The Eastasouth Journal of Information System and Computer Science
Vol. 3, No. 02, December 2025, pp. 202-213
ISSN: 3025-566X, DOI: 10.58812/esiscs.v3i02

Mapping Blockchain Identity Management Research: A Bibliometric Analysis (2010–2025)

Loso Judijanto
IPOSS Jakarta

Article Info

Article history:

Received Dec, 2025
Revised Dec, 2025
Accepted Dec, 2025

Keywords:

Authentication;
Blockchain;
Decentralized Identity;
Digital Identity;
Self-Sovereign Identity

ABSTRACT

This study presents a comprehensive bibliometric analysis of blockchain identity management research published between 2010 and 2025, aiming to map its intellectual structure, thematic evolution, and global collaboration patterns. Using data retrieved from the Scopus database and analyzed with VOSviewer, the study applies network visualization, overlay visualization, density mapping, citation analysis, and co-authorship analysis to uncover dominant research streams and emerging frontiers. The results reveal that the field is conceptually centered on blockchain-based authentication and decentralized identity management systems, with increasing scholarly attention toward privacy-preserving mechanisms such as zero-knowledge proofs, anonymity, and data protection. Thematic evolution indicates a clear transition from foundational infrastructure-oriented studies to application-driven and regulatory-sensitive research domains, including e-government, IoT, healthcare, and digital governance. Collaboration analysis highlights the leading role of China and India, supported by strong transcontinental linkages with the United States and European countries, reflecting a globally interconnected yet regionally concentrated research landscape. By systematically mapping publication trends, thematic clusters, and collaboration networks, this study provides a structured knowledge base that supports future theoretical development, guides practical implementation, and informs policy formulation in blockchain-based digital identity ecosystems.

Corresponding Author:

Name: Loso Judijanto
Institution: IPOSS Jakarta
Email: losojudijantobumn@gmail.com

1. INTRODUCTION

Blockchain technology has evolved from a niche concept associated with cryptocurrencies to a broader paradigm for secure, decentralized information management [1], [2]. Since the publication of Bitcoin's foundational paper in 2008, scholars and practitioners have increasingly recognized blockchain's potential for transforming digital trust frameworks by eliminating the dependence on centralized authorities [3], [4]. Among the numerous application domains, digital identity management has emerged as one of the most compelling areas, driven by a growing global need for secure, interoperable, and user-centric identity solutions [5]. Traditional

identity systems often rely on centralized repositories that are vulnerable to misuse and security breaches, prompting explorations into blockchain-based alternatives that offer enhanced transparency, privacy, and self-sovereignty [6].

The transition toward decentralized identity, sometimes termed Self-Sovereign Identity (SSI), reflects a significant shift in how identity is conceptualized and controlled in digital ecosystems. SSI frameworks aim to empower individuals with ownership over their identity credentials by leveraging blockchain's immutability and verifiability [7]. Over the past decade, researchers have investigated diverse blockchain architectures, cryptographic mechanisms, and trust models to develop robust identity solutions that can operate across borders and sectors. Such research continues to expand, supported by initiatives from governments, private organizations, and international standards bodies [8], [9]. The consistent rise in publications indicates not only growing interest but also the diversification of perspectives and technological approaches in the field.

Despite the rapid growth of blockchain identity research, the landscape of scholarly work remains highly fragmented. Studies vary widely in terms of theoretical frameworks, implementation contexts, and technological platforms, ranging from public to permissioned blockchains, and from financial applications to e-government services [10]. Furthermore, identity management intersects with interdisciplinary domains including cybersecurity, privacy law, digital governance, and user experience resulting in a complex and multifaceted body of knowledge [11], [12]. Mapping the evolution of this literature is essential to understanding how the field has progressed, identifying dominant themes, and revealing emerging research clusters and collaboration networks.

