SoK: A Taxonomy for Distributed-Ledger-Based Identity Management

Awid Vaziry, Sandro Rodriguez Garzon, Patrick Herbke, Carlo Segat, Axel Küpper

Service-centric Networking

Technische Universität Berlin / T-Labs

Berlin, Germany

{vaziry}|{sandro.rodriguezgarzon}|{p.herbke}|{carlo.segat}|{axel.kuepper}@tu-berlin.de

Abstract—The intersection of blockchain (distributed ledger) and identity management lacks a comprehensive architectural framework for classifying distributed-ledger-based identity solutions. This paper presents a methodologically developed taxonomy from analyzing 390 scientific papers and expert discussions. The resulting artifact comprises 22 dimensions with 113 characteristics organized into three groups: trust anchor implementations, identity architectures (identifiers and credentials), and ledger specifications. The taxonomy enables systematic analysis, comparison, and design of distributed-ledger-based identity solutions, as demonstrated through application to two distinct architectures. As the first methodology-driven taxonomy in this domain, this work advances standardization and enhances understanding of distributed-ledger-based identity architectures, providing researchers and practitioners with a structured framework for evaluating design decisions and implementation approaches.

Index Terms—Distributed Ledger Technology, Blockchain, Identity Management, Taxonomy, Literature Review

I. INTRODUCTION

UTILIZING blockchains and distributed ledgers for digital identities in future identity management (IDM) systems promises better trust, security, user control over personal data [1]. Yet, limited standardization, interoperability, and poor user experience of current solutions continue to hinder the widespread adoption of secure ledger-based identity systems [2].

Various research efforts, such as those by *Schardong et al.* [3] and *Lesavre et al.* [4] aim to conceptualize the current landscape of blockchain-enabled IDM solutions. However, from an architectural point of view, there is a lack of a holistic and unified conceptual framework to characterize and assess those solutions. This impedes effective communication and collaboration among researchers and application developers. To improve the organization of this field and to promote greater consistency and standardization, it is essential to organize and structure knowledge in the area of distributed-ledger-based IDM solutions with a focus on architectural design.

In this paper, we present the first comprehensive taxonomy for system architectures of distributed-ledger-based identity solutions, systematically organizing relevant characteristics to guide researchers and practitioners. Inspired by *Glass et al.* [5], a taxonomy is defined as a system of groupings that organizes and categorizes knowledge of a field, enabling researchers to study relationships between concepts, hypothesize about new ideas, and evaluate existing architectures. We employ a rigorous, iterative approach following the established guidelines of *Nickerson et al.* [6] and *Kundisch et al.* [7]. Our taxonomy emerges from an extensive analysis of 390 scientific papers from the field and insights from multiple expert discussion panels, with a special focus on the architectural

aspects of IDM solutions leveraging Distributed Ledger Technology (DLT). The resulting artifact comprises 22 dimensions with 113 characteristics, refined through three methodical iterations. To validate the taxonomy's practical utility and analytical power, we apply it exemplarily to two representative system architectures. It effectively classifies the solutions, highlighting key design decisions and potential shortcomings that might otherwise remain overlooked.

The article starts with a discussion of blockchain and IDM fundamentals in Section II, followed by a review of relevant taxonomies in Section III. The taxonomy's development methodology is presented in Section IV, while the taxonomy itself and its evaluation are detailed in Sections V and VII. Limitations and conclusions are discussed in Sections VIII and IX.

II. BACKGROUND

This section discusses the technical and theoretical concepts of blockchain, digital identity. It explores key identity-related terminology, decentralized identity frameworks, and DLTs, providing a foundation for this work

A. Identity Concepts and Terminology

Identity is defined by the International Organization for Standardization (ISO) as a "*set of attributes related to an entity*" [8], where an entity may be a person, organization, server, application, or service [9]. Building on this, we define identity as a collection of characteristic attributes that uniquely describe a physical or non-physical being within a specific system. Digital identity extends this concept to digital realm. Inspired by the definitions given by NIST [10], Domingo et al. [11], and Sedlmeir et al. [12], we define digital identity as a digital collection of attributes uniquely describing a physical or non-physical being within a specific system, enabling participation within this specific system and responding to identity-related transactions. IDM encompasses then the processes and technologies to create, manage, and authenticate identities. Key elements include identifiers (unique labels for digital identities), authentication (verification of identity control), authenticators (verification tools), and authorization (managing access) [9], [10].

B. Decentralized Digital Identity

User-centric identity systems have gained momentum in recent years [2], [13], driven by the privacy-preserving paradigm of Self-Sovereign Identity (SSI), alongside the technical concepts of Decentralized Identifiers (DIDs) [14], and Verifiable Credentials (VCs) [15]. SSI proclaims a system design that empowers individuals to control their digital identities without relying on central authorities by leveraging distributed ledgers for secure verification [1]. DIDs provide unique identification in a decentralized manner, resolving to DID documents containing metadata, cryptographic keys, and service endpoints. The DID documents of public DIDs are stored in verifiable data registries such as distributed ledgers, while their counterparts of private DIDs are derived from the identifier. VCs contain claims about a subject, must include the subject's identifier (often a DID), and are signed by an issuer to ensure integrity and non-repudiation. Holders can generate Verifiable Presentations (VPs) from VCs to selectively share verified information [10], [15].

C. Identity Roles and Trust Relationships

The issuer-holder-verifier model is fundamental to all decentralized identity frameworks. Issuers create and sign VCs about subjects. Holders (often the subjects themselves) control these VCs and determine when and with whom to share them through VPs. Verifiers authenticate the presented VPs, confirming their validity and provenance [15]. Traditional federated identity models operate with different roles. Identity Providers (IdPs) manage identity information and issue assertions about users. Relying Parties (RPs) or service providers trust these IdPs to verify user identities and validate assertions [16]. These established trust relationships form the foundation of identity transactions across both traditional and decentralized systems. Central to these are trust anchors which are fundamental elements that serve as the basis to establish trust in

identity systems. Trust anchors enable verification of credentials and assertions without requiring direct trust relationships between all entities. In traditional PKI systems, certificate authorities typically serve as trust anchors. In distributed ledger-based identity systems, trust anchors may include the distributed ledger itself, governance frameworks, or cryptographic keys registered on the ledger [14], [16].

D. Distributed Ledger Technology

DLT enables the maintenance of append-only transactional databases in a decentralized manner. Blockchain, the most prominent DLT implementation, secures data by bundling transactions into cryptographically linked blocks. This concept was introduced for the Bitcoin cryptocurrency [17], while Ethereum extended it with smart contracts for programmable transactions [18]. DLT networks are categorized by their permission models. Permissioned networks restrict who can read, write, and host nodes, typically governed by a single entity or a consortium [19]. Permissionless networks allow anyone to participate but they often require transaction fees to prevent spam and to compensate node operators. These fees, denominated in units like "gas" in Ethereum, create resource constraints that impact performance [20]. For IDM, DLT provides promising capabilities including immutable record-keeping and secure sharing of verification material, without a single point of failure. These properties address fundamental challenges in traditional IDM systems, particularly regarding security, privacy, and user control.

III. RELATED WORK

Various taxonomies have addressed DLT in combination with IDM in academic literature. *Lesavre et al.* [4] categorized DLT-based IDM systems based on architectures and governance models, emphasizing terminology and emerging standards. Yet, their work lacks a taxonomy with explicit dimensions and characteristics. *Schardong et al.* [3] conducted a structured literature review of over 80 articles on SSI, creating a hierarchical taxonomy. While contributing significantly to SSI research, their work did not explicitly address DLT-based solutions and used a tree-like structure rather than a dimensional framework. *Ngo et al.* [21] analyzed 361 articles on IDM with blockchain, focusing on research trends and metadata rather than architectural classification. *Amard et al.* [22] developed a taxonomy examining governance choices in digital identity infrastructures, using Nickerson's methodology but with a different analytical lens than our architectural design focus. *Yan et al.* [13] conducted a comprehensive interdisciplinary review of decentralized IDM, analyzing 149 articles to develop a "Task Structure-Technological Properties-Fit" framework. Their work identified two key task goals (identity value creation and maintenance), three stakeholder levels, and two technological properties (interoperability and self-sovereignty). While their framework provides valuable insights into the alignment between tasks and technologies, it focuses on the application of decentralized IDM across contexts rather than an architectural classification.

Existing taxonomies address specific sub-fields of DLT-based IDM, but their scope remains insufficient for categorizing contemporary solutions. Our research bridges this gap through a comprehensive methodology combining extensive literature review with expert consultations. The resulting framework enables systematic classification, analysis, and evaluation of DLT-based IDM architectures, advancing both theoretical understanding and practical implementation in this domain.

IV. METHODOLOGY

A taxonomy should be concise yet robust, comprehensive, expandable, and explanatory [6], [7]. Conciseness requires limited dimensions and characteristics, while robustness ensures sufficient differentiation of the objects of interest. Comprehensiveness demands classification of all known objects within the domain, and extendibility allows for the inclusion of new dimensions as the field evolves. The explanatory nature provides clear descriptions that enhance understanding

rather than merely listing features. The taxonomy development process presented here follows an iterative approach guided by a meta-characteristic that defines the taxonomy's focus and scope.

A. Problem and Objectives

In DLT-based IDM, solutions range from fully on-chain systems to those with minimal blockchain integration. However, there is no structured method to assess and compare these solutions, particularly regarding critical aspects such as trust sources, governance frameworks, and credential management. Researchers and practitioners developing these solutions often fail to report key dimensions of the architecture, hindering comprehensive evaluation and comparison. This taxonomy addresses this gap by providing a classification framework for researchers and practitioners, enabling effective communication and comparison of system architectures.

B. Meta-Characteristic and Approach

The meta-characteristic serves as the fundamental lens through which the phenomenon is observed and classified, guiding the selection of all dimensions and characteristics in the taxonomy. After careful consideration of the research objectives and target users, the meta-characteristic is defined as: **System Architectures of IDM Solutions utilizing Distributed Ledger Technology**.

C. Ending Conditions and Evaluation Goals

The taxonomy development follows Nickerson's methodology [6], employing eight objective conditions (covering completeness, consistency, uniqueness, and utility) and five subjective conditions (addressing conciseness, robustness, comprehensiveness, extendibility, and explanatory power). These conditions determine when the iterative development concludes. The taxonomy aims to provide a comprehensive framework spanning the complete spectrum of DLT-based IDM solutions while facilitating conceptual comparability through systematic classification of fundamental architectural components.

The evaluation criteria for the taxonomy are defined as: *Provision of a comprehensive taxonomy encompassing the complete spectrum of DLT-based IDM solutions* and *Facilitation of conceptual comparability through the identification and classification of fundamental architectural components*.

V. TAXONOMY DEVELOPMENT

This section describes the iterative development process for creating the taxonomy. The approach was structured and included a literature review, discussions with an expert panel, and validation against established taxonomies. Figure 1 illustrates the development and evaluation process.

A. Literature-Based Development (Iteration 1)

The first iteration followed an empirical-to-conceptual approach through a structured literature review. The search used the terms "blockchain" OR "distributed ledger" AND "identity" in publication titles across five databases (IEEE Xplore, SpringerLink, ACM Digital Library, Wiley Online Library, Science Direct) in October 2024. After removing duplicates, 440 articles were identified.

A categorization process was applied to organize the literature into coherent groups, resulting in the classification shown in Table I. The 51 articles in the "surveys and reviews" category were set aside for later analysis, while the remaining 390 articles were distributed among four experts for review. Each expert developed their own taxonomy based on their share of articles, guided by the meta-characteristic defined in Section IV-B.

B. Expert Panel Integration (Iteration 2)

The second iteration used an empirical-to-conceptual approach to integrate the four independently developed taxonomies. A panel of researchers analyzed similarities, differences, and limitations across these taxonomies, extracting the most important dimensions and characteristics. Through multiple discussions, the panel refined and consolidated these elements into a single, cohesive taxonomy.

Fig. 1: Taxonomy Development and Evaluation Process.

C. Validation and Refinement (Iteration 3)

The third iteration combined conceptual-to-empirical and empirical-to-conceptual methodologies to validate the taxonomy. This phase leveraged existing surveys, reviews, and taxonomies from subfields within DLT and identity management. The taxonomy was systematically tested against prior research to confirm its generalizability and robustness across diverse solution architectures. This iteration concluded the development process with all defined ending conditions met.

VI. TAXONOMY ARTIFACT

The final taxonomy artifact (Table II) comprises 22 dimensions and 113 serving as a guide for understanding and classifying DLT-based identity management solutions. It highlights the complexity of approaches, assisting in identifying the strengths and trade-offs of each method. The following is a description of each dimension and selected corresponding characteristics. We categorized every dimension into one of three main groups: 1) Trust Anchor, 2) Identity, and 3) Ledger.

Dimension Group 1: Trust Anchor: In this taxonomy, the dimensions of trust anchors are examined with an emphasis on the technical implementation of trusted components, such as how trust is established in verification materials

TABLE I: Articles reviewed by experts, sorted into technology categories and ordered by count.

Technology Categories	Count	References
SSI: Applications & Use Cases	69	[23]–[91]
Authentication & Access Control	66	[92]–[157]
Security, Privacy, & Trust	47	[158]–[204]
Decentralized Identifiers (DIDs)	44	[205]–[248]
SSI: Technical Architectures	39	[249]–[287]
Identity Governance	38	[288]–[325]
Cryptographic Algorithms	30	[326]–[355]
Identity Anonymization	25	[356]–[380]
Zero-Knowledge Proofs	21	[381]–[401]
Cloud and Edge Computing	6	[402]–[407]
No/Other Technology	4	[408]–[411]

(e.g., public keys), credential status information, and identifier-to-subject bindings. These technical mechanisms form the foundation upon which higher-level trust in issuers, credentials, and identity claims is built.

1) Trust Anchor Purpose: Each trust anchor has a specific role based on the involved entities and activities. For instance, during credential verification, a verifier uses a trust anchor to ensure the integrity of a subject's claims. Similarly, a user depends on a trust anchor to authenticate the source

of their digital wallet software.

2) Trust Anchor Model: A solution can use one or more trust anchors, each serving different or overlapping purposes. For instance, a system might trust cloud providers for operations and rely on governmental agencies for credential issuance. Additionally, having multiple trust anchors can enhance assurance during audits by verifying trusted history and credential use.

3) Trust Anchor Realization: A trust anchor can be established technically or non-technically. For instance, a trust anchor for the tamper-proof distribution of cryptographic material across administrative domains can be implemented as a distributed ledger that is commonly operated and governed by all parties following a consortia agreement. In another approach, the government acts as a single trust anchor, dictating by regulation which entities are trustworthy for verifying specific identity attributes.

Dimension Group 2: Identity: This group organizes identity-related dimensions and is divided into three subgroups: general identity dimensions, identifier-, and credential-specific dimensions.

4) Governance Structure: In this taxonomy, "Identity Governance" refers to where decision-making and authority of the non-ledger parts reside; whether in a single entity or distributed across multiple entities. Governance determines who can make and enforce rules about identity management processes, such as who can issue credentials, how disputes are resolved, and how system changes are approved.

5) Subject: This dimension specifies the types of entities that can possess identities within the IDM system. This dimension defines the scope and applicability of the identity solution.

6) Migration: The migration of an identity focuses on how the identifiers and/or credentials can be transferred from one system or environment to another. The ability to migrate an identity is crucial for ensuring portability and interoperability.

7) Lifespan: The lifespan specifies how long an identity artifact remains valid following its creation. This can be permanent or limited to specific uses, such as with an ephemeral credential.

Identity Subgroup: Identifier

8) Type: The identifier type refers to the form and nature of identifiers within the system. A physical identifier is a tangible object, like an ID card, while a logical identifier is a digital representation, such as an email address or DID.

9) Anchored: This dimension refers to where the source of truth of the identifier is located. Identifiers can be anchored on-chain transparently, as seen with many non-private DID methods. Alternatively, only the hash of the identifier may be stored on-chain. An example of non-anchored identifiers is peer DIDs, which are private, public-key-based identifiers.

