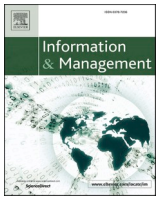
Information & Management 61 (2024) 104026

Contents lists available at ScienceDirect

Information & Management

journal homepage: www.elsevier.com/locate/im



Blockchain-driven decentralized identity management: An interdisciplinary review and research agenda

Zhiyue Yan [a], Xi Zhao [a], Yang (Alison) Liu [a], Xin (Robert) Luo [b,*]

[a] School of Management, Xi'an Jiaotong University, China
[b] Anderson School of Management, University of New Mexico, USA

ARTICLE INFO

Keywords:
Blockchain
Decentralized identity management
Interdisciplinary review
Research agenda

ABSTRACT

The rise of blockchain technology has sparked interest in decentralized identity management (DIdM). However, DIdM's interdisciplinary nature has led to a fragmented understanding. We propose a "Task Structure-Technological Properties-Fit" framework to clarify the application of DIdM across tasks and contexts. We conducted a comprehensive review of 149 DIdM papers to define task structure (task goals and stakeholder values), task goals (identity value creation and value maintenance), stakeholders (users, service providers, identity issuers, regulators, and infrastructure builders), and DIdM properties (interoperability and self-sovereignty). We explored how these elements could align and then highlight research gaps and present a DIdM research agenda.

1. Introduction

Digital identity management (IdM) encompasses the meticulous control procedure of digital identity credentials and identifiers [1] within diverse domains [1,2]. Historically, IdM operated within a centralized framework in which institutions and corporations served as custodians, safeguarding individual credentials and identifiers. However, escalating concerns regarding privacy, data breaches, and the intrusive reach of centralized entities [3] have spurred a global shift toward more secure and user-centric paradigms [4–10]. In response, decentralized identity management (DIdM), often referred to as blockchain-based identity management, has emerged; DIdM integrates blockchain technology into various domains, such as the Internet of Things (IoT) [11–13], Internet of Vehicles (IoV) [14–16], social media, and national identity management. The goal is to empower individuals by returning control of their data to them, thereby ensuring heightened security and transparency.

DIdM represents a paradigmatic shift in IdM, in which individuals or entities control their own identities, sidestepping the need for a centralized authority or intermediary by leveraging blockchain technology. In stark contrast to traditional IdM approaches, DIdM emphasizes interoperability and self-sovereignty properties, which implies that a user's identity becomes universally recognizable and usable across a myriad platforms, apps, and services while affording users absolute control over their own identities [17–19]. Users can create, manage, and delete their identities without seeking permission from a central authority. This reduced reliance on centralized authorities can substantially mitigate the risk of large-scale data breaches or the potential misuse of personal data. Notably, MIT Connection Science has duly acknowledged DIdM's highly resilient architecture and distributed nature and characterized it as a fundamental infrastructure for providing a "nervous system for digital social life." Established standards and projects, such as W3C and Diem (formerly Libra[1]) of Facebook,[2] are currently investing substantial resources in harnessing the unproven advantages of DIdM in the new digital economy.[3]

While brimming with promise, DIdM is a multifaceted concept interwoven with diverse disciplines, such as cryptography, blockchain technology, user experience design, and even sociology and legal studies. The multidimensionality of this domain makes it a fertile ground for research, exploration, and innovation. As research on DIdM in various fields continues to mature, the information systems (IS) field is experiencing a palpable surge in DIdM research each year. Previous papers have primarily focused on designing DIdM solutions for different industries, a few of which have already undergone successful pilot

* Corresponding author.
E-mail addresses: yanzhiyue@stu.xjtu.edu.cn (Z. Yan), zhaoxi1@xjtu.edu.cn (X. Zhao), liuyang.alison@xjtu.edu.cn (Y.(A. Liu), xinluo@unm.edu (X.(R. Luo).

[1] https://techcrunch.com/
[2] https://www.diem.com/en-us/
[3] https://identity.foundation/

https://doi.org/10.1016/j.im.2024.104026
Received 8 December 2022; Received in revised form 7 August 2024; Accepted 12 August 2024
Available online 14 August 2024

implementation [14,20–22]. In these papers and pilot initiatives, the scope of the identities under consideration extends beyond human identities to encompass nonhuman identities. Apart from the technical papers that delineate the design of DIdM solutions, several recent papers have discussed these solutions in terms of stakeholder engagement and their impact on managerial performance [17,23–32]; however, most of these works have taken primarily a technical perspective or have merely elucidated cases and applications within specific contexts. Consequently, a comprehensive understanding of DIdM from an IS management perspective remains starkly absent. We were thus motivated to perform this comprehensive literature review to provide researchers and practitioners with a holistic understanding of the potential of DIdM and accelerate pertinent research and their real-world implications in this context .

In essence, in this research, our endeavor is to develop a framework for DIdM research by addressing the following pivotal research questions that underpin this evolving domain. *(1) Which task structure does traditional IdM address? (2) Which technological properties does DIdM provide that distinguish it from traditional IdM? (3) How can we leverage the technological properties of DIdM to meet the task structure of IdM and improve its performance impacts?* To unravel these questions, we conducted a systematic literature review (SLR) that encompassed an exhaustive analysis of 149 articles on DIdM research. Consequently, two task goals, three stakeholder levels, and two technological properties were derived. Furthermore, we examined the fit of task structure and technological properties by exploring which task structure of DIdM can be supported by certain technological properties and what benefits and challenges will stakeholders experience after adopting and using DIdM.

Importantly, we demonstrated the paramount importance of aligning the collectively established stakeholder values with the behavioral processes necessary to accomplish specific goals, as this alignment serves as a pivotal catalyst for facilitating the adoption and use of DIdM. Such epistemological alignment not only streamlines the integration of DIdM, but also profoundly influences its subsequent efficacy in DIdM adoption and use. Our research makes significant contributions to the emerging landscape of DIdM, offering substantial value to both researchers and practitioners alike. From a research perspective, we provide researchers with a systematic and comprehensive understanding of how DIdM fulfills IdM tasks. This framework has utility in multiple research approaches. For example, design science research can use this framework to delineate task goals that align with specific stakeholders, select the focus and preferences of technological properties based on task structure, and design solutions that are more conducive to the adoption and use of DIdM. Additionally, empirical research can leverage this framework to propose and rigorously assess the effectiveness of DIdM in various tasks and contexts. By grounding studies in this comprehensive framework, researchers can provide insight into the practical applications and implications of DIdM, thereby advancing our collective understanding of this transformative technology.

In the next section, we introduce our combined review methods—that is, SLR and document co-citation analysis—which are applied to DIdM research. We then discuss the task structure of IdM and the technological properties of DIdM. We describe three important fits: the fit between efficient access control, secure distributed storage, and establishing identification; the fit between efficient access control, secure distributed storage, and identity value maintenance; and the fit between selective self-disclosure, automatically executed procedures, and identity value creation. Finally, based on these views, we propose suggestions for future research.

2. Research design: A systematic literature review and document co-citation analysis

In the era of Web 3.0, DIdM has been widely introduced in many domains to offer solutions to longstanding identity challenges, such as security, privacy, and interoperability property. Based on the general paradigm of interdisciplinary reviews [33–35] and the literature review methods used in the IS domain [36–38], we conducted a combined SLT approach on DIdM research published between 2016 and 2023 [37,39,40]. SLR is acclaimed as a replicable, transparent, objective, unbiased, and rigorous process. Therefore, we designed it as a mechanical process, including planning, execution, and reporting phases [41]. Recognizing the potential risk of unintended exclusion due to the rigid nature of a purely mechanical process [39], we introduced iterative refinements in the searching and inclusion and exclusion criteria sections [42]. This approach not only bolsters the comprehensiveness of our review, but also ensures that the diverse facets of DIdM research are duly accounted for, ultimately enhancing the depth and breadth of our analysis.

Fig. 1 depicts the flowchart of the literature review procedure in this SLR-guided study. Our systematic review unfolded through three distinct phases: planning, conducting, and reporting. In the planning phase, our initial step involved meticulous preparation to identify pertinent works related to DIdM, adhering to a structural search term approach [34,38]. We adopted a methodology akin to that used by Müßigmann et al. [39] to define our search terms. In our quest, we combed seven databases using specific keywords, titles, and abstracts as the search fields. This process underwent three iterations, each aimed at refining and pinpointing the most relevant search terms: (1) *blockchain* OR *decentralized* AND *identity*, (2) *blockchain* OR *decentralized* AND *digital identity management,* and (3) *decentralized identity* OR *decentralized identity management* OR *decentralized identity access management* OR *blockchain-based identity* OR *blockchain-based identity management* OR *blockchain-based identity access management* OR *blockchain-driven identity* OR *blockchain-driven identity management*. The search terms for the first iteration were established based on the baseline of the inclusion criteria, where we required that a paper must simultaneously contain both of these keywords to be included. We merged, deduplicated, and performed preliminary screening using the first round of literature to obtain a more relevant collection of literature related to DIdM. Thereafter, we consolidated the relevant vocabulary from the titles, abstracts, and keywords of this literature to derive new search terms for the second round of retrieval. This iterative method enabled us to progressively distill more precise search terms attuned to the nuances of the DIdM domain. Through this three-round iterative approach, we cultivated a curated collection of literature, consisting of 1,618 papers, which formed the epistemological foundation of our holistic review.

To comprehensively curate the relevant literature on DIdM, we adopted a recursive iterative approach that encompasses "*forward and backward searches and inclusion/exclusion*" as an integral component of the screening process during the conducting phase (see Table 1). This iterative procedure persisted until we reached a point at which no further increase in the number of papers in our literature collection was observed, thereby ensuring a thorough exploration of the research landscape. Our results were derived from an extensive search across multiple scholarly resources, including the AIS e-library and six prominent databases: Springer, ScienceDirect, Web of Science, IEEE Xplore, ACM, and Scopus. Following a meticulous screening process, a curated selection of 149 papers emerged as the final collection for our review.

Notably, our review adopted specific inclusion and exclusion criteria to maintain a focused scope. We excluded papers that centered primarily on decentralized applications unrelated to DIdM and those that aimed primarily to improve IdM design through techniques other than blockchain technology. A paper's inclusion in our review was contingent on an explicit discussion of the intersection of blockchain technology and IdM, thereby ensuring that the selected articles aligned closely with the DIdM domain.

The reporting phase includes both coding and profiling. To understand the development status of DIdM from an interdisciplinary perspective, we classified all literature according to Walstrom and Hardgrave's classifications of pure IS, hybrid IS, and non-IS journals [42,43]. Specifically, as shown in Appendix A1, this includes the expanded set of IS journals [44], special interest group (SIG, recommended by

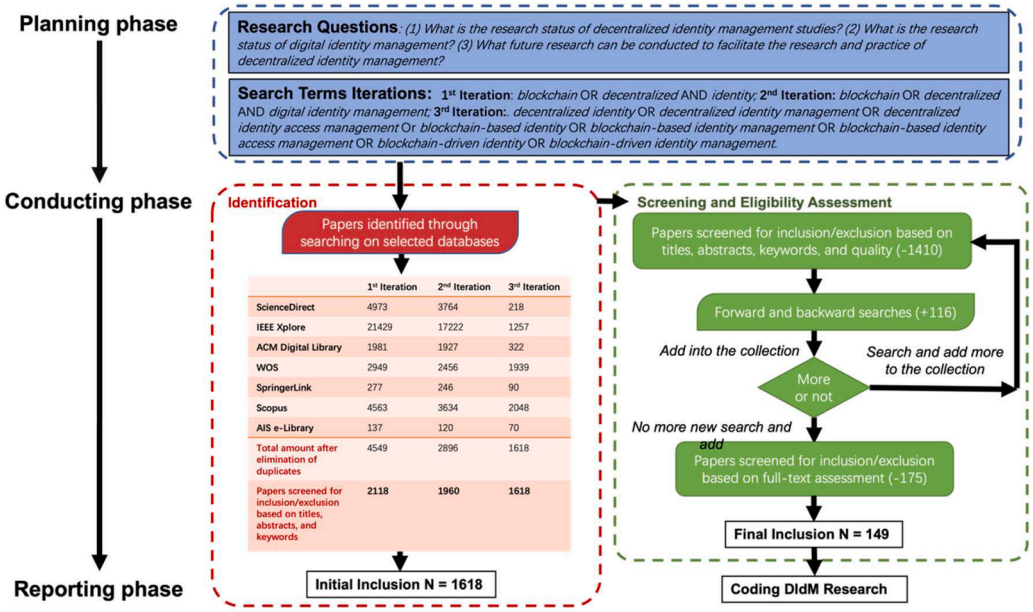


Fig. 1. Research Design Flowchart.

Table 1
Inclusion and Exclusion Criteria.

Inclusion criteria	Exclusion criteria
Peer-reviewed papers	1. Papers that focus more on other blockchain applications or decentralized applications but not on DIdM
Papers that clearly describe the blockchain application in identity management or describe blockchain-based identity management, DIdM, or IdM.	2. Papers that focus more on improving IdM with other decentralized techniques but not blockchain technology 3. Papers that are too short or for which full text cannot be found 4. Papers that are not written in English 5. Papers but not chapters of books or webpages

senior AIS scholars) [28], IS conferences (ICIS, AMCIS, ECIS, PACIS, and HICSS) [36], computer science journals and conferences, other IS journals or hybrid IS journals with high impact factors, and various other disciplinary sources (journals and conferences).

As depicted in Fig. 2, the research interest in DIdM exhibited a general upward trajectory from 2017 to 2023. A significant turning point was observed from 2021 to 2022, which signified the technological maturation of DIdM. Consequently, there was a sudden decline in the number of non-IS papers (mostly technical papers of DIdM design), hybrid IS papers, and the overall count of selected papers in 2022. But focusing solely on the IS field (showing as pure IS + hybrid IS), it is evident that research interest in DIdM within IS also has generally increased. Additionally, the meticulous analysis of the 149 selected papers involved detailed coding across various dimensions, including application domains, application phases, methodologies, research goal perspectives, stakeholders, and technological properties. The last four figures in Fig. 2 derived from the above coding results echo the trends observed, thereby affirming their resonance in the IS community. In particular, they show stronger similarities to non-IS or hybrid IS in more technically related subtopics. For applications in digital citizens, the increasing trend of DIdM research in IS is smoother and less affected by technological turning points.

3. Analysis findings

3.1. Results on publication topics

We categorized the papers based on application domains, application phases, research objectives, and stakeholders, as depicted in Fig. 3.

In terms of the application domain, DIdM was applied for human identity and device identity. Specifically, the most frequently discussed human identity research was web user and cloud identity (n = 31) and citizen identity (n = 38), and the most frequently discussed device identity research was the IoT or IoV device identity (n = 35). The popularity of device identity research lagged behind that of human identity research, possibly because human identity has two directions in the application process: a digital identity established directly in the digital domain and a digital identity established in the digital domain based on identity attributes in the physical domain. In contrast, most device identities are merely digital identities established in the digital realm based on identity attributes in the physical realm.

With regard to DIdM application phases, a research focus on phases of authentication (n = 80) and authorization (n = 80) has steadily increased and a focus on secondary use of data (n = 34) and user decision-making (n = 6) began to emerge in 2020. It is worth noting that apart from answering the question of "*how to use blockchain technology to improve the design of digital identity management functions, such as authentication and authorization*," recent studies have begun exploring "*how the use of DIdM will affect user decisions*" and "*how the use of DIdM affects the secondary use of data*." Studies were conducted from the perspective of users (n = 51), service providers and identity issuers (n = 41), and regulators and infrastructure builders (n = 38) (Fig. 3d) . Driven by technique-enabled sovereignty, numerous studies from 2017 to 2019 emphasized the advantages of DIdM from users' perspectives. Recently, more studies have been initiated from the perspective of regulators, infrastructure builders, service providers, and identity issuers. In fact, the focus is turning to platforms to investigate methods to promote the adoption and use of DIdM systems.

3.2. Results of the research methods

Fig. 4a presents a prominent number of studies using design methodology (n = 99), survey or case study (n = 20), literature review (n = 14), statistical analysis or experimental analysis (n = 8), and other

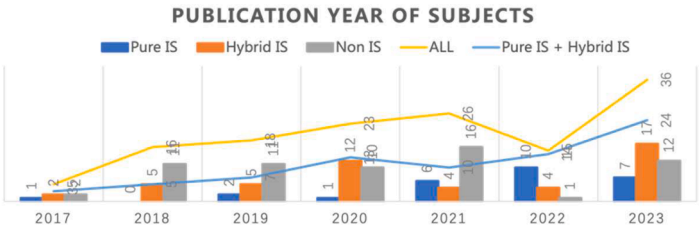


Figure 2. a

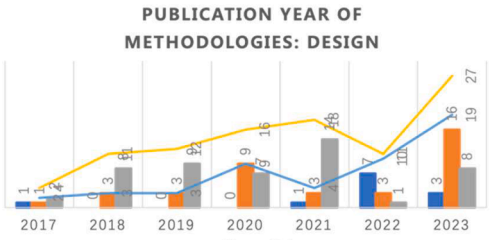


Figure 2. b

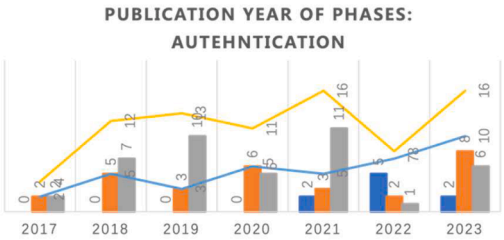


Figure 2. c

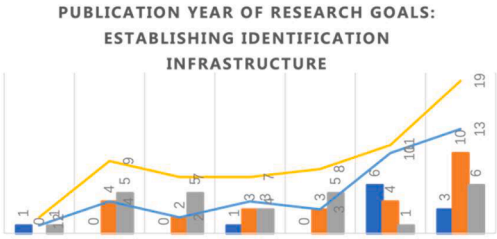


Figure 2. d

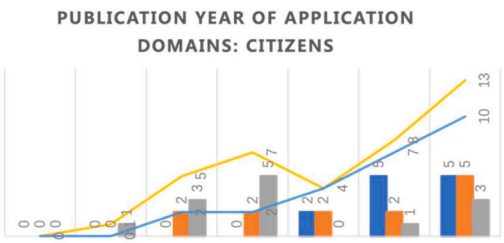


Figure 2. e

Fig. 2. IS-Relevance Paper Trend.

