, pp. 857–861, doi: 10.1109/CLOUD.2018.00121.

[98] L. Qin, F. Ma, H. G. Xie, and S. L. Zhang, "A distributed authentication scheme based on zero-knowledge proof," in *Proc. IEEE Int. Conf. Consum. Electron. Comput. Eng. (ICCECE)*, Guangzhou, China, Jan. 2021, pp. 203–207, doi: 10.1109/ICCECE51280.2021.9342568.

[99] S. Patel, A. Sahoo, B. K. Mohanta, S. S. Panda, and D. Jena, "DAuth: A decentralized web authentication system using Ethereum based blockchain," in *Proc. Int. Conf. Vis. Towards Emerg. Trends Commun. Netw. (ViTECoN)*, Vellore, India, Mar. 2019, pp. 1–5, doi: 10.1109/ViTECoN.2019.8899393.

[100] 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, doi: 10.1016/j.comcom.2020.08.021.

[101] K. Pinter, D. Schmelz, R. Lamber, S. Strobl, and T. Grechenig, "Towards a multi-party, blockchain-based identity verification solution to implement clear name laws for online media platforms," in *Business Process Management: Blockchain and Central and Eastern Europe Forum*, vol. 361. Cham, Switzerland: Springer, 2019, pp. 151–165, doi: 10.1007/978-3-030-30429-4_11.

[102] F. Dang, F. Gao, H. Liang, and Y. Sun, "Multi-dimensional identity authentication mechanism for power maintenance personnel based on blockchain," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, vol. 1274, Q. Liu, X. Liu, T. Shen, and X. Qiu, Eds. Singapore: Springer, Jun. 2020, pp. 883–889, doi: 10.1109/iwcmc48107.2020.9148178.

[103] S. Wang, R. Pei, and Y. Zhang, "EIDM: A Ethereum-based cloud user identity management protocol," *IEEE Access*, vol. 7, pp. 115281–115291, 2019, doi: 10.1109/ACCESS.2019.2933989.

[104] S. Alansari, F. Paci, A. Margheri, and V. Sassone, "Privacy-preserving access control in cloud federations," in *Proc. IEEE 10th Int. Conf. Cloud Comput. (CLOUD)*, Honolulu, CA, USA, Jun. 2017, pp. 757–760, doi: 10.1109/CLOUD.2017.108.

[105] S. Alansari, F. Paci, and V. Sassone, "A distributed access control system for cloud federations," in *Proc. IEEE 37th Int. Conf. Distrib. Comput. Syst. (ICDCS)*, Atlanta, GA, USA, Jun. 2017, pp. 2131–2136, doi: 10.1109/ICDCS.2017.241.

[106] Y. Chen, Y. Wang, Y. Wang, M. Li, G. Dong, and C. Liu, "CallChain: Identity authentication based on blockchain for telephony networks," in *Proc. IEEE 24th Int. Conf. Comput. Supported Cooperat. Work Design (CSCWD)*, Dalian, China, May 2021, pp. 416–421, doi: 10.1109/CSCWD49262.2021.9437650.

[107] G. Ra, D. Kim, D. Seo, and I. Lee, "A federated framework for fine-grained cloud access control for intelligent big data analytic by service providers," *IEEE Access*, vol. 9, pp. 47084–47095, 2021, doi: 10.1109/ACCESS.2021.3067958.

[108] Z. Wang and L. Chen, "Re-encrypted data access control scheme based on blockchain," in *Proc. IEEE 6th Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, Dec. 2020, pp. 1757–1764, doi: 10.1109/ICCC51575.2020.9345281.

[109] 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, doi: 10.1109/CJECE.2020.2970737.

[110] S. P. Otta and S. Panda, "Decentralized identity and access management of cloud for security as a service," in *Proc. 14th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, Jan. 2022, pp. 299–303, doi: 10.1109/COMSNETS53615.2022.9668529.

[111] M. Westerkamp, S. Gondor, and A. Kupper, "Tawki: Towards self-sovereign social communication," in *Proc. IEEE Int. Conf. Decentralized Appl. Infrastruct. (DAPPCON)*, Newark, CA, USA, Apr. 2019, pp. 29–38, doi: 10.1109/DAPPCON.2019.00014.

[112] 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, doi: 10.1016/j.ipm.2021.102572.

[113] X. Liang, S. Shetty, J. Zhao, D. Bowden, D. Li, and J. Liu, "Towards decentralized accountability and self-sovereignty in healthcare systems," in *Information and Communications Security*, vol. 10631, S. Qing, C. Mitchell, L. Chen, and D. Liu, Eds. Cham, Switzerland: Springer, 2018, pp. 387–398, doi: 10.1007/978-3-319-89500-0_34.

[114] E. Bandara, S. Shetty, R. Mukkamala, X. Liang, P. Foytik, N. Ranasinghe, and K. De Zoysa, "Casper: A blockchain-based system for efficient and secure customer credential verification," *J. Banking Financial Technol.*, vol. 6, no. 1, pp. 43–62, Jun. 2022, doi: 10.1007/s42786-021-00036-3.

[115] Y. Chen, C. Liu, Y. Wang, and Y. Wang, "A self-sovereign decentralized identity platform based on blockchain," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Athens, Greece, Sep. 2021, pp. 1–7, doi: 10.1109/ISCC53001.2021.9631518.

[116] Y. Liu, Q. Lu, H.-Y. Paik, and X. Xu, "Design patterns for blockchain-based self-sovereign identity," in *Proc. Eur. Conf. Pattern Lang. Programs*, Jul. 2020, pp. 1–14, doi: 10.1145/3424771.3424802.

[117] 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.

[118] A. Grüner, A. Mühle, T. Gayvoronskaya, and C. Meinel, "A comparative analysis of trust requirements in decentralized identity management," in *Advanced Information Networking and Applications*, vol. 926, L. Barolli, M. Takizawa, F. Xhafa, and T. Enokido, Eds. Cham, Switzerland: Springer, 2020, pp. 200–213, doi: 10.1007/978-3-030-15032-7_18.

[119] T. Chen, Y. Yu, Z. Duan, J. Gao, and K. Lan, "BlockChain/ABE-based fusion solution for e-government data sharing and privacy protection," in *Proc. 4th Int. Conf. Electron. Inf. Technol. Comput. Eng.*, Xiamen, China, Nov. 2020, pp. 258–264, doi: 10.1145/3443467.3443764.

[120] P. Lafourcade and M. Lombard-Platet, "Get-your-ID: Decentralized proof of identity," in *Foundations and Practice of Security*, vol. 12056, A. Benzekri, M. Barbeau, G. Gong, R. Laborde, and J. Garcia-Alfaro, Eds. Cham, Switzerland: Springer, 2020, pp. 327–336, doi: 10.1007/978-3-030-45371-8_20.

[121] A. Sabir and N. Fetais, "A practical universal consortium blockchain paradigm for patient data portability on the cloud utilizing delegated identity management," in *Proc. IEEE Int. Conf. Informat., IoT, Enabling Technol. (ICIoT)*, Doha, Qatar, Feb. 2020, pp. 484–489, doi: 10.1109/ICIoT48696.2020.9089583.

[122] A. A. Sathio, M. A. Dootio, A. Lakhan, M. U. Rehman, A. O. Pnhwar, and M. A. Sahito, "Pervasive futuristic healthcare and blockchain enabled digital identities-challenges and future intensions," in *Proc. Int. Conf. Comput., Electron. Commun. Eng. (iCCECE)*, Southend, U.K., Aug. 2021, pp. 30–35, doi: 10.1109/iCCECE52344.2021.9534846.

[123] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *Proc. 21st Euromicro Conf. Digit. Syst. Design (DSD)*, Aug. 2018, pp. 699–706, doi: 10.1109/DSD.2018.00008.

[124] F. Tang, S. Ma, Y. Xiang, and C. Lin, "An efficient authentication scheme for blockchain-based electronic health records," *IEEE Access*, vol. 7, pp. 41678–41689, 2019, doi: 10.1109/ACCESS.2019.2904300.

[125] X. Xiang, M. Wang, and W. Fan, "A permissioned blockchain-based identity management and user authentication scheme for e-health systems," *IEEE Access*, vol. 8, pp. 171771–171783, 2020, doi: 10.1109/ACCESS.2020.3022429.

[126] C. Dong, Z. Wang, S. Chen, and Y. Xiang, "BBM: A blockchain-based model for open banking via self-sovereign identity," in *Blockchain—ICBC 2020*, vol. 12404, Z. Chen, L. Cui, B. Palanisamy, and L.-J. Zhang, Eds. Cham, Switzerland: Springer, 2020, pp. 61–75, doi: 10.1007/978-3-030-59638-5_5.

[127] T. Xie, Y. Zhang, K. Gai, and L. Xu, "Cross-chain-based decentralized identity for mortgage loans," in *Knowledge Science, Engineering and Management*, vol. 12817, H. Qiu, C. Zhang, Z. Fei, M. Qiu, and S.-Y. Kung, Eds. Cham, Switzerland: Springer, 2021, pp. 619–633, doi: 10.1007/978-3-030-82153-1_51.

[128] Y. Su, J. Wu, C. Long, and L. Wei, "Secure decentralized machine identifiers for Internet of Things," in *Proc. The 2nd Int. Conf. Blockchain Technol.*, Hilo, HI, USA, Mar. 2020, pp. 57–62, doi: 10.1145/3390566.3391670.

[129] S. Wang, H. Li, J. Chen, J. Wang, and Y. Deng, "DAG blockchain-based lightweight authentication and authorization scheme for IoT devices," *J. Inf. Secur. Appl.*, vol. 66, May 2022, Art. no. 103134, doi: 10.1016/j.jisa.2022.103134.

[130] Z. Li, Y. Chu, X. Liu, Y. Zhang, J. Feng, and X. Xiang, "Physical unclonable function based identity management for IoT with blockchain," *Proc. Comput. Sci.*, vol. 198, pp. 454–459, Jan. 2022, doi: 10.1016/j.procs.2021.12.269.

[131] L. Wang, X. Huang, L. Chen, J. Fan, and M. Zhang, "Credible identity authentication mechanism of electric Internet of Things based on blockchain," in *Proc. 10th Int. Conf. Comput. Eng. Netw.*, vol. 1274, Q. Liu, X. Liu, T. Shen, and X. Qiu, Eds. Singapore: Springer, 2021, pp. 866–875, doi: 10.1007/978-981-15-8462-6_100.

[132] H. Wu, X. Feng, G. Kan, and X. Jiang, "BIPP: Blockchain-based identity privacy protection scheme in Internet of Vehicles for remote anonymous communication," in *Algorithms and Architectures for Parallel Processing*, vol. 13156, Y. Lai, T. Wang, M. Jiang, G. Xu, W. Liang, and A. Castiglione, Eds. Cham, Switzerland: Springer, 2022, pp. 489–506, doi: 10.1007/978-3-030-95388-1_32.

[133] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid BlockChain-based identity authentication scheme for multi-WSN," *IEEE Trans. Services Comput.*, vol. 13, no. 2, pp. 241–251, Mar. 2020, doi: 10.1109/TSC.2020.2964537.

[134] S. Banerjee, S. Bouzefrane, and A. Abane, "Identity management with hybrid blockchain approach: A deliberate extension with federated-inverse-reinforcement learning," in *Proc. IEEE 22nd Int. Conf. High Perform. Switching Routing (HPSR)*, Paris, France, Jun. 2021, pp. 1–6, doi: 10.1109/HPSR52026.2021.9481851.