10) Proof Material: The proof material refers to the location and type of location where the possession and control of the identifier is demonstrated. The self-contained characteristics indicate that the proof material is inherently included within the identifier(e.g. public-key).

11) Revocation: Revocation determines whether the architecture allows for invalidating an identifier and specifies where the revocation process is conducted and stored.

12) Recovery Mechanisms: The recovery mechanisms outline how a user can regain access to an identifier if the authenticator is lost.

13) Privacy: Privacy explains to what level the identifier is relatable to a subject's personal information.

Identity Subgroup: Credential

14) Type: Credential type refers to the various technical formats and standards used to implement the credential. The credential type is mutually inclusive, meaning two or more characteristics can apply to the same object under consideration. One example of ME credential type is a W3C VC implemented via a smart contract.

15) Anchored: This dimension indicates the location of the credential's source of truth. For instance, a system might have an on-chain credential identifier linked to an off-chain credential. Alternatively, the credential could be fully encrypted on-chain.

16) Storage: This dimension outlines credential storage locations and storage methods, including plain text, encrypted, or zk-proofs. Locations can

TABLE II: The artifact "Taxonomy", showing DLT-based identity management architecture-related dimensions and their characteristics. The dimensions are grouped into three groups, which partially contain further subgroups.

Mutually Exclusive (ME): [Y] = Within a given dimension, an object cannot simultaneously possess more than one characteristic. [N] = multiple characteristics can exist concurrently.

Group & Subgroup		Dimension	ME	Characteristics
Trust Anchor		Purpose	N	Trusted Issuer List • Trusted Verification Material • Trusted History of Verification Material • Trusted Operation • Trusted Storage of Credentials • Trusted Credential Status • Trusted History of Credential Status • Trusted History of Credentials Use
		Model	N	Single Trust Anchor • Multiple Independent Trust Anchors • Multiple Dependent Trust Anchors
		Realization	N	Distributed Ledger Technology • Distributed Hash Table • Distributed File System • Hardware Security Architecture (e.g. TEE's) • Certificate Transparency Logs • Web of Trust • Website • Contractual Agreement • Regulation/Law
Identity	General	Governance	Y	Decentralized Governance • Consortium-based Governance • Central Authority • By Regulation • No Governance
		Subject	N	Humans • Animals • Organizations • Devices • Smart Contracts • Software Applications • Digital Assets • Work Loads • Other
		Migration	Y	Without Issuer Interaction • With Issuer Interaction • Non-Transferable
		Lifespan	Y	Permanent • Time-Limited • Activity-Based • Ephemeral
	Identifier	Type	Y	Logical • Physical (Hardware-Bound) • Public-Key-Based • W3C Decentralized Identifier • Custom
		Anchored	Y	On-Chain Anchored • On-Chain Hashed • On Website • Self-Anchored • Not Anchored
		Proof Material	Y	On-Chain • Off-Chain Centralized • Off-Chain Decentralized • Off-Chain at Subject • Decentralized File System
		Revocation	Y	No Revocation • On-Chain Revocation • Off-Chain Revocation
		Recovery Mechanism	N	Multi-Signature Recovery • Time-Locked Recovery • Secret Sharing • Escrow-Based Recovery • Biometric Recovery • Other Mechanism • Other Decentralized Recovery • No Recovery Mechanism
		Privacy	Y	Anonymous • Pseudoanonymous • Non anonymous
	Credential	Type	N	Non-fungible Token • W3C Verifiable Credential • Other Token Standard • Smart-Contract-Based • Anonymous Credential • Certificate • Custom
		Anchored	Y	On-Chain Credential Identifier • On-Chain Hash • On-Chain Encrypted • Not anchored
		Storage	Y	Off-Chain at Subject • On-Chain Plain Text • On-Chain Encrypted • Off-Chain Centralized • Off-Chain Decentralized • Distributed File System
		Revocation	Y	No Revocation • On-Chain Revocation • Off-Chain Revocation
		Disclosure Control	Y	Only Full Disclosure • Combined Disclosure • Selective Disclosure • Zero Knowledge Proof
		Verifiability	Y	Non-Verifiable • Verifiable With Issuer Involvement • Verifiable Without Issuer Involvement
Ledger		Consensus Mechanism	Y	Proof-of-Work • Proof-of-Stake • Proof-of-Authority • Delegated Proof-of-Stake • Byzantine Fault Tolerance • DAG-based • Other
		Permission Level	Y	Public Permissionless • Public Permissioned • Private Permissioned
		Usage Overhead	Y	No Fees • Creation Fee Only • Usage Fee Only • Creation and Usage Fees • Time-based (Subscription) • Alternative Fee Models

be on-chain, off-chain, or both, and may be decentralized, centralized, or hybrid. The data format is not specified.

17) Revocation: Revocation determines whether the architecture allows for invalidating a credential and specifies where the revocation process is conducted and where the revocation status is stored. This dimension does not consider who is authorized to conduct revocation but only whether it is supported.

18) Disclosure Control: This concept relates to the amount of identity information shared during verification and the degree of control the subject has when disclosing a credential or specific parts of it.

19) Verifiability: Verifiability refers to whether a credential can be confirmed by a verifier. Credentials that are self-issued are not verifiable, while those from trusted issuers allow for independent verification without needing the issuer's involvement.

Dimension Group 3: Ledger

20) Consensus Mechanism: The consensus algorithm is a fundamental component of any distributed ledger-based solution and affects properties like fault tolerance, latency, decentralization, and security.

21) Usage Overhead: This dimension refers to how the DLT-based IDM system handles fees related to operational aspects such as the creation, usage, updating, and revocation of identity artifacts. Ledger-specific fees, such as transaction costs, are not included.

22) Permission Level: This dimension defines who can access the ledger. Public and private indicate its visibility, while permissioned means only authorized users can submit transactions, whereas permissionless allows anyone. Governance and participation rules are not covered by this dimension.

VII. EVALUATION

This section evaluates the taxonomy by applying it to two DLT-based IDM research papers and assessing the fulfillment of ending conditions.

A. First Evaluation

The first article proposes an architecture for decentralized identity management for Internet of Things (IoT) devices [117], addressing scalability and security challenges in large-scale IoT systems using smart contracts for access control, trust management, and reputation evaluation.

The classification result is shown in Table III (Solution 1). The authors address many relevant dimensions, especially within the ledger and identity groups, though credential disclosure control, revocation, and migration capabilities are not discussed. The solution utilizes W3C DIDs and VCs in combination with PKI and smart contracts with various on-chain anchors and off-chain hashes.

Had the authors used this taxonomy, they might have recognized their trust anchor architecture lacks description of the model—whether using single or multiple anchors and relationships. While the authors present a comprehensive architecture, our taxonomy could have guided them to explore additional crucial dimensions.

B. Second Evaluation

The paper "SAML Metadata Management with Distributed Ledger Technology" [296] explores managing SAML federation metadata with distributed ledger technology. The solution focuses on organizations as identity subjects and relies on PKI/X.509 certificates, suggesting the need for root Certificate Authorities, though trust anchor establishment is not explicitly discussed. The solution uses logical identifiers (domain names) anchored through the ACME protocol on websites. Its privacy model leverages Hyperledger Fabric's channel-based architecture to restrict transaction visibility among specific participants. The credential system uses X.509 certificates stored off-chain, with no explicit mention of revocation or recovery mechanisms. The ledger employs a permissioned, private model with configurable consensus and no associated fees. Applying the taxonomy to this paper reveals shortcomings including the lack of discussion on trust anchor establishment, governance structure, and revocation mechanisms. Additionally, by separating Identity

TABLE III: Application of the taxonomy for classifying two proposed DLT-based IDM architectures.

Group & Subgroup		Dimension	Classification of Solution 1 [117]	Classification of Solution 2 [296]
Trust		Purpose	Trusted verification material	N/A
		Model	N/A	N/A
		Realization	Distributed Ledger Technology	N/A
Identity	General	Governance	Central authority	N/A
		Subject	Devices (IoT)	Organizations
		Migration	N/A	N/A
		Lifespan	Permanent	Activity-based
	Identifier	Type	Public-key-based & W3C decentralized identifier	Logical (domain names)
		Anchored	On-chain anchored	On website
		Proof Material	On-chain	Off-chain at subject
		Revocation	On-chain revocation	N/A
		Recovery Mechanism	No recovery mechanism	N/A
		Privacy	Pseudoanonymous	Pseudoanonymous/non-anonymous depending on configurations
	Credential	Type	Smart-contract-based & W3C verifiable credential	Certificate (X.509)
		Anchored	On-chain hash	Not-anchored
		Storage	Off-chain at subject	Off-chain at subject
		Revocation	N/A	N/A
		Disclosure Control	N/A	Only full disclosure
		Verifiability	Verifiable without issuer involvement	Verifiable, issuer involvement not mentioned
Ledger		Consensus Mechanism	Proof-of-stake	Other - depending on configurations
		Permission Level	Public permissionless	Private permissioned
		Usage Overhead	No fees	No fees

into Identifier and Credential, the taxonomy highlights the tight coupling between identifier, verification material, and credential in X.509 certificates.

C. Classification Results

The taxonomy effectively classified two distinct architectural solutions, showcasing its versatility. The evaluation uncovered specific gaps that might have gone unnoticed without a systematic framework. The three-group structure organized complex interrelationships well, while separating Identity into general, identifier, and credential dimensions offered valuable clarity. The taxonomy successfully categorizes both approaches without modification, demonstrating comprehensive

dimension coverage and robustness validated by expert review. It enhances understanding of complex architectures and provides practical utility for both analysis and design. By highlighting architectural decisions and potential improvements, it serves as an analytical tool for researchers and a design guide for practitioners developing DLT-based identity solutions.

VIII. DISCUSSION

This research developed a comprehensive taxonomy for DLT-based identity management through a rigorous iterative process. Trust emerged as the central concern across various layers of DLT-based IDM architectures, reflected in the taxonomy's organization into three groups: trust anchor, identity (further subdivided into general, credential, and identifier dimensions), and ledger-related dimensions. The developed taxonomy represents a comprehensive artifact that significantly aids researchers and practitioners in designing and evaluating DLT-based IDM solutions. It provides a structured framework for classifying existing solutions, uncovering their shortcomings, and identifying improvements. The detailed nature of the taxonomy enables a nuanced analysis of both simple and complex architectures. During the second iteration of the taxonomy building, there was an active discussion on how to structure the research approach and whether the meta-characteristics should be further specialized. It was decided to maintain a comprehensive and holistic view of architecture for the purpose of creating a detailed taxonomy artifact. All experts identified and agreed that trust is a significant concern for all identity management architectures, particularly those incorporating a distributed ledger component. When the taxonomy was analyzed through the lens of "trust," it became evident that nearly every dimension is also related to trust. Consequently, the trust anchor dimension was chosen in a way that fits multiple layers and points of view. We encourage future researchers and practitioners to examine and report their solutions through the lenses of this taxonomy. The length and the revision steps of the dimensions may affect understandability. However, it was a deliberate choice to provide detailed and holistic coverage. The taxonomy underwent multiple revisions and expert reviews and was tested against existing taxonomies in the field. Another limitation could be the rapid evolution of the research field. However, we view the taxonomy as a living artifact and structured the dimensions to ensure their relevance and adaptability in the future. Future general research is needed to assess where large language models can effectively assist researchers in building the taxonomy. Additionally, creating a standard way to report taxonomy artifacts, using interactive tools or software that apply the taxonomy, could enhance its usability and accessibility. Researchers could expand the taxonomy by creating application-specific groups and dimensions. They can also use this extensive taxonomy to create more specialized taxonomies for their specific fields and subsequently expand upon them. Moreover, both researchers and practitioners could test and refine our trust anchor framework. This taxonomy could be applied to classify a wide range of popular DLT-based IDM solutions, enabling their categorization and grouping, identifying shortcomings, and facilitating comparison.

IX. CONCLUSION

This research presents the first comprehensive taxonomy at the intersection of IDM and DLT. Organized into three main components—trust anchor, identity, and ledger—the taxonomy provides researchers and practitioners with a systematic framework to analyze, compare, and design DLT-based identity solutions. The taxonomy's significant contribution lies in establishing a common language and classification system for a rapidly evolving field. By structuring the complex landscape of DLT-based identity architectures, it enables more effective communication between researchers and practitioners, facilitates the identification of research gaps, and supports the development of more robust and interoperable solutions. As distributed ledger technology continues to transform IDM approaches, this taxonomy offers

a foundation for standardization and improved architectural design. It provides conceptual clarity about fundamental components while remaining adaptable to emerging technologies and implementation patterns. Through this structured approach to understanding DLT-based identity architectures, the taxonomy supports both theoretical advancement and practical implementation in this critical domain.

REFERENCES

[1] P. Dunphy and F. A. Petitcolas, "A First Look at Identity Management Schemes on the Blockchain," *IEEE Security & Privacy*, vol. 16, no. 4, pp. 20–29, 2018.

[2] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. Raymond Choo, "Blockchain-based identity management systems: A review," *Journal of Network and Computer Applications*, vol. 166, Sep. 2020.

[3] F. Schardong and R. Custódio, "Self-Sovereign Identity: A Systematic Review, Mapping and Taxonomy," *Sensors*, vol. 22, no. 15, 2022.

[4] L. Lesavre, "A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems," National Institute of Standards and Technology, Tech. Rep., 2020.

[5] R. Glass and I. Vessey, "Contemporary application-domain taxonomies," *IEEE Software*, vol. 12, no. 4, pp. 63–76, Jul. 1995.

[6] R. C. Nickerson, U. Varshney, and J. Muntermann, "A method for taxonomy development and its application in information systems," *European Journal of Information Systems*, vol. 22, no. 3, pp. 336–359, 2013.

[7] D. Kundisch, J. Muntermann, A. M. Oberländer, D. Rau, M. Röglinger, T. Schoormann, and D. Szopinski, "An Update for Taxonomy Designers," *Business & Information Systems Engineering*, vol. 64, no. 4, pp. 421–439, 2022.

[8] International Organization for Standardization, "IT Security and Privacy — A framework for identity management — Part 1: Terminology and concepts," Geneva, 2019.

[9] International Telecommunication Union, "Recommendation ITU-T X.1252: Baseline identity management terms and definitions," Geneva, 2021.

[10] P. A. Grassi, M. E. Garcia, and J. L. Fenton, "Digital identity guidelines: revision 3," National Institute of Standards and Technology, Tech. Rep. NIST SP 800-63-3, 2017.

[11] D. I. A. Domingo, "How eIDAS can legally support digital identity and trustworthy DLT-based transactions in the Digital Single Market," *European Comission*, 2020.

[12] J. Sedlmeir, R. Smethurst, A. Rieger, and G. Fridgen, "Digital Identities and Verifiable Credentials," *Business & Information Systems Engineering*, vol. 63, no. 5, pp. 603–613, Oct. 2021.

[13] Z. Yan, X. Zhao, Y. A. Liu, and X. R. Luo, "Blockchain-driven decentralized identity management: An interdisciplinary review and research agenda," *Information & Management*, vol. 61, no. 7, p. 104026, 2024.

[14] M. Sporny, D. Longley, M. Sabadello, D. Reed, O. Steele, and C. Allen, "Decentralized Identifiers (DIDs) v1.0," *W3C Recommendation*, 2022.

[15] M. Sporny, D. Longley, and D. Chadwick, "Verifiable Credentials Data Model v1.1," *W3C Recommendation*, 2022.

[16] P. Windley, *Learning Digital Identity: Design, Deploy, and Manage Identity Architectures*. O'Reilly Media, 2023.

[17] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System," *Satoshi Nakamoto*, 2008.

[18] V. Buterin, "A next-generation smart contract and decentralized application platform," *Ethereum White Paper*, 2014.

[19] E. Androulaki, A. Barger, V. Bortnikov, C. Cachin, K. Christidis, A. De Caro, D. Enyeart, C. Ferris, G. Laventman, Y. Manevich, S. Muralidharan, C. Murthy, B. Nguyen, M. Sethi, G. Singh, K. Smith, A. Sorniotti, C. Stathakopoulou, M. Vukolić, S. W. Cocco, and J. Yellick, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the Thirteenth EuroSys Conference*. Porto Portugal: ACM, Apr. 2018, pp. 1–15.