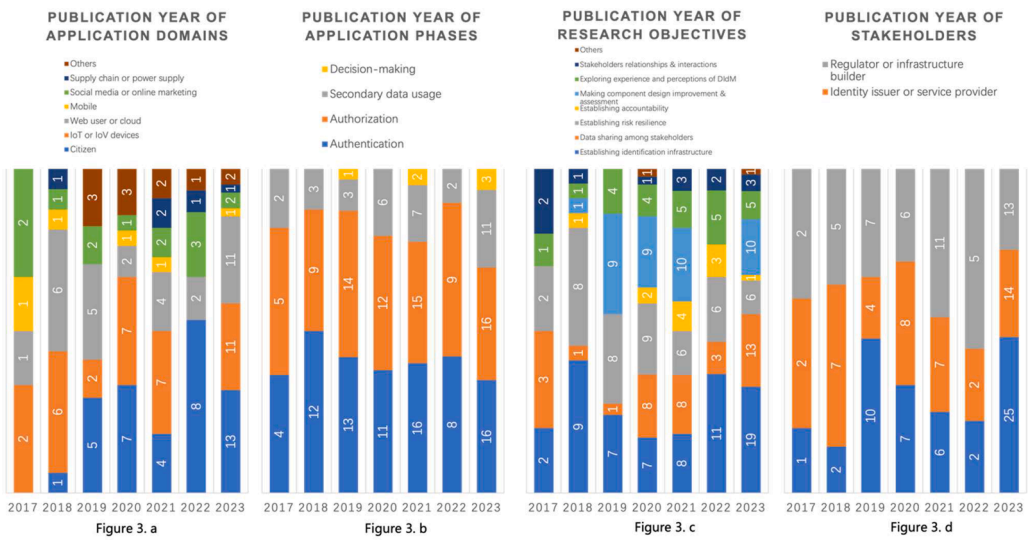


Figure 3. a

Figure 3. b

Figure 3. c

Figure 3. d

Fig. 3. Publication Year of Research Information.

methodologies (n = 8). Because of the absence of a sufficient number of mature applications of DIdM to provide real-world cases for empirical analysis before 2017, studies used only virtual simulation experiments to make DIdM assessments. The number of surveys or case studies increased after 2018, and statistical analyses and experimental analyses increased after 2020.

3.3. Results of the research clusters

Document co-citation analysis (DCA) is a method used to identify research themes. When a document is cited by multiple other documents, a co-citation relationship exists between them. DCA uses these co-citation relationships to construct a citation network in which documents are nodes and co-citation relationships are edges. This enables

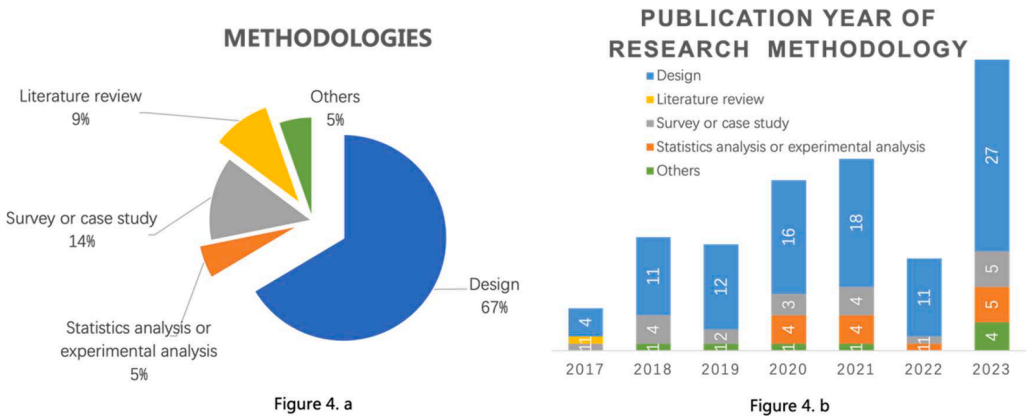


Fig. 4. Research Methodology Information.

researchers and practitioners understand research communities with unbiased recognition [45]. CiteSpace (version 5.8.R3 64bit) was used to visualize the data in our study. The metadata of the 149 studies were processed into a unified format and divided by year from 2016 to 2023. DCA revealed the mutual connections among documents by analyzing the relationships among citations. The node type parameter was set to "referenced" in our DCA. The networks used the functions "pathfinder" and "pruning sliced network" to highlight the key structure. As presented in Table 2, the characteristic indexes of the co-citation network were obtained in which the modularity of the network (Q value) demonstrates the robustness of the network structure ($Q > 0.3$) and the mean silhouette (S value) demonstrates the robustness of the clustering result ($S > 0.7$).

The clustering results from the cluster and timeline views are displayed in Fig. 5. From the cluster perspective, the DCA networks were divided into 20 co-citation clusters with different colors. It is evident that the clustering results are focused on application domains, such as e-health identity privacy (cluster 49), medical data (cluster 37), public sector (cluster 3), reputation portability (cluster 1), and self-sovereign social communication (cluster 12). Specific technical property improvements are highlighted as well, including a hybrid blockchain-based identity authentication scheme (cluster 25), a computational intelligence approach (cluster 21), and a self-contained authorization technique (cluster 2). Finally, we encoded the 15 largest clusters into four themes by examining the intercitations and intracitations and the log-likelihood regression labeling results among the clusters. The abstracts of these citations were then retrieved and analyzed to extract the following four themes: *DIdM application phases, DIdM technological properties, DIdM application domains,* and *DIdM research goals.*

These findings structurally reveal the current research status of the interdisciplinary development of DIdM. First, they reveal a general trend toward increasing popularity of DIdM research across different disciplines, application domains, application phases, and stakeholders year by year. Second, they reveal that DIdM studies have focused more on design and empirical research in recent years. We used DCA clustering results to reduce the subjective bias of manual coding. To establish an interdisciplinary understanding of DIdM research for IS scholars, we organized the review results into an adaptive extended task–technology fit (TTF) model, which is presented in the following section.

Table 2
Characteristic Indices of Co-Citation Networks.

Review paper collections	149 studies
Time span	2016–2023
Number of citing documents	149
Number of cited documents	4,963
Number of nodes	2,890
Number of links	11,832
Modularity (Q value)	0.9765
Mean silhouette (S value)	0.9677

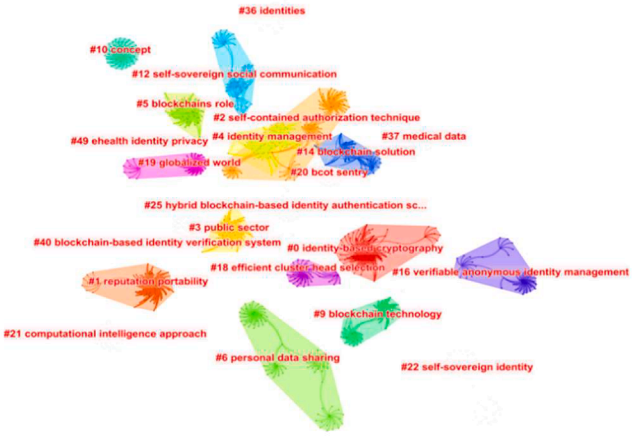


Fig. 5. Clusters of 149 Studies by DCA.

4. An extended TTF framework for DIdM

The TTF theory was initially proposed by Goodhue and Thompson in 1995 [46,47] and emphasizes that the impact of a technology's utilization or performance impacts depends on its fit for the task to be performed [45,48,49]. This theory has found extensive application across various studies within the IS discipline, such as in the deployment of enterprise systems, adoption of remote working technologies, and efficiency of health information systems [46,47,50–56]. The primary utility of the TTF framework lies in its ability to evaluate and enhance the congruence between technological functionality and task demands, thereby facilitating improvements in work efficiency and performance outcomes. Further, TTF also serves as a valuable metric for providing insight into the prediction of user acceptance and the willingness of individuals or organizations to adopt new technologies. In summary, the TTF theory serves as a powerful tool to better understand the key issues in IS research, analyzing and evaluating the adaptability of IS and their impact on performance.

We aimed to establish a framework based on the task structure of IdM, going beyond specific contexts and case details to map the technological properties of DIdM to the tasks of IdM (see Fig. 6). By identifying the fit of different task and technology combinations, the use of the DIdM system can be promoted, and further exploration of the effectiveness of DIdM implementation can be pursued. Driven by this aspiration, we found that the extended TTF theory fits well with our

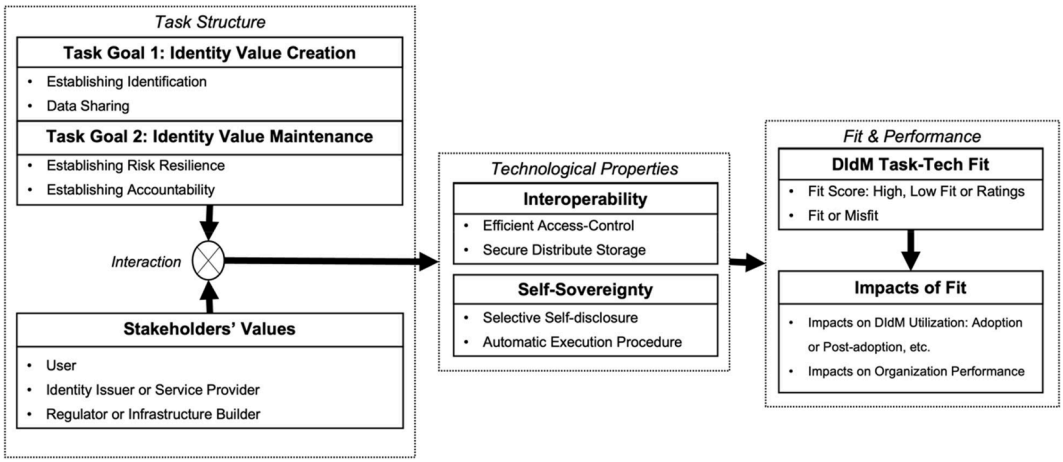


Fig. 6. Extended TTF of decentralized identity management research.

review and can systematically organize the existing literature.

There are three reasons that support the suitability of this theory for our research. The primary reason is that the TTF framework facilitates a deep dive into the compatibility of technological properties and task structures. While the existing DIdM literature has established themes of tasks and technologies (refer to appendices and analysis findings chapter), it falls short in terms of thoroughly examining their fit relationships. The extended TTF framework provides a theoretical foundation for assessing how well technology aligns with task goals, aiding in a detailed investigation of "how specific technological properties of DIdM fit a particular task structure, and the impact of this fit on DIdM's adoption and performance," which are crucial IS issues in the utilization and implementation of DIdM [55,57]. The second reason is that the extended TTF framework is especially particularly suitable for analyzing the use and adoption of blockchain-related technologies [57–60]. The basic structure of the TTF theory is very rather flexible in adaptation and extension [50,52,55,61,62], and, thus, enables the incorporation of additional factors like such as individual, social, or team traits and environmental elements as a third dimension that affects fit relationships [49,55–57,59,62,63]. This is particularly important for DIdM, as it naturally has characteristics that span organizations and systems and requires the extension of task goals to different stakeholders. Through the extended TTF framework, we can comprehensively evaluate the adaptability and effectiveness of DIdM systems. The third reason is that the extended TTF framework can help us systematically establish the research agenda for DIdM. We select "fit as profile deviation" to conceptualize and assess the fit between tasks and technologies [45,47,50,55,63] and, operationalize it as the deviation of the those profiles that comprise a feasible combination of IdM task goals and DIdM technological properties, thereby confirming the current research status and future research opportunities, including the ideal fit for task goals and DIdM technological properties, the proven fit with the addition dimensions, and the identification of the gap between the two [55]. We believe that this can lead to a clearer and more targeted research agenda to guide the theoretical development and practical application of DIdM [45,64].

To advance the fit process, we first identified the managerial goals of traditional digital identity management and the technological properties of DIdM. In general, the TTF theory usually abstracts task attributes or procedures from the perspectives of complexity as "tasks as tasks" and "tasks as behavioral requirements" [47,65,66]. In the research by Roth [57], the task was widely conceptualized as a *task structure*, representing the interactive result of organizational principles and federal values. The task structure is adaptively improved in our study, including *the jointly constituted values by stakeholders involved in the task* and *the behavioral processes needed to achieve specific task goals*. We believe that the task structure of IdM can be conceptualized as the interactive result of task goals and different stakeholders' values paradigms. To identify the main task structure of IdM research, we collected literature on IdM mainly from the AIS senior basket and SIG-recommended journals with high impact factors. After reviewing 28 papers on IdM, we identified three stakeholder roles: users, service providers or identity issuers, and regulatory agencies or infrastructure builders. We also concluded two basic task goals: *identity value creation* and *identity value maintenance*. Next, after comprehensively coding 149 papers on DIdM, we categorized DIdM's technological characteristics into two primary groups: "*Interoperability*" and "*Self-Sovereignty*." "*Efficient access control*" and "*secure distributed storage*" demonstrate *interoperability* characteristics, providing consistency and interoperability across multiple systems. On the other hand, "*selective self-disclosure*" and "*automated execution procedures*" reflect the property characteristic of autonomy, thereby emphasizing the proactivity and independence of users in data control. These categorizations are derived from the foundational technical components of DIdM, offering a complete overview of its technological functionality [57,59,60]. The two tasks and four subtasks of IdM (see Table 3) as well as the two key technological properties of DIdM) are coded below (see Table 4).

In the following sections, we describe the task structure and technological properties of DIdM in detail. Furthermore, we conceptualize fit as the deviation between the ideal and the actual implementation.

4.1. Task structure of digital identity management

In the reviewed papers, IdM usually establishes a set of requirements or principles around the demands of target enterprises, users, and other stakeholders. In this paper, we take these requirements, principles, or goals as IdM *task goals*. Through a comprehensive analysis of 28 IS papers related to IS IdM, we identified two main task goals and categorized them into three stakeholder levels for discussion. Detailed review records are provided in Appendix D1.

4.1.1. Task goal 1: Identity value creation

The value of traditional IdM stems from the primary and secondary uses of identity data. Achieving value through identity entails setting up accurate identification that bridges the physical and digital worlds. This involves crafting a detailed user profile and a robust digital infrastructure [67,68]. Such an infrastructure promotes interoperability and cost efficiency [69]. For example, Xu [70] found that unified IdM in crime databases improved criminal identity-matching accuracy, and Ma and Agarwal [71] noted that a positive user perception of identification boosted community contributions. Research on national identity or transnational identity has achieved value creation through economic

Table 3
Task Structure of Digital Identity Management Research.