Bibliometric analysis has become an increasingly valuable method for synthesizing knowledge in expanding research fields. By quantitatively analyzing publication patterns, citation networks, keyword co-occurrence, and authorship structures, bibliometrics provides systematic insights into the intellectual development of a discipline [13]. Applied to blockchain identity management, bibliometric approaches can illuminate how scholarly interest has shifted over time, which theoretical or technological approaches have gained prominence, and how global research collaborations have shaped the field's trajectory. Such analysis is particularly relevant given the rapid pace of technological advancement and the diversity of academic disciplines contributing to blockchain identity research.

Between 2010 and 2025, blockchain identity management has undergone distinct developmental phases from early conceptual discussions to more mature system architectures and pilot implementations. As new regulatory frameworks, such as the European Union's eIDAS revisions and various national digital identity strategies, influence technological innovation, the academic discourse has similarly evolved to address issues of scalability, compliance, interoperability, and ethical governance. Understanding how these external forces have shaped scholarly output is crucial for contextualizing research trends and anticipating future directions. A comprehensive bibliometric study covering this 15-year period can thus offer valuable insights into the discipline's evolution and its broader socio-technical implications.

Although the volume of research on blockchain-based identity management has expanded substantially from 2010 to 2025, systematic knowledge about the structure, development, and thematic evolution of this literature remains limited. Existing reviews are often narrative or conceptual, lacking a holistic, data-driven mapping of publication trends, influential authors, collaborative networks, and emerging research themes. Without such a comprehensive bibliometric analysis, scholars and practitioners face challenges in understanding the current state of knowledge, identifying research gaps, and positioning future studies within the broader intellectual landscape of blockchain identity management. This absence of consolidated

insights creates barriers to coordinated research efforts, evidence-based policymaking, and the informed development of next-generation identity solutions. This study aims to conduct a comprehensive bibliometric analysis of blockchain identity management research published between 2010 and 2025.

2. METHOD

This study employed a bibliometric research design to systematically analyze the scholarly landscape of blockchain-based identity management published between 2010 and 2025. Bibliometric analysis was selected because it enables quantitative assessment of large bodies of literature, uncovering patterns related to publication growth, citation impact, thematic evolution, and collaboration networks. Following established bibliometric procedures [14], the study focused on extracting objective indicators from peer-reviewed publications to map the intellectual and conceptual structure of the field. The approach allowed for a replicable and transparent examination of how blockchain identity research has evolved over the fifteen-year period.

Data collection was conducted from Scopus Database, which are recognized for their comprehensive coverage and standardized bibliographic metadata. Keywords such as "blockchain identity," "decentralized identity," "self-sovereign identity," "digital identity blockchain," and related terms were used to retrieve relevant publications. Boolean operators and field specifications (title, abstract, and keywords) were applied to ensure precision and completeness. The initial search results were screened to remove duplicates, non-academic documents, and irrelevant articles. Metadata extracted from the final dataset included authorship details, publication year, source title, institutional affiliation, citation counts, keywords, and country of origin. The collected data were analyzed using VOSviewer. VOSviewer was utilized to generate visualizations of co-authorship networks, keyword co-occurrence maps, and citation linkages, enabling the identification of influential authors, thematic clusters, and intellectual structures.