[20] S. D. Palma, R. Pareschi, and F. Zappone, "What is your Distributed (Hyper)Ledger?" in *WETSEB*. IEEE, 2021, pp. 27–33.

[21] T. T. T. Ngo, T. A. Dang, V. V. Huynh, and T. Cong Le, "A Systematic Literature Mapping on Using Blockchain Technology in Identity Management," *IEEE Access*, vol. 11, pp. 26 004–26 032, 2023.

[22] A. Amard, A. Rieger, E. Hartwich, T. Roth, A. Hoess, and G. Fridgen, "Designing Digital Identity Infrastructure: A Taxonomy of Strategic Governance Choices," *Proceedings of the 57th Hawaii International Conference on System Sciences*, 2024.

[23] N. Naik and P. Jenkins, "Self-sovereign identity specifications: Govern your identity through your digital wallet using blockchain technology," in *MobileCloud*. IEEE, 2020, pp. 90–95.

[24] M. Takemiya and B. Vanieiev, "Sora identity: Secure, digital identity on the blockchain," in *COMPSAC*. IEEE, 2018, pp. 582–587.

[25] S. S, S. M, N. Ahmed, A. Bhagavath, and N. B. R, "Decentralized digital identity wallet using principles of self-sovereign identity applied to blockchain," in *ICRAIE*. IEEE, 2022, pp. 337–341.

[26] P. Goswami and S. Sirsikar, "Self-sovereign identity to secure digital identity using blockchain technology," in *ICIPCN*. IEEE, 2024, pp. 826–831.

[27] R. Chen, H.-W. Tseng, J.-L. Lien, and W. Liao, "Blockchain-empowered identity management with a dual identity model for uavs in 5g networks," *IEEE Internet of Things Magazine*, vol. 5, no. 2, pp. 69–73, 2022.

[28] N. Naik and P. Jenkins, "uport open-source identity management system: An assessment of self-sovereign

identity and user-centric data platform built on blockchain," in *ISSE*. IEEE, 2020, pp. 1–7.

[29] E. Bandara, X. Liang, P. Foytik, S. Shetty, and K. D. Zoysa, "A blockchain and self-sovereign identity empowered digital identity platform," in *ICCCN*. IEEE, 2021, pp. 1–7.

[30] S. Terzi, C. Savvaidis, A. Sersemis, K. Votis, and D. Tzovaras, "Decentralizing identity management and vehicle rights delegation through self-sovereign identities and blockchain," in *COMPSAC*. IEEE, 2021, pp. 1217–1223.

[31] A. Jamal, R. A. A. Helmi, A. S. N. Syahirah, and M.-A. Fatima, "Blockchain-based identity verification system," in *ICSET*. IEEE, 2019, pp. 253–257.

[32] E. Bandara, X. Liang, P. Foytik, and S. Shetty, "Blockchain and self-sovereign identity empowered cyber threat information sharing platform," in *SMARTCOMP*. IEEE, 2021, pp. 258–263.

[33] C. Dong, F. Jiang, X. Li, A. Yao, G. Li, and X. Liu, "A blockchain-aided self-sovereign identity framework for edge-based uav delivery system," in *CCGrid*. IEEE, 2021, pp. 622–624.

[34] M. A. R. Tonu, S. Hridoy, M. A. Ali, and S. A. Azad, "Block - nid: A conceptual secure blockchain based national identity management system model," in *CSDE*. IEEE, 2019, pp. 1–7.

[35] S. A. Mansoori and P. Maheshwari, "Hei-bct: A framework to implement blockchain-based self-sovereign identity solution in higher education institutions," in *ITT*. IEEE, 2022, pp. 6–10.

[36] G.-A. Dima, A.-G. Jitariu, C. Pisa, and G. Bianchi, "Scholarium: Supporting identity claims through a permissioned blockchain," in *RTSI*. IEEE, 2018, pp. 1–6.

[37] S. Singh Sidhu, M. N. H. Nguyen, C. Ngene, and S. Rouhani, "Trust development for blockchain interoperability using self-sovereign identity integration," in *IEMCON*. IEEE, 2022, pp. 0033–0040.

[38] P. Rede, S. Iyer, S. Sharma, and S. Deshmukh, "Blockchain based identity management system using cryptography and steganography," in *ICIT*. IEEE, 2023, pp. 173–177.

[39] T. K. Saragih, E. Tanuwijaya, and G. Wang, "The use of blockchain for digital identity management in healthcare," in *CITSM*. IEEE, 2022, pp. 1–6.

[40] J. Kim, M. Choi, C. Lee, J. Woo, and J. W.-K. Hong, "Service applicable blockchain-based self-sovereign identity management system," in *ICBC*. IEEE, 2023, pp. 1–5.

[41] U. Cali, M. F. Dynge, M. S. Ferdous, and U. Halden, "Improved resilience of local energy markets using blockchain technology and self-sovereign identity," in *iGETblockchain*. IEEE, 2022, pp. 1–5.

[42] G. Sreenath, G. T. Sridhar, A. A. Sannabhadti, R. M. S J, and M. R. Kounte, "Blockchain based digital identity solution," in *IDCIoT*. IEEE, 2024, pp. 387–391.

[43] A. Thorve, M. Shirole, P. Jain, C. Santhumayor, and S. Sarode, "Decentralized identity management using blockchain," in *ICAC3N*. IEEE, 2022, pp. 1985–1991.

[44] S. R. Kumar and M. Goyal, "Administration of digital identities using blockchain," in *IC3I*. IEEE, 2022, pp. 2179–2183.

[45] R. Soltani, U. Trang Nguyen, and A. An, "A new approach to client onboarding using self-sovereign identity and distributed ledger," in *iThings*. IEEE, 2018, pp. 1129–1136.

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

[47] Q. Stokkink and J. Pouwelse, "Deployment of a Blockchain-Based Self-Sovereign Identity," in *2018 IEEE iThings*. Halifax, NS, Canada: IEEE, Jul. 2018, pp. 1336–1342.

[48] P. Datta, A. Bhowmik, A. Shome, and M. Biswas, "A secured smart national identity card management design using blockchain," in *ICAICT*. IEEE, 2020, pp. 291–296.

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

[50] A. Norta, A. Kormiltsyn, C. Udokwu, V. Dwivedi, S. Aroh, and I. Nikolajev, "A blockchain implementation for configurable multi-factor challenge-set self-sovereign identity authentication," in *Blockchain*. IEEE, 2022, pp. 455–461.

[51] E. Zeydan, J. Mangues, S. Arslan, and Y. Turk, "Blockchain-based self-sovereign identity solution for vehicular networks," in *DRCN*. IEEE, 2023, pp. 1–7.

[52] M. Popa, S. M. Stoklossa, and S. Mazumdar, "Chaindiscipline - towards a blockchain-iot-based self-sovereign identity management framework," *IEEE Transactions on Services Computing*, vol. 16, no. 5, pp. 3238–3251, 2023.

[53] Y. Chen, C. Liu, Y. Wang, and Y. Wang, "A self-sovereign decentralized identity platform based on blockchain," in *ISCC*. IEEE, 2021, pp. 1–7.

[54] M. L. Alessandria and A. Vizzarri, "Self-sovereign identity and blockchain applications for the automotive sector," in *AEIT AUTOMOTIVE*. IEEE, 2021, pp. 1–6.

[55] A. H. Rahat, M. R. Rumon, T. J. Joti, H. Tasnin, T. Akter, A. Shakil, and M. I. Hossain, "Blockchain based secured multipurpose identity (smid) management system for smart cities," in *CCWC*. IEEE, 2022, pp. 0737–0744.

[56] N. Sahi, A. Liang, W. Van Devanter, K. Oikonomou, and P. Zhang, "Self-sovereign identity in semi-permissioned blockchain networks leveraging ethereum and hyperledger fabric," in *ICDH*. IEEE, 2023, pp. 315–321.

[57] U. Ghosh, D. Das, S. Banerjee, and S. Mohanty, "Blockchain-based device identity management and authentication in cyber-physical systems," in *CCNC*. IEEE, 2024, pp. 1–6.

[58] B. V. Santhosh Krishna, B. Rajalakshmi, K. Ashok, I. H. Gundoo, and I. Aryan, "Self sovereign identity - blockchain based blood donation management method," in *ICSCSS*. IEEE, 2023, pp. 1512–1520.

[59] A. Abid, S. Cheikhrouhou, S. Kallel, and M. Jmaiel, "A blockchain-based self-sovereign identity approach for inter-organizational business processes," 2022, pp. 685–694.

[60] E. Zeydan, J. Mangues, S. S. Arslan, and Y. Turk, "Blockchain-based self-sovereign identity for routing

in inter-domain networks," *IEEE Communications Magazine*, vol. 62, no. 1, pp. 96–102, 2024.

[61] A. De Salve, D. Di Francesco Maesa, F. Federico, P. Mori, and L. Ricci, "Algoid: A blockchain reliant self-sovereign identity framework on algorand," in *ISCC*. IEEE, 2023, pp. 1162–1168.

[62] D. Mebrahtom, S. Hadish, A. Sbhatu, M. Aloqaily, and M. Guizani, "Trust but verify - blockchain-empowered decentralized authentication schema on the metaverse: A self-sovereign identity approach," in *iMETA*. IEEE, 2023, pp. 1–8.

[63] X. Li, C. Chen, M. Teng, and Y. Shi, "Blockchain-based traceable selective disclosure credentials for self-sovereign identity," in *CSCWD*. IEEE, 2024, pp. 1382–1387.

[64] E. Zeydan, L. Blanco, J. Mangues, S. Arslan, and Y. Turk, "Blockchain-based self-sovereign identity for federated learning in vehicular networks," in *CNSM*. IEEE, 2023, pp. 1–7.

[65] S. Becirovic, S. Cucko, M. Turkanovic, H. Supic, and S. Mrdovic, "Blockchain Redaction in Self-Sovereign Identity," in *2022 SoftCOM*, Split, Croatia, 2022, pp. 1–6.

[66] M. T. A. Tonoy, N. Munjal, R. A. Sinha, A. Paul, and H. S. Lamkuche, "Unlocking borderless identity: B-passport and the blockchain revolution," in *ICWITE*. IEEE, 2024, pp. 109–116.

[67] E. Zeydan, J. Mangues, S. S. Arslan, and Y. Turk, "Data sharing control with blockchain-based self-sovereign identity management system," *IEEE Reliability Magazine*, vol. 1, no. 3, pp. 62–70, 2024.

[68] S. P. Otta, S. Panda, and C. Hota, "Identity management with blockchain: Indian migrant workers prospective," in *IATMSI*. IEEE, 2022, pp. 1–6.

[69] Z. Zhang, R. Xiong, X. Di, and W. Ren, "Croauth: A cross-domain authentication scheme based on blockchain and decentralized identity," in *CSCWD*. IEEE, 2024, pp. 2016–2021.

[70] M. D. V. Barros and J. E. Martina, "Sovereignrx: An electronic prescription system based on high privacy, blockchain, and self-sovereign identity," in *Advanced Information Networking and Applications*, L. Barolli, Ed. Springer Nature Switzerland, 2024, vol. 202, pp. 372–383.

[71] S. Saha, S. N. Nova, and M. I. Iqbal, "Healthcare professionals credential verification model using blockchain-based self-sovereign identity," in *Proceedings of the Fourth International Conference on Trends in Computational and Cognitive Engineering*, M. S. Kaiser, S. Waheed, A. Bandyopadhyay, M. Mahmud, and K. Ray, Eds. Springer Nature Singapore, 2023, vol. 618, pp. 381–392.

[72] E. Bandara, X. Liang, P. Foytik, S. Shetty, N. Ranasinghe, K. De Zoysa, and W. K. Ng, "Promize - blockchain and self sovereign identity empowered mobile atm platform," in *Intelligent Computing*, K. Arai, Ed. Springer International Publishing, 2021, vol. 284, pp. 891–911.

[73] A. Farao, G. Paparis, S. Panda, E. Panaousis, A. Zarras, and C. Xenakis, "Inchain: a cyber insurance architecture with smart contracts and self-sovereign identity on top of blockchain," *International Journal of Information Security*, vol. 23, pp. 347–371, 2024.

[74] E. Bandara, X. Liang, P. Foytik, S. Shetty, C. Hall, D. Bowden, N. Ranasinghe, K. De Zoysa, and W. K. Ng, "Connect - blockchain and self-sovereign identity empowered contact tracing platform," in *Wireless Mobile Communication and Healthcare*, J. Ye, M. J. O'Grady, G. Civitarese, and K. Yordanova, Eds. Springer International Publishing, 2021, vol. 362, pp. 208–223.

[75] M. S. Prashanth, R. Karnati, M. S. Velpuru, and H. V. Reddy, "Blockchain-based digital identity management system for cybersecurity," in *Proceedings of the 5th International Conference on Data Science, Machine Learning and Applications; Volume 1*, A. Kumar, V. K. Gunjan, S. Senatore, and Y.-C. Hu, Eds. Springer Nature Singapore, 2025, vol. 1273, pp. 277–289.

[76] A. B. Chavan and K. Rajeswari, "Design and development of self-sovereign identity using ethereum blockchain," in *Sustainable Communication Networks and Application*, P. Karrupusamy, J. Chen, and Y. Shi, Eds. Springer International Publishing, 2020, vol. 39, pp. 523–531.

[77] G. Balastegui-García, E. M. S. Sabau, A. S. Payá, and H. Mora, "Corporate digital identity based on blockchain," in *Research and Innovation Forum 2022*, A. Visvizi, O. Troisi, and M. Grimaldi, Eds. Springer International Publishing, 2023, pp. 645–655.

[78] T. Rathee and P. Singh, "A self-sovereign identity management system using blockchain," in *Cyber Security and Digital Forensics*, K. Khanna, V. V. Estrela, and J. J. P. C. Rodrigues, Eds. Springer Singapore, 2022, vol. 73, pp. 371–379.

[79] M. A. E. Yousef, "Developing and implementing blockchain identity management to verify students' certifications and data (verion)," in *Proceedings of the Future Technologies Conference (FTC) 2022, Volume 2*, K. Arai, Ed. Springer International Publishing, 2023, vol. 560, pp. 16–35.

[80] P. Zhang and T.-T. Kuo, "The feasibility and significance of employing blockchain-based identity solutions in health care," in *Blockchain Technology and Innovations in Business Processes*, S. Patnaik, T.-S. Wang, T. Shen, and S. K. Panigrahi, Eds. Springer Singapore, 2021, vol. 219, pp. 189–208.

[81] T. Cippitelli, A. Marcelletti, and A. Morichetta, "Chorssi: A bpmn-based execution framework for self-sovereign identity systems on blockchain," in *Business Process Management: Blockchain, Robotic Process Automation and Educators Forum*, J. Köpke, O. López-Pintado, R. Plattfaut, J.-R. Rehse, K. Gdowska, F. Gonzalez-Lopez, J. Munoz-Gama, K. Smit, and J. M. E. M. Van Der Werf, Eds. Springer Nature Switzerland, 2023, vol. 491, pp. 5–20.

[82] S. M. M. Alam, M. A. A. Mamun, M. S. Hossain, and M. Samiruzzaman, "A novel approach to manage ownership and vat using blockchain-based digital identity," in *Ubiquitous Networking*, H. Elbiaze, E. Sabir, F. Falcone, M. Sadik, S. Lasaulce, and J. Ben Othman, Eds. Springer International Publishing, 2021, vol. 12845, pp. 255–268.

[83] M. A. A. Mamun, S. M. M. Alam, M. S. Hossain, and M. Samiruzzaman, "A novel approach to blockchain-based digital identity system," in *Advances in Information and Communication*, K. Arai, S. Kapoor, and R. Bhatia,

Eds. Springer International Publishing, 2020, vol. 1129, pp. 93–112.