Task Goals	Subtask Goals of IdM	Definition	Task Characteristics Based on Literature	Reviewed papers mentioned Task Structure
Identity Value Creation	***Establishing Identification***	Establishing accurate identification bridges the physical and digital worlds, thereby creating detailed user profiles and a robust digital infrastructure. It is the basis of identity value creation.	**Task solution scheme:** • Governments, law enforcement, and other infrastructure builders require users to register for identity infrastructure. • Identity issuers and service providers promote the interoperability of user identity information. • Users participate in the establishment of identity infrastructure, both actively and passively. **Task execution pain points: The main issues are related to user experience and the cost of infrastructure development.** • Users may lack interest in participating in the establishment of a widespread identity infrastructure. • Obstacles in interoperability among various identity issuers and service providers escalate the high cost of rebuilding or migrating identity infrastructure. • Ongoing debates on how to establish identity infrastructure, such as the balance between biometric credentials and user privacy, and the balance between multifactor authentication and user experience. **Task outcomes: Establishing widespread identity consistency can facilitate access for service providers, regulate monitoring, and improve user experience.** • Ensuring the identity data quality and consistency of a broad identity database: This improves the accuracy of identity matches, such as the precision in matching criminal identity data. • Achieving economic inclusivity through identification infrastructure: This implies reducing "invisible citizens," optimizing and simplifying resource allocation, and accommodating diverse socioeconomic activities. • Establishing identity authentication(physical) to build identity identification(psychological): This enhances users' positive perception of social identity, benefiting further participation in social activities.	• User Perspective: [175,76,9,69,75,176] • Identity Issuer or Service Provider Perspective: [175,70,71] • Regulator or Infrastructure Builder Perspective: [175,67,68,73,74,77,177,178]
	Data Sharing	After the initial phase of value creation from the identification infrastructure, the subsequent goal of harnessing identity information for added value is centered on data sharing.	**Task solution scheme:** • Infrastructure builders such as governments and law enforcement agencies establish unified data sharing rules, like GDPR. • Identity issuers and service providers implement rules for sharing user identities. Users have not yet fully participated in data-sharing tasks. **Task execution pain point: The main issues lie in users' perception of data ownership(the relationship between perceived control and rewards), interoperability between service providers, and communication among data sharing entities.** • Users face barriers to controlling data sharing. As users become more aware of the perception of ownership over their identity data, many may opt out of data exchanges if they feel their ability to control or their perceived level of control is diminished. • Interoperability barriers among service providers include unified encryption methods, data policies, data quality standards, and setting the correct level of data sharing consent (e.g., in electronic health record systems). • Communication barriers between data sharing entities, such as service providers, identity issuers,	• User Perspective: [8,79] • Identity Issuer or Service Provider Perspective: [80] • Regulator or Infrastructure Builder Perspective:

(*continued on next page*)

Table 3 (*continued*)

Task Goals	Subtask Goals of IdM	Definition	Task Characteristics Based on Literature	Reviewed papers mentioned Task Structure
			and users. For example, users may face bridging gaps in DIdM's IT knowledge. **Task outcomes: Accurate, consistent, timely, and extensive data sharing brings more network benefits to service providers and users but also introduces privacy and security risks.** • *First-party data collection and sharing:* Based on the social exchange theory, users share data with service providers in exchange for services, thereby achieving value creation and exchange. • Secondary data sharing: After obtaining data directly shared by users, service providers or identity providers trade packaged data assets or data services based on data assets with other service providers.	
Identity Value Maintenance	***Establishing Risk Resilience***	Establishing risk resilience involves effectively resisting or reducing risk damage from internal or external threats. This is the first step of identity value maintenance.	**Task solution scheme:** • Service providers and identity issuers prioritize enhancing access-control monitoring and authentication accuracy, including biometric authentication, multifactor authentication, and other techniques to combat identity theft. • Regulatory bodies establish risk management frameworks that cover technical measures, personnel, and procedures to protect the value of identities from abuse by service providers or identity issuers. • Users' security decisions involve entrusting the management of their identity information to intermediary institutions like identity issuers. These issuers help verify this information with other service providers, establishing a bridge for transactions. **Task execution pain point: The main issue lies in the contradiction between identity data protection and value creation tasks.** • Regulatory bodies are temporarily unable to truly participate in the task of establishing risk resilience. • The specialization level of service providers' authentication solutions often implies entrusting it to specialized external authenticators, thereby necessitating a careful evaluation of trade-offs and potential unintended consequences. • When evaluating privacy and usability, users may prioritize short-term benefits over long-term security and privacy investments, thus choosing to pay for usability or convenience rather than security and privacy. **Task outcomes: While identity data security and privacy protection can maintain the value of data identity, they may also harm traditional democratic norms.**	• User Perspective: [76,9,84] • Identity Issuer or Service Provider Perspective: [5,7,83,82] • Regulator or Infrastructure Builder Perspective: [77,86]
	Establishing Accountability	Establishing accountability involves establishing records for the use of identity data at each step to make responsibility clear. This step is taken to reclaim lost identity value.	**Task solution scheme:** • Regulators, service providers, and identity providers should establish clear policies and procedures for creating detailed access logs and monitoring systems to ensure that all activities can be tracked and audited. • These stakeholders should also develop effective incident response plans to swiftly act in the event of security incidents, thus minimizing potential damage. **Task execution pain point: The main challenge lies in establishing auditing entities within environments that host multiple central identity databases.** • Barriers exist between service providers and identity providers, thereby preventing the establishment of unified and transparent auditing records and mechanisms.	• Regulator or Infrastructure Builder Perspective: [8,81]

(*continued on next page*)

Table 3 (*continued*)

Task Goals	Subtask Goals of IdM	Definition	Task Characteristics Based on Literature	Reviewed papers mentioned Task Structure
			• Regulatory bodies and users are currently unable to fully engage in tasks related to identity data accountability. **Task outcomes: Identity data auditing capabilities can not only recover value losses but also increase the sense of accountability among data users, prompting them to proactively limit potential issues. However, this may also lead to some on-chain information leaks.**	

inclusion [68,72]. Citizens' access to the identification infrastructure often correlates with their economic participation. Such access can bring "invisible citizens" into the fold [73], streamline resource allocation, and encourage diverse civic participation [74].

However, the traditional IdM approach faces several challenges regarding the establishment of an identification infrastructure. First, users may lack interest in adopting a broad identification base [10] and may prefer intermediaries to manage their simple identities [9] because they have limited knowledge regarding the benefits and uses of this identification infrastructure [75]. Second, there are certain challenges to rebuilding or migrating the identification infrastructure [69]. To address these issues, Eriksson [67] proposed a generic design framework for identifiers to avoid the need to rebuild identification systems and mitigate the high costs associated with migration. The increasing platformization of IdM is associated with a growing emphasis on portability and interoperability to minimize such migration costs [68].

Third, there is an ongoing debate regarding the preferred approach to building an identification infrastructure. While general studies suggest that biometric credentials offer higher accuracy compared to physical devices, certain studies argue that incorporating biometric credentials may compromise user privacy considerations [69,76]. There is also an argument in favor of leveraging social identities to establish identification, as network characteristics make it challenging to create fraudulent identities [70].

After the initial phase of value creation from the identification infrastructure, the subsequent goal of harnessing identity information for added value is centered on data sharing [77]. Three of the papers that we reviewed predominantly applied the social exchange theory for theorizing data sharing [78]. The social exchange theory posits that social interactions are driven by an exchange-based process in which individuals are more inclined to engage in data sharing when they perceive the greater rewards and minimal privacy costs associated with such sharing. Spiekermann and Korunovska [79] introduced a theory suggesting that informed users develop a sense of ownership of their identity data, thus making them more aware of privacy risks when sharing data. If control is taken away, many might opt out of data exchanges, thereby emphasizing the importance of perceived control in data sharing.

Challenges also abound in data sharing. For example, electronic health record systems—a frequently debated domain of data sharing—have limited interoperability because of encryption methods, strict policies, issues in determining the appropriate consent level, poor interorganizational communication, and patients' limited knowledge of information technology [80]. Various technological approaches have been introduced to address these challenges and enhance data sharing. As discussed above, we can conclude that IdM creates business value through the identification of infrastructure and data sharing.

4.1.2. Task goal 2: Identity value maintenance

Traditional IdM not only creates value through identity data but also maintains value by adopting identity theft countermeasures [7]. Initially, privacy and security were focused on preventing authorization abuse [81] and improving the anti-risk capability of access control [7]. However, with the ongoing evolution of digitalization, simply strengthening risk resistance is no longer sufficient—establishing accountability before risks arise is now essential.

The first subtask goal of identity security and privacy protection is to *establish risk resilience*, which involves effectively resisting or reducing risk damage from internal or external threats. Service providers prioritize the enhancement of access monitoring [5] and the implementation of secure mechanisms [82]; however, it is imperative that they carefully evaluate the trade-offs and potential unintended consequences associated with measures such as biometric scanning and the delegation of control to external providers [82,83]. Early system users often relied on technology intermediaries to protect against privacy and security risks. These intermediaries, known as identity issuers, create a controlled environment in which users provide sensitive and identifying information and then the identity issuers help verify this information with other service providers, thereby establishing bridges for transactions. Theoretically, this approach reduces privacy and security risks in individual transactions; however, it also requires that users entrust their private information to intermediaries in the identity system. For users, improving the risk resilience of their identity management involves a trade-off between privacy disclosure and security decision-making [84]. However, in terms of paying for these technology intermediaries, users tend to prioritize usability or convenience over higher levels of security and privacy [76]. These findings align with the theory of intertemporal choice, which suggests that users may prioritize short-term benefits over long-term security and privacy investments [9]. In terms of user privacy, IdM systems can pose significant privacy concerns owing to their centralized repositories [84]. The concept of surveillance capitalism [85] suggests that these systems may undermine traditional democratic norms and, thus, their role in privacy and security protection may be challenged.

The second subtask goal in protecting identity information is to *establish accountability*. This involves establishing records for the use of identity data at each step in order to make responsibility clear. In traditional IdM research, the establishment of relevant laws or regulations is done to achieve this accountability, thus constructing power cultivation and restriction mechanisms [86]. Strategies to proactively limit possible issues can include increasing an individual's perception of accountability through measures such as identifiability, awareness of logging, awareness of auditing, and electronic presence [81].

Many IdM papers have emphasized the importance of establishing a trustworthy environment, considering it a task goal that is the same as establishing accountability. However, we argue that trust should not be a task goal. Trust follows a chronological sequence in IdM, arising as an emotional perception rather than an explicit requirement. In national IdM, trust is a sentiment outcome toward infrastructure builders, influenced by various factors. Building a trustworthy environment is broader than merely building accountability. Thus, establishing accountability is a task goal of IdM, but building trust is not.

Finally, there is a noticeable absence of comprehensive discussions involving various levels of stakeholders in traditional IdM research. This can be primarily attributed to the prevailing perception of identity data as an internal resource confined within organizational boundaries. The

Table 4
Technological Properties of Decentralized Identity Management Research.

Technological Properties		Definition	Concluded Characteristics Based on Literature	Reviewed papers mentioned technological properties
Interoperability properties	***Efficient Access Control***	Efficient access control refers to DIdM allowing users to authenticate and authorize in the same manner across multiple systems to access different services or resources. Specifically, in efficient access control, authentication refers to matching pre-stored identity information with a unique decentralized identifier, while authorization refers to permitting users to access services or resources after verification.	**Compared to traditional access control technologies, the key feature of access control in DIdM is** *providing users with a more seamless cross-system login experience* **and, thus, making identity management more efficient.** The DIdM paper has explored various access control methods, specifically improving the adaptability and accuracy of identity authentication through the technical integration access control; enhancing the granularity and sensitivity of identity authorization through attribute-based access control; addressing integration transition and computation restriction issues between systems through hybrid consensus access control. **Weakness:** Lower privacy level in attribute-based access control compared to traditional centralized identity management systems.	[11,20,25,29,30,42,51,58, 89–100,103–105,107,113,114, 124,126,137,138,143,145, 148–150,156,158,162,163,170, 171,179–187]
	Secure Distributed Storage	Secure distributed storage in distributed identity refers to the cryptographically secure storage that DIdM enables across multiple nodes, leveraging node-based decentralized consensus protocols to resist failure and tampering. The content involved in DIdM generally includes decentralized identifiers, credentials, and identity attributes.	**Compared to traditional identity data storage, the key feature of DIdM's storage lies in its ability** *to run multiple nodes by the systems and defend against failures and tampering, making identity management more secure***.** The DIdM paper has explored three main design choices to provide different levels of decentralization, specifically including decentralized storage methods for authentication solutions, credential storage, and the matching methods of credentials with decentralized identifiers. **Weakness:** Lower authentication efficiency compared to traditional centralized identity management systems.	[24,26,96,102,108,109,115,116, 118–120,122,139–142,147, 150–155,157,164,165,170,180, 181,188–197]
Self-sovereignty properties	***Selective Self-disclosure***	Selective self-disclosure enables users to decide when, where, and to whom they disclose certain identity information to meet specific needs and scenarios. This process is typically facilitated through a unified interface standard or a globally unified namespace and then executed automatically by smart contracts.	**Compared to traditional identity disclosure, a key feature of DIdM is its ability to** *allow users to selectively disclose their personal identity information, enhancing users' control over their data and protecting their privacy.* The DIdM papers mainly explore specific design solutions based on methods like zero-knowledge proofs. However, implementing selective self-disclosure might require complex technical support. **Weakness:** Redundancy in credentials and consequent additional effort and responsibility for users compared to traditional centralized identity management systems.	[22,23,101,103,106,107,123, 167,169,172,173,184,186,193, 198–204]
	Automatic Execution Procedure	Automatic execution procedure utilizes blockchain technology, such as smart contracts, to manage digital identifiers and credentials among various stakeholders—including issuers, users, service providers, and DIDM systems—automatically executing specific actions when predetermined conditions are met.	**Compared to traditional identity management systems, the significant characteristic of DIdM's execution procedure is that** *smart contract-driven automatic execution can support users in autonomously managing their identities without intermediaries.* To manage their identity information accurately, users must understand the actual workings of the DIdM execution procedure, including its true scope, limitations, and the associated duties and responsibilities. **Weakness:** Challenging to achieve thorough IdM for users and unable to promptly intercept or halt the execution of smart contracts, compared to traditional centralized identity management systems.	[22,27,28,80,111,116,121,122, 125–127,131,132,144,166,171, 172,180,181,185,187,201,203, 205,206]

focus of identity management activities is typically on the development and functioning of a solitary identity issuer. From among the 28 papers examined, more than half discussed multiple tasks for a single role; however, when discussing a single task, basically only one or two stakeholders are involved. Only one paper discussed more than two stakeholders.

4.2. Technological properties of DIdM

Traditional IdM often faces task–goal trade-offs, such as data sharing versus privacy risk. However, DIdM—with its unique technological properties—allows for the simultaneous achievement of these goals. On reviewing all the DIdM studies of reviews and surveys, we observed that existing DIdM research primarily conceptualizes blockchain-driven DIdM as a self-sovereign identity, focusing on technical details extracted from this architecture [18,87]. Additionally, most discussions of DIdM's technological properties lean more toward blockchain technology than IdM [17,88], thus obscuring how DIdM can be distinguished from traditional IdM and how DIdM can solve existing challenges related to IdM.

In our systematic review of 149 DIdM papers, we identified two key technological properties and four functionalities. These properties and functionalities help better distinguish DIdM from traditional IdM and general blockchain technology and accommodate technical details and condensing management insights.

4.2.1. Property 1: Interoperability

4.2.1.1. Efficient access control. *Access control* is a prominent topic in DIdM, with discussions focused on authenticating and authorizing eligible users to enter the systems for services or resources. Specifically, authentication verifies the match between prestored identity information and a unique identifier, while authorization grants rights after this verification. DIdM papers have explored various approaches to access control, including technique integration access control, attribute-based access control, and hybrid consensus access control [89–99].

Most DIdM papers on access control propose the creation of user-generated identities with on-chain public keys and off-chain private keys for authentication [92,100,101]. Technique integration enhances the adaptability of authentication to specific environments, such as incorporating individual attributes for national identity authentication [102] or deploying lightweight self-authenticated public keys in resource-constrained devices [103]. Furthermore, it improves authentication accuracy through integrated methods, such as biometric key generation [98] and dynamic membership authentication schemes [95].

Although attribute-based access control is a common security solution, it involves privacy concerns in blockchain-driven solutions because of its reliance on collecting user attributes for refined authorization [104–106]. Various solutions have been proposed to mitigate attribute exposure [107,108–110], such as confidential attribute registration [111], certificateless public key cryptography [112], offline storage [103], and dual blockchain architecture storage [96]. Innovative solutions update authorization schemes to help prevent identity fraud, such as disposable identity management [113] and access rights delegation models [105].

Hybrid consensus access control introduces a degree of decentralized consensus into IdM, addressing transitional challenges and computational limitations. Scholars have proposed hierarchical blockchain networks and cross-chain channel-based models [114]. This model aids the loan process by enabling relay-based cross-chain data exchange, which results in on-chain computation with greater computing power and reduced disintermediation [115].

4.2.1.2. Secure distribute storage. This functionality interacts with the functionality of access control and includes three design choices for decentralization. The access-control process involves three stakeholders (i.e., identity issuer, user, and service provider) and two components (i.e., credentials and identifiers). In traditional IdM, the service provider and identity issuer may be the same enterprise, storing identifiers and credentials in its central database. Although all reviewed DIdM studies used blockchain technology for distributed data storage to a certain extent, centralization and intermediaries were not completely eliminated.

The level of decentralization depends on identifier and credential storage decisions and decentralized consensus. We define three common design choices here [116,117]. The first of these is determining how decentralized the authentication solution will be. Currently, the most common solution for authentication is to use blockchains for public key storage and smartphones for private key storage, which is known as a decentralized public key infrastructure [100,117–119]. However, a few studies have integrated this decentralized method with centralized authentication methods—such as quick response (QR) codes [18] or biometric authentication [91,120]—to provide more assurance. These designs use the blockchain as an index; however, the authenticator may have the attributes copied and stored in centralized databases.

The second design choice is the level of decentralization of the credential storage. The most decentralized solution would be for the metadata of credentials to be added and stored off-chain by users and for bound decentralized identifiers to be stored on-chain [18]. However, Kassem and Alsayed [116] were apprehensive that if users were given full control of their identity, problems might occur, such as addition of false data or neglection of false attributes, particularly in offline circumstances.