[135] Y. Tu, J. Gan, Y. Hu, R. Jin, Z. Yang, and M. Liu, "Decentralized identity authentication and key management scheme," in *Proc. IEEE 3rd Conf. Energy Internet Energy Syst. Integr. (EI2)*, Changsha, China, Nov. 2019, pp. 2697–2702, doi: 10.1109/EI247390.2019.9062013.

[136] I. A. Obiri, J. Yang, Q. Xia, and J. Gao, "A sovereign PKI for IoT devices based on the blockchain technology," in *Proc. 18th Int. Comput. Conf. Wavelet Act. Media Technol. Inf. Process. (ICCWAMTIP)*, Chengdu, China, Dec. 2021, pp. 110–115, doi: 10.1109/ICCWAMTIP53232.2021.9674095.

[137] G. Ra, T. Kim, and I. Lee, "VAIM: Verifiable anonymous identity management for human-centric security and privacy in the Internet of Things," *IEEE Access*, vol. 9, pp. 75945–75960, 2021, doi: 10.1109/ACCESS.2021.3080329.

[138] X. Wang, F. Gao, J. Zhang, X. Feng, and X. Hu, "Cross-domain authentication mechanism for power terminals based on blockchain and credibility evaluation," in *Proc. 5th Int. Conf. Comput. Commun. Syst. (ICCCS)*, Shanghai, China, May 2020, pp. 936–940, doi: 10.1109/ICCCS49078.2020.9118421.

[139] 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.

[140] Y. Fan, G. Zhao, W. Shang, J. Shang, W. Lin, and Z. Wang, "A preliminary design for authenticity of IoT big data in cloud computing," in *Proc. 29th Int. Conf. Comput. Commun. Netw. (ICCCN)*, Honolulu, HI, USA, Aug. 2020, pp. 1–2, doi: 10.1109/ICCCN49398.2020.9209646.

[141] B. Guehguih and H. Lu, "Blockchain-based privacy-preserving authentication and message dissemination scheme for VANET," in *Proc. 5th Int. Conf. Syst., Control Commun.*, Wuhan, China, Dec. 2019, pp. 16–21, doi: 10.1145/3377458.3377466.

[142] B. Liu, K. Yu, C. Feng, and K.-K.-R. Choo, "Cross-domain authentication for 5G-enabled UAVs: A blockchain approach," in *Proc. 4th ACM MobiCom Workshop Drone Assist. Wireless Commun. 5G Beyond*, Oct. 2021, pp. 25–30, doi: 10.1145/3477090.3481053.

[143] Y. Ren, X. Li, S.-F. Sun, X. Yuan, and X. Zhang, "Privacy-preserving batch verification signature scheme based on blockchain for vehicular ad-hoc networks," *J. Inf. Secur. Appl.*, vol. 58, May 2021, Art. no. 102698, doi: 10.1016/j.jisa.2020.102698.

[144] X. Feng, Q. Shi, Q. Xie, and L. Liu, "An efficient privacy-preserving authentication model based on blockchain for VANETs," *J. Syst. Archit.*, vol. 117, Aug. 2021, Art. no. 102158, doi: 10.1016/j.sysarc.2021.102158.

[145] X. Zhan, X. Cheng, W. Guo, K. Yin, and X. Lu, "An distributed CA system: Identity authentication system in transnational railway transportation based on blockchain," in *Proc. Int. Conf. Comput. Inf. Sci. Artif. Intell. (CISAI)*, Kunming, China, Sep. 2021, pp. 989–994, doi: 10.1109/CISAI54367.2021.00198.

[146] H. Liu, P. Zhang, G. Pu, T. Yang, S. Maharjan, and Y. Zhang, "Blockchain empowered cooperative authentication with data traceability in vehicular edge computing," *IEEE Trans. Veh. Technol.*, vol. 69, no. 4, pp. 4221–4232, Apr. 2020, doi: 10.1109/TVT.2020.2969722.

[147] P. Zhang, H. Liu, and Y. Zhang, "Blockchain enabled cooperative authentication with data traceability in vehicular edge computing," in *Proc. Comput., Commun. IoT Appl. (ComComAp)*, Shenzhen, China, Oct. 2019, pp. 299–304, doi: 10.1109/ComComAp46287.2019.9018754.

[148] H. Li, L. Pei, D. Liao, S. Chen, M. Zhang, and D. Xu, "FADB: A fine-grained access control scheme for VANET data based on blockchain," *IEEE Access*, vol. 8, pp. 85190–85203, 2020, doi: 10.1109/ACCESS.2020.2992203.

[149] X. Li, J. Zhang, X. Niu, and J. Guan, "Blockchain-based certificateless identity management mechanism in cloud-native environments," in *Proc. ACM Int. Conf. Intell. Comput. Emerg. Appl.*, Jinan, China, Dec. 2021, pp. 139–145, doi: 10.1145/3491396.3506537.

[150] M. A. Abubakar, Z. Jaroucheh, A. Al-Dubai, and X. Liu, "Blockchain-based identity and authentication scheme for MQTT protocol," in *Proc. 3rd Int. Conf. Blockchain Technol.*, Shanghai China, Mar. 2021, pp. 73–81, doi: 10.1145/3460537.3460549.

[151] 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, doi: 10.1016/j.ipm.2021.102556.

[152] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102050, doi: 10.1016/j.cose.2020.102050.

[153] J. Deng, L. Jiao, L. Zhang, Y. Ren, and W. Yin, "Design of identity authentication scheme for dynamic service command system based on SM2 algorithm and blockchain technology," in *Advances in Internet, Data & Web Technologies*, vol. 118, L. Barolli, E. Kulla, and M. Ikeda, Eds. Cham, Switzerland: Springer, 2022, pp. 31–37, doi: 10.1007/978-3-030-95903-6_4.

[154] Y. Chen, G. Dong, Y. Hao, Z. Zhang, H. Peng, and S. Yu, "An open identity authentication scheme based on blockchain," in *Algorithms Architectures for Parallel Process.*, vol. 11944, S. Wen, A. Zomaya, and L. T. Yang, Eds. Cham, Switzerland: Springer, 2020, pp. 421–438, doi: 10.1007/978-3-030-38991-8_28.

[155] D. Patole, Y. Borse, J. Jain, and S. Maher, "Personal identity on blockchain," in *Advances in Computing and Intelligent Systems*, H. Sharma, K. Govindan, R. C. Poonia, S. Kumar, and W. M. El-Medany, Eds. Singapore: Springer, 2020, pp. 439–446, doi: 10.1007/978-981-15-0222-4_41.

[156] W. Ao, S. Fu, C. Zhang, and M. Xu, "A secure certificateless identity authentication scheme based on blockchain," in *Trusted Computing and Information Security*, vol. 1149, W. Han, L. Zhu, and F. Yan, Eds. Singapore: Springer, 2020, pp. 251–266, doi: 10.1007/978-981-15-3418-8_16.

[157] B. Leiding and A. Norta, "Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance," in *Future Data and Security Engineering*, vol. 10646, T. K. Dang, R. Wagner, J. Küng, N. Thoai, M. Takizawa, and E. J. Neuhold, Eds. Cham, Switzerland: Springer, 2017, pp. 181–196, doi: 10.1007/978-3-319-70004-5_13.

[158] H. Gulati and C.-T. Huang, "Self-sovereign dynamic digital identities based on blockchain technology," in *Proc. SoutheastCon*, Huntsville, AL, USA, Apr. 2019, pp. 1–6, doi: 10.1109/SoutheastCon42311.2019.9020518.

[159] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, and S. Guerreiro, "SSIBAC: Self-sovereign identity based access control," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Guangzhou, China, Dec. 2020, pp. 1935–1943, doi: 10.1109/TRUSTCOM50675.2020.00264.

[160] 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.

[161] W. Ao, S. Fu, C. Zhang, Y. Huang, and F. Xia, "A secure identity authentication scheme based on blockchain and identity-based cryptography," in *Proc. IEEE 2nd Int. Conf. Comput. Commun. Eng. Technol. (CCET)*, Beijing, China, Aug. 2019, pp. 90–95, doi: 10.1109/CCET48361.2019.8989361.

[162] A. Abraham, S. More, C. Rabensteiner, and F. Horandner, "Revocable and offline-verifiable self-sovereign identities," in *Proc. IEEE 19th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Guangzhou, China, Dec. 2020, pp. 1020–1027, doi: 10.1109/TrustCom50675.2020.00136.

[163] 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)*, Guilin, China, Oct. 2019, pp. 42–49, doi: 10.1109/CyberC.2019.00017.

[164] Z. Zhao and Y. Liu, "A blockchain based identity management system considering reputation," in *Proc. 2nd Int. Conf. Inf. Syst. Comput. Aided Educ. (ICISCAE)*, Dalian, China, Sep. 2019, pp. 32–36, doi: 10.1109/ICISCAE48440.2019.221582.

[165] C. Lin, D. He, X. Huang, M. K. Khan, and K.-K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," *IEEE Access*, vol. 6, pp. 28203–28212, 2018, doi: 10.1109/ACCESS.2018.2837650.

[166] K. Mudliar, H. Parekh, and P. Bhavathankar, "A comprehensive integration of national identity with blockchain technology," in *Proc. Int. Conf. Commun. Inf. Comput. Technol. (ICCICT)*, Feb. 2018, pp. 1–6, doi: 10.1109/ICCICT.2018.8325891.

[167] J. Liu, Y. Wu, L. L. Shi, Z. Li, and C. Liu, "A public blockchain-based identity management scheme and Ptri net-based verification," in *Proc. 20th Int. Conf. Ubiquitous Comput. Commun.*, London, U.K., Dec. 2021, pp. 361–368, doi: 10.1109/IUCC-CIT-DSCI-SmartCNS55181.2021.00065.

[168] D. Chakravarty and T. Deshpande, "Blockchain-enhanced identities for secure interaction," in *Proc. IEEE Int. Symp. Technol. Homeland Secur. (HST)*, Woburn, MA, USA, Oct. 2018, pp. 1–4, doi: 10.1109/THS.2018.8574130.

[169] Y. Lu, X. Zhang, C. Zhang, S. Dai, P. Ma, and L. Jiang, "A study of two-way authentication for decentralized network identities," in *Proc. 14th Int. Conf. Measuring Technol. Mechatronics Autom. (ICMTMA)*, Changsha, China, Jan. 2022, pp. 861–865, doi: 10.1109/ICMTMA54903.2022.00175.

[170] B. Liu, L. Xiao, J. Long, M. Tang, and O. Hosam, "Secure digital certificate-based data access control scheme in blockchain," *IEEE Access*, vol. 8, pp. 91751–91760, 2020, doi: 10.1109/ACCESS.2020.2993921.

[171] W. Jing, "A decentralized user authentication model based on activity proof: Use the new user identity credential: Activity map," in *Proc. Int. Conf. Commun., Inf. Syst. Comput. Eng. (CISCE)*, Kuala Lumpur, Malaysia, Jul. 2020, pp. 207–212, doi: 10.1109/CISCE50729.2020.00047.

[172] T. Xiong, R. Zhang, J. Liu, T. Huang, Y. Liu, and F. R. Yu, "A blockchain-based and privacy-preserved authentication scheme for inter-constellation collaboration in space-ground integrated networks," *Comput. Netw.*, vol. 206, Apr. 2022, Art. no. 108793, doi: 10.1016/j.comnet.2022.108793.

[173] M. Xiao, Z. Ma, and T. Li, "Privacy-preserving and scalable data access control based on self-sovereign identity management in large-scale cloud storage," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, vol. 12382, G. Wang, B. Chen, W. Li, R. Di Pietro, X. Yan, and H. Han, Eds. Cham, Switzerland: Springer, 2021, pp. 1–18, doi: 10.1007/978-3-030-68851-6_1.