[84] A. Norta, C. Udokwu, and S. Craß, "Real-world asset identity authentication in blockchain enabled inter-organizational process-aware systems involving adjustable challenge-response evaluation sets," *SN Computer Science*, vol. 5, p. 936, 2024.

[85] C.-D. Au and H. Michael, "Dezentrale identitäten für personen und unternehmen in der blockchain: Self-sovereign identity am beispielprojekt „lissi"," in *Banking & Innovation 2022/2023*, M. Seidel and S. Reuse, Eds. Springer Fachmedien Wiesbaden, 2023, pp. 597–608.

[86] G. Ishmaev, "Sovereignty, privacy, and ethics in blockchain-based identity management systems," *Ethics and Information Technology*, vol. 23, pp. 239–252, 2021.

[87] M. Shuaib, S. Alam, M. Shabbir Alam, and M. Shahnawaz Nasir, "Self-sovereign identity for healthcare using blockchain," *Materials Today: Proceedings*, vol. 81, pp. 203–207, 2023.

[88] Y. Zhuang, C.-R. Shyu, S. Hong, P. Li, and L. Zhang, "Self-sovereign identity empowered non-fungible patient tokenization for health information exchange using blockchain technology," *Computers in Biology and Medicine*, vol. 157, p. 106778, 2023.

[89] L. Stockburger, G. Kokosioulis, A. Mukkamala, R. R. Mukkamala, and M. Avital, "Blockchain-enabled decentralized identity management: The case of self-sovereign identity in public transportation," *Blockchain: Research and Applications*, vol. 2, p. 100014, 2021.

[90] M. Shuaib, N. H. Hassan, S. Usman, S. Alam, S. Bhatia, A. Mashat, A. Kumar, and M. Kumar, "Self-sovereign identity solution for blockchain-based land registry system: A comparison," *Mobile Information Systems*, vol. 2022, pp. 1–17, 2022.

[91] Y. Kurihara, "Self-Sovereign Identity and Blockchain-Based Content Management," in *Human-Centric Computing in a Data-Driven Society*. Springer International Publishing, 2020, vol. 590, pp. 130–140.

[92] V. Valentin Vallois, A. Mehaoua, and M. Amziani, "Blockchain-based identity and access management in industrial iot systems," in *IFIP/IEEE*. IEEE, 2021.

[93] W. Ao, S. Fu, C. Zhang, Y. Huang, and F. Xia, "A secure identity authentication scheme based on blockchain and identity-based cryptography," in *CCET*. IEEE, 2019, pp. 90–95.

[94] C. DeCusatis, M. Zimmermann, and A. Sager, "Identity-based network security for commercial blockchain services," in *CCWC*. IEEE, 2018, pp. 474–477.

[95] A. Chowdhary, S. Agrawal, and B. Rudra, "Blockchain based framework for student identity and educational certificate verification," in *ICESC*. IEEE, 2021, pp. 916–921.

[96] G. Zhao, B. Di, and H. He, "Design and implementation of the digital education transaction subject two-factor identity authentication system based on blockchain," in *ICACT*. IEEE, 2020, pp. 176–180.

[97] P. Gururaj, "Identity management using permissioned blockchain," in *ICOMBI*. IEEE, 2020, pp. 1–3.

[98] M. Mukhandi, F. Damiao, J. Granjal, and J. P. Vilela, "Blockchain-based device identity management with

[99] consensus authentication for iot devices," in *CCNC*. IEEE, 2022, pp. 433–436.

[99] H. Huang and X. Chen, "Power mobile terminal identity authentication mechanism based on blockchain," in *IWCMC*. IEEE, 2020, pp. 195–198.

[100] B. N. Biswas, S. D. Bhitkar, and S. N. Pundkar, "Secure login: A blockchain based web application for identity access management system," in *INCET*. IEEE, 2021, pp. 1–5.

[101] Y. Zhou, Q. Liu, M. Liu, Y. Wang, and C. Ren, "Research on blockchain-based identity verification between iov entities," in *HPBD&IS*. IEEE, 2020, pp. 1–6.

[102] J. Zhu, Y. Wei, and X. Shang, "Decentralized dynamic identity authentication system based on blockchain," in *INSAI*. IEEE, 2021, pp. 1–4.

[103] D. Chakravarty and T. Deshpande, "Blockchain-enhanced identities for secure interaction," in *HST*. IEEE, 2018, pp. 1–4.

[104] F. Dang, F. Gao, H. Liang, and Y. Sun, "Multi-dimensional identity authentication mechanism for power maintenance personnel based on blockchain," in *IWCMC*. IEEE, 2020, pp. 215–219.

[105] J. Cao, X. Chen, E. Li, H. Xing, J. Zhang, G. Mu, C. Miao, and C. Xu, "Design of identity authentication scheme in smart grid based on blockchain," in *ICFTIC*. IEEE, 2022, pp. 1093–1100.

[106] J. Drga, I. Homoliak, J. Vanco, A. Vasilakos, M. Perešíni, and P. Hanacek, "Detecting and preventing credential misuse in otp-based two and half factor authentication toward centralized services utilizing blockchain-based identity management," in *ICBC*. IEEE, 2023, pp. 1–4.

[107] V. Aanandaram and P. Deepalakshmi, "Blockchain-based digital identity for secure authentication of iot devices in 5g networks," in *INCOS*. IEEE, 2024, pp. 1–6.

[108] W. Xu, Y. Song, H. Liang, L. Sun, and Y. Xie, "A blockchain-based identity control scheme for cross-organizational data sharing," in *BigDataSecurity*. IEEE, 2024, pp. 156–160.

[109] Z. Cui, F. Xue, S. Zhang, X. Cai, Y. Cao, W. Zhang, and J. Chen, "A hybrid blockchain-based identity authentication scheme for multi-wsn," *IEEE Transactions on Services Computing*, pp. 1–1, 2020.

[110] N. Malik, P. Nanda, A. Arora, X. He, and D. Puthal, "Blockchain based secured identity authentication and expeditious revocation framework for vehicular networks," in *TrustCom/BigDataSE*. IEEE, 2018, pp. 674–679.

[111] T. Mikula and R. H. Jacobsen, "Identity and access management with blockchain in electronic healthcare records," in *DSD*. IEEE, 2018, pp. 699–706.

[112] X. Xiang, M. Wang, and W. Fan, "A permissioned blockchain-based identity management and user authentication scheme for e-health systems," *IEEE Access*, vol. 8, pp. 171 771–171 783, 2020.

[113] S. A. George, A. Jaekel, and I. Saini, "Secure identity management framework for vehicular ad-hoc network using blockchain," in *ISCC*. IEEE, 2020, pp. 1–6.

[114] M. Hegde, R. R. Rao, and B. M. Nikhil, "Ddmia: Distributed dynamic mutual identity authentication for referrals in blockchain-based health care networks," *IEEE Access*, vol. 10, pp. 78 557–78 575, 2022.

[115] S. Varshney, P. Vats, S. Choudhary, and D. Singh, "A blockchain-based framework for iot based secure identity management," in *ICIPTM*. IEEE, 2022, pp. 227–234.

[116] S. Ismail, D. Dawoud, and H. Reza, "Towards a lightweight identity management and secure authentication for iot using blockchain," in *AIIoT*. IEEE, 2022, pp. 077–083.

[117] R. Xiong, W. Ren, X. Hao, J. He, and K.-K. R. Choo, "Bdim: A blockchain-based decentralized identity management scheme for large scale internet of things," *IEEE Internet of Things Journal*, vol. 10, no. 24, pp. 22 581–22 590, 2023.

[118] P. Lv, Y. Wang, Y. Wang, C. Liu, Q. Zhou, and Z. Xu, "A highly reliable cross-domain identity authentication protocol based on blockchain in edge computing environment," in *CSCWD*. IEEE, 2022, pp. 1040–1046.

[119] K. Dissanayake, P. Somarathne, U. Fernando, D. Pathmasiri, C. Liyanapathirana, and D. L. Rupasinghe, ""trust pass" - blockchain-based trusted digital identity platform towards digital transformation," in *IISEC*. IEEE, 2021, pp. 1–6.

[120] S. Das, M. Sahil, N. K. Pandit, R. Priyadarshini, and S. P. Gochhayat, "Bsciam: A blockchain based secure cloud identity and access management framework," in *SCEECS*. IEEE, 2024, pp. 1–6.

[121] Y. Chen, Q. Yang, X. Zeng, D. Yang, and X. Li, "A new identity authentication and key agreement protocol based on multi-layer blockchain in edge computing," *IEEE Access*, vol. 12, pp. 3274–3291, 2024.

[122] H. Bao, X. Zhang, G. Wang, R. Tian, J. Duan, and Y. Zhao, "Smart-pki: A blockchain-based distributed identity validation scheme for iot devices," in *ICC*. IEEE, 2023, pp. 4749–4754.

[123] L. Chen, T. Zhang, Y. Ma, and Z. Dai, "Lightweight blockchain-based identity authentication scheme for power terminal," in *IC2ECS*. IEEE, 2023, pp. 634–640.

[124] I. O. Joshua, M. O. Arowolo, M. O. Adebiyi, K. A. Gbolagade, J. O. Olaniyan, and E. T. Aderemi, "Design and implementation of a single sign-in identity (ssid) on the banking system using a blockchain algorithm," in *SEB4SDG*. IEEE, 2024, pp. 1–12.

[125] J. Song, Y. Ju, Y. Wang, Y. Zou, C. Deng, X. Yuan, and C. Chen, "Blockchain identity authentication-aided trustworthy multicast routing strategy for leo satellite networks," in *iThings*. IEEE, 2023, pp. 256–261.

[126] G. Lian, Q. Sun, Y. Zou, Z. Gao, X. Wang, and T.-X. Zheng, "Blockchain identity authentication-based secure cooperative communications for smart grid cps," in *SmartIoT*. IEEE, 2023, pp. 72–79.

[127] M. J. Sunitha, C. Asendra, B. Kumar, E. H. Goud, and S. Basha, "User authentication scheme and identity management for e-health systems using blockchain technology," in *ICKECS*. IEEE, 2024, pp. 1–7.

[128] L. Xin, W. Zhijun, and Y. Meng, "T-atmchain: Blockchain-based identity authentication for air traffic management," *China Communications*, pp. 1–17, 2024.

[129] M. Chen, M. Qin, Y. Huang, Z. Liang, T. Liu, and C. Zhong, "Research on identity authentication of iot devices based on blockchain," in *ICPICS*. IEEE, 2022, pp. 458–465.

[130] Z. Dong, W. Tong, Z. Zhang, J. Li, W. Yang, and Y. Shen, "Blockchain-based identity authentication oriented to multi-cluster uav networking," in *Blockchain*. IEEE, 2023, pp. 68–73.

[131] C. Sullivan and E. Burger, "Blockchain, digital identity, e-government," in *Business Transformation through Blockchain*, H. Treiblmaier and R. Beck, Eds. Springer International Publishing, 2019, pp. 233–258.

[132] M. Polychronaki, D. G. Kogias, and C. Z. Patrikakis, "Identity management in internet of things with blockchain," in *Blockchain based Internet of Things*, D. De, S. Bhattacharyya, and J. J. P. C. Rodrigues, Eds. Springer Singapore, 2022, vol. 112, pp. 209–236.

[133] S. P. Otta and S. Panda, "Cloud identity and access management solution with blockchain," in *Blockchain Technology: Applications and Challenges*, S. K. Panda, A. K. Jena, S. K. Swain, and S. C. Satapathy, Eds. Springer International Publishing, 2021, vol. 203, pp. 243–270.

[134] X. Yu, R. Ge, and F. Li, "Research on blockchain-based identity authentication scheme in social networks," in *Machine Learning for Cyber Security*, X. Chen, H. Yan, Q. Yan, and X. Zhang, Eds. Springer International Publishing, 2020, vol. 12486, pp. 558–565.

[135] Y. Guo, X. Chen, S. Tian, L. Yang, X. Liang, J. Lian, D. Jin, A. Balabontsev, and Z. Zhang, "Blockchain based trusted identity authentication in ubiquitous power internet of things," in *Intelligent Computing Theories and Application*, D.-S. Huang, K.-H. Jo, J. Li, V. Gribova, and A. Hussain, Eds. Springer International Publishing, 2021, vol. 12837, pp. 294–302.

[136] J. Wang, S. Wei, and H. Liu, "Decentralized identity authentication with trust distributed in blockchain backbone," in *Blockchain – ICBC 2019*, J. Joshi, S. Nepal, Q. Zhang, and L.-J. Zhang, Eds. Springer International Publishing, 2019, vol. 11521, pp. 202–210.

[137] Z. Zhang, S. Shao, C. Zhong, S. Sun, and P. Lin, "Trusted identity authentication mechanism for power maintenance personnel based on blockchain," in *The 10th International Conference on Computer Engineering and Networks*, Q. Liu, X. Liu, T. Shen, and X. Qiu, Eds. Springer Singapore, 2021, vol. 1274, pp. 883–889.

[138] W. Ao, S. Fu, C. Zhang, and M. Xu, "A secure certificateless identity authentication scheme based on blockchain," in *Trusted Computing and Information Security*, W. Han, L. Zhu, and F. Yan, Eds. Springer Singapore, 2020, vol. 1149, pp. 251–266.

[139] D. Bao and L. You, "Two-factor identity authentication scheme based on blockchain and fuzzy extractor," *Soft Computing*, vol. 27, pp. 1091–1103, 2023.

[140] C. Han and F. Wen, "Certificateless identity management and authentication scheme based on blockchain technology," in *Proceeding of 2021 International Conference on Wireless Communications, Networking and Applications*, Z. Qian, M. Jabbar, and X. Li, Eds. Springer Nature Singapore, 2022, pp. 1077–1088.

[141] L. Moyo and J. Du Toit, "The use of blockchain for identity and access management (iam) in multi-cloud," in *Proceedings of Ninth International Congress on Information and Communication Technology*, X.-S. Yang,

S. Sherratt, N. Dey, and A. Joshi, Eds. Springer Nature Singapore, 2024, vol. 1003, pp. 149–159.

[142] C. Laroiya, M. K. Bhatia, S. Madan, and C. Komalavalli, "Iot and blockchain-based method for device identity verification," in *International Conference on Innovative Computing and Communications*, D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, and A. Jaiswal, Eds. Springer Nature Singapore, 2023, vol. 473, pp. 269–280.

[143] Z. Tu, H. Zhou, K. Li, H. Song, and W. Wang, "A blockchain-based user identity authentication method for 5g," in *Mobile Internet Security*, I. You, H. Kim, T.-Y. Youn, F. Palmieri, and I. Kotenko, Eds. Springer Nature Singapore, 2022, vol. 1544, pp. 335–351.

[144] Y. Fu, J. Shao, Q. Huang, Q. Zhou, H. Feng, X. Jia, R. Wang, and W. Feng, "Non-transferable blockchain-based identity authentication," *Peer-to-Peer Networking and Applications*, vol. 16, pp. 1354–1364, 2023.

[145] Y. Chen, G. Dong, Y. Hao, Z. Zhang, H. Peng, and S. Yu, "An Open Identity Authentication Scheme Based on Blockchain," in *Algorithms and Architectures for Parallel Processing*. Cham: Springer International Publishing, 2020, pp. 421–438.

[146] S. Li, M. Liu, and S. Wei, "A distributed authentication protocol using identity-based encryption and blockchain for leo network," in *Security, Privacy, and Anonymity in Computation, Communication, and Storage*, G. Wang, M. Atiquzzaman, Z. Yan, and K.-K. R. Choo, Eds. Springer International Publishing, 2017, vol. 10656, pp. 446–460.

[147] B. Leiding and A. Norta, "Mapping requirements specifications into a formalized blockchain-enabled authentication protocol for secured personal identity assurance," in *Future Data and Security Engineering*. Springer, 2017, pp. 181–196.

[148] J.-C. Huang, M.-H. Shu, B.-M. Hsu, and C.-M. Hu, "Service architecture of iot terminal connection based on blockchain identity authentication system," *Computer Communications*, vol. 160, pp. 411–422, 2020.