The third design choice is how decentralized the credentials will be when linked to decentralized identifiers. One approach to this could be to maintain a large registry to link credentials with decentralized identifiers, such as in the case of Uport; another could be to map authentication methods with decentralized identifiers. The latter approach could lead to the development of more decentralized trust by introducing more authentication methods; however, it could be undetectably attacked if third-party issuers colluded with the holder of the credentials [121].

4.2.2. Property 2: Self-sovereignty

The main goal for DIdM users is to rely on it as a technical basis for human–computer interactions to participate in more cultural and socioeconomic activities [20]. *Selective self-disclosure* and *automatic execution processes* are functionalities that support the *self-sovereignty property* of DIdM.

4.2.2.3. Selective self-disclosure. In traditional IdM, identity establishment and data sharing are completed through a third-party intermediary. In contrast, DIdM does not go through a third-party intermediary [22,122,123], thereby allowing users to choose which identity information to share [22,124] through a unified interface standard [121] or a unified global namespace [111,125], which is then automatically executed directly by the smart contract with a preset code [116,126,127].

As discussed earlier, in most existing DIdM applications, users' sensitive credentials are stored in their own mobile devices, while immutability is promised by bound decentralized identifiers on blockchain networks. In this ideal condition, private credentials will not be exposed to people with ulterior motives; meanwhile, related decentralized identifiers can achieve the goal of consistency—that is, *selective self-disclosure* in DIdM is the technological characteristic that establishes a credential stating, for example, that "*Rick has reached the age of 21*" rather than to establish a replica of "*Rick's social security information.*"

However, *selective self-disclosure* also brings redundancy to credentials and, thus, makes it difficult for users to confirm which credentials can prove which information. Users may need more education and training to fully understand how to properly use selective self-disclosure

techniques and how to identify and address potential security risks. For example, in the fields of financial transactions or healthcare, users may need to provide sufficient identity information while protecting their privacy to meet regulatory requirements or ensure the legitimacy of transactions. In such cases, balancing the need for privacy protection and information disclosure will likely be a complex issue.

4.2.2.4. Automatic execution procedure. We define an automatic execution procedure as the use of blockchain technology, such as smart contracts, to manage digital identifiers and credentials among different stakeholders, including issuers, users, service providers, and the DIdM system [28]. Traditional IdM, as presented in Table 5, follows a streamlined workflow and the identity issuer is the agent for execution [14]. IdM aggregates user identities and service resources to provide usability and also causes users to gradually lose the self-sovereignty of their own identities. As presented in Table 5, DIdM helps maintain users' self-sovereignty through smart, automatic, contract-driven execution. With DIdM, stakeholders can hold, sync, and maintain a copy of the identity ledger for tamper-proof transactions and consensus and smart contracts can be achieved without a trusted third party [128–130]. Once users determine how and when their digital identities are created, maintained, processed, and decommissioned, they can directly invoke smart contracts for their digital identities, which will be auto-executed as programmed [80,121,127,131].

However, the self-sovereignty property of DIdM might poses challenges [132]. One possible issue is that the so-called *self-sovereign experience* implies that, except in automatically executed programs, the most important factor in a user's control of their identity is the "human factor" [128]. Greater self-sovereignty in these interactions may result in greater user liability, which users find difficult to evaluate [133]. Only if the user is aware of how control in DIdM truly works—including its true scope, limits, and associated obligations and liabilities—can they think about how specific control modes (smart contract modes) and control styles (smart contract parameters) should be used under various circumstances [128]. Thus, there might be inconsistencies between the operation results and the short-term goals in immature cases [134–136].

4.3. Fit between task structure and technological properties

Based on the discussed pain points of IdM tasks and the analysis of DIdM technological properties, we propose the following ideal fit:

- **Propositions 1, 2, and 3:** The identity value creation task of establishing identification should result in a good fit when using DIdM technologies that emphasize *efficient access control, secure distributed storage, or automatically executed procedure.*
- **Propositions 4, 5, and 6:** The identity value creation task of data sharing should result in a good fit when using DIdM technologies that emphasize *secure distributed storage, selective self-disclosure, or automatically executed procedure.*
- **Propositions 7, 8, and 9:** The identity value maintenance task of establishing risk resilience should result in a good fit when using DIdM technologies that emphasize *efficient access control, secure distributed storage, or selective self-disclosure.*
- **Propositions 10, 11, and 12:** The identity value maintenance task of establishing accountability should result in a good fit when using DIdM technologies that emphasize *efficient access control, secure distributed storage, or automatically executed procedure.*

To determine the possible fit between technological properties and task structure that have been discussed in the literature, we coded 149 related papers using the aforementioned framework. By extending the TTF framework to include a stakeholder dimension, we comprehensively and systematically discussed proven fits. Specifically, if the paper elaborates on the task goal, specific technological properties, and corresponding stakeholders, we recorded and marked the matches (see Appendix D2). We assumed that the more times they fit, the more attention their effectiveness would receive. In most cases presented in Table 6.2, this could indicate that a certain technological property is likely to perform better with the task or although occasionally it might not yet perform well, it merits discussion and improvement to achieve a better fit.

Table 6.2 summarizes the results of our review, including the actual number of papers and whether the certain fits mentioned in reviewed papers are proven or well discussed. In Table 6.2, the actual number of papers reflects the level of attention these areas have received, while the gray grids reflect that certain fits are proven or well discussed. This relatively lower focus may suggest that these areas have not yet received adequate attention in current research, possibly because DIdM is still in the early stage of construction and promotion. At this stage, research priorities lean toward establishing identification and establishing risk resilience. Furthermore, early DIdM studies have not systematically differentiated between the values of different stakeholders when exploring various tasks. This oversight has led to the neglect of the diverse solution schemes and execution pain points faced by different DIdM stakeholders for the same task. Such shortcomings of perspective may further contribute to the lack of attention that certain areas have received. Against this backdrop, our discussion focuses on the alignment between the marked task structures and technical attributes. A thorough analysis of this alignment can reveal current research gaps and directions for future improvement.

4.4. Proven fit between efficient access control, secure distributed storage, and establishment of identification

When establishing the identification infrastructure in DIdM, it is mostly regulators and infrastructure builders who consider the need for business process integration and gradual system transition in specific domains in the early years. To achieve this, unified standards and enforcement methods are developed. These include unified access control standards for multiple systems (including the unified standard of identifiers, credentials, authentication, and authorization methods) [22,93,94,103,120,137–139] and distributed ledgers to store the same identifier reference and matching methods between identifiers and credentials (a few of which also save credentials) [99,119,140,141], thereby ensuring that each participant can apply to add records to the chain with distributed consensus to maintain the consistent enforcement of identities [92,142]. In most DIdM research, adopting interoperability properties is believed to achieve process integration—the goal of naturally establishing identification. Therefore, DIdM solutions in domains such as smart citizen, electronic health, and electronic education [22,26,30,91,123,137,143,144] aim to establish a unified standard or absolute

Table 5
Execution Process of Traditional IdM and DIdM.

Execution Procedure	Traditional IdM Executors	DIdM Executors
Pre-authentication	User – Identity Issuer (Assert credentials and set related ID in a centralized database)	User – Identity Issuer – Blockchain (Assert credentials and set-related decentralized identifier on chain)
Authentication	User – Identity Issuer (Match credentials with ID)	User – Identity Issuer – Blockchain (Match credentials with DID)
Authorization	Identity Issuer – service provider (Provide ID with service)	Blockchain – service provider (Provide DID with service)
Secondary data use	Identity Issuer – service provider (Provide credentials)	Service provider – Blockchain (Ask for credentials and record on chain)
Decision-making	Identity Issuer – User (Sign privacy Consent)	User – Blockchain (Disclose privacy proactively)

Table 6.1
Ideal fit of decentralized identity management (X indicates fit).

	Technological Properties	Interoperability		Self-sovereignty	
Tasks		Efficient Access Control	Secure Distributed Storage	Selective Self-Disclosure	Automatically Executed Procedure
Identity Value Creation	Establishing Identification	X(P1)	X(P2)		X(P3)
	Data Sharing		X(P4)	X(P5)	X(P6)
Identity Value Maintenance	Establishing Risk Resilience	X(P7)	X(P8)	X(P9)	
	Establishing Accountability	X(P10)	X(P11)		X(P12)

authority among multiple systems, thus encouraging or forcing stakeholders to adopt DIdM [91,125,144–146]. However, these compulsory methods by regulators may require users to disclose their real names and addresses to service providers, which could lead to undesirable outcomes [125,132,144,147].

For example, in the field of humanitarian operations management, the establishment of identification infrastructure using DIdM interoperability properties is believed to address issues such as inconsistent refugee identity information, duplicate relief work, slow aid disbursement, high transaction costs, and collaboration difficulties among rescue parties [30,89,91,102]. However, a few studies have posited that the DIdM identification infrastructure still faces certain postadoption issues, including selection bias (e.g., uneven access opportunities to obtain technology for different classes), follow-up maintenance (e.g., lack of supervision mechanisms and personnel), and discrimination application (e.g., malicious service providers use identity data to engage in service discrimination) [30].

Given that the adoption or use of DIdM in establishing identification by regulators in specific practices has not met expectations [148], a few identification infrastructure design schemes have begun to consider the matching of technology and tasks from the perspective of users. These programs aim to encourage the broader adoption of DIdM by improving interoperability technology in terms of privacy concerns [103] and ease of use [1–5]. For example, Siddarth et al. [141] proposed "proof of personality protocols" that suggest using cryptocurrency as an incentive layer for the operation of an identity network [149]. We believe that incorporating the perspectives of multiple stakeholders is crucial for achieving better identification. This approach is an inevitable choice for enhancing matching results based on empirical evidence. In summary, the fit between efficient access control and secure distributed storage is important for establishing an identification structure. In addition, other identification infrastructure design schemes have begun to consider improving the role positioning of service providers and identity issuers in "efficient access control" and "secure distributed storage," shifting them from adversaries of "*user-centricity*" to supporters of "*platform operation efficiency*." For example, research is beginning to establish temporary pairings between data providers and consumers or identity providers and verifiers for IoT, law enforcement, taxi companies, and other clients, thereby defining DIdM as enhancing the execution capacity and reducing the security risks of cross-domain authentication and authorization for platforms.

4.5. *Proven fit between efficient access control, secure distributed storage, and identity value maintenance*

The task goals of identity value maintenance are divided into "risk resilience" and "accountability" [109,122]. Most DIdM research employs access control schemes based on distributed storage and corresponding consensus to solve security risks, such as Sybil attacks, spoofing attacks, message substitution attacks, message replay attacks, man-in-the-middle attacks, and denial of service. Interoperability properties enable multiple participants to maintain a synchronized ledger and confirm the accurate version of the record as long as more than one-half of the nodes are not attacked [80,150–152]. This record ensures security for admission control [114,153], collaboration credibility [154,155], and an accountability basis [147]. Most of these DIdM studies resorted to computer science methods—such as virtual simulation, baseline comparison, and case analysis—to evaluate which security requirements the solution has met and whether the solution can resist certain specific risks.

On the one hand, regulators and infrastructure builders give special attention to improving the security of access control by increasing confidentiality, anonymity, and unlinkability[4] during the DIdM design phase, to maintain the security of the overall DIdM ecosystem and meet the requirements [107,108,114,143,156]. From this perspective, a pair of adversaries is generally assumed: a malicious unauthorized user and a

[4] Confidentiality refers to the security of identity data, such as credentials, attributes, and identifiers; anonymity refers to the security of a username; unlinkability refers to the security of the linkage between credentials and identifiers.

Table 6.2
Proven fit of decentralized identity management.

		Technological Properties	Interoperability		Self-sovereignty		
Tasks	**Subtasks**		***Efficient Access Control***	***Secure Distributed Storage***	***Selective Self-disclosure***	***Automatically executed procedure***	**Total**
Identity Value Creation	***Establishing Identification***	User	P1a: Ideal High Fit Proven: 12 papers	P2a: Ideal Low Fit Proven: 7 paper	No Ideal Fit Proven: 2 papers	P3a: Ideal High Fit Proven: 10 papers	31
		Identity Issuer or Service Provider	P1b: Ideal Low Fit Proven: 5 paper	P2b: Ideal Low Fit Proven: 5 papers	No Ideal Fit Proven: 2 papers	P3b: Ideal Low Fit Proven: 3 paper	15
		Regulator or Infrastructure Builder	P1c: Ideal High Fit Proven:18 papers	P2c: Ideal High Fit Proven: 11 papers	No Ideal Fit Proven: 1 paper	P3c: Ideal High Fit Proven: 3 paper	33
	Data Sharing	User	No Ideal Fit Proven: 5 papers	P4a: Ideal Low Fit Proven: 6 paper	P5a: Ideal High Fit Proven: 9 papers	P6a: Ideal High Fit Proven: 7 papers	27
		Identity Issuer or Service Provider	No Ideal Fit Proven: 5 papers	P4b: Ideal High Fit Proven: 2 paper	P5a: Ideal Low Fit Proven: 5 papers	P6b: Ideal Low Fit Proven: 3 papers	15
		Regulator or Infrastructure Builder	No Ideal Fit Proven: 5 papers	P4c: Ideal Low Fit Proven: 5 papers	P5c: Ideal Low Fit Proven: 1 paper	P6c: Ideal Low Fit Proven: 2 paper	13
Identity Value Maintenance	***Establishing Risk Resilience***	User	P7c: Ideal High Fit Proven: 5 papers	P8c: Ideal High Fit Proven: 3 papers	P9c: Ideal High Fit Proven: 5 papers	No Ideal Fit Proven: 3 papers	16
		Identity Issuer or Service Provider	P7c: Ideal High Fit Proven: 8 papers	P8c: Ideal High Fit Proven: 9 papers	P9c: Ideal Low Fit Proven: 2 papers	No Ideal Fit Proven: 1 paper	20
		Regulator or Infrastructure Builder	P7c: Ideal High Fit Proven: 7 papers	P8c: Ideal High Fit Proven: 3 papers	P9c: Ideal Low Fit Proven: 1 paper	No Ideal Fit Proven: 2 papers	13
	Establishing Accountability	User	P10a: Ideal High Fit Proven: 2 papers	P11a: Ideal High Fit Proven: 2 paper	No Ideal Fit Proven: 2 paper	P12a: Ideal High Fit Proven: 2 paper	8
		Identity Issuer or Service Provider	P10b: Ideal Low Fit Proven: 2 papers	P11b: Ideal Low Fit Proven: 4 papers	No Ideal Fit Proven: 1 paper	P12b: Ideal Low Fit Proven: 2 paper	9
		Regulator or Infrastructure Builder	P10c: Ideal High Fit Proven: 2 papers	P11c: Ideal High Fit Proven: 5 papers	No Ideal Fit Proven: 1 paper	P12c: Ideal High Fit Proven: 1 paper	9
		Total	76	62	32	39	

service provider who performs loyally. The security risks mainly originate from external sources; thus, cloud service infrastructure builders prioritize access control security [104]. Similar scenarios exist in public infrastructure domains, such as power grids [152]. However, DIdM must also consider the security of improved access control for DIdM when using integrated technique access control—such as biometrics and artificial intelligence—which may be combined with risky authentication, credential storage, or identifier matching schemes [22,90,91,98].

On the other hand, service providers prioritize distributed storage and consensus for risk resilience to maintain data credibility in DIdM [143,157]. This facilitates efficient and secure data collaboration in most cases, such as IoT and IoV identities [97,99,139,151,158–161]. As these devices increasingly participate in the collection, processing, and exchange of data with each other and with service providers, stakeholders in the field interact more equitably in data-driven service production [11]; in this case, service providers consider more risk resilience, while regulators prioritize accountability over privacy. It must be noted that security risks originate mainly from internal sources, such as frequent device replacements [149,162] and the need for equal collaboration [97,114,163–165]. Thus, IoT focuses on the secure requirement of mutual authentication [145]. When evaluating implementation effects, studies have explored the balance between collaborative security and efficiency [145]; however, there is no established baseline for efficiency owing to the limited literature in this context [114]. Generally measured indicators of collaboration efficiency may include mutual authentication latency, throughput, communication overhead, and computing cost [158]. Hence, efficient access control and secure distributed storage interactively facilitate that maintenance of identity value.

4.6. Proven fit between selective self-disclosure, automatic executed procedure, and identity value creation

Selective self-disclosure and an automatically executed procedure together constitute the self-sovereignty property that distinguishes DIdM from traditional IdM. These studies focus mainly on the user subject in terms of the adoption and use effects of DIdM and assume that the higher the user's level of identity disclosure, the higher the level of value created.

Specifically, certain studies have proposed fully automated processes for the establishment of identification. This approach aims to reduce costs and barriers while considering service providers' needs, such as establishing reputation layers [127] or blacklisting screening mechanisms [166]. However, the impact of these automated identity establishment methods is limited to the user experience aspect, without considering the benefits that other stakeholders may obtain from this. Furthermore, most researchers believe that DIdM can improve the level of system adoption and data sharing by enhancing the technical

properties of user sovereignty [23,167]. This is because, from the perspective of the social exchange theory, DIdM can enhance the subject's level of perceived control while disclosing the user's identity, including enhancing perceived safety [80,94], perceived control over disclosed credentials [107,116,124,131], and perceived transparency [90,107]. In addition, the automatic execution procedure can improve a user's disclosure level by enhancing the subject's motivation for data sharing [80]. For example, when a user is aware of or has participated in the efficient collaboration of data sharing, perceived usefulness and perceived ease of use enhance the motivation for data sharing [114]; moreover, when users recognize or receive economic incentives for data sharing, the expectation of benefits enhances their motivation for data sharing [23].