[174] A. Shobanadevi, S. Tharewal, M. Soni, D. D. Kumar, I. R. Khan, and P. Kumar, "Novel identity management system using smart blockchain technology," *Int. J. Syst. Assurance Eng. Manage.*, vol. 13, no. S1, pp. 496–505, Mar. 2022, doi: 10.1007/s13198-021-01494-0.

[175] D. Bao and L. You, "Two-factor identity authentication scheme based on blockchain and fuzzy extractor," *Soft Comput.*, vol. 27, no. 2, pp. 1091–1103, Jan. 2023, doi: 10.1007/s00500-021-05936-6.

[176] C. Zhuang, Q. Dai, and Y. Zhang, "BCPPT: A blockchain-based privacy-preserving and traceability identity management scheme for intellectual property," *Peer-Peer Netw. Appl.*, vol. 15, no. 1, pp. 724–738, Jan. 2022, doi: 10.1007/s12083-021-01277-1.

[177] X. Yu, R. Ge, and F. Li, "Research on blockchain-based identity authentication scheme in social networks," in *Machine Learning for Cyber Security*, vol. 12486, X. Chen, H. Yan, Q. Yan, and X. Zhang, Eds. Cham, Switzerland: Springer, 2020, pp. 558–565, doi: 10.1007/978-3-030-62223-7_49.

[178] J. Wang, S. Li, and S. Wei, "Identity-based cross-domain authentication by blockchain via PKI environment," in *Blockchain Technology and Application*, vol. 1176, X. Si, H. Jin, Y. Sun, J. Zhu, L. Zhu, X. Song, and Z. Lu, Eds. Singapore: Springer, 2020, pp. 131–144, doi: 10.1007/978-981-15-3278-8_9.

[179] F. Liu, B. Yang, L. Su, K. Wang, and J. Yan, "A blockchain based scheme for authentic telephone identity," in *Blockchain and Trustworthy Systems*, vol. 1267, Z. Zheng, H.-N. Dai, X. Fu, and B. Chen, Eds. Singapore: Springer, 2020, pp. 675–682, doi: 10.1007/978-981-15-9213-3_52.

[180] X. Huang, Q. Guo, Q. Yao, and X. Huo, "Trusted identity cross-domain dynamic authorization mechanism based on master-slave chain," in *Proc. 10th Int. Conf. Comput. Eng. Netw.*, vol. 1274, Q. Liu, X. Liu, T. Shen, and X. Qiu, Eds. Singapore: Springer, 2021, pp. 876–882, doi: 10.1007/978-981-15-8462-6_101.

[181] 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. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr.*, Fukuoka, Japan, Aug. 2019, pp. 320–325, doi: 10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.

[182] H. Huang and X. Chen, "Power mobile terminal identity authentication mechanism based on blockchain," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Limassol, Cyprus, Jun. 2020, pp. 195–198, doi: 10.1109/IWCMC48107.2020.9148258.

[183] F. Dang, F. Gao, H. Liang, and Y. Sun, "Multi-dimensional identity authentication mechanism for power maintenance personnel based on blockchain," in *Proc. Int. Wireless Commun. Mobile Comput. (IWCMC)*, Limassol, Cyprus, Jun. 2020, pp. 215–219, doi: 10.1109/IWCMC48107.2020.9148178.

[184] 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, doi: 10.1109/TVT.2020.2986041.

[185] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: A novel blockchain-based trust model for cloud identity management," in *Proc. IEEE 16th Int. Conf. Dependable, Autonomic Secure Comput., 16th Int. Conf. Pervasive Intell. Comput., 4th Int. Conf. Big Data Intell. Comput. Cyber Sci. Technol. Congr.*, Aug. 2018, pp. 724–729, doi: 10.1109/DASC/PiCom/DataCom/CyberSciTec.2018.00126.

[186] N. Choi and H. Kim, "Hybrid blockchain-based unification ID in smart environment," in *Proc. 22nd Int. Conf. Adv. Commun. Technol. (ICACT)*, PyeongChang, South Korea, Feb. 2020, pp. 166–170, doi: 10.23919/ICACT48636.2020.9061430.
[187] T. Zhong, P. Shi, and J. Chang, "JointCloud cross-chain verification model of decentralized identifiers," in *Proc. IEEE Int. Perform., Comput., Commun. Conf. (IPCCC)*, Austin, TX, USA, Oct. 2021, pp. 1–8, doi: 10.1109/IPCCC51483.2021.9679363.
[188] S. Ganta, "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)*, Tiruchirappalli, India, May 2019, pp. 454–457, doi: 10.1109/IMICPW.2019.8933182.
[189] 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)*, Tiruchirappalli, India, May 2019, pp. 288–292, doi: 10.1109/IMICPW.2019.8933273.
[190] Y. Zhou, Y. Guan, Z. Zhang, and F. Li, "A blockchain-based access control scheme for smart grids," in *Proc. Int. Conf. Netw. Netw. Appl. (NaNA)*, Daegu, South Korea, Oct. 2019, pp. 368–373, doi: 10.1109/NaNA.2019.00070.
[191] 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.*, Vellore, India, Feb. 2020, pp. 1–5, doi: 10.1109/ic-ETITE47903.2020.469.
[192] A. Chowdhary, S. Agrawal, and B. Rudra, "Blockchain based framework for Student identity and educational certificate verification," in *Proc. 2nd Int. Conf. Electron. Sustain. Commun. Syst. (ICESC)*, Coimbatore, India, Aug. 2021, pp. 916–921, doi: 10.1109/ICESC51422.2021.9532968.
[193] M. M. Al-Musawi, "Transforming one-stop e-services in iraq: Focusing on perception of blockchain technology in digital identity system," in *Proc. IEEE Global Humanitarian Technol. Conf. (GHTC)*, Seattle, WA, USA, Oct. 2020, pp. 1–4, doi: 10.1109/GHTC46280.2020.9342959.
[194] S. Bakare, S. C. Shinde, and R. Hubballi, "A blockchain framework for secure digital identity transactions in Indian agri-subsidy system: Issues, challenges and benefits," in *Proc. 4th Int. Conf. Comput. Commun. Technol. (ICCCT)*, Chennai, India, Dec. 2021, pp. 138–143, doi: 10.1109/ICCCT53315.2021.9711868.
[195] 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)*, Washington, DC, USA, Jun. 2019, pp. 1–8, doi: 10.1109/CNS.2019.8802771.
[196] M. Shuaib, S. Alam, M. S. Alam, and M. S. Nasir, "Self-sovereign identity for healthcare using blockchain," *Mater. Today, Proc.*, vol. 2021, Mar. 2021, Art. no. S2214785321021027, doi: 10.1016/j.matpr.2021.03.083.
[197] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity," *Inf. Manage.*, vol. 59, no. 7, Nov. 2022, Art. no. 103553, doi: 10.1016/j.im.2021.103553.
[198] 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.*, Oct. 2020, pp. 2221–2227, doi: 10.1109/IECON43393.2020.9254545.
[199] A. Ouaddah, A. A. Elkalam, and A. A. Ouahman, "Harnessing the power of blockchain technology to solve IoT security & privacy issues," in *Proc. 2nd Int. Conf. Internet Things, Data Cloud Comput.*, Cambridge, U.K., Mar. 2017, pp. 1–10, doi: 10.1145/3018896.3018901.
[200] X. Fan, Q. Chai, L. Xu, and D. Guo, "DIAM-IoT: A decentralized identity and access management framework for Internet of Things," in *Proc. 2nd ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, Oct. 2020, pp. 186–191, doi: 10.1145/3384943.3409436.
[201] L. Tan, N. Shi, K. Yu, M. Aloqaily, and Y. Jararweh, "A blockchain-empowered access control framework for smart devices in green Internet of Things," *ACM Trans. Internet Technol.*, vol. 21, no. 3, pp. 1–20, Jun. 2021, doi: 10.1145/3433542.
[202] Z. Tian, B. Yan, Q. Guo, J. Huang, and Q. Du, "Feasibility of identity authentication for IoT based on blockchain," *Proc. Comput. Sci.*, vol. 174, pp. 328–332, Jan. 2020, doi: 10.1016/j.procs.2020.06.094.
[203] 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)*, Dublin, Ireland, Jun. 2020, pp. 1–6, doi: 10.1109/GIOTS49054.2020.9119623.
[204] 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)*, Halifax, NS, Canada, Jul. 2018, pp. 994–1000, doi: 10.1109/Cybermatics_2018.2018.00187.
[205] 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)*, Toronto, ON, Canada, May 2020, pp. 1–9, doi: 10.1109/ICBC48266.2020.9169411.
[206] 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)*, Tucson, AZ, USA, Sep. 2017, pp. 69–79, doi: 10.1109/ICCAC.2017.14.
[207] A. Yasin and L. Liu, "An online identity and smart contract management system," in *Proc. IEEE 40th Annu. Comput. Softw. Appl. Conf. (COMPSAC)*, Atlanta, GA, USA, Jun. 2016, pp. 192–198, doi: 10.1109/COMPSAC.2016.2.
[208] P. R. Carnley, P. Rowland, D. Bishop, S. Bagui, and M. Miller, "Trusted digital identities for mobile devices," in *Proc. IEEE Int. Conf. Dependable, Autonomic Secure Comput., Int. Conf. Pervasive Intell. Comput., Int. Conf. Cloud Big Data Comput., Int. Conf. Cyber Sci. Technol. Congr.*, Calgary, AB, Canada, Aug. 2020, pp. 483–490, doi: 10.1109/DASC-PICom-CBDCom-CyberSciTech49142.2020.00090.
[209] T. Le and M. W. Mutka, "CapChain: A privacy preserving access control framework based on blockchain for pervasive environments," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Jun. 2018, pp. 57–64, doi: 10.1109/SMARTCOMP.2018.00074.
[210] S. Malik, N. Gupta, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TradeChain: Decoupling traceability and identity in blockchain enabled supply chains," in *Proc. IEEE 20th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Shenyang, China, Oct. 2021, pp. 1141–1152, doi: 10.1109/TrustCom53373.2021.00155.
[211] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain: Res. Appl.*, vol. 2, no. 2, Jun. 2021, Art. no. 100014, doi: 10.1016/j.bcra.2021.100014.
[212] C. Dong, F. Jiang, X. Li, A. Yao, G. Li, and X. Liu, "A blockchain-aided self-sovereign identity framework for edge-based UAV delivery system," in *Proc. IEEE/ACM 21st Int. Symp. Cluster, Cloud Internet Comput. (CCGrid)*, Melbourne, VIC, Australia, May 2021, pp. 622–624, doi: 10.1109/CCGrid51090.2021.00074.
[213] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *Proc. 17th IEEE Int. Conf. Trust, Secur. Privacy Comput. Commun./12th IEEE Int. Conf. Big Data Sci. Eng.*, New York, NY, USA, Aug. 2018, pp. 674–679, doi: 10.1109/TrustCom/BigDataSE.2018.00099.
[214] Z. Gao, L. Xu, G. Turner, B. Patel, N. Diallo, L. Chen, and W. Shi, "Blockchain-based identity management with mobile device," in *Proc. 1st Workshop Cryptocurrencies Blockchains Distrib. Syst.*, Munich Germany, Jun. 2018, pp. 66–70, doi: 10.1145/3211933.3211945.
[215] W. Shao, C. Jia, Y. Xu, K. Qiu, Y. Gao, and Y. He, "AttriChain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain," *Comput. Secur.*, vol. 99, Dec. 2020, Art. no. 102069, doi: 10.1016/j.cose.2020.102069.
[216] A. Satybaldy, M. Nowostawski, and J. Ellingsen, "Self-sovereign identity systems: Evaluation framework," in *Privacy Identity Management. Data for Better Living: AI Privacy*, vol. 576, M. Friedewald, M. Önen, E. Lievens, S. Krenn, and S. Fricker, Eds. Cham, Switzerland: Springer, 2020, pp. 447–461, doi: 10.1007/978-3-030-42504-3_28.
[217] R. Geetha, T. Padmavathy, and G. U. Srikanth, "A scalable block chain framework for user identity management in a decentralized network," *Wireless Pers. Commun.*, vol. 123, no. 4, pp. 3719–3736, Apr. 2022, doi: 10.1007/s11277-021-09310-5.
[218] 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)*, Halifax, NS, Canada, Jul. 2018, pp. 1129–1136, doi: 10.1109/Cybermatics_2018.2018.00205.