[149] M. Kara, H. R. Merzeh, M. A. Aydın, and H. H. Balık, "Voipchain: A decentralized identity authentication in voice over ip using blockchain," *Computer Communications*, vol. 198, pp. 247–261, 2023.

[150] C.-H. Liao, X.-Q. Guan, J.-H. Cheng, and S.-M. Yuan, "Blockchain-based identity management and access control framework for open banking ecosystem," *Future Generation Computer Systems*, vol. 135, pp. 450–466, 2022.

[151] Z. Tian, B. Yan, Q. Guo, J. Huang, and Q. Du, "Feasibility of identity authentication for iot based on blockchain," *Procedia Computer Science*, vol. 174, pp. 328–332, 2020.

[152] W. Wang, B. Yan, B. Chai, R. Shen, A. Dong, and J. Yu, "EBIAS: ECC-enabled blockchain-based identity authentication scheme for IoT device," *High-Confidence Computing*, vol. 5, p. 100240, 2024.

[153] S. Gao, Q. Su, R. Zhang, J. Zhu, Z. Sui, and J. Wang, "A privacy-preserving identity authentication scheme based on the blockchain," *Security and Communication Networks*, vol. 2021, pp. 1–10, 2021.

[154] H. Wang and Y. Jiang, "A novel blockchain identity authentication scheme implemented in fog computing," *Wireless Communications and Mobile Computing*, vol. 2020, pp. 1–7, 2020.

[155] G. Zhao, B. Di, and H. He, "A novel decentralized cross-domain identity authentication protocol based on blockchain," *Transactions on Emerging Telecommunications Technologies*, vol. 33, 2022.

[156] E. S. Babu, A. K. Dadi, K. K. Singh, S. R. Nayak, A. K. Bhoi, and A. Singh, "A distributed identity-based authentication scheme for internet of things devices using permissioned blockchain system," *Expert Systems*, vol. 39, p. e12941, 2022.

[157] A. Ganeshan, S. Jayagopalan, B. Perumal, and V. Sarveshwaran, "Secure identity key and blockchain-based authentication approach for secure data communication in multi-wsn," *Concurrency and Computation: Practice and Experience*, vol. 35, p. e7861, 2023.

[158] O. H. Padmanegara, R. K. Putri, R. Yuliani, and E. K. Masli, "Blockchain and the public sector: Blockchain-based identity management systems for public services and the impact on privacy and security risks," in *ICONDBTM*. IEEE, 2023, pp. 1–6.

[159] N. Priya, M. Ponnavaikko, and R. Aantonny, "An efficient system framework for managing identity in educational system based on blockchain technology," in *ic-ETITE*. IEEE, 2020, pp. 1–5.

[160] Y. Guo, Z. Qi, X. Xian, H. Wu, Z. Yang, J. Zhang, and L. Wenyin, "WISChain: An online insurance system based on blockchain and denglu1 for web identity security," in *HotICN*. IEEE, 2018, pp. 242–243.

[161] A. S. Sani, D. Yuan, K. Meng, and Z. Y. Dong, "Idenx: A blockchain-based identity management system for supply chain attacks mitigation in smart grids," in *PESGM*. IEEE, 2020, pp. 1–5.

[162] B. Li, M. Ma, and R. Xia, "Hierarchical identity-based security mechanism using blockchain in named data networking," in *HotICN*. IEEE, 2020, pp. 148–153.

[163] L. Zeng, W. Qiu, X. Wang, H. Wang, Y. Yao, and D. He, "A persistent data structure for managing digital identity data implemented on the blockchain," in *ICPICS*. IEEE, 2021, pp. 226–230.

[164] H. V, S. J. Quraishi, and S. Sinha, "Single identity system for identification papers based on blockchain," in *ICICICT*. IEEE, 2022, pp. 1484–1490.

[165] J. A. Costales, S. Shiromani, and M. Devaraj, "The impact of blockchain technology to protect image and video integrity from identity theft using deepfake analyzer," in *ICIDCA*. IEEE, 2023, pp. 730–733.

[166] C. R. A. N. Sharma, D. Swetchana, and S. M. Rajagopal, "AI anomaly detection with decentralized identity management on blockchain," in *CONECCT*. IEEE, 2024, pp. 1–6.

[167] J. Zhou, J. Hong, C. Zhu, F. Zou, and C. Hua, "Trustful blockchain-enabled identity management for vanet with short-latency authentication," in *ICNC*. IEEE, 2024, pp. 659–663.

[168] N. Goyal, V. Veeraiah, A. Namdev, R. Anand, A. Gupta, and S. Shilpa, "IoT based blockchain system for security from identity theft in industrial automation," in *Trends in Quantum Computing and Emerging Business Technologies*. IEEE, 2024, pp. 1–4.

[169] D. W. Kravitz and J. Cooper, "Securing user identity and transactions symbiotically: IoT meets blockchain," in *GIoTS*. IEEE, 2017, pp. 1–6.

[170] D.-P. Le, H. Meng, L. Su, S. L. Yeo, and V. Thing, "BIFF: A blockchain-based iot forensics framework with identity privacy," in *TENCON*. IEEE, 2018, pp. 2372–2377.

[171] K. Bendiab, N. Kolokotronis, S. Shiaeles, and S. Boucherkha, "WiP: A novel blockchain-based trust model for cloud identity management," in *DASC/PiCom/DataCom/CyberSciTech*. IEEE, 2018, pp. 724–729.

[172] M. P. Bhattacharya, P. Zavarsky, and S. Butakov, "Enhancing the security and privacy of self-sovereign identities on hyperledger indy blockchain," in *ISNCC*. IEEE, 2020, pp. 1–7.

[173] P. K. Deb, A. Mukherjee, and S. Misra, "CovChain: Blockchain-enabled identity preservation and anti-infodemics for covid-19," *IEEE Network*, vol. 35, no. 3, pp. 42–47, 2021.

[174] Y. Zheng, Y. Li, Z. Wang, C. Deng, Y. Luo, Y. Li, and J. Ding, "Blockchain-based privacy protection unified identity authentication," in *CyberC*. IEEE, 2019, pp. 42–49.

[175] X. Ren, F. Lin, Z. Chen, C. Tang, Z. Zheng, and M. Li, "BIA: A blockchain-based identity authorization mechanism," in *MSN*. IEEE, 2020, pp. 98–105.

[176] J. Zheng, X. Huang, J. Odoom, and Y. Xiang, "A privacy-aware electronic medical record sharing scheme based on blockchain and identity-based cryptography," in *ICBCTIS*. IEEE, 2023, pp. 94–100.

[177] N. H. M. Arafat, M. I. Pramanik, S. Jahan, M. N. Uddin, M. S. Islam, and K. F. Akter, "BloSecR: A conceptual framework of identity documents' security on blockchain in refugee issues and conserving fundamental rights," in *CONIT*. IEEE, 2022, pp. 1–6.

[178] H. Xu, X. Zhang, Q. Cui, and X. Tao, "A dynamic blockchain-based mutual authenticating identity management system for next-generation network," *IEEE Communications Magazine*, vol. 61, no. 8, pp. 116–122, 2023.

[179] B. Alamri, I. Richardson, and K. Crowley, "Cybersecuriy risk management and evaluation framework of blockchain identity management systems in hiot: Experts evaluation," *IEEE Access*, vol. 12, pp. 144 652–144 683, 2024.

[180] R. Selvanambi, B. Taneja, P. Agrawal, H. J. Thakor, and M. Karuppiah, "Blockchain-based identity management systems," in *Cyber Security and Network Security*, S. Pramanik, D. Samanta, M. Vinay, and A. Guha, Eds. Wiley, 2022, pp. 95–127.

[181] S. Sakka, V. Liagkou, and C. Stylios, "A blockchain identity privacy management framework for a healthcare application," in *Blockchain*. IEEE, 2024, pp. 599–604.

[182] K. Janani and S. Ramamoorthy, "A security framework to enhance iot device identity and data access through blockchain consensus model," *Cluster Computing*, vol. 27, no. 3, pp. 2877–2900, 2024.

[183] F. Angiulli, F. Fassetti, A. Furfaro, A. Piccolo, and D. Saccà, "Achieving service accountability through blockchain and digital identity," in *Information Systems in the Big Data Era*, J. Mendling and H. Mouratidis, Eds. Springer International Publishing, 2018, vol. 317, pp. 16–23.

[184] T. Rathee and P. Singh, "Secure data sharing using merkle hash digest based blockchain identity management," *Peer-to-Peer Networking and Applications*, vol. 14, no. 6, pp. 3851–3864, 2021.

[185] J. N. Benedict, S. Udhayakumar, B. R. Vikram, and C. Vignesh, "Identity management using blockchain network for fail-safe e-governance," in *Advances in Smart System Technologies*, P. Suresh, U. Saravanakumar, and M. S. Hussein Al Salameh, Eds. Springer Singapore, 2021, vol. 1163, pp. 747–757.

[186] S. H. G. Salem, A. Y. Hassan, M. S. Moustafa, and M. N. Hassan, "Blockchain-based biometric identity management," *Cluster Computing*, vol. 27, no. 3, pp. 3741–3752, 2024.

[187] Y. Yuan, J. Zhang, W. Xu, and Z. Li, "Identity-based public data integrity verification scheme in cloud storage system via blockchain," *The Journal of Supercomputing*, vol. 78, no. 6, pp. 8509–8530, 2022.

[188] S. K. Jena and R. C. Barik, "Decentralized digital identity: A new form of secured identity using blockchain technology," in *Key Digital Trends Shaping the Future of Information and Management Science*, L. Garg, D. S. Sisodia, N. Kesswani, J. G. Vella, I. Brigui, S. Misra, and D. Singh, Eds. Springer International Publishing, 2023, vol. 671, pp. 93–102.

[189] V. Odelu, "IMBUA: Identity management on blockchain for biometrics-based user authentication," in *Blockchain and Applications*, J. Prieto, A. K. Das, S. Ferretti, A. Pinto, and J. M. Corchado, Eds. Springer International Publishing, 2020, vol. 1010, pp. 1–10.

[190] L. Wang, X. Huang, L. Chen, J. Fan, and M. Zhang, "Credible identity authentication mechanism of electric internet of things based on blockchain," in *The 10th International Conference on Computer Engineering and Networks*, Q. Liu, X. Liu, T. Shen, and X. Qiu, Eds. Springer Singapore, 2021, vol. 1274, pp. 866–875.

[191] C. Zhuang, Q. Dai, and Y. Zhang, "BCPPT: A blockchain-based privacy-preserving and traceability identity management scheme for intellectual property," *Peer-to-Peer Networking and Applications*, vol. 15, no. 1, pp. 724–738, 2022.

[192] Z. Zhang, J. Xu, G. Dong, and J. Lin, "Application and challenges of blockchain in heterogeneous identity trust," in *Blockchain and Trustworthy Systems*, H.-N. Dai, X. Liu, D. X. Luo, and X. Chen, Eds. Springer Singapore, 2021, vol. 1490, pp. 163–168.

[193] A. Pillai, V. Saraswat, and A. V. Ramachandran, "Protection guidelines for blockchain based digital identity," in *Hybrid Intelligent Systems*, A. Abraham, P. Siarry, V. Piuri, N. Gandhi, G. Casalino, O. Castillo, and P. Hung, Eds. Springer International Publishing, 2022, vol. 420, pp. 636–646.

[194] A. Pillai, V. Saraswat, and A. Vasanthakumary Ramachandran, "Attacks on blockchain based digital identity," in *Blockchain and Applications*, J. Prieto, A. Partida, P. Leitão, and A. Pinto, Eds. Springer International Publishing, 2022, vol. 320, pp. 329–338.

[195] X. Zou, X. Deng, T.-Y. Wu, and C.-M. Chen, "A collusion attack on identity-based public auditing scheme via blockchain," in *Advances in Intelligent Information Hiding and Multimedia Signal Processing*, J.-S. Pan, J. Li, P.-W. Tsai, and L. C. Jain, Eds. Springer Singapore, 2020, vol. 156, pp. 97–105.

[196] Y. Yang, W. Wan, S. Zhang, J. Zhang, Z. Qin, and J. Xia, "A blockchain-based risk assessment model for heterogeneous identity alliance," in *Advances in Artificial Intelligence and Security*, X. Sun, X. Zhang, Z. Xia, and E. Bertino, Eds. Springer International Publishing, 2022, vol. 1588, pp. 14–27.

[197] J. Xue, C. Xu, J. Zhao, and J. Ma, "Identity-based public auditing for cloud storage systems against malicious auditors via blockchain," *Science China Information Sciences*, vol. 62, no. 3, p. 32104, 2019.

[198] B. Li and M. Ma, "An advanced hierarchical identity-based security mechanism by blockchain in named data networking," *Journal of Network and Systems Management*, vol. 31, no. 1, p. 13, 2023.

[199] I. Damgård, C. Ganesh, H. Khoshakhlagh, C. Orlandi, and L. Siniscalchi, "Balancing privacy and accountability in blockchain identity management," in *Topics in Cryptology – CT-RSA 2021*, K. G. Paterson, Ed. Springer International Publishing, 2021, vol. 12704, pp. 552–576.

[200] A. Norta, R. Matulevičius, and B. Leiding, "Safeguarding a formalized blockchain-enabled identity-authentication protocol by applying security risk-oriented patterns," *Computers & Security*, vol. 86, pp. 253–269, 2019.

[201] F. Wang, Y. Gai, and H. Zhang, "Blockchain user digital identity big data and information security process protection based on network trust," *Journal of King Saud University - Computer and Information Sciences*, vol. 36, no. 4, p. 102031, 2024.

[202] D. Awasthi, P. Khare, and V. Kumar Srivastava, "RFDB: Robust watermarking scheme with fuzzy-dncnn using blockchain technique for identity verification," *Expert Systems with Applications*, vol. 255, p. 124554, 2024.

[203] P. Sharma, N. R. Moparthi, S. Namasudra, V. Shanmuganathan, and C. Hsu, "Blockchain-based iot architecture to secure healthcare system using identity-based encryption," *Expert Systems*, vol. 39, no. 10, p. e12915, 2022.

[204] K. Janani and S. Ramamoorthy, "Piot -fortifying iot device identity and data access: A security framework empowered by blockchain," *SECURITY AND PRIVACY*, vol. 7, no. 6, p. e443, 2024.

[205] A. Dixit, M. Smith-Creasey, and M. Rajarajan, "A decentralized iiot identity framework based on self-sovereign identity using blockchain," in *LCN*. IEEE, 2022, pp. 335–338.

[206] A. H. M. Amin, N. Abdelmajid, and F. N. Kiwanuka, "Identity-of-things model using composite identity on permissioned blockchain network," in *SDS*. IEEE, 2020, pp. 171–176.

[207] M. Dabrowski and P. Pacyna, "Blockchain-based identity discovery between heterogeneous identity management systems," in *CSP*. IEEE, 2022, pp. 131–137.

[208] K. Mudliar, H. Parekh, and P. Bhavathankar, "A comprehensive integration of national identity with blockchain technology," in *ICCICT*. IEEE, 2018, pp. 1–6.

[209] R. Chen, F. Shu, S. Huang, L. Huang, H. Liu, J. Liu, and K. Lei, "BIdM: A blockchain-enabled cross-domain identity management system," *Journal of Communications and Information Networks*, vol. 6, no. 1, pp. 44–58, 2021.

[210] G. Malik, K. Parasrampuria, S. P. Reddy, and S. Shah, "Blockchain based identity verification model," in *ViTECoN*. IEEE, 2019, pp. 1–6.

[211] Y. Liang, "Identity verification and management of electronic health records with blockchain technology," in *ICHI*. IEEE, 2019, pp. 1–3.

[212] M. Htet, P. T. Yee, and J. R. Rajasekera, "Blockchain based digital identity management system: A case study of myanmar," in *ICAIT*. IEEE, 2020, pp. 42–47.

[213] Z. Zhang, Y. Sun, P. Huang, and C. Wang, "A blockchain and multi factor fusion based electronic identity registration and verification system," in *ICCSMT*. IEEE, 2022, pp. 431–435.