However, the default assumption in DIdM research that "the higher the level of identity disclosure by users, the higher the level of value creation" has not been widely demonstrated [105,109], and research on how to promote identity disclosure remains limited [149]. Further, DIdM research related to economic inclusion has explored the theoretical level of how self-disclosure can contribute to economic inclusion [19,22,28,69,168]. For example, Wang and Fennie discussed DIdM' s specific use in leveraging crypto refugee status to provide financial assistance, and Russo and Antonia argued that this needs to be coordinated with the specific requirements of the General Data Protection Relationship to enable enterprises to meet the data minimization principle [27,169]. These studies break away from the technical aspects of identity disclosure and explore the impact of this technology on users, organizations, and countries, taking the first step toward the inclusion of DIdM in IS research. Therefore, it is important to establish a fit between selective self-disclosure and automatically executed procedures to achieve business value through DIdM.

5. Research gaps and future opportunities

After reviewing existing research on DIdM and aligning it with the extended TTF framework, we identified the main research themes as well as three research gaps and future opportunities. It is evident from Table 6.2 that most DIdM studies overlook TTF between certain DIdM technological properties and task structure, because after incorporating the TTF framework with stakeholder dimensions, we found that almost one-half of the ideal fits were not well explored. Moreover, although there have been a few recent empirical studies on DIdM adoption and use, a more comprehensive qualitative and quantitative analysis is still required to understand how it impacts DIdM utilization or organization performance. Finaly, there is a research gap regarding the philosophical paradigm of DIdM in Web 3.0. Based on these gaps, we propose future directions.

5.1. Research gap 1: Inadequate research on leveraging DIdM's technological properties to align with the task structure of IdM to achieve or enhance fit

Stakeholders may have different values in the same task goal. We have conceptualized the task structure of IdM as the interactive result of task goals and different stakeholders' values. This reveals the various perspectives of specific task solution schemes and task execution pain points for different stakeholders. For example, identity issuers focus on process improvement and reducing reputation risk, while service providers value the cost reduction of sharing identity information; moreover, regulatory authorities prioritize consistency in identity information disclosure [170–172]. Additionally, stakeholder groups in DIdM experience different interactions compared to traditional IdM in the creation or maintenance of identity value [171]. This results in different and dynamic power relationships among stakeholders in the long-term process of TTF. Specifically, disintermediation in DIdM can weaken platform owners' control [72,134] and gradually decrease barriers to entry in the transition term [108,173]. Traditional value-creation interactions are transformed into stable and equal triangular relationships in DIdM among the three levels of stakeholders [174].

Thus, we propose exploring how to leverage the technological properties of DIdM to align with the task structure of IdM to achieve or enhance fit—specifically, how to make DIdM design choices for certain IdM tasks from the perspective of different stakeholder values. We then list future opportunities based on the unproven fit of Table 6.2 in Section 4.

a) Leverage DIdM's interoperability property to fit the task of identity value creation**.** Most published studies have assumed that the adoption process of DIdM technology will have a low fit or even a negative impact on the value creation of identity issuer level. There is little discussion on how service providers and identity issuers can reasonably and progressively transition from centralized identity management to DIdM while also accomplishing their identity value creation tasks. For example, organizations can transit from centralized IdM to DIdM through hybrid consensus access control to facilitate better iteration. This includes how to select decentralized storage of credentials and designing unified identifiers, authentication methods, and authorization and delegation mechanisms without creating barriers or high transition costs. For example, the authorized delegation mechanism can perform reputation verification in a small network range to support frequent data sharing and reduce the losses of identity of issuers caused by the inability to monopolize identity data.
b) Leverage DIdM's interoperability property to fit the task of identity value maintenance**.** Overall, most current research assumes that the interoperability property of DIdM can address almost all risk and accountability issues for stakeholders. However, an exploration of whether different stakeholders from various fields have distinct demands in this matter has been limited; for example, different domains may have specific design requirements for the decentralized storage of credentials. It is important to identify organizational risks related to DIdM and to study trust assessment and risk management methods.
c) Leverage DIdM's self-sovereignty property to fit the task of identity value creation. Current research has predominantly emphasized the assistance of self-sovereignty in user-level identity value creation, overlooking the potential alignment with other stakeholders, such as regulatory agencies. It has been suggested that research should concentrate on fostering collaboration among various organizations and departments, implementing effective communication strategies and establishing standards and shared automatic procedures for DIdM. This could involve regulators developing automatic execution procedures for registration, verification, sharing, and selective disclosure of credentials. Moreover, exploring user attitudes, adapting the automatic execution of DIdM, addressing challenges, and providing essential support are essential components to consider.
d) Leverage DIdM's self-sovereignty property to fit the task of identity value maintenance**.** Current research has rarely addressed how to use selective self-disclosure and automatic execution procedures to identity value maintenance. However, these two aspects can serve as essential service model carriers and log carriers for continuous identity value maintenance for users and regulatory agencies. For example, regulators can develop automated business processes that adhere to legal and regulatory standards for auditing purposes. In addition, users can investigate and assess new business models or service experiences based on self-maintained identity value supported by automated execution and selective self-disclosure programs.

5.2. Research gap 2: Insufficient research on the impact of fit on DIdM utilization and organizational performance for diverse stakeholders

We consider exploring the impacts of TTF on DIdM adoption, postadoption, and performance from different stakeholders' perspectives. While a few papers have focused on the use of DIdM technological properties to achieve self-sovereignty, privacy, security, and trust without compromising efficiency, these discussions alone might not be sufficient to convince stakeholders to transition to new IdM systems. Therefore, it is crucial to highlight the specific benefits that individuals and organizations can gain through this transition and to explore the cause-and-effect relationship between DIdM TTF and its impacts. This will enable a more informed understanding of the potential impacts and advantages associated with DIdM utilization and organizational performance.

Thus, we propose exploring the benefits and drawbacks of fits, particularly in terms of DIdM adoption, postadoption, and organization performance. We then list future opportunities based on the framework presented in Section 4. By examining these factors from a management perspective, academics and practitioners can ensure a technically sound and organizationally effective transition to DIdM.

a) Impacts of the fit between DIdM's interoperability property and identity value creation. Occasionally, a certain design choice represents the TTF of DIdM technological properties and task structures. Fit impacts the utilization and performance of DIdM; for example, storing credentials on mobile phones may reduce users' willingness to register in the infrastructure because refugees pose challenges to accessing technology. Unified identifiers may initially deter service providers from joining; however, ultimately, they enhance the effectiveness of data sharing and collaboration.
b) Impacts of the fit between DIdM's interoperability property and identity value maintenance. Fits influence the effectiveness of risk resistance and accountability; for example, the design of distributed storage may fit the user's task goal but may not consider the goal of the regulator. However, the fit of distributed storage and the entire task structure impacts the risk resistance of the digital ecosystem, user risk perception, and regulatory effects. Thus, exploring the impact of trust assessment and risk management methods on DIdM among stakeholders is crucial. The fits of these methods not only relate to privacy and security tasks but also may affect the efficiency of value creation.
c) Impacts of the fit between the self-sovereignty property of DIdM use and identity value creation. For example, self-sovereignty properties will reshape service providers' business models and lead to further transition in the business model of the traditional platform economy, but this fit will have an impact on the organization's performance. For example, the design, adoption, and use of selective self-disclosure can influence the number of disclosed attributes and connected networks in DIdM. Meanwhile, the fits also may moderate the construction of trust networks in digital ecosystems, including self-organizing communities and other social communities.
d) Impacts of the fit between the self-sovereignty property of DIdM use and identity value maintenance. For example, the fit of design choice may moderate the effectiveness of establishing risk resilience and accountability. Thus, studying the legal and regulatory requirements of DIdM across different regions and their impact on system design, adoption, and use is crucial. Therefore, exploring the potential impact of selective self-disclosure on the supervision process and the role of stakeholders in ensuring ethical use and compliance are important areas of investigation.

5.3. Research gap 3: Inadequate research on the reversal of identity ontology in web 3.0

With the strengthening of individual sovereignty and cross-organization brought about by DIdM, digital identity has become more integrated for users, thereby establishing broader identification. This may challenge the belief that digital identity reflects physical reality. In the future, digital identities may be created before physical ones and recognized by the physical world [207,208]. These digital identities, such as credit scores and social media reputation, are often generated and stored automatically. Users may not be aware of these identities, thus making it difficult to manage them properly. Only a few studies have discussed applications of DIdM in these domains [183]. These applications focus mainly on privacy consent and monitoring secondary data use, such as contact tracking during the COVID-19 pandemic [28].

We believe that this will prevail in the process of the platformization of DIdM, gradually promoting the ontological reversal of digital identity, and have a certain impact on the identity theory in the IS field. For example, existing identity theories are based mainly on the two directions of material-based and membership-based identities. Both these identity theories assume that a user's identity management is "*the user's presentation of the digital identity is a subjective decision.*" However, in the future, the display of digital identity might become an objective display.

a) Users' behaviors in Web 3.0 may be affected by the reversal [176]. For example, the phenomenon that digital identities are generated before physical identities may cause privacy concerns among users, thereby restricting their behaviors in digital spaces, such as reducing unethical behavior or increasing knowledge-sharing behavior. However, users may strengthen their cognition because of these passively generated digital identities. For example, users' medals or badges strengthen their sense of belonging to the community and, thus, further strengthen their contributions to the community.
b) The design of IdM should be changed. With the automatic generation and storage of digital identities, such as credit scores and social media reputation, users may not be fully aware of these identities and face challenges in effectively managing them. This presents an opportunity to focus on developing strategies and tools to enhance users' understanding of and control over their imperceptible decentralized digital identities.

Through an in-depth study of these research directions, we can obtain a more comprehensive understanding of the design, adoption, and use of DIdM and guide further development and application in these aspects.

6. Conclusion and limitations

With the integration of blockchain technology into numerous identity management solutions, the theoretical and practical underpinnings of DIdM are becoming increasingly complicated to support. Consequently, a thorough review and synthesis of the existing DIdM literature is imperative to pave the way for new research endeavors. In this pursuit, we used SLR and DCA methodologies to meticulously scour the landscape of DIdM papers. Following a rigorous quality assessment, we curated a selection of 149 papers for in-depth analysis.

Using an extended TTF model, we distilled key insights from the review findings, shedding light on the essential tasks of IdM and the technological attributes of DIdM. Our comprehensive literature review demonstrates a compelling alignment between the technological characteristics of DIdM and the tasks inherent in traditional IdM. Furthermore, in the digital age, DIdM has not only emerged as a reconciler of conflicting IdM tasks but has also shown remarkable adaptability to the multilayered task structure of IdM. We also emphasize the importance of framing these tasks within the context of stakeholder values and interactions among diverse stakeholders. By formulating tasks that better encapsulate the practical value demands of stakeholders, we can effectively catalyze progress in IdM in the digital era.

Nonetheless, it is important to acknowledge the limitations of our

present study. Our suggestions for future research directions are drawn primarily from prevalent topics in the field; this may have limited the scope of our study and it may not have encompassed all potential avenues of DIdM research. As the field of DIdM continues to mature, a more comprehensive literature review is warranted. We contend that DIdM research should transcend the sole focus on technical aspects, evolving into an amalgamation of blockchain technology and its social implications within the digital ecosystem. This holistic perspective should accurately mirror the specific requirements stemming from the realms of business, culture, and technology.

Author statement

All authors equally contributed to the design and development of this research.

CRediT authorship contribution statement

Zhiyue Yan: Writing – original draft, Visualization, Validation, Methodology, Formal analysis, Data curation, Conceptualization. **Xi Zhao:** Writing – review & editing, Supervision, Resources, Project administration, Investigation, Funding acquisition, Data curation. **Yang (Alison) Liu:** Writing – review & editing, Supervision, Resources, Project administration, Investigation, Funding acquisition. **Xin (Robert) Luo:** Writing – review & editing, Supervision, Resources, Project administration.

Acknowledgments

This work is supported by the National Natural Science Foundation of China (Grant No. 72231007 and Grant No. 72202172).

Supplementary materials

Supplementary material associated with this article can be found, in the online version, at doi:10.1016/j.im.2024.104026.

References

[1] International Telecommunication Union—Joint Coordination Activity for Identity Management (JCA-IdM), Scope of identity management, (n.d.).
[2] P.J. Windley, Digital Identity: Unmasking identity management architecture (IMA), O'Reilly Media, Inc., 2005.
[3] J. Carroll, J. Murphy, M. St Kilda, Who am I? I am Me! identity management in a networked world, in: 2004.
[4] R. Dhamija, L. Dusseault, The seven flaws of identity management: usability and security challenges, IEEE Secur. Priv. 6 (2008) 24–29, https://doi.org/10.1109/MSP.2008.49.
[5] J. Wang, Z. Shan, M. Gupta, H.R. Rao, A Longitudinal study of unauthorized access attempts on information systems: the role of opportunity contexts, MIS. Q. 43 (2019) 601–622, https://doi.org/10.25300/misq/2019/14751.
[6] E.A. Whitley, U. Gal, A. Kjærgaard, Who do you think you are? A review of the complex interplay between information systems, identification and identity, Eur. J. Inf. Syst. (2014), https://doi.org/10.1057/ejis.2013.34.
[7] I. Bose, A.C. Man Leung, Adoption of identity theft countermeasures and its short- and long-term impact on firm value, MIS. Q. 43 (2019) 313–327, https://doi.org/10.25300/misq/2019/14192.
[8] Kathy McGrath, Identity verification and societal challenges explaining the gap between service provision and development outcomes, MIS. Q. 40 (2016) 485–500, https://doi.org/10.25300/MISQ/2016/40.2.12.
[9] H Roßnagel, J Zibuschka, O Hinz, J Muntermann, Users' willingness to pay for web identity management systems, Eur. J. Inf. Syst. 23 (2019) 36–50, https://doi.org/10.1057/ejis.2013.33.
[10] P. Seltsikas, R.M. O'Keefe, Expectations and outcomes in electronic identity management: the role of trust and public value, Eur. J. Inf. Syst. 19 (2017) 93–103, https://doi.org/10.1057/ejis.2009.51.
[11] D. Preuveneers, W. Joosen, E. Ilie-Zudor, Trustworthy data-driven networked production for customer-centric plants, Ind. Manag. Data Syst. 117 (2017) 2305–2324, https://doi.org/10.1108/imds-10-2016-0419.
[12] C. Lin, D. He, X. Huang, K.-K.R. Choo, A.V. Vasilakos, BSeIn: A blockchain-based secure mutual authentication with fine-grained access control system for industry 4.0, J. Netw. Comput. Appl. 116 (2018) 42–52, https://doi.org/10.1016/j.jnca.2018.05.005.
[13] X. Zhu, Y. Badr, J. Pacheco, S. Hariri, Autonomic identity framework for the internet of things, in: 2017: pp. 69–79. https://doi.org/10.1109/ICCAC.2017.14.
[14] M. Kuperberg, Blockchain-based identity management: a survey from the enterprise and ecosystem perspective, IEEE Trans. Eng. Manag. 67 (2020) 1008–1027, https://doi.org/10.1109/tem.2019.2926471.
[15] X.Y. Zhu, Y. Badr, Identity management systems for the internet of things: a survey towards blockchain solutions, Sensors 18 (2018) 18, https://doi.org/10.3390/s18124215.
[16] Y. Liu, D.B. He, M.S. Obaidat, N. Kumar, M.K. Khan, K.K.R. Choo, Blockchain-based identity management systems: A review, J. Netw. Comput. Appl. 166 (2020) 11.
[17] G. Laatikainen, T. Kolehmainen, M. Li, M. Hautala, A. Kettunen, P. Abrahamsson, Towards a trustful digital world: exploring self-sovereign identity ecosystems, in:, in: PACIS-2021, 2021 https://aisel.aisnet.org/pacis2021/19.
[18] Alexander Mühle, A. Grüner, T. Gayvoronskaya, C. Meinel, A survey on essential components of a self-sovereign identity, Comput. Sci. Rev. 30 (2018) 80–86, https://doi.org/10.1016/j.cosrev.2018.10.002.
[19] E. Lim, F. Tan, C. Ryan, Controlling your own story using a digital identity solution: creation of economic identity for financial inclusion and protection, in: ECIS-2022, 2022. https://aisel.aisnet.org/ecis2022_rip/13.
[20] P. Dunphy, F.A.P. Petitcolas, A first look at identity management schemes on the blockchain, IEEE Secur. Priv. 16 (2018) 20–29, https://doi.org/10.1109/MSP.2018.3111247.
[21] X.Y. Zhu, Y. Badr, IEEE, a survey on blockchain-based identity management systems for the internet of things, in: IEEE Int. Congr. Cybermatics IEEE Conf. Internet Things Green Comput. Commun. Cyber Phys. Soc. Comput. Smart Data Blockchain Comput. Inf. Technol, IeeeNEW YORK, 2018, pp. 1568–1573, https://doi.org/10.1109/Cybermatics_2018.2018.00263.
[22] F. Wang, P. De Filippi, Self-sovereign identity in a globalized world: credentials-based identity systems as a driver for economic inclusion, Front. Blockchain 2 (2019) 22, https://doi.org/10.3389/fbloc.2019.00028.
[23] J. Cabinakova, N.K. Ostern, J. Krönung, Understanding prototype user acceptance of centralised and decentralised identity management systems, in: ECIS-2019, 2019. https://aisel.aisnet.org/ecis2019_rp/170.
[24] N. Ostern, J. Cabinakova, Pre-Prototype Testing: Empirical Insights on the Expected Usefulness of Decentralized Identity Management Systems, in: HICSS-52, 2019, https://doi.org/10.24251/HICSS.2019.222.
[25] R. Rana, R.N. Zaeem, K.S. Barber, An Assessment of blockchain identity solutions: minimizing risk and liability of authentication, in: 19th IEEEWICACM Int. Conf. Web Intell., Assoc Computing Machinery, NEW YORK, 2019, pp. 26–33, https://doi.org/10.1145/3350546.3352497.
[26] A. Khurshid, V. Rajeswaren, S. Andrews, Using blockchain technology to mitigate challenges in service access for the homeless and data exchange between providers: qualitative study, J. Med. Internet Res. 22 (2020) e16887, https://doi.org/10.2196/16887.
[27] G. Kondova, J. Erbguth, Acm, self-sovereign identity on public blockchains and the GDPR, in: 35th Annu. ACM Symp. Appl. Comput., Assoc Computing Machinery, NEW YORK, 2020, pp. 342–345, https://doi.org/10.1145/3341105.3374066.
[28] W.M. Xin, IEEE, fighting COVID-19 and helping economy reopen by using blockchain technology, in: IEEECIC Int. Conf. Commun. China ICCC, NEW YORK, Ieee, 2020, pp. 102–105.
[29] S. Feulner, J. Sedlmeir, V. Schlatt, N. Urbach, Exploring the use of self-sovereign identity for event ticketing systems, Electron. Mark. 32 (2022) 1759–1777, https://doi.org/10.1007/s12525-022-00573-9.
[30] K. Hunt, A. Narayanan, J. Zhuang, Blockchain in humanitarian operations management: A review of research and practice, Socioecon. Plann. Sci. 80 (2022) 101175, https://doi.org/10.1016/j.seps.2021.101175.
[31] J. Sedlmeir, T. Barbereau, J. Huber, L. Weigl, T. Roth, Transition pathways towards design principles of self-sovereign identity, in: ICIS-2022, 2022. https://aisel.aisnet.org/icis2022/is_implement/is_implement/4.
[32] N. Alam, X. Liang, T. Sultana, Impact of blockchain-based digital identity on privacy concern and privacy protective behavior, in: PACIS-2022, 2022. https://aisel.aisnet.org/pacis2022/326.
[33] H. Chughtai, M.D. Myers, A.G. Young, T. Borsa, V. Cardo, Ö. Demirkol, C. Morgan, S. Morton, C. Prior, J. Wilkin, E. Young, S.M. Özkula, Demarginalizing interdisciplinarity in is research: interdisciplinary research in marginalization, Commun. Assoc. Inf. Syst. (2020) 296–315, https://doi.org/10.17705/1CAIS.04613.
[34] J. Jiang, A.-F. Cameron, IT-enabled self-monitoring for chronic disease self-management: an interdisciplinary review, MIS Q. 44 (2020) 451–508, https://doi.org/10.25300/misq/2020/15108.
[35] M. Tarafdar, R.M. Davison, Research in information systems: intra-disciplinary and inter-disciplinary approaches, J. Assoc. Inf. Syst. 19 (2018), https://doi.org/10.17705/1jais.00500.
[36] S. Li, E. Karahanna, Online recommendation systems in a B2C E-commerce context: a review and future directions, J. Assoc. Inf. Syst. 16 (2015) 72–107, https://doi.org/10.17705/1jais.00389.
[37] M. Fakhar Manesh, M.M. Pellegrini, G. Marzi, M. Dabic, Knowledge management in the fourth industrial revolution: mapping the literature and scoping future avenues, IEEE Trans. Eng. Manag. 68 (2021) 289–300, https://doi.org/10.1109/tem.2019.2963489.
[38] M.H. ur Rehman, K. Salah, E. Damiani, D. Svetinovic, Trust in blockchain cryptocurrency ecosystem, IEEE Trans. Eng. Manag. 67 (2020) 1196–1212, https://doi.org/10.1109/tem.2019.2948861.