[219] D. Maldonado-Ruiz, J. Torres, and N. E. 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)*, Paris, France, Sep. 2020, pp. 45–46, doi: 10.1109/BRAINS49436.2020.9223300.

[220] D. N. Kirupanithi and A. Antonidoss, "Hierarchical deterministic protocol for the defragmentation of identity in a blockchain-based framework," in *Proc. 5th Int. Conf. I-SMAC*, Palladam, India, Nov. 2021, pp. 1497–1504, doi: 10.1109/I-SMAC52330.2021.9640809.

[221] 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)*, Granada, Spain, Oct. 2019, pp. 519–528, doi: 10.1109/IOTSMS48152.2019.8939249.

[222] P. Szalachowski, "Password-authenticated decentralized identities," *IEEE Trans. Inf. Forensics Security*, vol. 16, pp. 4801–4810, 2021, doi: 10.1109/TIFS.2021.3116429.

[223] P. Mishra, V. Modanwal, H. Kaur, and G. Varshney, "Pseudo-biometric identity framework: Achieving self-sovereignty for biometrics on blockchain," in *Proc. IEEE Int. Conf. Syst., Man, Cybern. (SMC)*, Melbourne, VIC, Australia, Oct. 2021, pp. 945–951, doi: 10.1109/SMC52423.2021.9659136.

[224] L. Zhang, H. Li, L. Sun, Z. Shi, and Y. He, "Poster: Towards fully distributed user authentication with blockchain," in *Proc. IEEE Symp. Privacy-Aware Comput. (PAC)*, Washington, DC, USA, Aug. 2017, pp. 202–203, doi: 10.1109/PAC.2017.28.

[225] H. Halpin, "Nym credentials: Privacy-preserving decentralized identity with blockchains," in *Proc. Crypto Valley Conf. Blockchain Technol. (CVCBT)*, Rotkreuz, Switzerland, Jun. 2020, pp. 56–67, doi: 10.1109/CVCBT50464.2020.00010.

[226] R. U. Haque, A. S. M. T. Hasan, A. Daria, Q. Qu, and Q. Jiang, "Towards convergence of blockchain and self-sovereign identity for privacy-preserving secure federated learning," in *Big Data and Security*, vol. 1563, Y. Tian, T. Ma, M. K. Khan, V. S. Sheng, and Z. Pan, Eds. Singapore: Springer, 2022, pp. 243–255, doi: 10.1007/978-981-19-0852-1_19.

[227] C. Yang, L. Tan, N. Shi, B. Xu, Y. Cao, and K. Yu, "AuthPrivacyChain: A blockchain-based access control framework with privacy protection in cloud," *IEEE Access*, vol. 8, pp. 70604–70615, 2020, doi: 10.1109/ACCESS.2020.2985762.

[228] L. Tan, N. Shi, C. Yang, and K. Yu, "A blockchain-based access control framework for cyber-physical-social system big data," *IEEE Access*, vol. 8, pp. 77215–77226, 2020, doi: 10.1109/ACCESS.2020.2988951.

[229] G. Zhao, H. He, B. Di, Q. Xia, and Z. Fu, "A blockchain-based system for student e-portfolio assessment using smart contract," in *Proc. 4th Int. Conf. Comput. Sci. Artif. Intell.*, Zhuhai, China, Dec. 2020, pp. 34–40, doi: 10.1145/3445815.3445821.

[230] O. S. Saleh, O. Ghazali, and N. B. Idris, "A new decentralized certification verification privacy control protocol," in *Proc. 3rd Int. Cyber Resilience Conf. (CRC)*, Langkawi Island, Malaysia, Jan. 2021, pp. 1–6, doi: 10.1109/CRC50527.2021.9392485.

[231] E. Bandara, X. Liang, P. Foytik, S. Shetty, C. Hall, D. Bowden, N. Ranasinghe, K. De Zoysa, and W. K. Ng, "Connect—Blockchain and self-sovereign identity empowered contact tracing platform," in *Wireless Mobile Communication and Healthcare*, vol. 362, J. Ye, M. J. O'Grady, G. Civitarese, and K. Yordanova, Eds. Cham, Switzerland: Springer, 2021, pp. 208–223, doi: 10.1007/978-3-030-70569-5_13.

[232] A. Alabdullatif, K. Alajaji, N. S. Al-Serhani, R. Zagrouba, and M. AlDossary, "Improving an identity authentication management protocol in IIoT," in *Proc. 2nd Int. Conf. Comput. Appl. Inf. Secur. (ICCAIS)*, Riyadh, Saudi Arabia, May 2019, pp. 1–6, doi: 10.1109/CAIS.2019.8769499.

[233] H. Gunasinghe, A. Kundu, E. Bertino, H. Krawczyk, S. Chari, K. Singh, and D. Su, "PrivIdEx: Privacy preserving and secure exchange of digital identity Assets," in *Proc. World Wide Web Conf.*, San Francisco, CA, USA, May 2019, pp. 594–604, doi: 10.1145/3308558.3313574.

[234] V. Odelu, "*IMBUA*: Identity management on blockchain for biometrics-based user authentication," in *Blockchain and Applications*, vol. 1010, J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, Eds. Cham, Switzerland: Springer, 2020, pp. 1–10, doi: 10.1007/978-3-030-23813-1_1.

[235] P. Jakubeit, A. Dercksen, and A. Peter, "SSI-AWARE: Self-sovereign identity authenticated backup with auditing by remote entities," in *Information Security Theory and Practice*, vol. 12024, M. Laurent and T. Giannetsos, Eds. Cham, Switzerland: Springer, 2020, pp. 202–219, doi: 10.1007/978-3-030-41702-4_13.

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

[237] 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, doi: 10.1109/IS.2018.8710547.

[238] 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)*, Rennes, France, Jul. 2020, pp. 1–6, doi: 10.1109/ISCC50000.2020.9219594.

[239] J. Lauinger, J. Ernstberger, E. Regnath, M. Hamad, and S. Steinhorst, "A-PoA: Anonymous proof of authorization for decentralized identity management," in *Proc. IEEE Int. Conf. Blockchain Cryptocurrency (ICBC)*, May 2021, pp. 1–9, doi: 10.1109/ICBC51069.2021.9461082.

[240] Y. Tan, W. Li, J. Yin, and Y. Deng, "A universal decentralized authentication and authorization protocol based on blockchain," in *Proc. Int. Conf. Cyber-Enabled Distrib. Comput. Knowl. Discovery (CyberC)*, Chongqing, China, Oct. 2020, pp. 7–14, doi: 10.1109/CyberC49757.2020.00012.

[241] S. Li, M. Liu, and S. Wei, "A distributed authentication protocol using identity-based encryption and blockchain for LEO network," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, vol. 10656, G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, Eds. Cham, Switzerland: Springer, 2017, pp. 446–460, doi: 10.1007/978-3-319-72389-1_36.

[242] H. Yildiz, C. Ritter, L. T. Nguyen, B. Frech, M. M. Martinez, and A. Kupper, "Connecting self-sovereign identity with federated and user-centric identities via SAML integration," in *Proc. IEEE Symp. Comput. Commun. (ISCC)*, Athens, Greece, Sep. 2021, pp. 1–7, doi: 10.1109/ISCC53001.2021.9631453.

[243] G. Zhao, B. Di, and H. He, "Design and implementation of the digital education transaction subject two-factor identity authentication system based on blockchain," in *Proc. 22nd Int. Conf. Adv. Commun. Technol. (ICACT)*, Feb. 2020, pp. 176–180, doi: 10.23919/ICACT48636.2020.9061393.

[244] D. A. Belurgikar, J. Kanak Kshirsagar, K. K. Dhananjaya, and N. Vineeth, "Identity solutions for verification using blockchain technology," in *Proc. 1st Int. Conf. Adv. Technol. Intell. Control, Environ., Comput. Commun. Eng. (ICATIECE)*, Bangalore, India, Mar. 2019, pp. 121–126, doi: 10.1109/ICATIECE45860.2019.9063802.

[245] G.-A. Dima, A.-G. Jitariu, C. Pisa, and G. Bianchi, "Scholarium: Supporting identity claims through a permissioned blockchain," in *Proc. IEEE 4th Int. Forum Res. Technol. Soc. Ind. (RTSI)*, Sep. 2018, pp. 1–6, doi: 10.1109/RTSI.2018.8548407.

[246] M. A. A. Mamun, S. M. M. Alam, S. M. Hossain, and M. Samiruzzaman, "A novel approach to blockchain-based digital identity system," in *Advances in Information and Communication*, vol. 1129, K. Arai, S. Kapoor, and R. Bhatia, Eds. Cham, Switzerland: Springer, 2020, pp. 93–112, doi: 10.1007/978-3-030-39445-5_9.

[247] A. A. Musoke, P. Dushimimana, and M. Saint, "Identity inclusion: A digital national identification for all," in *Science and Technologies for Smart Cities*, vol. 372, S. Paiva, S. I. Lopes, R. Zitouni, N. Gupta, S. F. Lopes, and T. Yonezawa, Eds. Cham, Switzerland: Springer, 2021, pp. 511–525, doi: 10.1007/978-3-030-76063-2_34.

[248] J. Blue, J. Condell, and T. Lunney, "Proving yourself: Addressing the refugee identity crisis with Bayesi-chain probability & digital footprints," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Istanbul, Turkey, Jun. 2019, pp. 1–6, doi: 10.1109/ISNCC.2019.8909145.

[249] Y. Luo, G. Lu, and Y. Wu, "Design and analysis of blood donation model based on blockchain and KNN," in *Proc. 3rd Blockchain Internet Things Conf.*, Ho Chi Minh City, Vietnam, Jul. 2021, pp. 32–37, doi: 10.1145/3475992.3475997.

[250] G. Shobana and M. Suguna, "Block chain technology towards identity management in health care application," in *Proc. 3rd Int. Conf. I-SMAC*, Palladam, India, Dec. 2019, pp. 531–535, doi: 10.1109/I-SMAC47947.2019.9032472.

[251] Y. Liang, "Identity verification and management of electronic health records with blockchain technology," in *Proc. IEEE Int. Conf. Healthcare Informat. (ICHI)*, Xi'an, China, Jun. 2019, pp. 1–3, doi: 10.1109/ICHI.2019.8904712.

[252] K. O. Asamoah, H. Xia, S. Amofa, O. I. Amankona, K. Luo, Q. Xia, J. Gao, X. Du, and M. Guizani, "Zero-chain: A blockchain-based identity for digital city operating system," *IEEE Internet Things J.*, vol. 7, no. 10, pp. 10336–10346, Oct. 2020, doi: 10.1109/JIOT.2020.2986367.