[214] S. Srivastava, V. Grover, M. Nallakaruppan, B. Krishwanth, and K. Saravanan, "Decentralization of identities using blockchain," in *UPCON*. IEEE, 2023, pp. 1304–1309.

[215] V. Nehra, A. Mj, H. Khanna, and N. Jindal, "Decentralized digital identity verification system using blockchain technology," in *ICIPTM*. IEEE, 2024, pp. 1–6.

[216] S. Katta, K. Alrawashdeh, J. Adebayo, M. Tulasi, and M. Dokka, "Blockchain-based distributed hybrid cloud identity management for securing iot devices in the cloud," in *NAECON*. IEEE, 2023, pp. 67–72.

[217] Z. Peng, J. Deng, S. Gao, H. Cui, and B. Xiao, "vDID: Blockchain-enabled verifiable decentralized identity management for web 3.0," in *IWQoS*. IEEE, 2024, pp. 1–2.

[218] A. S. Omar and O. Basir, "Identity management in iot networks using blockchain and smart contracts," in *iThings*. IEEE, 2018, pp. 994–1000.

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

[220] D. Maldonado-Ruiz, J. Torres, N. El Madhoun, and M. Badra, "An innovative and decentralized identity framework based on blockchain technology," in *NTMS*. IEEE, 2021, pp. 1–8.

[221] B. C. Ghosh, V. Ramakrishna, C. Govindarajan, D. Behl, D. Karunamoorthy, E. Abebe, and S. Chakraborty, "Decentralized cross-network identity management for blockchain interoperation," in *ICBC*. IEEE, 2021, pp. 1–9.

[222] Y. Liu, B. Zhao, Z. Zhao, J. Liu, X. Lin, Q. Wu, and W. Susilo, "SS-DID: A secure and scalable web3 decentralized identity utilizing multilayer sharding blockchain," *IEEE Internet of Things Journal*, vol. 11, no. 15, pp. 25694–25705, 2024.

[223] D. A. Belurgikar, J. Kanak Kshirsagar, K. K. Dhananjaya, and N. Vineeth, "Identity solutions for verification using

blockchain technology," in *ICATIECE*. IEEE, 2019, pp. 121–126.

[224] Y. Chen, Y. Wang, Y. Wang, M. Li, G. Dong, and C. Liu, "CallChain: Identity authentication based on blockchain for telephony networks," in *CSCWD*. IEEE, 2021, pp. 416–421.

[225] L. Zou, J. Chen, Q. Lan, Z. Zhou, C. Ma, and Z. Yang, "Application of blockchain digital identity technology in healthcare consumer finance system," in *ICPECA*. IEEE, 2022, pp. 1212–1219.

[226] X. Zhan, X. Cheng, W. Guo, K. Yin, and X. Lu, "An distributed ca system: Identity authentication system in transnational railway transportation based on blockchain," in *CISAI*. IEEE, 2021, pp. 989–994.

[227] J. Hao, J. Gao, P. Xiang, J. Zhang, Z. Chen, H. Hu, and Z. Chen, "TDID: Transparent and efficient decentralized identity management with blockchain," in *SMC*. IEEE, 2023, pp. 1752–1759.

[228] K. R. N'Goran, J.-L. Tetchueng, Y. Kermarrec, A. P. B. Brou, and O. Asseu, "Blockchain-based identity and access management in a community cloud," in *SoftCOM*. IEEE, 2023, pp. 1–6.

[229] A. A. Varfolomeev and L. H. Al-Farhani, "Blockchain based digital identity management system for smart city services," in *ICITAMS*. IEEE, 2023, pp. 79–85.

[230] S. B. Öztürk and M. Aydos, "A blockchain based decentralized identity, access management, and trust evaluation framework for iot," in *ISCTürkiye*. IEEE, 2023, pp. 1–6.

[231] J. Guo, W. Yu, S. Ai, and J. Cao, "A decentralized identity based energy trading system over a blockchain network," in *ICEI*. IEEE, 2023, pp. 63–67.

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

[233] P. Sharma, W. Wilfred Godfrey, and A. Trivedi, "When blockchain meets iot: a comparison of the performance of communication protocols in a decentralized identity solution for iot using blockchain," *Cluster Computing*, vol. 27, no. 1, pp. 269–284, 2024.

[234] Y. Zhang, L. Zhang, Q. Zhang, P. Zheng, X. Jia, and X. Chen, "DSBT: Research on soulbound token mechanism based on consortium blockchain and decentralized identity," in *Computational and Experimental Simulations in Engineering*, S. Li, Ed. Springer International Publishing, 2024, vol. 145, pp. 489–506.

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

[236] D. Patole, Y. Borse, J. Jain, and S. Maher, "Personal identity on blockchain," in *Advances in Computing and Intelligent Systems*, H. Sharma, K. Govindan, R. C. Poonia, S. Kumar, and W. M. El-Medany, Eds. Springer Singapore, 2020, pp. 439–446.

[237] Z. Wang, M. Duan, and M. Wang, "An updatable and revocable decentralized identity management scheme based on blockchain," in *Data Science*, Z. Yu, Q. Han, H. Wang, B. Guo, X. Zhou, X. Song, and Z. Lu, Eds. Springer Nature Singapore, 2023, vol. 1879, pp. 372–388.

[238] A. Berbar and A. Belkhir, "Blockchain-based identity management," in *IoT-Enabled Energy Efficiency Assessment of Renewable Energy Systems and Micro-grids in Smart Cities*, M. Hatti, Ed. Springer Nature Switzerland, 2024, vol. 984, pp. 78–85.

[239] S. Odeh, A. Samara, R. Rizqallah, and L. Shaheen, "Digital identity using hyperledger fabric as a private blockchain-based system," in *Blockchain and Applications, 4th International Congress*, J. Prieto, F. L. Benítez Martínez, S. Ferretti, D. Arroyo Guardeño, and P. Tomás Nevado-Batalla, Eds. Springer International Publishing, 2023, vol. 595, pp. 153–161.

[240] L. Zhang, "A cross network identity authentication scheme for uavs based on layered blockchain technology," in *Advances in Intelligent Networking and Collaborative Systems*, L. Barolli, Ed. Springer Nature Switzerland, 2024, vol. 225, pp. 131–141.

[241] S. He, T. Sun, Q. Tang, C. Wu, N. Lipka, C. Wigington, and R. Jain, "Secure and efficient agreement signing atop blockchain and decentralized identity," in *Blockchain and Trustworthy Systems*, D. Svetinovic, Y. Zhang, X. Luo, X. Huang, and X. Chen, Eds. Springer Nature Singapore, 2022, vol. 1679, pp. 3–17.

[242] D. Das, K. Dasgupta, and U. Biswas, "A secure blockchain-enabled vehicle identity management framework for intelligent transportation systems," *Computers and Electrical Engineering*, vol. 105, p. 108535, 2023.

[243] E. Zeydan, J. Mangues-Bafalluy, S. Arslan, and Y. Turk, "Blockchain-based self-sovereign identity solution for aerial base station integrated networks," *Vehicular Communications*, vol. 47, p. 100759, 2024.

[244] Y. Gong, B. Yu, L. Yang, F. Meng, L. Liu, X. Hu, and Z. Xu, "Toward next-generation networks: A blockchain-based approach for core network architecture and roaming identity verification," *Digital Communications and Networks*, p. S2352864824000993, 2024.

[245] A. Bhattacharya, "Blockchain-based identity management," in *Blockchain for Business*, S. Tyagi and S. Bhatia, Eds. Wiley, 2021, pp. 141–158.

[246] J. Li and Y. Jing, "Establishing an international engagement model of digital identity based on blockchain," *Mobile Information Systems*, vol. 2022, pp. 1–7, 2022.

[247] A. Gupta, R. Gupta, K. Gohil, S. Tanwar, and D. Garg, "Blockchain-based decentralized oracle network framework for identity management in metaverse environment," *SECURITY AND PRIVACY*, vol. 7, p. e414, 2024.

[248] "Identity as a panacea for the real world," in *Blockchain for Real World Applications*, R. Garg, Ed. Wiley, 2022, pp. 87–113.

[249] D. A. Torres, "Tutorial: Decentralized digital identity with blockchain," in *ICEDEG*. IEEE, 2021, pp. 12–12.

[250] N. Naik and P. Jenkins, "Sovrin network for decentralized digital identity: Analysing a self-sovereign identity system

based on distributed ledger technology," in *ISSE*. IEEE, 2021, pp. 1–7.

[251] P. Bhattacharjee, C. Prakash, S. Gairola, S. S. Lala, and P. Mukherjee, "DigiBlock: Digital self-sovereign identity on distributed ledger based on blockchain," in *ASSIC*. IEEE, 2022, pp. 1–7.

[252] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, S. S. Arslan, Y. Turk, A. Kumar Yadav, and M. Liyanage, "Blockchain-based self-sovereign identity: Taking control of identity in federated learning," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 5764–5781, 2024.

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

[254] Z. Song and Y. Yu, "The digital identity management system model based on blockchain," in *ICBCTIS*. IEEE, 2022, pp. 131–137.

[255] D. N. Kirupanithi and A. Antonidoss, "Self-sovereign identity management system on blockchain based applications using chameleon hash," in *ICOSEC*. IEEE, 2021, pp. 386–390.

[256] S. Srivastava, D. Agarwal, and B. Chaurasia, "Secure decentralized identity management using blockchain," in *TrustCom*. IEEE, 2023, pp. 1355–1360.

[257] J. H. M. Emati, H. P. Mboussam, and V. K. Tchendji, "Feasibility study of improving blockchain-based self-sovereign identity security using artificial intelligence and lightweight cryptography," in *AFRICON*. IEEE, 2023, pp. 01–03.

[258] M. S. Ferdous, F. Chowdhury, and M. O. Alassafi, "In search of self-sovereign identity leveraging blockchain technology," *IEEE Access*, vol. 7, pp. 103 059–103 079, 2019.

[259] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan, and S. Wang, "An identity management system based on blockchain," in *PST*. IEEE, 2017, pp. 44–4409.

[260] S. Malik, N. Gupta, V. Dedeoglu, S. S. Kanhere, and R. Jurdak, "TradeChain: Decoupling traceability and identity in blockchain enabled supply chains," in *TrustCom*. IEEE, 2021, pp. 1141–1152.

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

[262] P. Mishra, V. Modanwal, H. Kaur, and G. Varshney, "Pseudo-biometric identity framework: Achieving self-sovereignty for biometrics on blockchain," in *SMC*. IEEE, 2021, pp. 945–951.

[263] K. A. M. Ahmed, S. F. Saraya, J. F. Wanis, and A. M. T. Ali-Eldin, "A self-sovereign identity architecture based on blockchain and the utilization of customer's banking cards: The case of bank scam calls prevention," in *ICCES*. IEEE, 2020, pp. 1–8.

[264] S. Bakare, S. C. Shinde, and R. Hubballi, "A blockchain framework for secure digital identity transactions in indian agri-subsidy system: Issues, challenges and benefits," in *ICCCT*. IEEE, 2021, pp. 138–143.

[265] A. Imtiaz, R. G. Rozario, P. Chakraborty, P. C. Talukder, and P. Roy, "Smart identity management system using blockchain technology," in *ICBDS*. IEEE, 2023, pp. 1–7.

[266] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, A. Aydeger, S. S. Arslan, Y. Turk, J. Bas, and S. K. Mishra, "Enhanced security with quantum key distribution and blockchain for digital identities," in *MeditCom*. IEEE, 2024, pp. 489–494.

[267] D. N. Kirupanithi and A. Antonidoss, "Hierarchical deterministic protocol for the defragmentation of identity in a blockchain-based framework," in *I-SMAC*. IEEE, 2021, pp. 1497–1504.

[268] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, S. S. Arslan, and Y. Turk, "Post-quantum blockchain-based decentralized identity management for resource sharing in open radio access networks," *IEEE Transactions on Green Communications and Networking*, vol. 8, no. 3, pp. 895–909, 2024.

[269] R. R. Sekar, A. Masna, S. Sharma, A. Abraham, and P. R. Pagilla, "Decentralized identity and access management (iam) using blockchain," in *ISCS*. IEEE, 2024, pp. 1–6.

[270] R. K, V. G. Sankar S, V. C, S. S.B, and A. Ramanan S, "Sign up wallet: A blockchain and machine learning based self-sovereign identity model for enhanced digital security," in *ICICV*. IEEE, 2024, pp. 851–857.

[271] A. Al Badi, F. Hajamohideen, and D. Alsaqri, "Enhancing identity management: Exploring the potential of blockchain technology," in *ICETCI*. IEEE, 2023, pp. 283–290.

[272] K. Moriyama and A. Otsuka, "Permissionless blockchain-based sybil-resistant self-sovereign identity utilizing attested execution secure processors," in *Blockchain*. IEEE, 2022, pp. 1–10.

[273] E. Zeydan, L. Blanco, J. Mangues-Bafalluy, A. Aydeger, S. Arslan, and Y. Turk, "Integrating quantum-secured blockchain identity management in open ran for 6g networks," in *LCN*. IEEE, 2024, pp. 1–7.

[274] S. Azouvi, M. Al-Bassam, and S. Meiklejohn, "Who am i? secure identity registration on distributed ledgers," in *Data Privacy Management, Cryptocurrencies and Blockchain Technology*, J. Garcia-Alfaro, G. Navarro-Arribas, H. Hartenstein, and J. Herrera-Joancomartí, Eds. Springer International Publishing, 2017, vol. 10436, pp. 373–389.

[275] B. Nassr Eddine, A. Ouaddah, and A. Mezrioui, "Blockchain-based self sovereign identity systems: High-level processing and a challenges-based comparative analysis," in *International Conference on Advanced Intelligent Systems for Sustainable Development*, J. Kacprzyk, M. Ezziyyani, and V. E. Balas, Eds. Springer Nature Switzerland, 2023, vol. 637, pp. 489–500.

[276] M. Chawla and S. Gupta, "The changing landscape of identity and access management with blockchain-based self-sovereign identity," in *ICT Infrastructure and Computing*, M. Tuba, S. Akashe, and A. Joshi, Eds. Springer Nature Singapore, 2023, vol. 520, pp. 691–702.

[277] F. Schardong, R. Custódio, L. Pioli, and J. Meyer, "Matching metadata on blockchain for self-sovereign identity," in *Business Process Management Workshops*, A. Marrella and B. Weber, Eds. Springer International Publishing, 2022, vol. 436, pp. 421–433.

[278] L. Anania, G. Le Gars, and R. Van Kranenburg, "Disposable identities? why digital identity matters

to blockchain disintermediation and for society," in *Disintermediation Economics*, E. Kaili and D. Psarrakis, Eds. Springer International Publishing, 2021, pp. 297–327.

[279] C. Dong, Z. Wang, S. Chen, and Y. Xiang, "BBM: A blockchain-based model for open banking via self-sovereign identity," in *Blockchain – ICBC 2020*, Z. Chen, L. Cui, B. Palanisamy, and L.-J. Zhang, Eds. Springer International Publishing, 2020, vol. 12404, pp. 61–75.

[280] Y.-H. Lee, Z.-Y. Liu, R. Tso, and Y.-F. Tseng, "Blockchain-based self-sovereign identity system with attribute-based issuance," in *Information Security Practice and Experience*, C. Su, D. Gritzalis, and V. Piuri, Eds. Springer International Publishing, 2022, vol. 13620, pp. 21–38.

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

[282] S. Sinha and C. Pradhan, "Blockchain technology enabled digital identity management in smart cities," in *Security and Privacy Applications for Smart City Development*, S. C. Tamane, N. Dey, and A.-E. Hassanien, Eds. Springer International Publishing, 2021, vol. 308, pp. 135–153.

[283] A. De Salve, D. Di Francesco Maesa, P. Mori, L. Ricci, and A. Puccia, "A multi-layer trust framework for self sovereign identity on blockchain," *Online Social Networks and Media*, vol. 37-38, p. 100265, 2023.