3. RESULT AND DISCUSSIONS

3.1 Network Visualization

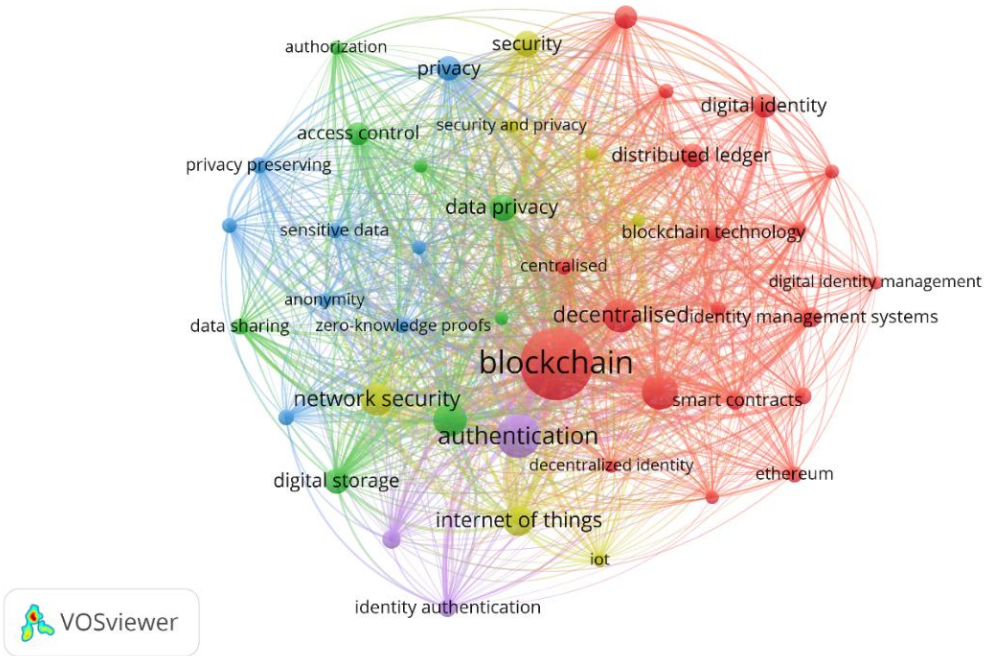

Figure 1. Network Visualization
Source: Data Analysis Result, 2025

The first figure here illustrates the intellectual structure of blockchain identity management research, with "blockchain" positioned as the dominant and most central node. Its large size and dense linkages indicate that blockchain serves as the core technological foundation connecting diverse research streams. Surrounding this hub, multiple thematic clusters emerge, showing that identity management research is not monolithic but rather composed of interrelated subfields that collectively shape the evolution of decentralized identity systems. The red cluster on the right highlights a strong focus on digital identity and decentralized identity management systems, closely associated with terms such as smart contracts, Ethereum, distributed ledger, and blockchain technology. This cluster represents the system and application layer of the literature, where scholars explore how blockchain infrastructures and programmable logic enable decentralized identity management, governance mechanisms, and practical deployment scenarios. The prominence of these terms suggests that much of the field's growth has been driven by technical architectures and platform-oriented solutions.

The green cluster emphasizes security- and privacy-oriented mechanisms, including data privacy, zero-knowledge proofs, anonymity, privacy-preserving, and data sharing. This cluster reflects a critical research stream addressing one of the core challenges of blockchain identity management: balancing transparency with confidentiality. Its dense connections to the central blockchain node indicate that privacy-enhancing technologies are not peripheral but integral to the design of decentralized identity systems, especially in regulatory and sensitive-data contexts. The blue cluster is centered on access control, authorization, sensitive data, and network security, highlighting research concerned with control mechanisms and secure data handling. This cluster bridges technical security approaches with identity management functions, suggesting that blockchain-based identity solutions are increasingly framed as part of broader cybersecurity and access management ecosystems, rather than as standalone identity tools. Its overlap with the green privacy cluster underscores the close conceptual relationship between access control and privacy protection. The purple and yellow clusters point to emerging and cross-domain applications, particularly authentication, identity authentication, Internet of Things (IoT), and digital storage. These clusters are positioned slightly more peripherally but remain well connected to the core network, indicating growing interest in applying blockchain identity frameworks to distributed environments such as IoT.