[253] F. S. De Cristo, W. M. Shbair, L. Trestioreanu, R. State, and A. Malhotra, "Self-sovereign identity for the financial sector: A case study of PayString service," in *Proc. IEEE Int. Conf. Blockchain (Blockchain)*, Melbourne, VIC, Australia, Dec. 2021, pp. 213–220, doi: 10.1109/Blockchain53845.2021.00036.

[254] M. Mukhandi, E. Andrade, F. Damião, J. Granjal, and J. P. Vilela, "Blockchain-based scalable authentication for IoT: Poster abstract," in *Proc. 18th Conf. Embedded Networked Sensor Syst.*, Nov. 2020, pp. 667–668, doi: 10.1145/3384419.3430465.

[255] M. Mukhandi, "Decentralised and scalable security for IoT devices," in *Proc. 19th ACM Conf. Embedded Networked Sensor Syst.*, Coimbra, Portugal, Nov. 2021, pp. 411–412, doi: 10.1145/3485730.3492901.

[256] M. T. A. Ahmed, F. Hashim, S. J. Hashim, and A. Abdullah, "Hierarchical blockchain structure for node authentication in IoT networks," *Egyptian Informat. J.*, vol. 23, no. 2, pp. 345–361, Jul. 2022, doi: 10.1016/j.eij.2022.02.005.

[257] J.-C. Huang, M.-H. Shu, B.-M. Hsu, and C.-M. Hu, "Service architecture of IoT terminal connection based on blockchain identity authentication system," *Comput. Commun.*, vol. 160, pp. 411–422, Jul. 2020, doi: 10.1016/j.comcom.2020.06.027.

[258] Y. Guo, X. Chen, S. Tian, Le Yang, X. Liang, J. Lian, D. Jin, A. Balabontsev, and Z. Zhang., "Blockchain based trusted identity authentication in ubiquitous power Internet of Things," in *Intelligent Computing Theories and Application*, vol. 12837, D.-S. Huang, K.-H. Jo, J. Li, V. Gribova, and A. Hussain, Eds. Cham, Switzerland: Springer, 2021, pp. 294–302, doi: 10.1007/978-3-030-84529-2_25.

[259] A. Giaretta, S. Pepe, and N. Dragoni, "UniquID: A quest to reconcile identity access management and the IoT," in *Software Technology: Methods and Tools*, vol. 11771, M. Mazzara, J.-M. Bruel, B. Meyer, and A. Petrenko, Eds. Cham, Switzerland: Springer, 2019, pp. 237–251, doi: 10.1007/978-3-030-29852-4_20.

[260] 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)*, New Orleans, LA, USA, Jun. 2020, pp. 1–6, doi: 10.1109/WF-IoT48130.2020.9221144.

[261] M. Mukhandi, F. Damiao, J. Granjal, and J. P. Vilela, "Blockchain-based device identity management with consensus authentication for IoT devices," in *Proc. IEEE 19th Annu. Consum. Commun. Netw. Conf. (CCNC)*, Las Vegas, NV, USA, Jan. 2022, pp. 433–436, doi: 10.1109/CCNC49033.2022.9700534.

[262] N. M. Ahmad, S. F. A. Razak, S. Kannan, I. Yusof, and A. H. M. Amin, "Improving identity management of cloud-based IoT applications using blockchain," in *Proc. Int. Conf. Intell. Adv. Syst. (ICIAS)*, Aug. 2018, pp. 1–6, doi: 10.1109/ICIAS.2018.8540564.

[263] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *Proc. Global Internet Things Summit (GIoTS)*, Geneva, Switzerland, Jun. 2017, pp. 1–6, doi: 10.1109/GIOTS.2017.8016280.

[264] M. Simic, M. Vucetic, T. Unkasevic, Z. Banjac, and M. Stankovic, "Entity identification and security solutions in IoT based on PKI and blockchain technology," in *Proc. 19th Int. Symp. INFOTEH-JAHORINA (INFOTEH)*, Mar. 2020, pp. 1–6, doi: 10.1109/INFOTEH48170.2020.9066282.

[265] S. Sun, R. Du, S. Chen, and W. Li, "Blockchain-based IoT access control system: Towards security, lightweight, and cross-domain," *IEEE Access*, vol. 9, pp. 36868–36878, 2021, doi: 10.1109/ACCESS.2021.3059863.

[266] 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)*, Sydney, NSW, USA, Nov. 2020, pp. 485–490, doi: 10.1109/LCN48667.2020.9314816.

[267] S. Terzi, A. Zacharaki, A. Nizamis, K. Votis, D. Ioannidis, D. Tzovaras, and I. Stamelos, "Transforming the supply-chain management and industry logistics with blockchain smart contracts," in *Proc. 23rd Pan-Hellenic Conf. Informat.*, Nicosia, Cyprus, Nov. 2019, pp. 9–14, doi: 10.1145/3368640.3368655.

[268] 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)*, Montreal, QC, Canada, Aug. 2020, pp. 1–5, doi: 10.1109/PESGM41954.2020.9281929.

[269] S. Terzi, C. Savvaidis, A. Sersemis, K. Votis, and D. Tzovaras, "Decentralizing identity management and vehicle rights delegation through self-sovereign identities and blockchain," in *Proc. IEEE 45th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Madrid, Spain, Jul. 2021, pp. 1217–1223, doi: 10.1109/COMPSAC51774.2021.00168.

[270] A. H. M. Amin, N. Abdelmajid, and F. N. Kiwanuka, "Identity-of-things model using composite identity on permissioned blockchain network," in *Proc. 7th Int. Conf. Softw. Defined Syst. (SDS)*, Paris, France, Apr. 2020, pp. 171–176, doi: 10.1109/SDS49854.2020.9143887.

[271] Y. Zhou, Q. Liu, M. Liu, Y. Wang, and C. Ren, "Research on blockchain-based identity verification between IoV entities," in *Proc. Int. Conf. High Perform. Big Data Intell. Syst.*, Shenzhen, China, May 2020, pp. 1–6, doi: 10.1109/HPBDIS49115.2020.9130597.

[272] M. L. Alessandria and A. Vizzarri, "Self-sovereign identity and blockchain applications for the automotive sector," in *Proc. AEIT Int. Conf. Electr. Electron. Technol. Automot.*, Nov. 2021, pp. 1–6, doi: 10.23919/AEITAUTOMOTIVE52815.2021.9662861.

[273] J. G. Faísca and J. Q. Rogado, "Decentralized semantic identity," in *Proc. 12th Int. Conf. Semantic Syst.*, Leipzig, Germany, Sep. 2016, pp. 177–180, doi: 10.1145/2993318.2993348.

[274] A. G. Abbasi and Z. Khan, "VeidBlock: Verifiable identity using blockchain and ledger in a software defined network," in *Proc. 10th Int. Conf. Utility Cloud Comput.*, Austin, TX, USA, Dec. 2017, pp. 173–179, doi: 10.1145/3147234.3148088.

[275] A. B. Chavan and K. Rajeswari, "Design and development of self-sovereign identity using Ethereum blockchain," in *Sustainable Communication Networks and Application*, vol. 39, P. Karrupusamy, J. Chen, and Y. Shi, Eds. Cham, Switzerland: Springer, 2020, pp. 523–531, doi: 10.1007/978-3-030-34515-0_55.

[276] T. Rathee and P. Singh, "A self-sovereign identity management system using blockchain," in *Cyber Security and Digital Forensics*, vol. 73, K. Khanna, V. V. Estrela, and J. J. P. C. Rodrigues, Eds. Singapore: Springer, 2022, pp. 371–379, doi: 10.1007/978-981-16-3961-6_31.

[277] E. S. Sin and T. T. Naing, "Digital identity management system using blockchain technology," in *Proc. Int. Conf. Innov. Comput. Commun.*, vol. 1166, D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, and A. Jaiswal, Eds. Singapore: Springer, 2021, pp. 895–906, doi: 10.1007/978-981-15-5148-2_78.

[278] T. Rathee and P. Singh, "Secure data sharing using Merkle hash digest based blockchain identity management," *Peer-Peer Netw. Appl.*, vol. 14, no. 6, pp. 3851–3864, Nov. 2021, doi: 10.1007/s12083-021-01212-4.

[279] F. Angiulli, F. Fassetti, A. Furfaro, A. Piccolo, and D. Saccà, "Achieving service accountability through blockchain and digital identity," in *Information Systems in the Big Data Era*, vol. 317, J. Mendling and H. Mouratidis, Eds. Cham, Switzerland: Springer, 2018, pp. 16–23, doi: 10.1007/978-3-319-92901-9_2.

[280] J. Wang, S. Wei, and H. Liu, "Decentralized identity authentication with trust distributed in blockchain backbone," in *Blockchain—ICBC 2019*, vol. 11521, J. Joshi, S. Nepal, Q. Zhang, and L.-J. Zhang, Eds. Cham, Switzerland: Springer, 2019, pp. 202–210, doi: 10.1007/978-3-030-23404-1_14.

[281] F. Buccafurri, G. Lax, A. Russo, and G. Zunino, "Integrating digital identity and blockchain," in *Proc. Move Meaningful Internet Syst. Conf.*, vol. 11229, H. Panetto, C. Debruyne, H. A. Proper, C. A. Ardagna, D. Roman, and R. Meersman, Eds. Cham, Switzerland: Springer, 2018, pp. 568–585, doi: 10.1007/978-3-030-02610-3_32.

[282] A. M. Thomas, R. Ramaguru, and M. Sethumadhavan, "Distributed identity and verifiable claims using Ethereum standards," in *Inventive Communication and Computational Technologies*, vol. 311, G. Ranganathan, X. Fernando, and F. Shi, Eds. Singapore: Springer, 2022, pp. 621–636, doi: 10.1007/978-981-16-5529-6_48.

[283] A.-E. Panait and R. F. Olimid, "On using zk-SNARKs and zk-STARKs in blockchain-based identity management," in *Innovative Security Solutions for Information Technology and Communications*, vol. 12596, D. Maimut, A.-G. Oprina, and D. Sauveron, Eds. Cham, Switzerland: Springer, 2021, pp. 130–145, doi: 10.1007/978-3-030-69255-1_9.

[284] S. Azouvi, M. Al-Bassam, and S. Meiklejohn, "Who am I? Secure identity registration on distributed ledgers," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, vol. 10436, J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, Eds. Cham, Switzerland: Springer, 2017, pp. 373–389, doi: 10.1007/978-3-319-67816-0_21.

[285] E. Bandara, X. Liang, P. Foytik, S. Shetty, and K. D. Zoysa, "A blockchain and self-sovereign identity empowered digital identity platform," in *Proc. Int. Conf. Comput. Commun. Netw. (ICCCN)*, Athens, Greece, Jul. 2021, pp. 1–7, doi: 10.1109/ICCCN52240.2021.9522184.

[286] 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)*, Halifax, NS, Canada, Jul. 2018, pp. 1475–1482, doi: 10.1109/Cybermatics_2018.2018.00250.

[287] Q. Stokkink, G. Ishmaev, D. Epema, and J. Pouwelse, "A truly self-sovereign identity system," in *Proc. IEEE 46th Conf. Local Comput. Netw. (LCN)*, Edmonton, AB, Canada, Oct. 2021, pp. 1–8, doi: 10.1109/LCN52139.2021.9525011.

[288] 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)*, Montreal, QC, Canada, Oct. 2020, pp. 1–7, doi: 10.1109/ISNCC49221.2020.9297357.

[289] R. Chen, F. Shu, S. Huang, L. Huang, H. Liu, J. Liu, and K. Lei, "BIdM: A blockchain-enabled cross-domain identity management system," *J. Commun. Inf. Netw.*, vol. 6, no. 1, pp. 44–58, Mar. 2021, doi: 10.23919/JCIN.2021.9387704.