[284] M. S. Ferdous, U. Cali, U. Halden, and W. Prinz, "Leveraging self-sovereign identity & distributed ledger technology in renewable energy certificate ecosystems," *Journal of Cleaner Production*, vol. 422, p. 138355, 2023.

[285] A. A. Agarkar, M. Karyakarte, G. Chavhan, M. Patil, R. Talware, and L. Kulkarni, "Blockchain aware decentralized identity management and access control system," *Measurement: Sensors*, vol. 31, p. 101032, 2024.

[286] R. Seifert, "Digital identities – self-sovereignty and blockchain are the keys to success," *Network Security*, vol. 2020, pp. 17–19, 2020.

[287] V. Schlatt, J. Sedlmeir, S. Feulner, and N. Urbach, "Designing a framework for digital kyc processes built on blockchain-based self-sovereign identity," *Information & Management*, vol. 59, no. 7, p. 103553, 2022.

[288] N. Naik and P. Jenkins, "Governing principles of self-sovereign identity applied to blockchain enabled privacy preserving identity management systems," in *ISSE*. IEEE, 2020, pp. 1–6.

[289] R. Mecozzi, G. Perrone, D. Anelli, N. Saitto, E. Paggi, and D. Mancini, "Blockchain-related identity and access management challenges: (de)centralized digital identities regulation," in *Blockchain*. IEEE, 2022, pp. 443–448.

[290] M. M. Al-Musawi, "Transforming one-stop e-services in iraq: Focusing on perception of blockchain technology in digital identity system," in *GHTC*. IEEE, 2020, pp. 1–4.

[291] S. Choudhari, S. K. Das, and S. Parasher, "Interoperable blockchain solution for digital identity management," in *I2CT*. IEEE, 2021, pp. 1–6.

[292] W. Zhao, N. Yang, G. Li, and K. Zhang, "Research on digital identity technology and application based on identification code and trusted account blockchain fusion," in *AINIT*. IEEE, 2021, pp. 405–409.

[293] X. Qian, J. Li, and Y. Liu, "A regulated identity management system based on blockchain platform," in *EEBDA*. IEEE, 2023, pp. 103–108.

[294] A. Habib, T. Refat, and M. T. Ahad, "Blockchain based secured refugee identity management by using the assistance smart contract," in *ICREST*. IEEE, 2023, pp. 101–105.

[295] K. Lee, M. Lee, and H. Park, "A study on the factors affecting the intention to adopt of blockchain-based identity certification services in the defense sector," in *BCD*. IEEE, 2022, pp. 57–61.

[296] M. Grabatin and W. Hommel, "Reliability and scalability improvements to identity federations by managing saml metadata with distributed ledger technology," in *NOMS*. IEEE, 2018, pp. 1–6.

[297] A. Gruner, A. Muhle, T. Gayvoronskaya, and C. Meinel, "A quantifiable trust model for blockchain-based identity management," in *iThings*. IEEE, 2018, pp. 1475–1482.

[298] A. Theodouli, K. Moschou, K. Votis, D. Tzovaras, J. Lauinger, and S. Steinhorst, "Towards a blockchain-based identity and trust management framework for the iov ecosystem," in *GIoTS*. IEEE, 2020, pp. 1–6.

[299] A. Furfaro, L. Argento, D. Saccá, F. Angiulli, and F. Fassetti, "An infrastructure for service accountability based on digital identity and blockchain 3.0," in *INFOCOM WKSHPS*. IEEE, 2019, pp. 632–637.

[300] A. Sabir and N. Fetais, "A practical universal consortium blockchain paradigm for patient data portability on the cloud utilizing delegated identity management," in *ICIoT*. IEEE, 2020, pp. 484–489.

[301] V. Lemieux, A. Voskobojnikov, and M. Kang, "Addressing audit and accountability issues in self-sovereign identity blockchain systems using archival science principles," in *COMPSAC*. IEEE, 2021, pp. 1210–1216.

[302] S. Banerjee, S. Bouzefrane, and A. Abane, "Identity management with hybrid blockchain approach: A deliberate extension with federated-inverse-reinforcement learning," in *HPSR*. IEEE, 2021, pp. 1–6.

[303] I. Alom, R. M. Eshita, A. Ibna Harun, M. S. Ferdous, M. Kamrul Bashar Shuhan, M. J. M. Chowdhury, and M. Shahidur Rahman, "Dynamic management of identity federations using blockchain," in *ICBC*. IEEE, 2021, pp. 1–9.

[304] B. Tao, H.-N. Dai, H. Xie, and F. L. Wang, "Structural identity representation learning for blockchain-enabled metaverse based on complex network analysis," *IEEE Transactions on Computational Social Systems*, vol. 10, no. 5, pp. 2214–2225, 2023.

[305] D. Peralta-Velecela, M. C. Caceres-Salamea, and V. Morocho, "Digital identity proposal for unified medical record using blockchain technology," in *ETCM*. IEEE, 2021, pp. 1–6.

[306] J.-q. Liu, Y. Wu, L.-l. LShi, Z.-y. Li, and C. Liu, "A public blockchain-based identity management scheme and petri net-based verification," in *IUCC/CIT/DSCI/SmartCNS*. IEEE, 2021, pp. 361–368.

[307] B. Kumar Mohanta, M. Kumar Dehury, and S. Varma Kalidindi, "Identity management in iot using blockchain," in *ICCCNT*. IEEE, 2022, pp. 1–6.

[308] C. Zhang, M. Zhao, W. Zhang, Q. Fan, J. Ni, and L. Zhu, "Privacy-preserving identity-based data rights governance for blockchain-empowered human-centric metaverse communications," *IEEE Journal on Selected Areas in Communications*, vol. 42, no. 4, pp. 963–977, 2024.

[309] H. Li, T. Xie, and J. Xie, "A decentrlized trading model based on public blockchain with regulatable bi-tiered identities," in *ISPA/BDCloud/SocialCom/SustainCom*. IEEE, 2021, pp. 1189–1198.

[310] J. Hong, J. Zhou, Y. Li, J. Cheng, and C. Hua, "AcBF: A revocable blockchain-based identity management enabling low-latency authentication," in *ICDCS*. IEEE, 2024, pp. 312–321.

[311] E. S. Sin and T. T. Naing, "Digital identity management system using blockchain technology," in *International Conference on Innovative Computing and Communications*, D. Gupta, A. Khanna, S. Bhattacharyya, A. E. Hassanien, S. Anand, and A. Jaiswal, Eds. Springer Singapore, 2021, vol. 1166, pp. 895–906.

[312] A. Shobanadevi, S. Tharewal, M. Soni, D. D. Kumar, I. R. Khan, and P. Kumar, "Novel identity management system using smart blockchain technology," *International Journal of System Assurance Engineering and Management*, vol. 13, pp. 496–505, 2022.

[313] R. J. Ong, S. Sudin, R. A. A. Raof, and K. Y. Choong, "Utilizing blockchain technology for farmer identity management and land registry systems in agriculture," in *Intelligent System*, J. M. R. S. Tavares, S. Pal, V. C. Gerogiannis, and B. T. Hung, Eds. Springer Nature Singapore, 2024, pp. 459–467.

[314] S. Gilda, T. Jain, and A. Dhalla, "None shall pass: A blockchain-based federated identity management system," in *Inventive Computation and Information Technologies*, S. Smys, K. A. Kamel, and R. Palanisamy, Eds. Springer Nature Singapore, 2023, vol. 563, pp. 329–352.

[315] S. El Haddouti, A. Ouaguid, and M. D. Ech-Cherif El Kettani, "Fedidchain: An innovative blockchain-enabled framework for cross-border interoperability and trust management in identity federation systems," *Journal of Network and Systems Management*, vol. 31, p. 42, 2023.

[316] F. Buccafurri, G. Lax, A. Russo, and G. Zunino, "Integrating digital identity and blockchain," in *OTM 2018 Conferences*, H. Panetto, C. Debruyne, H. A. Proper, C. A. Ardagna, D. Roman, and R. Meersman, Eds. Springer International Publishing, 2018, vol. 11229, pp. 568–585.

[317] M. K. B. Shuhan, S. M. Hasnayeen, T. K. Das, M. N. Sakib, and M. S. Ferdous, "Decentralised identity federations using blockchain," *International Journal of Information Security*, vol. 23, pp. 2759–2782, 2024.

[318] K. Pinter, D. Schmelz, R. Lamber, S. Strobl, and T. Grechenig, "Towards a multi-party, blockchain-based identity verification solution to implement clear name laws for online media platforms," in *Blockchain and Central and Eastern Europe Forum*, C. Di Ciccio, R. Gabryelczyk, L. García-Bañuelos, T. Hernaus, R. Hull, M. Indihar Štemberger, A. Kő, and M. Staples, Eds. Springer International Publishing, 2019, vol. 361, pp. 151–165.

[319] R. Neisse, G. Steri, and I. N. Fovino, "Blockchain-based identity management and data usage control (extended abstract)," in *Privacy and Identity Management*, M. Hansen, E. Kosta, I. Nai-Fovino, and S. Fischer-Hübner, Eds. Springer International Publishing, 2018, vol. 526, pp. 237–239.

[320] M. Nuss, A. Puchta, and M. Kunz, "Towards blockchain-based identity and access management for internet of things in enterprises," in *Trust, Privacy and Security in Digital Business*, S. Furnell, H. Mouratidis, and G. Pernul, Eds. Springer International Publishing, 2018, vol. 11033, pp. 167–181.

[321] J. Wang, S. Li, and S. Wei, "Identity-based cross-domain authentication by blockchain via pki environment," in *Blockchain Technology and Application*, X. Si, H. Jin, Y. Sun, J. Zhu, L. Zhu, X. Song, and Z. Lu, Eds. Springer Singapore, 2020, vol. 1176, pp. 131–144.

[322] W. Shao, C. Jia, Y. Xu, K. Qiu, Y. Gao, and Y. He, "AttriChain: Decentralized traceable anonymous identities in privacy-preserving permissioned blockchain," *Computers & Security*, vol. 99, p. 102069, 2020.

[323] P. Li, H. Xu, and T. Ma, "An efficient identity tracing scheme for blockchain-based systems," *Information Sciences*, vol. 561, pp. 130–140, 2021.

[324] P. M. Yawalkar, D. N. Paithankar, A. R. Pabale, R. V. Kolhe, and P. William, "Integrated identity and auditing management using blockchain mechanism," *Measurement: Sensors*, vol. 27, p. 100732, 2023.

[325] S. Magar, M. Doshi, S. Talib, and H. Dalvi, "Blockchain-based reliable supply chain management (scm) for vaccine distribution and traceability using identity management approach," in *Unleashing the Potentials of Blockchain Technology for Healthcare Industries*. Elsevier, 2023, pp. 175–213.

[326] H. Xiong, L. Gong, R. Li, S. Kumari, C.-M. Chen, and M. Amoon, "Blockchain-enabled distributed identity-based ring signature with identity abort for consumer electronics," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 3, pp. 5340–5352, 2024.

[327] S. Anwar, V. K. Shukla, S. S. Rao, B. K. Sharma, and P. Sharma, "Framework for financial auditing process through blockchain technology, using identity based cryptography," in *ITT*. IEEE, 2019, pp. 099–103.

[328] D. Maldonado-Ruiz, J. Torres, and N. El Madhoun, "3BI-ECC: a decentralized identity framework based on blockchain technology and elliptic curve cryptography," in *BRAINS*. IEEE, 2020, pp. 45–46.

[329] L. Zhang and Y. Ge, "Identity authentication based on domestic commercial cryptography with blockchain in the heterogeneous alliance network," in *ICCECE*. IEEE, 2021, pp. 191–195.

[330] S. Gupta, A. K. Bairwa, S. S. Kushwaha, and S. Joshi, "Decentralized identity management system using the amalgamation of blockchain technology," in *ICCT*. IEEE, 2023, pp. 1–6.

[331] Y. Yu, Z. Li, Y. Tu, Y. Yuan, Y. Li, and Z. Pang, "Blockchain-based distributed identity cryptography key management," in *ICCRD*. IEEE, 2023, pp. 236–240.

[332] Z. Duan, J. Zhu, and J. Y. Zhao, "IAM-BDSS: A secure ciphertext-policy and identity-attribute management data sharing scheme based on blockchain," in *ICBCTIS*. IEEE, 2022, pp. 117–122.

[333] U. Archana, M. Jeyalaxmi, A. Vijayaprabhu, K. Dhanalakshmi, Y. Geetha, and Y. P. Ragini, "Enhanced cyber logic: A robust design of identity based encryption mechanism to secure data using blockchain technology," in *CONIT*. IEEE, 2024, pp. 1–5.

[334] C. Lin, D. He, X. Huang, M. Khurram Khan, and K.-K. R. Choo, "A new transitively closed undirected graph authentication scheme for blockchain-based identity management systems," *IEEE Access*, vol. 6, pp. 28 203–28 212, 2018.

[335] Y. Yang, D. He, P. Vijayakumar, B. B. Gupta, and Q. Xie, "An efficient identity-based aggregate signcryption scheme with blockchain for iot-enabled maritime transportation system," *IEEE Transactions on Green Communications and Networking*, vol. 6, no. 3, pp. 1520–1531, 2022.

[336] B. Zhou, H. Li, and L. Xu, "An authentication scheme using identity-based encryption & blockchain," in *ISCC*. IEEE, 2018, pp. 00 556–00 561.

[337] V. Srivastava, S. K. Debnath, B. Bera, A. K. Das, Y. Park, and P. Lorenz, "Blockchain-envisioned provably secure multivariate identity-based multi-signature scheme for internet of vehicles environment," *IEEE Transactions on Vehicular Technology*, vol. 71, no. 9, pp. 9853–9867, 2022.

[338] Z. Wan, W. Liu, and H. Cui, "HIBEChain: A hierarchical identity-based blockchain system for large-scale iot," *IEEE Transactions on Dependable and Secure Computing*, vol. 20, no. 2, pp. 1286–1301, 2023.

[339] J. Zhang and F. Zhang, "Identity-based key agreement for blockchain-powered intelligent edge," *IEEE Internet of Things Journal*, vol. 9, no. 9, pp. 6688–6702, 2022.

[340] J. Cai, X. Tao, and C. Wang, "Cooperative authentication scheme for heterogeneous networks based on identity group signature and blockchain," *IEEE Transactions on Vehicular Technology*, vol. 73, no. 1, pp. 1394–1399, 2024.

[341] Z. Wang, L. Qian, D. Chen, and G. Sun, "Sharing of encrypted lock keys in the blockchain-based renting house system from time- and identity-based proxy reencryption," *China Communications*, vol. 19, no. 5, pp. 164–177, 2022.

[342] R. Geetha, S. Kalpana, R. Roopa Chandrika, M. Preetha, P. Santhoshini, and E. E. Nithila, "An advanced decentralized architecture enabled logical identity based encryption logic using blockchain assistance," in *CONIT*. IEEE, 2024, pp. 1–6.

[343] R. Li, Z. Wang, L. Fang, C. Peng, W. Wang, and H. Xiong, "Efficient blockchain-assisted distributed identity-based signature scheme for integrating consumer electronics in metaverse," *IEEE Transactions on Consumer Electronics*, vol. 70, no. 1, pp. 3770–3780, 2024.

[344] Z. Bao, D. He, C. Peng, M. Luo, and K.-K. R. Choo, "An identity-based adaptor signature scheme and its applications in the blockchain system," *IEEE Open Journal of the Computer Society*, vol. 4, pp. 231–242, 2023.

[345] S. Alotaibi, H. Alsobhi, M. Zhao, and F. K. Hussain, "Blockchain for identity management: Ensuring trust and integrity in the education sector," in *ICEBE*. IEEE, 2023, pp. 122–128.

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

[347] M. Plaza, S. Batzel, T. Wojda, and M. M. Alcaro, "Digital identity, computational reliabilism, and the future of iomt: Epistemic reasoning and the role of blockchain in removing human tampering from pharmacovigilance decision making," in *Blockchain in Healthcare*, S. Stawicki, Ed. Springer International Publishing, 2023, vol. 10, pp. 97–116.