[39] B. Musigmann, H. von der Gracht, E. Hartmann, Blockchain technology in logistics and supply chain management—a bibliometric literature review from 2016 to January 2020, IEEE Trans. Eng. Manag 67 (2020) 988–1007, https://doi.org/10.1109/tem.2020.2980733.
[40] C.M. Trujillo, T.M. Long, Document co-citation analysis to enhance transdisciplinary research, Sci. Adv. 4 (2018) e1701130, https://doi.org/10.1126/sciadv.1701130.
[41] W.A. Cram, M. Templier, G. Pare, Re)considering the concept of literature review reproducibility, J. Assoc. Inf. Syst. 21 (2020) 1103–1114, https://doi.org/10.17705/1jais.00630.
[42] K.A. Walstrom, B.C. Hardgrave, Forums for information systems scholars: III, Inf. Manage. 39 (2001) 117–124, https://doi.org/10.1016/S0378-7206(01)00084-2.
[43] K.A. Walstrom, B.C. Hardgrave, R.L. Wilson, Forums for management information systems scholars, Commun. ACM 38 (1995) 93–107, https://doi.org/10.1145/203330.203348.
[44] H.C. Chan, V. Guness, H.-W. Kim, A method for identifying journals in a discipline: An application to information systems, Inf. Manage. 52 (2015) 239–246, https://doi.org/10.1016/j.im.2014.11.003.
[45] M.C. Howard, J.C. Rose, Refining and extending task–technology fit theory: creation of two task–technology fit scales and empirical clarification of the construct, Inf. Manage. 56 (2019) 103134, https://doi.org/10.1016/j.im.2018.12.002.
[46] D.L. Goodhue, R.L. Thompson, Task-technology fit and individual performance, MIS. Q. 19 (1995) 213, https://doi.org/10.2307/249689.
[47] I. Zigurs, B.K. Buckland, A theory of task/technology fit and group support systems effectiveness, MIS. Q. 22 (1998) 313, https://doi.org/10.2307/249668.
[48] K. Mathieson, M. Keil, Beyond the interface: Ease of use and task/technology fit, Inf. Manage. 34 (1998) 221–230, https://doi.org/10.1016/S0378-7206(98)00058-5.
[49] G. Im, Effects of cognitive and social factors on system utilization and performance outcomes, Inf. Manage. 51 (2014) 129–137, https://doi.org/10.1016/j.im.2013.10.002.
[50] A.R. Dennis, B.H. Wixom, R.J. Vandenberg, Understanding fit and appropriation effects in group support systems via meta-analysis, MIS. Q. 25 (2001) 167, https://doi.org/10.2307/3250928.
[51] A.I. Shirani, M.H.A. Tafti, J.F. Affisco, Task and technology fit: a comparison of two technologies for synchronous and asynchronous group communication, Inf. Manage. 36 (1999) 139–150, https://doi.org/10.1016/S0378-7206(99)00015-4.
[52] M.T. Dishaw, D.M. Strong, Extending the technology acceptance model with task–technology fit constructs, Inf. Manage. 36 (1999) 9–21, https://doi.org/10.1016/S0378-7206(98)00101-3.
[53] Volkoff Strong, Understanding organization—enterprise system fit: a path to theorizing the information technology artifact, MIS. Q. 34 (2010) 731, https://doi.org/10.2307/25750703.
[54] M.T. Dishaw, D.M. Strong, Supporting software maintenance with software engineering tools: A Computed task–technology fit analysis, J. Syst. Softw. 44 (1998) 107–120, https://doi.org/10.1016/S0164-1212(98)10048-1.
[55] J. Gebauer, M.J. Shaw, M.L. Gribbins, Task-technology fit for mobile information systems, J. Inf. Technol. 25 (2010) 259–272, https://doi.org/10.1057/jit.2010.10.
[56] C. Serrano, C. Serrano, E. Karahanna, University of Georgia, the compensatory interaction between user capabilities and technology capabilities in influencing task performance: an empirical assessment in telemedicine consultations, MIS Q. 40 (2016) 597–621, https://doi.org/10.25300/MISQ/2016/40.3.04.
[57] T. Roth, A. Stohr, J. Amend, G. Fridgen, A. Rieger, Blockchain as a driving force for federalism: A theory of cross-organizational task-technology fit, Int. J. Inf. Manag. 68 (2023) 102476, https://doi.org/10.1016/j.ijinfomgt.2022.102476.
[58] R. Kohli, T.-P. Liang, Special section: strategic integration of blockchain technology into organizations, J. Manag. Inf. Syst. 38 (2021) 282–287, https://doi.org/10.1080/07421222.2021.1912910.
[59] T.-P. Liang, R. Kohli, H.-C. Huang, Z.-L. Li, What drives the adoption of the blockchain technology? A fit-viability perspective, J. Manag. Inf. Syst. 38 (2021) 314–337, https://doi.org/10.1080/07421222.2021.1912915.
[60] E. Toufaily, T. Zalan, S.B. Dhaou, A framework of blockchain technology adoption: An investigation of challenges and expected value, Inf. Manage. 58 (2021) 103444, https://doi.org/10.1016/j.im.2021.103444.
[61] M. Pagani, Determinants of adoption of high speed data services in the business market: Evidence for a combined technology acceptance model with task technology fit model, Inf. Manage. 43 (2006) 847–860, https://doi.org/10.1016/j.im.2006.08.003.
[62] T.-C. Lin, C.-C. Huang, Understanding knowledge management system usage antecedents: An integration of social cognitive theory and task technology fit, Inf. Manage. 45 (2008) 410–417, https://doi.org/10.1016/j.im.2008.06.004.
[63] S. Cane, R. McCarthy, Analyzing the factors that affect information systems use: a task-technology fit meta-analysis, J. Comput. Inf. Syst. (2009).
[64] R.M. Fuller, A.R. Dennis, Does fit matter? The impact of task-technology fit and appropriation on team performance in repeated tasks, Inf. Syst. Res. 20 (2009) 2–17, https://doi.org/10.1287/isre.1070.0167.
[65] I. Zigurs, D. Khazanchi, From profiles to patterns: a new view of task-technology fit, Inf. Syst. Manag. 25 (2008) 8–13, https://doi.org/10.1080/10580530701777107.
[66] R.S. Rai, F. Selnes, Conceptualizing task-technology fit and the effect on adoption – A case study of a digital textbook service, Inf. Manage. 56 (2019) 103161, https://doi.org/10.1016/j.im.2019.04.004.
[67] P.J.Å. Owen Eriksson, Rethinking the meaning of identifiers in information infrastructures, J. Assoc. Inf. Syst. 11 (2010).
[68] P. Tammpuu, A. Masso, Transnational digital identity as an instrument for global digital citizenship: the case of Estonia's E-residency, Inf. Syst. Front. 21 (2019) 621–634, https://doi.org/10.1007/s10796-019-09908-y.
[69] E.A. Whitley, U. Gal, A. Kjaergaard, Who do you think you are? A review of the complex interplay between information systems, identification and identity, Eur. J. Inf. Syst. 23 (2014) 17–35, https://doi.org/10.1057/ejis.2013.34.
[70] G.A.W. Jennifer Xu, Complex problem solving_ identity matching based on social context, J. Assoc. Inf. Syst. 8 (2007) 525–545, https://doi.org/10.17705/1jais.00141.
[71] M. Ma, R. Agarwal, Through a glass darkly: information technology design, identity verification, and knowledge contribution in online communities, Inf. Syst. Res. 18 (2007) 42–67, https://doi.org/10.1287/isre.1070.0113.
[72] C. Bonina, K. Koskinen, B. Eaton, A. Gawer, Digital platforms for development: Foundations and research agenda, Inf. Syst. J. (2021), https://doi.org/10.1111/isj.12326.
[73] S. Madon, E. Schoemaker, Digital identity as a platform for improving refugee management, Inf. Syst. J. 31 (2021) 929–953, https://doi.org/10.1111/isj.12353.
[74] A. Addo, P.K. Senyo, Advancing E-governance for development: digital identification and its link to socioeconomic inclusion, Gov. Inf. Q. 38 (2021) 101568, https://doi.org/10.1016/j.giq.2021.101568.
[75] E. Schoemaker, D. Baslan, B. Pon, N. Dell, Identity at the margins: data justice and refugee experiences with digital identity systems in Lebanon, Jordan, and Uganda, Inf. Technol. Dev. 27 (2021) 13–36, https://doi.org/10.1080/02681102.2020.1785826.
[76] O. Ogbanufe, D.J. Kim, Comparing fingerprint-based biometrics authentication versus traditional authentication methods for e-payment, Decis. Support Syst. (2018), https://doi.org/10.1016/j.dss.2017.11.003.
[77] B. Otjacques, P. Hitzelberger, F. Feltz, Interoperability of E-Government Information Systems: Issues of Identification and Data Sharing, J. Manag. Inf. Syst. 23 (2007) 29–51, https://doi.org/10.2753/mis0742-1222230403.
[78] H. Xu, J. Chen, A.B. Whinston, Identity management and tradable reputation, MIS. Q. 42 (2018) 577–593, https://doi.org/10.25300/misq/2018/13634.
[79] S. Spiekermann, J. Korunovska, Towards a value theory for personal data, J. Inf. Technol. 32 (2017) 62–84, https://doi.org/10.1057/jit.2016.4.
[80] J.K. Sadeghi R, V.R. Prybutok, B. Sauser, Theoretical and practical applications of blockchain in healthcare information management, Inf. Manage. 59 (2022) 103649, https://doi.org/10.1016/j.im.2022.103649.
[81] A. Vance, P.B. Lowry, D. Eggett, Using accountability to reduce access policy violations in information systems, J. Manag. Inf. Syst. 29 (2014) 263–290, https://doi.org/10.2753/mis0742-1222290410.
[82] H. Li, S. Yoo, W.J. Kettinger, The roles of IT Strategies and Security Investments in reducing organizational security breaches, J. Manag. Inf. Syst. 38 (2021) 222–245, https://doi.org/10.1080/07421222.2021.1870390.
[83] C. Abdalla Mikhaeil, T.L. James, Examining the case of French hesitancy toward IDaaS solutions: Technical and social contextual factors of the organizational IDaaS privacy calculus, Inf. Manage. 60 (2023) 103779, https://doi.org/10.1016/j.im.2023.103779.
[84] C.P. Robert E. Crossler, Robbing peter to pay Paul_ surrendering privacy for security_s sake in an identity ecosystem, J. Assoc. Inf. Syst. 18 (2017) 487–516, https://doi.org/10.17705/1jais.00463.
[85] S. Zuboff, Big other: surveillance capitalism and the prospects of an information civilization, J. Inf. Technol. 30 (2015) 75–89, https://doi.org/10.1057/jit.2015.5.
[86] R. Medaglia, B. Eaton, J. Hedman, E.A. Whitley, Mechanisms of power inscription into IT governance: lessons from two national digital identity systems, Inf. Syst. J. (2021), https://doi.org/10.1111/isj.12325.
[87] K.C. Toth, A. Anderson-Priddy, Self-Sovereign Digital Identity: A Paradigm Shift for Identity, IEEE Secur. Priv. 17 (2019) 17–27, https://doi.org/10.1109/msec.2018.2888782.
[88] T. Rathee, P. Singh, A systematic literature mapping on secure identity management using blockchain technology, J. King Saud Univ. - Comput. Inf. Sci. (2021), https://doi.org/10.1016/j.jksuci.2021.03.005.
[89] A. Visvizi, H. Mora, E.G. Varela-Guzman, The case of rWallet: A blockchain-based tool to navigate some challenges related to irregular migration, Comput. Hum. Behav. 139 (2023) 107548, https://doi.org/10.1016/j.chb.2022.107548.
[90] M. Chanson, Efficient biometric-based identity management on the Blockchain for smart industrial applications, Pervasive Mob. Comput. 71 (2021) 101322, https://doi.org/10.1016/j.pmcj.2020.101322.
[91] S.S. Darnell, J. Sevilla, 3 stages of a pan-african identity framework for establishing self-sovereign identity with blockchain, Front. Blockchain 4 (2021) 9, https://doi.org/10.3389/fbloc.2021.631640.
[92] S. Figueroa-Lorenzo, J. Añorga Benito, S. Arrizabalaga, Modbus access control system based on SSI over Hyperledger fabric blockchain, Sensors 21 (2021) 5438, https://doi.org/10.3390/s21165438.
[93] B.C. Ghosh, V. Ramakrishna, C. Govindarajan, D. Behl, D. Karunamoorthy, E. Abebe, S. Chakraborty, IEEE, decentralized cross-network identity management for blockchain interoperation, in: 2021 IEEE Int. Conf. Blockchain Cryptocurrency, IEEE, NEW YORK, 2021, https://doi.org/10.1109/icbc51069.2021.9461064.
[94] A. Hoess, T. Roth, J. Sedlmeir, G. Fridgen, A. Rieger, With or without blockchain? Towards a decentralized, SSI-based eRoaming Architecture, in: HICSS-55, 2022, https://doi.org/10.24251/HICSS.2022.562.
[95] C. Lin, D. He, X. Huang, M. Khurram Khan, K.-K.R. Choo, A new transitively closed undirected graph authentication scheme for blockchain-based identity