[290] D. N. Kirupanithi and A. Antonidoss, "Self-sovereign identity management system on blockchain based applications using chameleon hash," in *Proc. 2nd Int. Conf. Smart Electron. Commun. (ICOSEC)*, Trichy, India, Oct. 2021, pp. 386–390, doi: 10.1109/ICOSEC51865.2021.9591734.

[291] L. Zeng, W. Qiu, X. Wang, H. Wang, Y. Yao, and D. He, "A persistent data structure for managing digital identity data implemented on the blockchain," in *Proc. IEEE Int. Conf. Power, Intell. Comput. Syst. (ICPICS)*, Shenyang, China, Jul. 2021, pp. 226–230, doi: 10.1109/ICPICS52425.2021.9524162.

[292] V. Lemieux, A. Voskobojnikov, and M. Kang, "Addressing audit and accountability issues in self-sovereign identity blockchain systems using archival science principles," in *Proc. IEEE 45th Annu. Comput., Softw., Appl. Conf. (COMPSAC)*, Madrid, Spain, Jul. 2021, pp. 1210–1216, doi: 10.1109/COMPSAC51774.2021.00167.

[293] H. Siddiqui, M. Idrees, I. Gudymenko, D. L. Quoc, and C. Fetzer, "Credentials as a service providing self sovereign identity as a cloud service using trusted execution environments," in *Proc. IEEE Int. Conf. Cloud Eng. (IC2E)*, San Francisco, CA, USA, Oct. 2021, pp. 210–216, doi: 10.1109/IC2E52221.2021.00036.

[294] X. Ren, F. Lin, Z. Chen, C. Tang, Z. Zheng, and M. Li, "BIA: A blockchain-based identity authorization mechanism," in *Proc. 16th Int. Conf. Mobility, Sens. Netw. (MSN)*, Tokyo, Japan, Dec. 2020, pp. 98–105, doi: 10.1109/MSN50589.2020.00031.

[295] S. Choudhari, S. K. Das, and S. Parasher, "Interoperable blockchain solution for digital identity management," in *Proc. 6th Int. Conf. Converg. Technol. (I2CT)*, Maharashtra, India, Apr. 2021, pp. 1–6, doi: 10.1109/I2CT51068.2021.9418220.

[296] 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)*, New York, NY, USA, Aug. 2018, pp. 1406–1412, doi: 10.1109/TrustCom/BigDataSE.2018.00195.

[297] K. Inoue, D. Suzuki, T. Kurita, and S. Imai, "Cooperative task scheduling for personal identity verification in networked systems," in *Proc. 32nd Int. Teletraffic Congr.*, Osaka, Japan, Sep. 2020, pp. 97–105, doi: 10.1109/ITC3249928.2020.00020.

[298] 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)*, Shah Alam, Malaysia, Oct. 2019, pp. 253–257, doi: 10.1109/ICSEngT.2019.8906403.

[299] R. Soltani, U. T. Nguyen, and A. An, "Decentralized and privacy-preserving key management model," in *Proc. Int. Symp. Netw., Comput. Commun. (ISNCC)*, Montreal, QC, Canada, Oct. 2020, pp. 1–7, doi: 10.1109/ISNCC49221.2020.9297294.

[300] K. Dissanayake, P. Somarathne, U. Fernando, D. Pathmasiri, C. Liyanapathirana, and D. L. Rupasinghe, "'Trust Pass'—Blockchain-based trusted digital identity platform towards digital transformation," in *Proc. 2nd Int. Informat. Softw. Eng. Conf. (IISEC)*, Ankara, Turkey, Dec. 2021, pp. 1–6, doi: 10.1109/IISEC54230.2021.9672336.

[301] 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)*, Paris, France, Sep. 2020, pp. 71–78, doi: 10.1109/BRAINS49436.2020.9223292.

[302] B. N. Biswas, S. D. Bhitkar, and S. N. Pundkar, "Secure login: A blockchain based web application for identity access management system," in *Proc. 2nd Int. Conf. Emerg. Technol. (INCET)*, Belagavi, India, May 2021, pp. 1–5, doi: 10.1109/INCET51464.2021.9456352.

[303] A. B. Jacob, P. Prakash, P. Karhana, and P. Swain, "ChainAccess: Blockchain based web-access through biometrics," in *Proc. 12th Int. Conf. Comput. Commun. Netw. Technol. (ICCCNT)*, Kharagpur, India, Jul. 2021, pp. 1–6, doi: 10.1109/ICCCNT51525.2021.9579481.

[304] 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.*, New York, NY, USA, Aug. 2018, pp. 37–42, doi: 10.1109/TrustCom/BigDataSE.2018.00016.

[305] P. Boontaetae, A. Sangpetch, and O. Sangpetch, "RDI: Real digital identity based on decentralized PKI," in *Proc. 22nd Int. Comput. Sci. Eng. Conf. (ICSEC)*, Chiang Mai, Thailand, Nov. 2018, pp. 1–6, doi: 10.1109/ICSEC.2018.8712663.

[306] 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)*, Calgary, AB, Canada, Aug. 2017, pp. 4409–4444, doi: 10.1109/PST.2017.00016.

[307] J. Blue, J. Condell, T. Lunney, and E. Furey, "Bayesi-chain: Intelligent identity authentication," in *Proc. 29th Irish Signals Syst. Conf. (ISSC)*, Jun. 2018, pp. 1–6, doi: 10.1109/ISSC.2018.8585369.

[308] N. Sundareswaran, S. Sasirekha, I. J. Louis Paul, S. Balakrishnan, and G. Swaminathan, "Optimised KYC blockchain system," in *Proc. Int. Conf. Innov. Trends Inf. Technol. (ICITIIT)*, Kottayam, India, Feb. 2020, pp. 1–6, doi: 10.1109/ICITIIT49094.2020.9071533.

[309] C. Rao and Z. Lin, "VAPKI: A blockchain-based identification system with validation and authentication," in *Proc. 7th Int. Conf. Comput. Commun. (ICCC)*, Chengdu, China, Dec. 2021, pp. 1551–1556, doi: 10.1109/ICCC54389.2021.9674554.

[310] K. Wittek, L. Lazzati, D. Bothe, A.-J. 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)*, Dortmund, Germany, Mar. 2020, pp. 1–5, doi: 10.1109/E-TEMS46250.2020.9111805.

[311] S. K. Radha, I. Taylor, J. Nabrzyski, and I. Barclay, "Verifiable badging system for scientific data reproducibility," *Blockchain, Res. Appl.*, vol. 2, no. 2, Jun. 2021, Art. no. 100015, doi: 10.1016/j.bcra.2021.100015.

[312] F. Schardong, R. Custódio, L. Pioli, and J. Meyer, "Matching metadata on blockchain for self-sovereign identity," in *Proc. Bus. Process Manage. Workshops*, vol. 436, A. Marrella and B. Weber, Eds. Cham, Switzerland: Springer, 2022, pp. 421–433, doi: 10.1007/978-3-030-94343-1_32.

[313] J. Li, Q. He, R. Liang, and B. Jiang, "Smart tourism identity authentication service based on blockchain and decentralized identifier," in *Blockchain and Trustworthy Systems*, vol. 1490, H.-N. Dai, X. Liu, D. X. Luo, J. Xiao, and X. Chen, Eds. Singapore: Springer, 2021, pp. 545–558, doi: 10.1007/978-981-16-7993-3_42.

[314] J. N. Benedict, S. Udhayakumar, B. R. Vikram, and C. Vignesh, "Identity management using blockchain network for fail-safe e-governance," in *Advances in Smart System Technologies*, vol. 1163, P. Suresh, U. Saravanakumar, and M. S. H. A. Salameh, Eds. Singapore: Springer, 2021, pp. 747–757, doi: 10.1007/978-981-15-5029-4_63.

[315] M. G. Aruna, M. K. Hasan, S. Islam, K. G. Mohan, P. Sharan, and R. Hassan, "Cloud to cloud data migration using self sovereign identity for 5G and beyond," *Cluster Comput.*, vol. 25, no. 4, pp. 2317–2331, Aug. 2022, doi: 10.1007/s10586-021-03461-7.

[316] S. M. M. Alam, M. A. A. Mamun, M. S. Hossain, and M. Samiruzzaman, "A novel approach to manage ownership and VAT using blockchain-based digital identity," in *Ubiquitous Networking*, vol. 12845, H. Elbiaze, E. Sabir, F. Falcone, M. Sadik, S. Lasaulce, and J. B. Othman, Eds. Cham, Switzerland: Springer, 2021, pp. 255–268, doi: 10.1007/978-3-030-86356-2_21.

[317] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, and J. S. Deogun, "Identity management using blockchain for cognitive cellular networks," in *Proc. IEEE Int. Conf. Commun. (ICC)*, Paris, France, May 2017, pp. 1–6, doi: 10.1109/ICC.2017.7996830.