[348] J. Deng, L. Jiao, L. Zhang, Y. Ren, and W. Yin, "Design of identity authentication scheme for dynamic service command system based on sm2 algorithm and blockchain technology," in *Advances in Internet, Data & Web Technologies*, L. Barolli, E. Kulla, and M. Ikeda, Eds. Springer International Publishing, 2022, vol. 118, pp. 31–37.

[349] H. Yu and X. Bai, "Identity-based searchable attribute signcryption in lattice for a blockchain-based medical system," *Frontiers of Information Technology & Electronic Engineering*, vol. 25, no. 3, pp. 461–471, 2024.

[350] ——, "Identity-based searchable attribute signcryption for blockchain," *Journal of Ambient Intelligence and Humanized Computing*, vol. 14, no. 12, pp. 16 785–16 794, 2023.

[351] C. A. L. Montesinos and E. J. E. Cárdenas, "Verification of peruvian identity document fraud through ocr, hash algorithm, and simulated blockchain database," in *Knowledge Management and Artificial Intelligence for Growth*, I. Bianchi and G. A. Dávila, Eds. Springer Nature Switzerland, 2024, vol. 8, pp. 165–188.

[352] L. Wang, M. Hu, Z. Jia, Y. Cheng, J. Fu, Y. Wang, and B. Gong, "Identity-based threshold group signature scheme of blockchain verification," in *Trusted Computing and Information Security*, W. Han, L. Zhu, and F. Yan, Eds. Springer Singapore, 2020, vol. 1149, pp. 144–158.

[353] A.-C. Careja and N. Tapus, "Digital identity using blockchain technology," *Procedia Computer Science*, vol. 221, pp. 1074–1082, 2023.

[354] H. Zhang and F. Zhao, "Cross-domain identity authentication scheme based on blockchain and pki system," *High-Confidence Computing*, vol. 3, no. 1, p. 100096, 2023.

[355] L. Wang, Y. Yuan, and Y. Ding, "Analysis and design of identity authentication for iot devices in the blockchain using hashing and digital signature algorithms," *International Journal of Distributed Sensor Networks*, vol. 2023, pp. 1–12, 2023.

[356] D. Kirupanithi and A. Antonidoss, "Self-sovereign identity creation on blockchain using identity based encryption," in *ICICCS*. IEEE, 2021, pp. 299–304.

[357] Z. Zhao and Y. Liu, "A blockchain based identity management system considering reputation," in *ICISCAE*. IEEE, 2019, pp. 32–36.

[358] S. A. Khan, A. Jadhav, I. E. Bharadwaj, M. Rooj, and S. Shiravale, "Blockchain and the identity based encryption scheme for high data security," in *ICCMC*. IEEE, 2020, pp. 1005–1008.

[359] J. Kim, S. Lee, Y. Kim, and S. Cho, "A graph embedding-based identity inference attack on blockchain systems," in *ICEIC*. IEEE, 2022, pp. 1–3.

[360] S. Rattanabunno, W. Werapun, J. Suaboot, T. Karode, and M. Puongmanee, "An eoa identity tracing system (aits) on ethereum blockchain," in *ICINT*. IEEE, 2023, pp. 61–65.

[361] Y. Xia, H. Yuan, J. Qin, Q. Yuan, and J. Zhao, "An efficient anonymous identity authentication based on cp-abe and consortium blockchain for iov," in *ICECAI*. IEEE, 2023, pp. 10–17.

[362] S. Raju, S. Boddepalli, S. Gampa, Q. Yan, and J. S. Deogun, "Identity management using blockchain for cognitive cellular networks," in *ICC*. IEEE, 2017, pp. 1–6.

[363] X. Liu, Z. Tang, P. Li, S. Guo, X. Fan, and J. Zhang, "A graph learning based approach for identity inference in dapp platform blockchain," *IEEE Transactions on Emerging Topics in Computing*, vol. 10, no. 1, pp. 438–449, 2022.

[364] Z. Bao, D. He, M. K. Khan, M. Luo, and Q. Xie, "PBidm: Privacy-preserving blockchain-based identity management system for industrial internet of things," *IEEE Transactions on Industrial Informatics*, vol. 19, no. 2, pp. 1524–1534, 2023.

[365] Z. Gong-Guo and O. Zuo, "Personal health data identity authentication matching scheme based on blockchain," in *CBFD*. IEEE, 2021, pp. 419–425.

[366] M. Zhai, Y. Ren, G. Feng, and X. Zhang, "Fine-grained and fair identity authentication scheme for mobile networks based on blockchain," *China Communications*, vol. 19, no. 6, pp. 35–49, 2022.

[367] F. Liang, X. Xing, and G. Wang, "IPP-HF: An identity privacy protection scheme for consortium blockchain hyperledger fabric," in *SmartWorld/UIC/ScalCom/DigitalTwin/PriComp/Meta*. IEEE, 2022, pp. 1984–1989.

[368] C. Li, Z. Wang, P. Cao, X. Duan, Y. Xu, and J. Li, "A trading scheme of power blockchain based on identity-based ring signature for anonymity and anti-forgery," in *ECNCT*. IEEE, 2023, pp. 241–245.

[369] S. Huang, H. Li, R. Xiong, W. Ren, J. He, and Y. Ren, "A commitment and ring signature based scheme for amount and identity privacy protection in blockchain," in *TrustCom*. IEEE, 2023, pp. 292–299.

[370] K. Zhang, C. K. M. Lee, and Y. P. Tsang, "Stateless blockchain-based lightweight identity management architecture for industrial iot applications," *IEEE Transactions on Industrial Informatics*, vol. 20, no. 6, pp. 8394–8405, 2024.

[371] P. Prabha and K. Chatterjee, "RSHealth: A ring signature scheme for identity anonymization and transaction privacy in blockchain based e-healthcare systems," *IEEE Access*, vol. 12, pp. 117 701–117 720, 2024.

[372] H. Li, L. Pei, D. Liao, G. Sun, and D. Xu, "Blockchain meets vanet: An architecture for identity and location privacy protection in vanet," *Peer-to-Peer Networking and Applications*, vol. 12, no. 5, pp. 1178–1193, 2019.

[373] F. Fu, G. Lu, J. Huang, and T. Dreibholz, "A survey of blockchain-based identity anonymity research," in *Proceedings of the 13th International Conference on Computer Engineering and Networks*, Y. Zhang, L. Qi, Q. Liu, G. Yin, and X. Liu, Eds. Springer Nature Singapore, 2024, vol. 1127, pp. 447–455.

[374] J. Shen, J. Zhou, Y. Xie, S. Yu, and Q. Xuan, "Identity inference on blockchain using graph neural network," in *Blockchain and Trustworthy Systems*, H.-N. Dai, X. Liu, D. X. Luo, J. Xiao, and X. Chen, Eds. Springer Singapore, 2021, vol. 1490, pp. 3–17.

[375] H. Wu, X. Feng, G. Kan, and X. Jiang, "BIPP: Blockchain-based identity privacy protection scheme in internet of vehicles for remote anonymous communication," in *Algorithms and Architectures for Parallel Processing*, Y. Lai, T. Wang, M. Jiang, G. Xu, W. Liang, and A. Castiglione, Eds. Springer International Publishing, 2022, vol. 13156, pp. 489–506.

[376] S. Devidas, N. R. Rekha, and Y. V. Subba Rao, "Identity verifiable ring signature scheme for privacy protection in blockchain," *International Journal of Information Technology*, vol. 15, no. 5, pp. 2559–2568, 2023.

[377] Z. Li, Y. Chu, X. Liu, Y. Zhang, J. Feng, and X. Xiang, "Physical unclonable function based identity management for iot with blockchain," *Procedia Computer Science*, vol. 198, pp. 454–459, 2022.

[378] N. D. Sarier, "Efficient biometric-based identity management on the blockchain for smart industrial applications," *Pervasive and Mobile Computing*, vol. 71, p. 101322, 2021.

[379] L. Yanhui, Z. Jianbiao, M. Salman Pathan, Y. Yijian, Z. Puzhe, S. Maroc, and A. Nag, "Research on identity authentication system of internet of things based on blockchain technology," *Journal of King Saud University - Computer and Information Sciences*, vol. 34, no. 10, pp. 10 365–10 377, 2022.

[380] J. Wang, G. Sun, Y. Gu, and K. Liu, "ConGradetect: Blockchain-based detection of code and identity privacy vulnerabilities in crowdsourcing," *Journal of Systems Architecture*, vol. 114, p. 101910, 2021.

[381] A. R. Raipurkar, S. Bobde, A. Tripahi, and M. Sahu, "Digital identity system using blockchain-based self sovereign identity & zero knowledge proof," in *OCIT*. IEEE, 2023, pp. 611–616.

[382] D. Augot, H. Chabanne, O. Clemot, and W. George, "Transforming face-to-face identity proofing into anonymous digital identity using the bitcoin blockchain," in *PST*. IEEE, 2017, pp. 25–2509.

[383] J. W. Heo, G. Ramachandran, and R. Jurdak, "Decentralised redactable blockchain: A privacy-preserving approach to addressing identity tracing challenges," in *ICBC*. IEEE, 2024, pp. 215–219.

[384] J. Yin, Y. Xiao, Q. Pei, Y. Ju, L. Liu, M. Xiao, and C. Wu, "SmartDID: A novel privacy-preserving identity based on blockchain for iot," *IEEE Internet of Things Journal*, vol. 10, no. 8, pp. 6718–6732, 2023.

[385] W. Li, C. Meese, H. Guo, and M. Nejad, "Blockchain-enabled identity verification for safe ridesharing leveraging zero-knowledge proof," in *HotICN*. IEEE, 2020, pp. 18–24.

[386] D. A. Luong and J. H. Park, "Privacy-preserving identity management system on blockchain using zk-snark," *IEEE Access*, vol. 11, pp. 1840–1853, 2023.

[387] M. Dieye, P. Valiorgue, J.-P. Gelas, E.-H. Diallo, P. Ghodous, F. Biennier, and E. Peyrol, "A self-sovereign identity based on zero-knowledge proof and blockchain," *IEEE Access*, vol. 11, pp. 49 445–49 455, 2023.

[388] M. Akram and A. Sen, "A case study evaluation of blockchain for digital identity verification and management in bfsi using zero-knowledge proof," in *DASA*. IEEE, 2022, pp. 1295–1299.

[389] J. Jose Diaz Rivera, A. Muhammad, and W.-C. Song, "Securing digital identity in the zero trust architecture: A blockchain approach to privacy-focused multi-factor authentication," *IEEE Open Journal of the Communications Society*, vol. 5, pp. 2792–2814, 2024.

[390] K. Jiang, Y. Gao, J. Xiao, and F. Zou, "Unified identity authentication system based on blockchain," in *ICCC*. IEEE, 2020, pp. 2191–2200.

[391] W. Tang, S. S. Mukherjee, S. Park, C. Chenli, H. Oh, J. Kim, and T. Jung, "GrAC: Graph-based anonymous credentials from identity graphs on blockchain," in *Blockchain*. IEEE, 2024, pp. 113–122.

[392] Z. Song, E. Yan, J. Song, R. Jiang, Y. Yu, and T. Chen, "A blockchain-based digital identity system with privacy, controllability, and auditability," *Arabian Journal for Science and Engineering*, 2024.

[393] H. V. A. Le, Q. D. N. Nguyen, T. H. Tran, and T. Nakano, "Securing digital futures: Exploring decentralised systems and blockchain for enhanced identity protection," in *Intelligence of Things: Technologies and Applications*, N.-N. Dao, T. N. Thinh, and N. T. Nguyen, Eds. Springer Nature Switzerland, 2023, vol. 188, pp. 200–212.

[394] X. Shang, M. Dai, and X. Liu, "Blockchain-enhanced device to device network identity verification based on zero knowledge proof," in *Data Science and Information Security*, H. Jin, Y. Pan, and J. Lu, Eds. Springer Nature Singapore, 2024, vol. 2059, pp. 124–134.

[395] A.-E. Panait and R. F. Olimid, "On using zk-snarks and zk-starks in blockchain-based identity management," in *Innovative Security Solutions for Information Technology and Communications*, D. Maimut, A.-G. Oprina, and D. Sauveron, Eds. Springer International Publishing, 2021, vol. 12596, pp. 130–145.

[396] T. Wang, H. Shen, J. Chen, F. Chen, Q. Wu, and D. Xie, "A hybrid blockchain-based identity authentication scheme for mobile crowd sensing," *Future Generation Computer Systems*, vol. 143, pp. 40–50, 2023.

[397] N. D. Sarier, "Comments on biometric-based non-transferable credentials and their application in blockchain-based identity management," *Computers & Security*, vol. 105, p. 102243, 2021.

[398] J. Tian, Y. Zhao, X. Yang, X. Zhao, R. Chen, and Y. Yu, "Identity-based threshold (multi) signature with private accountability for privacy-preserving blockchain," *High-Confidence Computing*, vol. 4, no. 4, p. 100271, 2024.

[399] L. Lourinho, S. Kendzierskyj, and H. Jahankhani, "Securing the digital witness identity using blockchain and zero-knowledge proofs," in *Strategy, Leadership, and AI in the Cyber Ecosystem*. Elsevier, 2021, pp. 159–194.

[400] X. Yang and W. Li, "A zero-knowledge-proof-based digital identity management scheme in blockchain," *Computers & Security*, vol. 99, p. 102050, 2020.

[401] M. A. Prada-Delgado, I. Baturone, G. Dittmann, J. Jelitto, and A. Kind, "PUF-derived iot identities in a zero-knowledge protocol for blockchain," *Internet of Things*, vol. 9, p. 100057, 2020.

[402] A. A. Varfolomeev and L. H. Al-Farhani, "Blockchain based cloud authentication framework for digital identity management in smart city," in *ICITAMS*. IEEE, 2023, pp. 86–90.

[403] N. M. Ahmad, S. F. Abdul Razak, S. Kannan, I. Yusof, and A. H. Muhamad Amin, "Improving identity management of cloud-based iot applications using blockchain," in *ICIAS*. IEEE, 2018, pp. 1–6.

[404] A. A. Sathio, M. Ali Dootio, A. Lakhan, M. U. Rehman, A. Orangzeb Pnhwar, and M. A. Sahito, "Pervasive futuristic healthcare and blockchain enabled digital identities-challenges and future intensions," in *iCCECE*. IEEE, 2021, pp. 30–35.

[405] X. Xu, Y. Guo, and Y. Guo, "Fog-enabled private blockchain-based identity authentication scheme for smart home," *Computer Communications*, vol. 205, pp. 58–68, 2023.

[406] D. Pavithran, J. N. Al-Karaki, and K. Shaalan, "Edge-based blockchain architecture for event-driven iot using hierarchical identity based encryption," *Information Processing & Management*, vol. 58, no. 3, p. 102528, 2021.

[407] R. Mu, B. Gong, Z. Ning, J. Zhang, Y. Cao, Z. Li, W. Wang, and X. Wang, "An identity privacy scheme for blockchain-based on edge computing," *Concurrency and Computation: Practice and Experience*, vol. 34, p. e6545, 2022.

[408] G. Uteyev and R. F. Gibadullin, "Development of the decentralized biometric identity verification system using blockchain technology and computer vision," in *SmartIndustryCon*. IEEE, 2024, pp. 350–355.

[409] M. J. Haber and D. Rolls, "Blockchain and identity management," in *Identity Attack Vectors*. Apress, 2020, pp. 175–187.

[410] B. Kamala, D. Harini, and A. Akshaya Selvi, "Digital identity system for real world asset using blockchain," in *Deep Sciences for Computing and Communications*, A. U. R., K. Kottursamy, G. Raja, A. K. Bashir, U. Kose, R. Appavoo, and V. Madhivanan, Eds. Springer Nature Switzerland, 2024, vol. 2176, pp. 19–26.

[411] R. Islam, Y. Fujiwara, S. Kawata, and H. Yoon, "Correction to: Unfolding identity of financial institutions in bitcoin blockchain by weekly pattern of network flows," *Evolutionary and Institutional Economics Review*, vol. 18, no. 2, pp. 459–460, 2021.