management systems, IEEe Access. 6 (2018) 28203–28212, https://doi.org/10.1109/access.2018.2837650.
[96] S. Pal, T. Rabehaja, A. Hill, M. Hitchens, V. Varadharajan, On the integration of blockchain to the internet of things for enabling access right delegation, IEEe Internet. Things. J. 7 (2020) 2630–2639, https://doi.org/10.1109/jiot.2019.2952141.
[97] K.M. Sadique, R. Rahmani, P. Johannesson, IMSC-EIoTD: identity management and secure communication for edge IoT devices, Sensors 20 (2020) 6546, https://doi.org/10.3390/s20226546.
[98] N.D. Sarier, Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management, Comput. Secur. 105 (2021) 102243, https://doi.org/10.1016/j.cose.2021.102243.
[99] S.V. Sudarsan, O. Schelen, U. Bodin, Survey on delegated and self-contained authorization techniques in CPS and IoT, IEEe Access. 9 (2021) 98169–98184, https://doi.org/10.1109/access.2021.3093327.
[100] J. Xu, K. Xue, H. Tian, J. Hong, D.S.L. Wei, P. Hong, An identity management and authentication scheme based on redactable blockchain for mobile networks, IEEE Trans. Veh. Technol. 69 (2020) 6688–6698, https://doi.org/10.1109/tvt.2020.2986041.
[101] S. Friebe, I. Sobik, M. Zitterbart, Ieee, DecentID: Decentralized and privacy-preserving identity storage system using smart contracts, in: 17th IEEE Int. Conf. Trust Secur. Priv. Comput. Commun, NEW YORK, Ieee, 2018, pp. 37–42, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00016.
[102] K. Mudliar, H. Parekh, A comprehensive integration of national identity with blockchain technology, in: Proc. - 2018 Int. Conf. Commun. Inf. Comput. Technol. ICCICT 2018, Institute of Electrical and Electronics Engineers Inc., 2018, pp. 1–6, https://doi.org/10.1109/ICCICT.2018.8325891.
[103] X. Ren, F. Lin, Z. Chen, C. Tang, Z. Zheng, M. Li, BIA: a blockchain-based identity authorization mechanism, in: 2020 16th Int. Conf. Mobil. Sens. Netw. MSN, LOS ALAMITOS, IEEE Computer Soc, 2020, pp. 98–105, https://doi.org/10.1109/msn50589.2020.00031.
[104] A. Ghorbel, Accountable privacy preserving attribute-based access control for cloud services enforced using blockchain, Int. J. Inf. Secur. (2022), https://doi.org/10.1007/s10207-021-00565-4.
[105] B. Kim, W. Shin, D.-Y. Hwang, K.-H. Kim, Attribute-based access control(ABAC) with decentralized identifier in the blockchain-based energy transaction platform, in: 2021 Int. Conf. Inf. Netw. ICOIN, NEW YORK, Ieee, 2021, pp. 845–848, https://doi.org/10.1109/icoin50884.2021.9333894.
[106] M. Schanzenbach, T. Kilian, J. Schutte, C. Banse, ZKlaims: Privacy-preserving Attribute-based Credentials using Non-interactive Zero-knowledge Techniques, in: 16th Int. Jt. Conf. E-Bus. Telecommun. ICETE, Scitepress, SETUBAL, 2019, pp. 325–332, https://doi.org/10.5220/0007772903250332.
[107] X. Yang, W. Li, A zero-knowledge-proof-based digital identity management scheme in blockchain, Comput. Secur. 99 (2020) 102050, https://doi.org/10.1016/j.cose.2020.102050.
[108] H. Gunasinghe, A. Kundu, E. Bertino, H. Krawczyk, K. Singh, S. Chari, D. Su, M. Assoc Comp, PrivIdEx: privacy preserving and secure exchange of digital identity assets, in: WWW 19 World Wide Web Conf., Assoc Computing Machinery, NEW YORK, 2019, pp. 594–604, https://doi.org/10.1145/3308558.3313574.
[109] H. Halpin, Ieee, Nym credentials: privacy-preserving decentralized identity with blockchains, in: Crypto Val. Conf. Blockchain Technol. CVCBT, Ieee Computer Soc, LOS ALAMITOS, 2020, pp. 56–67, https://doi.org/10.1109/cvcbt50464.2020.00010.
[110] J. Sedlmeir, R. Smethurst, A. Rieger, G. Fridgen, Digital Identities and Verifiable Credentials, Bus. Inf. Syst. Eng 63 (2021) 603–613, https://doi.org/10.1007/s12599-021-00722-y.
[111] P. Szalachowski, Password-Authenticated Decentralized Identities, IEEE Trans. Inf. Forensics Secur. 16 (2021) 4801–4810, https://doi.org/10.1109/tifs.2021.3116429.
[112] W.J. Ao, S.J. Fu, C. Zhang, Y.Z. Huang, F. Xia, Ieee, A Secure Identity Authentication Scheme Based on Blockchain and Identity-based Cryptography, Ieee, NEW YORK, 2019, pp. 90–95.
[113] J. Isohanni, L. Goulden, K.M. Hermsen, M. Ross, J. Vanbockryck, Ieee, Disposable identities; enabling trust-by-design to build more sustainable data driven value, in: IEEE Int. Conf. Cyber Secur. Resil. IEEE CSR, NEW YORK, Ieee, 2021, pp. 378–383, https://doi.org/10.1109/csr51186.2021.9527950.
[114] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, J. Chen, A hybrid blockchain-based identity authentication scheme for multi-WSN, IEEE Trans. Serv. Comput. 13 (2020), https://doi.org/10.1109/tsc.2020.2964537, 1–1.
[115] T.X. Xie, Y. Zhang, K.K. Gai, L. Xu, Cross-Chain-Based Decentralized Identity for Mortgage Loans, in: 14th Int. Conf. Knowl. Sci. Eng. Manag. KSEM, Springer International Publishing Ag, CHAM, 2021, pp. 619–633, https://doi.org/10.1007/978-3-030-82153-1_51.
[116] J. Alsayed Kassem, S. Sayeed, H. Marco-Gisbert, Z. Pervez, K. Dahal, DNS-IdM: A blockchain identity management system to secure personal data sharing in a network, Appl. Sci. 9 (2019) 2953, https://doi.org/10.3390/app9152953.
[117] S. Cucko, M. Turkanovic, Decentralized and self-sovereign identity: systematic mapping study, IEEe Access. 9 (2021) 139009–139027, https://doi.org/10.1109/access.2021.3117588.
[118] R. Soltani, U.T. Nguyen, A.J. An, Ieee, practical key recovery model for self-sovereign identity based digital wallets, in: IEEE 17th Int Conf Dependable Auton. Secure Comp IEEE 17th Int Conf Pervas Intell. Comp IEEE 5th Int Conf Cloud Big Data Comp IEEE 4th Cyber Sci. Technol. Congr. DASCPiComCBDComCyberSciTech, Ieee Computer Soc, LOS ALAMITOS, 2019, pp. 320–325, https://doi.org/10.1109/DASC/PiCom/CBDCom/CyberSciTech.2019.00066.
[119] C. Patsonakis, K. Samari, A. Kiayias, M. Roussopoulos, On the practicality of a smart contract PKI, in: 1st IEEE Int. Conf. Decentralized Appl. Infrastruct, NEW YORK, Ieee, 2019, pp. 109–118, https://doi.org/10.1109/dappcon.2019.00022.
[120] A. Othman, J. Callahan, Ieee, the horcrux protocol: a method for decentralized biometric-based self-sovereign identity, in: Int. Jt. Conf. Neural Netw. IJCNN, NEW YORK, Ieee, 2018.
[121] M. Westerkamp, S. Gondor, A. Kupper, Tawki: towards self-sovereign social communication,, in: 1st IEEE Int. Conf. Decentralized Appl. Infrastruct. IEEE DAPPCON, NEW YORK, Ieee, 2019, pp. 29–38, https://doi.org/10.1109/dappcon.2019.00014.
[122] C.S. Sung, J.Y. Park, Understanding of blockchain-based identity management system adoption in the public sector, J. Enterp. Inf. Manag. 34 (2021) 1481–1505, https://doi.org/10.1108/jeim-12-2020-0532.
[123] R. Smethurst, Digital Identity Wallets and their Semantic Contradictions, in: ECIS-2023, 2023. https://aisel.aisnet.org/ecis2023_rp/288.
[124] Z. Li, A verifiable credentials system with privacy-preserving based on blockchain, J. Inf. Secur. 13 (2022) 43–65, https://doi.org/10.4236/jis.2022.132003.
[125] K.O. Asamoah, H. Xia, S. Amofa, O.I. Amankona, K.C. Luo, Q. Xia, J.B. Gao, X. J. Du, M. Guizani, Zero-chain: a blockchain-based identity for digital city operating system, IEEe Internet. Things. J. 7 (2020) 10336–10346, https://doi.org/10.1109/jiot.2020.2986367.
[126] J.H. Wang, S.J. Wei, H.Z. Liu, Decentralized identity authentication with trust distributed in blockchain backbone, in: 2019 Int. Conf. Blockchain ICBC, CHAM, Springer International Publishing Ag, 2019, pp. 202–210, https://doi.org/10.1007/978-3-030-23404-1_14.
[127] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan, S. Wang, An Identity Management System Based on Blockchain, in: 2017 15th Annu. Conf. Priv. Secur. Trust, Ieee Computer Soc, LOS ALAMITOS, 2017, pp. 44–53, https://doi.org/10.1109/pst.2017.00016.
[128] C.J. Bennett, C.D. Raab, The governance of privacy: Policy instruments in global perspective, Routledge (2017).
[129] National Research Council, Engaging privacy and information technology in a digital age, National Academies Press, 2007.
[130] M. Wiener, M. Mähring, U. Remus, C. Saunders, W.A. Cram, Moving is project control research into the digital era: the "Why" of control and the concept of control purpose, Inf. Syst. Res. 30 (2019) 1387–1401, https://doi.org/10.1287/isre.2019.0867.
[131] S. Lim, M.-H. Rhie, D. Hwang, K.-H. Kim, A subject-centric credential management method based on the verifiable credentials, in: 2021 Int. Conf. Inf. Netw. ICOIN, NEW YORK, Ieee, 2021, pp. 508–510, https://doi.org/10.1109/icoin50884.2021.9333857.
[132] A.J. Zwitter, O.J. Gstrein, E. Yap, Digital Identity and the Blockchain: Universal Identity Management and the Concept of the "Self-Sovereign" Individual, Front. Blockchain 3 (2021) 14, https://doi.org/10.3389/fbloc.2020.00026.
[133] A.F. Westin, Privacy and freedom, Wash. Lee Law Rev. 25 (1968) 166.
[134] P. Constantinides, O. Henfridsson, G.G. Parker, Introduction—platforms and Infrastructures in the Digital Age, Inf. Syst. Res. 29 (2018) 381–400, https://doi.org/10.1287/isre.2018.0794.
[135] A. Ghazawneh, O. Henfridsson, Balancing platform control and external contribution in third-party development: the boundary resources model, Inf. Syst. J. 23 (2013) 173–192, https://doi.org/10.1111/j.1365-2575.2012.00406.x.
[136] D. Tilson, K. Lyytinen, C. Sørensen, Research commentary—digital infrastructures: the missing IS research agenda, Inf. Syst. Res. 21 (2010) 748–759, https://doi.org/10.1287/isre.1100.0318.
[137] Jong-Hyouk Lee, BIDaaS: blockchain based ID as a service, , IEEe Access. 6 (2018) 2274–2278, https://doi.org/10.1109/access.2017.2782733.
[138] R. Belchior, B. Putz, G. Pernul, M. Correia, A. Vasconcelos, S. Guerreiro, SSIBAC: self-sovereign identity based access control, in: 19th IEEE Int. Conf. Trust Secur. Priv. Comput. Commun, LOS ALAMITOS, Ieee Computer Soc, 2020, pp. 1935–1943, https://doi.org/10.1109/TrustCom50675.2020.00264.
[139] R. Ansay, J. Kempf, O. Berzin, C. Xi, I. Sheikh, Ieee, gnomon: decentralized identifiers for Securing 5G IoT device registration and software update, in: IEEE Glob. Commun. Conf, NEW YORK, Ieee, 2019.
[140] A. Dixit, W. Asif, M. Rajarajan, Ieee, smart-contract enabled decentralized identity management framework for industry 4.0. 46th Annu. Conf, IEEE-Ind.-Electron.-Soc., Ieee, NEW YORK, 2020, pp. 2221–2227.
[141] D. Siddarth, S. Ivliev, S. Siri, P. Berman, Who watches the watchmen? A review of subjective approaches for sybil-resistance in proof of personhood protocols, Front. Blockchain 3 (2020) 16, https://doi.org/10.3389/fbloc.2020.590171.
[142] J. Lauinger, J. Ernstberger, E. Regnath, M. Hamad, S. Steinhorst, A-PoA: anonymous proof of authorization for decentralized identity management, in: 2021 IEEE Int. Conf. Blockchain Cryptocurrency, IeeeNEW YORK, 2021, https://doi.org/10.1109/icbc51069.2021.9461082.
[143] A. Norta, R. Matulevičius, B. Leiding, Safeguarding a formalized Blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns, Comput. Secur. 86 (2019) 253–269, https://doi.org/10.1016/j.cose.2019.05.017.
[144] K. Pinter, D. Schmelz, R. Lamber, S. Strobl, T. Grechenig, Towards a multi-party, blockchain-based identity verification solution to implement clear name laws for online media platforms, in: Blockchain Forum Cent. East. Eur. Forum CEE Forum 17th Int. Conf. Bus. Process Manag. BPM, CHAM, Springer International Publishing Ag, 2019, pp. 151–165, https://doi.org/10.1007/978-3-030-30429-4_11.