[318] N.-C. Ursache, "Swarm communication using self sovereign identities," in *Proc. 20th RoEduNet Conf., Netw. Educ. Res. (RoEduNet)*, Iasi, Romania, Nov. 2021, pp. 1–6, doi: 10.1109/RoEduNet54112.2021.9638293.
[319] J.-H. Lee, "BIDaaS: Blockchain based ID as a service," *IEEE Access*, vol. 6, pp. 2274–2278, 2017, doi: 10.1109/ACCESS.2017.2782733.
[320] U. Korkmaz, H. I. Altunlu, A. Ozkan, and E. Karaarslan, "Sustainable member motivation system proposal for NGOs: NGO-TR," in *Proc. 1st Int. Informat. Softw. Eng. Conf. (UBMYK)*, Ankara, Turkey, Nov. 2019, pp. 1–5, doi: 10.1109/UBMYK48245.2019.8965505.
[321] 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)*, Edmonton, AB, Canada, May 2019, pp. 1–5, doi: 10.1109/CCECE.2019.8861955.
[322] N. Naik and P. Jenkins, "Your identity is yours: Take back control of your identity using GDPR compatible self-sovereign identity," in *Proc. 7th Int. Conf. Behavioural Social Comput. (BESC)*, Bournemouth, U.K., Nov. 2020, pp. 1–6, doi: 10.1109/BESC51023.2020.9348298.
[323] D. N. Kirupanithi and A. Antonidoss, "Self-sovereign identity creation on blockchain using identity based encryption," in *Proc. 5th Int. Conf. Intell. Comput. Control Syst. (ICICCS)*, Madurai, India, May 2021, pp. 299–304, doi: 10.1109/ICICCS51141.2021.9432099.
[324] 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, doi: 10.1109/MobileCloud48802.2020.00021.
[325] S. E. Haddouti and M. D. E.-C. E. Kettani, "Analysis of identity management systems using blockchain technology," in *Proc. Int. Conf. Adv. Commun. Technol. Netw. (CommNet)*, Rabat, Morocco, Apr. 2019, pp. 1–7, doi: 10.1109/COMMNET.2019.8742375.
[326] B. Alzahrani, "An information-centric networking based registry for decentralized identifiers and verifiable credentials," *IEEE Access*, vol. 8, pp. 137198–137208, 2020, doi: 10.1109/ACCESS.2020.3011656.
[327] A.-E. Drăgnoiu, "Using blockchain technology for software identity maintenance," in *Proc. 22nd Int. Middleware Conf., Doctoral Symp.*, Dec. 2021, pp. 25–28, doi: 10.1145/3491087.3493682.
[328] N. Naik, P. Grace, and P. Jenkins, "An attack tree based risk analysis method for investigating attacks and facilitating their mitigations in self-sovereign identity," in *Proc. IEEE Symp. Ser. Comput. Intell. (SSCI)*, Orlando, FL, USA, Dec. 2021, pp. 1–8, doi: 10.1109/SSCI50451.2021.9659929.
[329] Z. Tu, H. Zhou, K. Li, H. Song, and W. Wang, "A blockchain-based user identity authentication method for 5G," in *Mobile Internet Security*, vol. 1544, I. You, H. Kim, T.-Y. Youn, F. Palmieri, and I. Kotenko, Eds. Singapore: Springer, 2022, pp. 335–351, doi: 10.1007/978-981-16-9576-6_23.
[330] 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.
[331] 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)*, Paris, France, Sep. 2020, pp. 59–60, doi: 10.1109/BRAINS49436.2020.9223309.
[332] N. Kulabukhova, A. Ivashchenko, I. Tipikin, and I. Minin, "Self-sovereign identity for IoT devices," in *Computational Science and Its Applications—ICCSA 2019*, vol. 11620, S. Misra, O. Gervasi, B. Murgante, E. Stankova, V. Korkhov, C. Torre, A. M. A. C. Rocha, D. Taniar, B. O. Apduhan, and E. Tarantino, Eds. Cham, Switzerland: Springer, 2019, pp. 472–484, doi: 10.1007/978-3-030-24296-1_37.
[333] 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)*, Halifax, NS, Canada, Jul. 2018, pp. 1568–1573, doi: 10.1109/Cybermatics_2018.2018.00263.
[334] G. Fedrecheski, J. M. Rabaey, L. C. P. Costa, P. C. C. Ccori, W. T. Pereira, and M. K. Zuffo, "Self-sovereign identity for IoT environments: A perspective," in *Proc. Global Internet Things Summit (GIoTS)*, Dublin, Ireland, Jun. 2020, pp. 1–6, doi: 10.1109/GIOTS49054.2020.9119664.
[335] S. M. Rajesh, S. Pattar, R. Prabha, and S. H. Manjula, "An overview of blockchain technology for identity and access management in the IoT ecosystem," in *Proc. 14th Int. Conf. Commun. Syst. Netw. (COMSNETS)*, Bengaluru, India, Jan. 2022, pp. 1–6, doi: 10.1109/COMSNETS53615.2022.9668412.
[336] R. P. Sukumaran and S. Benedict, "Survey on blockchain enabled authentication for industrial Internet of Things," in *Proc. 5th Int. Conf. I-SMAC*, Palladam, India, Nov. 2021, pp. 1510–1516, doi: 10.1109/I-SMAC52330.2021.9640973.
[337] I. Butun and P. Osterberg, "A review of distributed access control for blockchain systems towards securing the Internet of Things," *IEEE Access*, vol. 9, pp. 5428–5441, 2021, doi: 10.1109/ACCESS.2020.3047902.
[338] G. Kondova and J. Erbguth, "Self-sovereign identity on public blockchains and the GDPR," in *Proc. 35th Annu. ACM Symp. Appl. Comput.*, Mar. 2020, pp. 342–345, doi: 10.1145/3341105.3374066.
[339] M. Alharbi and F. K. Hussain, "A systematic literature review of blockchain technology for identity management," in *Advanced Information Networking and Applications*, vol. 451, L. Barolli, F. Hussain, and T. Enokido, Eds. Cham, Switzerland: Springer, 2022, pp. 345–359, doi: 10.1007/978-3-030-99619-2_33.
[340] A. Giannopoulou, "Data protection compliance challenges for self-sovereign identity," in *Blockchain and Applications*, vol. 1238, J. Prieto, A. Pinto, A. K. Das, and S. Ferretti, Eds. Cham, Switzerland: Springer, 2020, pp. 91–100, doi: 10.1007/978-3-030-52535-4_10.
[341] M. Alharbi and F. K. Hussain, "Blockchain-based identity management for personal data: A survey," in *Advances on Broad-Band Wireless Computing, Communication and Applications*, vol. 346, L. Barolli, Ed. Cham, Switzerland: Springer, 2022, pp. 167–178, doi: 10.1007/978-3-030-90072-4_17.
[342] X. Yang and J. Chan, "Blockchain and identity management," in *Context-Aware Systems and Applications*, vol. 409, P. C. Vinh and A. Rakib, Eds. Cham, Switzerland: Springer, 2021, pp. 192–204, doi: 10.1007/978-3-030-93179-7_15.
[343] S. Ghesmati, W. Fdhila, and E. Weippl, "Studying Bitcoin privacy attacks and their impact on Bitcoin-based identity methods," in *Business Process Management: Blockchain and Robotic Process Automation Forum*, vol. 428, J. González Enríquez, S. Debois, P. Fettke, P. Plebani, I. van de Weerd, and I. Weber, Eds. Cham, Switzerland: Springer, 2021, pp. 85–101, doi: 10.1007/978-3-030-85867-4_7.
[344] A. Grüner, A. Mühle, M. Meinig, and C. Meinel, "A taxonomy of trust models for attribute assurance in identity management," in *Web, Artificial Intelligence and Network Applications*, vol. 1150, L. Barolli, F. Amato, F. Moscato, T. Enokido, and M. Takizawa, Eds. Cham, Switzerland: Springer, 2020, pp. 65–76, doi: 10.1007/978-3-030-44038-1_7.
[345] W. Fdhila, N. Stifter, K. Kostal, C. Saglam, and M. Sabadello, "Methods for decentralized identities: Evaluation and insights," in *Business Process Management: Blockchain and Robotic Process Automation Forum*, vol. 428, J. G. Enríquez, S. Debois, P. Fettke, P. Plebani, I. van de Weerd, and I. Weber, Eds. Cham, Switzerland: Springer, 2021, pp. 119–135, doi: 10.1007/978-3-030-85867-4_9.
[346] 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)*, Vienna, Austria, Oct. 2020, pp. 1–7, doi: 10.1109/ISSE49799.2020.9272223.
[347] 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)*, Vienna, Austria, Oct. 2020, pp. 1–6, doi: 10.1109/ISSE49799.2020.9272212.
[348] N. Naik and P. Jenkins, "Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system based on distributed ledger technology," in *Proc. IEEE Int. Symp. Syst. Eng. (ISSE)*, Vienna, Austria, Sep. 2021, pp. 1–7, doi: 10.1109/ISSE51541.2021.9582551.
[349] N. Naik and P. Jenkins, "Does Sovrin network offer sovereign identity?" in *Proc. IEEE Int. Symp. Syst. Eng. (ISSE)*, Vienna, Austria, Sep. 2021, pp. 1–6, doi: 10.1109/ISSE51541.2021.9582472.
[350] 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)*, Paris, France, Sep. 2020, pp. 92–96, doi: 10.1109/BRAINS49436.2020.9223281.
[351] H. Nusantoro, R. Supriati, N. Azizah, N. P. L. Santoso, and S. Maulana, "Blockchain based authentication for identity management," in *Proc. 9th Int. Conf. Cyber IT Service Manage. (CITSM)*, Bengkulu, Indonesia, Sep. 2021, pp. 1–8, doi: 10.1109/CITSM52892.2021.9589001.
[352] Y. Fukami, T. Shimizu, and H. Matsushima, "The impact of decentralized identity architecture on data exchange," in *Proc. IEEE Int. Conf. Big Data (Big Data)*, Orlando, FL, USA, Dec. 2021, pp. 3461–3465, doi: 10.1109/BigData52589.2021.9671674.

[353] 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.

[354] R. N. Zaeem and K. S. Barber, "How much identity management with blockchain would have saved us? A longitudinal study of identity theft," in *Proc. Bus. Inf. Syst. Workshops*, vol. 394, W. Abramowicz and G. Klein, Eds. Cham, Switzerland: Springer, 2020, pp. 158–168, doi: 10.1007/978-3-030-61146-0_13.

[355] A.-E. Panait, R. F. Olimid, and A. Stefanescu, "Analysis of uPort open, an identity management blockchain-based solution," in *Trust, Privacy and Security in Digital Business*, vol. 12395, S. Gritzalis, E. R. Weippl, G. Kotsis, A. M. Tjoa, and I. Khalil, Eds. Cham, Switzerland: Springer, 2020, pp. 3–13, doi: 10.1007/978-3-030-58986-8_1.

[356] N. Kulabukhova, "Self-sovereign identity as trusted root in knowledge based systems," in *Computational Science and Its Applications—ICCSA 2020*, vol. 12251, O. Gervasi, B. Murgante, S. Misra, C. Garau, I. Blečić, D. Taniar, B. O. Apduhan, A. M. A. C. Rocha, E. Tarantino, C. M. Torre, and Y. Karaca, Eds. Cham, Switzerland: Springer, 2020, pp. 14–24, doi: 10.1007/978-3-030-58808-3_2.

[357] O. Mounnan, A. A. E. Kalam, and L. E. Haourani, "Decentralized access control infrastructure using blockchain for big data," in *Proc. IEEE/ACS 16th Int. Conf. Comput. Syst. Appl. (AICCSA)*, Abu Dhabi, United Arab Emirates, Nov. 2019, pp. 1–8, doi: 10.1109/AICCSA47632.2019.9035221.

[358] 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)*, Rhodes Island, Greece, Nov. 2020, pp. 462–469, doi: 10.1109/Blockchain50366.2020.00067.

[359] H. Wang, Y. Yuan, and F. Yang, "A personal data determination method based on blockchain technology and smart contract," in *Proc. 4th Int. Conf. Cryptogr., Secur. Privacy*, Nanjing China, Jan. 2020, pp. 89–94, doi: 10.1145/3377644.3377656.

[360] A. Gruner, A. Muhle, and C. Meinel, "ATIB: Design and evaluation of an architecture for brokered self-sovereign identity integration and trust-enhancing attribute aggregation for service provider," *IEEE Access*, vol. 9, pp. 138553–138570, 2021, doi: 10.1109/ACCESS.2021.3116095.

[361] E. Bandara, X. Liang, P. Foytik, and S. Shetty, "Blockchain and self-sovereign identity empowered cyber threat information sharing platform," in *Proc. IEEE Int. Conf. Smart Comput. (SMARTCOMP)*, Irvine, CA, USA, Aug. 2021, pp. 258–263, doi: 10.1109/SMARTCOMP52413.2021.00057.

[362] B. Kim, W. Shin, D.-Y. Hwang, and K.-H. Kim, "Attribute-based access control (ABAC) with decentralized identifier in the blockchain-based energy transaction platform," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jan. 2021, pp. 845–848, doi: 10.1109/ICOIN50884.2021.9333894.

[363] D. A. Filvà, F. J. García-Peñalvo, M. A. Forment, D. F. Escudero, and M. J. Casañ, "Privacy and identity management in learning analytics processes with blockchain," in *Proc. 6th Int. Conf. Technol. Ecosyst. Enhancing Multiculturality*, Salamanca, Spain, Oct. 2018, pp. 997–1003, doi: 10.1145/3284179.3284354.

[364] R. Seifert, "Digital identities—Self-sovereignty and blockchain are the keys to success," *Netw. Secur.*, vol. 2020, no. 11, pp. 17–19, Nov. 2020, doi: 10.1016/S1353-4858(20)30131-8.

[365] A. Abraham, K. Koch, S. More, S. Ramacher, and M. Stopar, "Privacy-preserving eID derivation to self-sovereign identity systems with offline revocation," in *Proc. IEEE 20th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Shenyang, China, Oct. 2021, pp. 506–513, doi: 10.1109/TrustCom53373.2021.00080.

[366] 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.