[145] X. Xiang, M. Wang, W. Fan, A permissioned blockchain-based identity management and user authentication scheme for E-health systems, IEEe Access. 8 (2020) 171771–171783, https://doi.org/10.1109/access.2020.3022429.
[146] H. Li, L. Zhu, M. Shen, F. Gao, X. Tao, S. Liu, Blockchain-Based Data Preservation System for Medical Data, J. Med. Syst. 42 (2018) 13, https://doi.org/10.1007/s10916-018-0997-3.
[147] L. Argento, F. Buccafurri, A. Furfaro, S. Graziano, A. Guzzo, G. Lax, F. Pasqua, D. Saccà, ID-service: a blockchain-based platform to support digital-identity-aware service accountability, Appl. Sci. 11 (2021) 165, https://doi.org/10.3390/app11010165.
[148] S. Galanti, Ç.Y. Özsoy, Can blockchain help improve financial inclusion? A comparative study, J. Econ. Issues 57 (2023) 438–449, https://doi.org/10.1080/00213624.2023.2200650.
[149] S. Terzi, C. Savvaidis, A. Sersemis, K. Votis, D. Tzovaras, Decentralizing identity management and vehicle rights delegation through self-sovereign identities and blockchain, in: 45th Annu. Int. IEEE-Comput.-Soc. Comput. Softw. Appl. Conf. COMPSAC, LOS ALAMITOS, Ieee Computer Soc, 2021, pp. 1217–1223, https://doi.org/10.1109/compsac51774.2021.00168.
[150] N. Kshetri, Blockchain's roles in strengthening cybersecurity and protecting privacy, Telecommun. Policy 41 (2017) 1027–1038, https://doi.org/10.1016/j.telpol.2017.09.003.
[151] Mohamed Tahar Hammi, B. Hammi, P. Bellot, A. Serhrouchni, T.C. Schmidt, G. Hege, M. Wählisch, H.L. Cycon, M. Palkow, D. Marpe, Bubbles of trust: a decentralized blockchain-based authentication system for IoT, Comput. Secur. 78 (2018) 126–142, https://doi.org/10.1016/j.cose.2018.06.004.
[152] C. DeCusatis, L. Kulvinder, Secure Ieee, Decentralized Energy Resource Management using the Ethereum Blockchain, in: 17th IEEE Int. Conf. Trust Secur. Priv. Comput. Commun, NEW YORK, ieee, 2018, pp. 1907–1913, https://doi.org/10.1109/TrustCom/BigDataSE.2018.00290.
[153] A.S. Patil, R. Hamza, A. Hassan, N. Jiang, H. Yan, J. Li, Efficient privacy-preserving authentication protocol using PUFs with blockchain smart contracts, Comput. Secur. 97 (2020) 101958, https://doi.org/10.1016/j.cose.2020.101958.
[154] Z. Lu, W. Liu, Q. Wang, G. Qu, Z. Liu, A Privacy-Preserving Trust Model Based on Blockchain for VANETs, IEEe Access. 6 (2018), https://doi.org/10.1109/access.2018.2864189.
[155] A. Gruner, A. Muhle, T. Gayvoronskaya, C. Meinel, A Quantifiable, Trust model for blockchain-based identity management, in: 2018 IEEE Int. Conf. Internet Things IThings IEEE Green Comput. Commun. GreenCom IEEE Cyber Phys. Soc. Comput. CPSCom IEEE Smart Data SmartData, NEW YORK, Ieee, 2018, pp. 1475–1482, https://doi.org/10.1109/Cybermatics_2018.2018.00250.
[156] G. Ra, T. Kim, I. Lee, VAIM: verifiable anonymous identity management for human-centric security and privacy in the internet of things, IEEe Access. 9 (2021) 75945–75960, https://doi.org/10.1109/access.2021.3080329.
[157] A. Jamal, R.A.A. Helmi, A.S.N. Syahirah, M.A. Fatima, Ieee, blockchain-based identity verification system, in: 9th IEEE Int. Conf. Syst. Eng. Technol. ICSET, NEW YORK, Ieee, 2019, pp. 253–257.
[158] M.A. Bouras, Q. Lu, S. Dhelim, H. Ning, A lightweight blockchain-based IoT identity management approach, Future Internet. 13 (2021) 24, https://doi.org/10.3390/fi13020024.
[159] M. Chanson, M. Chanson, A. Bogner, ETH Zurich, D.Bilgeri Switzerland, ETH Zurich, E.Fleisch Switzerland, ETH Zurich /University of St. Gallen, Switzerland, F. Wortmann, University of St. Gallen, Switzerland, Blockchain for the IoT: Privacy-Preserving Protection of Sensor Data, J. Assoc. Inf. Syst. 6 (2018) 1272–1307, https://doi.org/10.17705/1jais.00567.
[160] K. Christidis, M. Devetsikiotis, Blockchains and smart contracts for the internet of things, IEEe Access. 4 (2016) 2292–2303, https://doi.org/10.1109/ACCESS.2016.2566339.
[161] I. Mistry, S. Tanwar, S. Tyagi, N. Kumar, Blockchain for 5G-enabled IoT for industrial automation: A systematic review, solutions, and challenges, Mech. Syst. Signal Process. 135 (2020), https://doi.org/10.1016/j.ymssp.2019.106382.
[162] G. Ali, N. Ahmad, Y. Cao, M. Asif, H. Cruickshank, Q.E. Ali, Blockchain based permission delegation and access control in internet of things (BACI), Comput. Secur. 86 (2019) 318–334, https://doi.org/10.1016/j.cose.2019.06.010.
[163] M. Saqib, A.H. Moon, A systematic security assessment and review of internet of things in the context of authentication, Comput. Secur. 125 (2023) 103053, https://doi.org/10.1016/j.cose.2022.103053.
[164] Y. Chen, Y.Z. Wang, Y. Wang, M.X. Li, G.C. Dong, C. Liu, CallChain: identity authentication based on blockchain for telephony networks, in: 24th IEEE Int. Conf. Comput. Support. Coop. Work Des., NEW YORK, Ieee, 2021, pp. 416–421, https://doi.org/10.1109/cscwd49262.2021.9437650.
[165] H. Liu, P.F. Zhang, G.G. Pu, T. Yang, S. Maharjan, Y. Zhang, Blockchain empowered cooperative authentication with data traceability in vehicular edge computing, IEEE Trans. Veh. Technol. 69 (2020) 4221–4232, https://doi.org/10.1109/tvt.2020.2969722.
[166] R. Yang, M.H. Au, Q. Xu, Z. Yu, Decentralized blacklistable anonymous credentials with reputation, Comput. Secur. 85 (2019) 353–371, https://doi.org/10.1016/j.cose.2019.05.009.
[167] C. Anderson, A. Carvalho, M. Kaul, J.W. Merhout, Blockchain innovation for consent self-management in health information exchanges, Decis. Support Syst. (2023) 114021, https://doi.org/10.1016/j.dss.2023.114021.
[168] A.M. Al-Khouri, Digital identity: Transforming GCC economies, Innovation 16 (2014) 184–194. https://doi.org/10.1080/14479338.2014.11081981.
[169] A. Russo, G. Lax, B. Dromard, M. Mezred, A System to access online services with minimal personal information disclosure, Inf. Syst. Front. 24 (2022) 1563–1575, https://doi.org/10.1007/s10796-021-10150-8.
[170] M.S. Ferdous, U. Cali, U. Halden, W. Prinz, Leveraging self-sovereign identity & distributed ledger technology in renewable energy certificate ecosystems, J. Clean. Prod. 422 (2023) 138355, https://doi.org/10.1016/j.jclepro.2023.138355.
[171] H. Xu, X. Zhang, Q. Cui, X. Tao, C. Pujari, B. Muniyal, B CC, A. Rao, V. Sadiname, M. Rajarajan, Identity resilience in the digital health ecosystem: a key recovery-enabled framework, Comput. Biol. Med. 167 (2023) 107702, https://doi.org/10.1016/j.compbiomed.2023.107702.
[172] C. Wang, S. Wang, X. Cheng, Y. He, K. Xiao, S. Fan, A privacy and efficiency-oriented data sharing mechanism for IoTs, IEEE Trans. Big Data 9 (2023) 174–185, https://doi.org/10.1109/TBDATA.2022.3148181.
[173] J. Yin, Y. Xiao, Q. Pei, Y. Ju, L. Liu, M. Xiao, C. Wu, SmartDID: A Novel Privacy-Preserving Identity Based on Blockchain for IoT, IEEe Internet. Things. J. 10 (2023) 6718–6732, https://doi.org/10.1109/JIOT.2022.3145089.
[174] M.A. Bouras, Q.H. Lu, F. Zhang, Y.L. Wan, T. Zhang, H.S. Ning, Distributed ledger technology for ehealth identity privacy: state of the art and future perspective, Sensors 20 (2020) 20, https://doi.org/10.3390/s20020483.
[175] S. Masiero, V. Arvidsson, Degenerative outcomes of digital identity platforms for development, Inf. Syst. J. 31 (2021) 903–928, https://doi.org/10.1111/isj.12351.
[176] U. Schultze, Performing embodied identity in virtual worlds, Eur. J. Inf. Syst. 23 (2014) 84–95, https://doi.org/10.1057/ejis.2012.52.
[177] A. Martin, L. Taylor, Exclusion and inclusion in identification: regulation, displacement and data justice, Inf. Technol. Dev. 27 (2021) 50–66, https://doi.org/10.1080/02681102.2020.1811943.
[178] S. Masiero, S. Bailur, Digital identity for development: the quest for justice and a research agenda, Inf. Technol. Dev. 27 (2020) 1–12, https://doi.org/10.1080/02681102.2021.1859669.
[179] X. Zhou, D. He, M.K. Khan, W. Wu, K.-K.R. Choo, S. Huh, M. Shim, J. Lee, S. S. Woo, H. Kim, H. Lee, DID we miss anything?: Towards privacy-preserving decentralized ID architecture, IEEE Trans. Dependable Secure Comput 20 (2023) 4881–4898, https://doi.org/10.1109/TDSC.2023.3235951.
[180] Y. Lu, J. Zhang, Y. Qi, S. Qi, Y. Li, H. Song, Y. Liu, Safety warning! Decentralised and automated incentives for disqualified drivers auditing in ride-hailing services, IEEE Trans. Mob. Comput. 22 (2023) 1748–1762, https://doi.org/10.1109/TMC.2021.3108012.
[181] E.S. Fathalla, M. Azab, C. Xin, H. Wu, PT-SSIM: A Proactive, Trustworthy self-sovereign identity management system, IEEE Internet. Things. J. 10 (2023) 17155–17169, https://doi.org/10.1109/JIOT.2023.3273988.
[182] L. Weigl, T. Barbereau, G. Fridgen, The construction of self-sovereign identity: Extending the interpretive flexibility of technology towards institutions, Gov. Inf. Q. 40 (2023) 101873, https://doi.org/10.1016/j.giq.2023.101873.
[183] M. Hesse, T. Teubner, Reputation portability - quo vadis? Electron. Mark. 30 (2020) 331–349, https://doi.org/10.1007/s12525-019-00367-6.
[184] W. Du, H. Liu, G. Luo, J. Zhang, W. Xu, A Consortium blockchain-enabled evidence sharing system for public interest litigation, J. Glob. Inf. Manag. 31 (2023) 1–19, https://doi.org/10.4018/JGIM.330422.
[185] Y. Zhuang, C.-R. Shyu, S. Hong, P. Li, L. Zhang, Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology, Comput. Biol. Med. 157 (2023) 106778, https://doi.org/10.1016/j.compbiomed.2023.106778.
[186] J. Alupotha, Double-blind proof of existence for decentralized identities, IEEe Access. 11 (2023) 132180–132195, https://doi.org/10.1109/ACCESS.2023.3336410.
[187] K. Yang, Z. Zhang, T. Youliang, J. Ma, A Secure authentication framework to guarantee the traceability of avatars in metaverse, IEEE Trans. Inf. Forensics Secur. 18 (2023) 3817–3832, https://doi.org/10.1109/TIFS.2023.3288689.
[188] M. Popa, S.M. Stoklossa, S. Mazumdar, ChainDiscipline - towards a blockchain-IoT-based self-sovereign identity management framework, IEEE Trans. Serv. Comput. 16 (2023) 3238–3251, https://doi.org/10.1109/TSC.2023.3279871.
[189] Y. Chi, H. Duan, W. Cai, Z.J. Wang, V.C.M. Leung, Networking parallel Web3 metaverses for interoperability, IEEE Netw. 37 (2023) 34–41, https://doi.org/10.1109/MNET.2023.3320660.
[190] T. Guggenberger, D. Kühne, V. Schlatt, N. Urbach, Designing a cross-organizational identity management system: Utilizing SSI for the certification of retailer attributes, Electron. Mark. (2023) 33, https://doi.org/10.1007/s12525-023-00620-z.
[191] X. Li, T. Jing, R. Li, H. Li, X. Wang, D. Shen, BDRA: Blockchain and decentralized identifiers assisted secure registration and authentication for VANETs, IEEe Internet. Things. J. 10 (2023) 12140–12155, https://doi.org/10.1109/JIOT.2022.3164147.
[192] H. Halpin, in: Acm, NEXTLEAP: Decentralizing Identity with Privacy for Secure Messaging, in: 12th Int. Conf. Availab. Reliab. Secur., Assoc Computing Machinery, NEW YORK, 2017, https://doi.org/10.1145/3098954.3104056.
[193] R. Xiong, W. Ren, X. Hao, J. He, K.-K.R. Choo, BDIM: A Blockchain-Based Decentralized Identity Management Scheme for Large Scale Internet of Things, IEEe Internet. Things. J. 10 (2023) 22581–22590, https://doi.org/10.1109/JIOT.2023.3303922.
[194] K.P. Jørgensen, R. Beck, Universal Wallets, Bus. Inf. Syst. Eng. 64 (2022) 115–125, https://doi.org/10.1007/s12599-021-00736-6.
[195] L. Cocco, R. Tonelli, M. Marchesi, Blockchain and Self Sovereign Identity to Support Quality in the Food Supply Chain, Future Internet. 13 (2021) 301, https://doi.org/10.3390/fi13120301.
[196] T.T.M. Eddy, B.B. Georges, N.E.P. Salomon, Towards a New Model for the Production of Civil Status Records Using Blockchain, J. Inf. Secur. 14 (2022) 52–75, https://doi.org/10.4236/jis.2023.141005.

[197] M. Nuss, A. Puchta, M. Kunz, Towards blockchain-based identity and access management for internet of things in enterprises, in: 15th Int. Conf. Trust Priv. Secur. Digit. Bus. Trust, CHAM, Springer International Publishing Ag, 2018, pp. 167–181, https://doi.org/10.1007/978-3-319-98385-1_12.
[198] D.D.F. Maesa, A. Lisi, P. Mori, L. Ricci, G. Boschi, Self sovereign and blockchain based access control: Supporting attributes privacy with zero knowledge, J. Netw. Comput. Appl. 212 (2023) 103577, https://doi.org/10.1016/j.jnca.2022.103577.
[199] S. Bag, M.A. Azad, F. Hao, A privacy-aware decentralized and personalized reputation system, Comput. Secur. 77 (2018) 514–530, https://doi.org/10.1016/j.cose.2018.05.005.
[200] J.Parra Moyano, O. Ross, KYC optimization using distributed ledger technology, Bus. Inf. Syst. Eng. 59 (2017) 411–423, https://doi.org/10.1007/s12599-017-0504-2.
[201] B. Faber, G.C. Michelet, N. Weidmann, R.R. Mukkamala, R. Vatrapu, BPDIMS:A Blockchain-based Personal Data and Identity Management System, in: HICSS-52, 2019, https://doi.org/10.24251/HICSS.2019.821.
[202] G. Ishmaev, Sovereignty, privacy, and ethics in blockchain-based identity management systems, Ethics Inf. Technol. 23 (2021) 239–252, https://doi.org/10.1007/s10676-020-09563-x.
[203] J. Sedlmeir, J. Lautenschlager, G. Fridgen, N. Urbach, The transparency challenge of blockchain in organizations, Electron. Mark. 32 (2022) 1779–1794, https://doi.org/10.1007/s12525-022-00536-0.
[204] W. Shao, C. Jia, Y. Xu, K. Qiu, Y. Gao, Y. He, AttriChain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain, Comput. Secur. 99 (2020) 102069, https://doi.org/10.1016/j.cose.2020.102069.
[205] V. Vasylkovskyi, S. Guerreiro, J. Sequeira, Designing and Validating a Blockchain-based Architecture to Enforce Privacy in Human Robot Interaction, in: HICSS-54, 2021, https://doi.org/10.24251/HICSS.2021.069.
[206] V. Schlatt, J. Sedlmeir, S. Feulner, N. Urbach, Designing a framework for digital KYC processes built on blockchain-based self-sovereign identity, Inf. Manage 59 (2022) 103553, https://doi.org/10.1016/j.im.2021.103553.
[207] R.L. Baskerville, M.D. Myers, Y. Yoo, Digital First: the ontological reversal and new challenges for information systems research, MIS. Q. 44 (2020) 509–523, https://doi.org/10.25300/misq/2020/14418.
[208] R.L. Baskerville, M.D. Myers, Reconceptualizing users: The roles and activities of people as they engage with digital technologies, J. Inf. Technol. (2023) 02683962231183455, https://doi.org/10.1177/02683962231183455.

Zhiyue Yan is a Ph.D. Candidate in the School of Management at Xi'an Jiaotong University, China. Her main research interests are platform economy, applications of blockchain, and digital identity management.

Xi Zhao is a Professor of Information Systems at the School of Management, Xi'an Jiaotong University, China. He received his Ph.D. degree in Computer Science from the Ecole Centrale de Lyon, France. He was a Research Assistant Professor in the Department of Computer Science, University of Houston. His research interests include blockchain platform and behavior computing. His research has been published in *Journal of Operations Management, Information Systems Research, IEEE Transactions on Pattern Analysis and Machine Intelligence, IEEE Transactions on Knowledge and Data Engineering*, etc.

Yang (Alison) Liu is an Associate Professor of Information Systems and Intelligent Business at Xi'an Jiaotong University. She received her Ph.D. in Information Sytems and Analytics from National University of Singapore. Her main research interests are digital economy, human-computer interaction, online consumer behavior, and business applications of AI. Her work has been published in leading IS/Business journals, including *Information Systems Research, Journal of Management Information Systems,* and *Journal of the Association for Information Systems*. She has served as track chair and associate editor for prominent international conferences in the field of information systems (e.g. ICIC and PACIS), and as an anonymous reviewer for MIS Quarterly, Information Systemes Research, Journal of Management Information Systems, etc.

Xin (Robert) Luo is a Special Assistant to the Dean for Research Advancement, an Endowed Dean's Professor of Research Excellence, and a Distinguished Professor of Management Information Systems and Information Assurance at the Anderson School of Management of the University of New Mexico, Albuquerque, USA. He received his Ph.D. in Information Systems from Mississippi State University, USA. His research has been published in leading IS/ business journals, including the *Information Systems Research, Journal of Operations Management, Production and Operations Management, Journal of Management Information Systems, Journal of the Association for Information Systems, European Journal of Information Systems, Information Systems Journal, Journal of Strategic Information Systems, Journal of Information Technology, Decision Sciences, Decision Support Systems, Information & Management*, and *IEEE Transactions on Engineering Management*. He has served as an ad hoc Associate Editor for *MIS Quarterly* and an Associate Editor for the *European Journal of Information Systems*, and currently serves as a Guest AE for the *Journal of Management Information Systems* and an Associate Editor for the *Journal of the Association for Information Systems, Decision Sciences, Decision Support Systems, Information & Management, Electronic Commerce Research*, and the *Journal of Electronic Commerce Research*. He also sits on the Editorial Review Board of *Information Systems Research*. His research interests center around behavioral information systems security management and privacy protection, innovative technologies for strategic decision-making, and cross-cultural IT management. He is the Co-Editor-in-Chief of the *International Journal of Accounting and Information Management*.