[367] M. Shuaib, S. Alam, M. Shahnawaz Nasir, and M. S. Alam, "Immunity credentials using self-sovereign identity for combating COVID-19 pandemic," *Mater. Today, Proc.*, vol. 2021, Mar. 2021, Art. no. S2214785321021155, doi: 10.1016/j.matpr.2021.03.096.

[368] Y. Jing, X. You, D. Bi, and H. Li, "The decentralized identity and its application for industrial internet," in *Proc. 3rd Int. Academic Exchange Conf. Sci. Technol. Innov. (IAECST)*, Guangzhou, China, Dec. 2021, pp. 671–674, doi: 10.1109/IAECST54258.2021.9695674.

[369] J. Xingzhong, X. Qingshui, M. Haifeng, C. Jiageng, and Z. Haozhi, "The research on identity authentication scheme of Internet of Things equipment in 5G network environment," in *Proc. IEEE 19th Int. Conf. Commun. Technol. (ICCT)*, Xi'an, China, Oct. 2019, pp. 312–316, doi: 10.1109/ICCT46805.2019.8947126.

[370] Y. Kurihara, "Self-sovereign identity and blockchain-based content management," in *Human-Centric Computing in a Data-Driven Society*, vol. 590, D. Kreps, T. Komukai, T. V. Gopal, and K. Ishii, Eds. Cham, Switzerland: Springer, 2020, pp. 130–140, doi: 10.1007/978-3-030-62803-1_11.

[371] G. Ishmaev, "Sovereignty, privacy, and ethics in blockchain-based identity management systems," *Ethics Inf. Technol.*, vol. 23, no. 3, pp. 239–252, Sep. 2021, doi: 10.1007/s10676-020-09563-x.

[372] R. S. Malyan and A. K. Madan, "Blockchain technology as a tool to manage digital identity: A conceptual study," in *Advances in Manufacturing and Industrial Engineering*, R. M. Singari, K. Mathiyazhagan, and H. Kumar, Eds. Singapore: Springer, 2021, pp. 635–647, doi: 10.1007/978-981-15-8542-5_55.

[373] A.-E. Panait, "Is the user identity perception influenced by the blockchain technology?" in *Proc. IEEE Int. Conf. Intell. Secur. Informat. (ISI)*, Arlington, VA, USA, Nov. 2020, pp. 1–3, doi: 10.1109/ISI49825.2020.9280530.

[374] A. Gruner, A. Muhle, and C. Meinel, "Analyzing interoperability and portability concepts for self-sovereign identity," in *Proc. IEEE 20th Int. Conf. Trust, Secur. Privacy Comput. Commun. (TrustCom)*, Shenyang, China, Oct. 2021, pp. 587–597, doi: 10.1109/TrustCom53373.2021.00089.

[375] K. Schmidt, A. Muhle, A. Gruner, and C. Meinel, "Clear the fog: Towards a taxonomy of self-sovereign identity ecosystem members," in *Proc. 18th Int. Conf. Privacy, Secur. Trust (PST)*, Auckland, New Zealand, Dec. 2021, pp. 1–7, doi: 10.1109/PST52912.2021.9647797.

[376] D. A. Torres, "Tutorial: Decentralized digital identity with blockchain," in *Proc. 8th Int. Conf. eDemocracy eGovernment (ICEDEG)*, Quito, Ecuador, Jul. 2021, p. 12, doi: 10.1109/ICEDEG52154.2021.9530967.

[377] G. Abdourahime and D. Mall, "Analysis of authentication mechanisms and identity management in IoT: The resource constraints and security needs," in *Proc. Int. Conf. Inf. Syst. Adv. Technol. (ICISAT)*, Tebessa, Algeria, Dec. 2021, pp. 1–6, doi: 10.1109/ICISAT54145.2021.9678456.

[378] Y. Jing, J. Li, Y. Wang, and H. Li, "The introduction of digital identity evolution and the industry of decentralized identity," in *Proc. 3rd Int. Academic Exchange Conf. Sci. Technol. Innov. (IAECST)*, Guangzhou, China, Dec. 2021, pp. 504–508, doi: 10.1109/IAECST54258.2021.9695553.

[379] Q. Yang and X. Zhu, "Research on smart party building identity online based on blockchain," in *Proc. Int. Conf. Cyberspace Innov. Adv. Technol.*, Guangzhou China, Dec. 2020, pp. 425–430, doi: 10.1145/3444370.3444608.

[380] R. Rivera, J. G. Robledo, V. M. Larios, and J. M. Avalos, "How digital identity on blockchain can contribute in a smart city environment," in *Proc. Int. Smart Cities Conf. (ISC2)*, Sep. 2017, pp. 1–4, doi: 10.1109/ISC2.2017.8090839.

[381] J. Isohanni, L. Goulden, K. M. Hermsen, M. Ross, and J. Vanbockryck, "Disposable identities; enabling trust-by-design to build more sustainable data driven value," in *Proc. IEEE Int. Conf. Cyber Secur. Resilience (CSR)*, Rhodes, Greece, Jul. 2021, pp. 378–383, doi: 10.1109/CSR51186.2021.9527950.

[382] A. Kupper, "Decentralized identifiers and self-sovereign identity—A new identity management for 6G integration? MobileCloud 2021 invited talk," in *Proc. IEEE Int. Conf. Joint Cloud Comput. (JCC)*, Oxford, U.K., Aug. 2021, p. 71, doi: 10.1109/JCC53141.2021.00023.

[383] P. Gururaj, "Identity management using permissioned blockchain," in *Proc. Int. Conf. Mainstreaming Block Chain Implement. (ICOMBI)*, Bengaluru, India, Feb. 2020, pp. 1–3, doi: 10.23919/ICOMBI48604.2020.9203031.

[384] 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 Autom. (ETFA)*, Zaragoza, Spain, Sep. 2019, pp. 1173–1180, doi: 10.1109/ETFA.2019.8869262.

[385] P. Dunphy, L. Garratt, and F. Petitcolas, "Decentralizing digital identity: Open challenges for distributed ledgers," in *Proc. IEEE Eur. Symp. Secur. Privacy Workshops*, London, U.K., Apr. 2018, pp. 75–78, doi: 10.1109/EuroSPW.2018.00016.

[386] C. Sullivan and E. Burger, "E-residency and blockchain," *Comput. Law Secur. Rev.*, vol. 33, no. 4, pp. 470–481, 2017, doi: 10.1016/j.clsr.2017.03.016.

[387] H. Halpin, "Vision: A critique of immunity passports and W3C decentralized identifiers," in *Security Standardisation Research*, vol. 12529, T. van der Merwe, C. Mitchell, and M. Mehrnezhad, Eds. Cham, Switzerland: Springer, 2020, pp. 148–168, doi: 10.1007/978-3-030-64357-7_7.
[388] M. Nuss, A. Puchta, and M. Kunz, "Towards blockchain-based identity and access management for Internet of Things in enterprises," in *Trust, Privacy and Security in Digital Business*, vol. 11033, S. Furnell, H. Mouratidis, and G. Pernul, Eds. Cham, Switzerland: Springer, 2018, pp. 167–181, doi: 10.1007/978-3-319-98385-1_12.
[389] 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)*, New Orleans, LA, USA, Jun. 2020, pp. 1–2, doi: 10.1109/WF-IoT48130.2020.9221130.
[390] I. Damgård, C. Ganesh, H. Khoshakhlagh, C. Orlandi, and L. Siniscalchi, "Balancing privacy and accountability in blockchain identity management," in *Topics in Cryptology—CT-RSA 2021*, vol. 12704, K. G. Paterson, Ed. Cham, Switzerland: Springer, 2021, pp. 552–576, doi: 10.1007/978-3-030-75539-3_23.
[391] R. Neisse, G. Steri, and I. N. Fovino, "Blockchain-based identity management and data usage control (extended abstract)," in *Privacy and Identity Management. The Smart Revolution*, vol. 526, M. Hansen, E. Kosta, I. Nai-Fovino, and S. Fischer-Hübner, Eds. Cham, Switzerland: Springer, 2018, pp. 237–239, doi: 10.1007/978-3-319-92925-5_15.
[392] A. Pillai, V. Saraswat, and A. V. Ramachandran, "Attacks on blockchain based digital identity," in *Blockchain and Applications*, vol. 320, J. Prieto, A. Partida, P. Leitšo, and A. Pinto, Eds. Cham, Switzerland: Springer, 2022, pp. 329–338, doi: 10.1007/978-3-030-86162-9_33.
[393] S. Manski and B. Manski, "No gods, no masters, no coders? The future of sovereignty in a blockchain world," *Law Critique*, vol. 29, no. 2, pp. 151–162, Jul. 2018, doi: 10.1007/s10978-018-9225-z.
[394] 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)*, Pulau Pinang, Malaysia, Nov. 2019, pp. 30–35, doi: 10.1109/AINS47559.2019.8968708.
[395] K.-H. Kim, S. Lim, D.-Y. Hwang, and K.-H. Kim, "Analysis on the privacy of DID service properties in the DID document," in *Proc. Int. Conf. Inf. Netw. (ICOIN)*, Jeju Island, South Korea, Jan. 2021, pp. 745–748, doi: 10.1109/ICOIN50884.2021.9333997.
[396] A. Satybaldy and M. Nowostawski, "Review of techniques for privacy-preserving blockchain systems," in *Proc. 2nd ACM Int. Symp. Blockchain Secure Crit. Infrastruct.*, Oct. 2020, pp. 1–9, doi: 10.1145/3384943.3409416.

T. T. TRAM NGO was born in Vietnam, in 1988. She received the B.S. and M.S. degrees in computer science from Marseilles Polytech University, Marseilles, France, in 2012.

From 2012 to 2016, she was a Research Assistant with the LISIC Laboratory, Calais, France. From 2015 to 2016, she was an Assistant Professor with the Information Department, University of the Littoral Opal Coast, Calais. Since 2019, she has been with Viettel Solutions, Viettel Group, as a Research and Development Engineer, where she is currently a Computer Science Engineer. Her research interests include computer vision, artificial intelligence, and blockchain technology.

T. ANH DANG was born in Vietnam, in 1985. He graduated from Hanoi University of Technology, in 2009, in the top five percent of his faculty.

In his current position as the Deputy General Manager with Bitel Peru, he has built an organization that sets new high standards in efficiency and delivers excellent production quality. After joining Viettel Group, in 2009, he has held many important positions such as a Chief of Representative Office with Viettel ICT and the Research and Development Director with Viettel Solutions. His research interests include writing on medium, developing mobile apps, data science, teaching, leadership development, and organizational growth with an emphasis on core services development of information and communication technology.

V. VUONG HUYNH was born in 1989, in Vietnam. He graduated from the Danang University of Technology.

In 2014, he joined Viettel Solutions as a Software Development Engineer, where he has held different positions such as Technology Research Engineer, Project Manager, and Product Team Leader. He is currently the Deputy Manager of the Research and Development Center, Viettel Solutions. His research interests include system architecture, performance optimization when deploying products, and the development of 4.0 technologies such as the IoT, big data, and AI. Currently, he is researching and developing products related to blockchain technology, especially focusing on blockchain technology to support businesses.

T. CONG LE was born in Vietnam, in 1983. He graduated from the Hanoi University of Technology, in 2006.

As a Deputy Director General with Viettel Solutions, he is in charge of technical matters of the organization in order to ensure the production of high-quality software products, taking advantage of the latest world technologies. Since 2007, he has been with Viettel Groups and has held many important technical positions such as the Director of the Product Development Center, the Head of the Technology Department, and the Vice General Director of the Enterprise Solutions Division.