3.2 *Overlay Visualization*

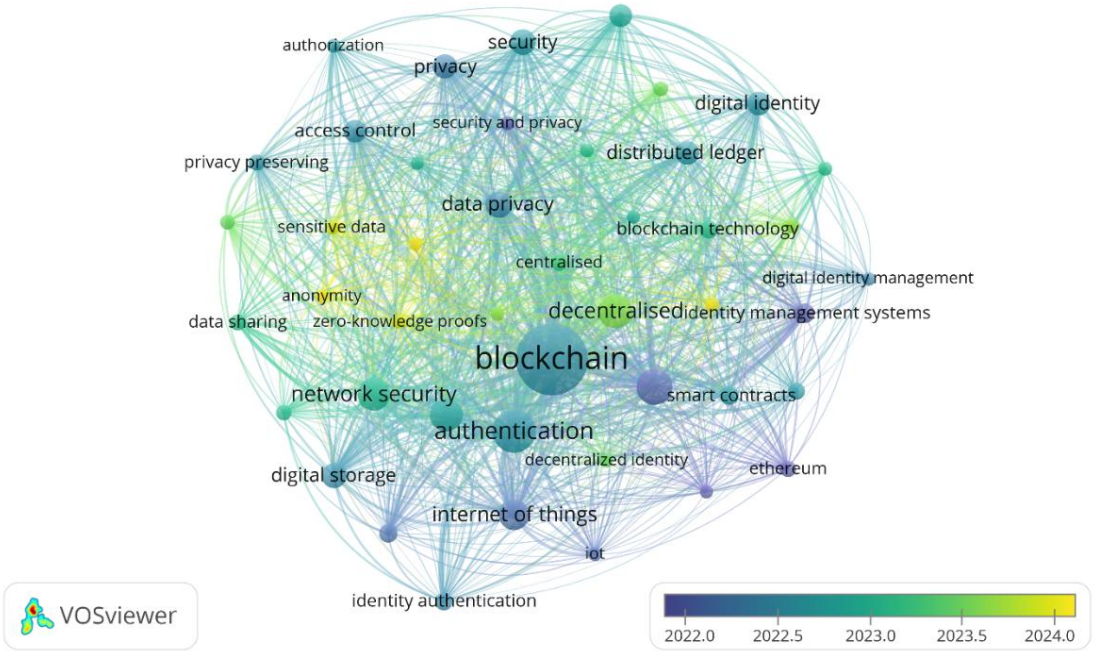

Figure 2. Overlay Visualization
Source: Data Analysis Result, 2025

Figure 2 maps blockchain identity management research by incorporating a temporal dimension, where node colors represent the average publication year of keywords. The central position of "blockchain" and "authentication" (colored in cooler tones) indicates that these concepts constitute the foundational core of the field and have been consistently studied over a longer period. Their dense interconnections with most other keywords confirm that early research largely focused on leveraging blockchain as a secure infrastructure for identity authentication and verification. Keywords shown in green to yellow hues such as zero-knowledge proofs, anonymity, data sharing, and privacy preserving reflect more recent research attention (around 2023–2024). This temporal shift highlights a growing scholarly emphasis on advanced privacy-enhancing technologies within blockchain identity systems. The emergence of these topics suggests that, as the field matures, researchers are moving beyond basic identity frameworks toward addressing complex challenges related to data protection, regulatory compliance, and trust minimization. Meanwhile, application-oriented terms like digital identity, decentralised identity management systems, smart contracts, Ethereum, and Internet of Things (IoT) occupy intermediate to recent time positions, indicating an ongoing transition from conceptual and architectural studies to implementation and domain-specific use cases.

3.3 *Citation Analysis*

Table 1. Most Cited Article

Citations	Author and Year	Title
2811	[15]	Hyperledger Fabric: A Distributed Operating System for Permissioned Blockchains

Citations	Author and Year	Title
1684	[16]	1 Blockchain's roles in meeting key supply chain management objectives
949	[17]	A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda
786	[18]	Can Blockchain Strengthen the Internet of Things?
761	[19]	Blockchain in healthcare applications: Research challenges and opportunities
698	[20]	A survey on privacy protection in blockchain system
594	[21]	Blockchain's roles in strengthening cybersecurity and protecting privacy
586	[22]	Integrating blockchain for data sharing and collaboration in mobile healthcare applications
370	[23]	Privacy-Preserving Solutions for Blockchain: Review and Challenges
366	[24]	Blockchain-Assisted Secure Device Authentication for Cross-Domain Industrial IoT

Source: Scopus, 2025

3.4 Density Visualization

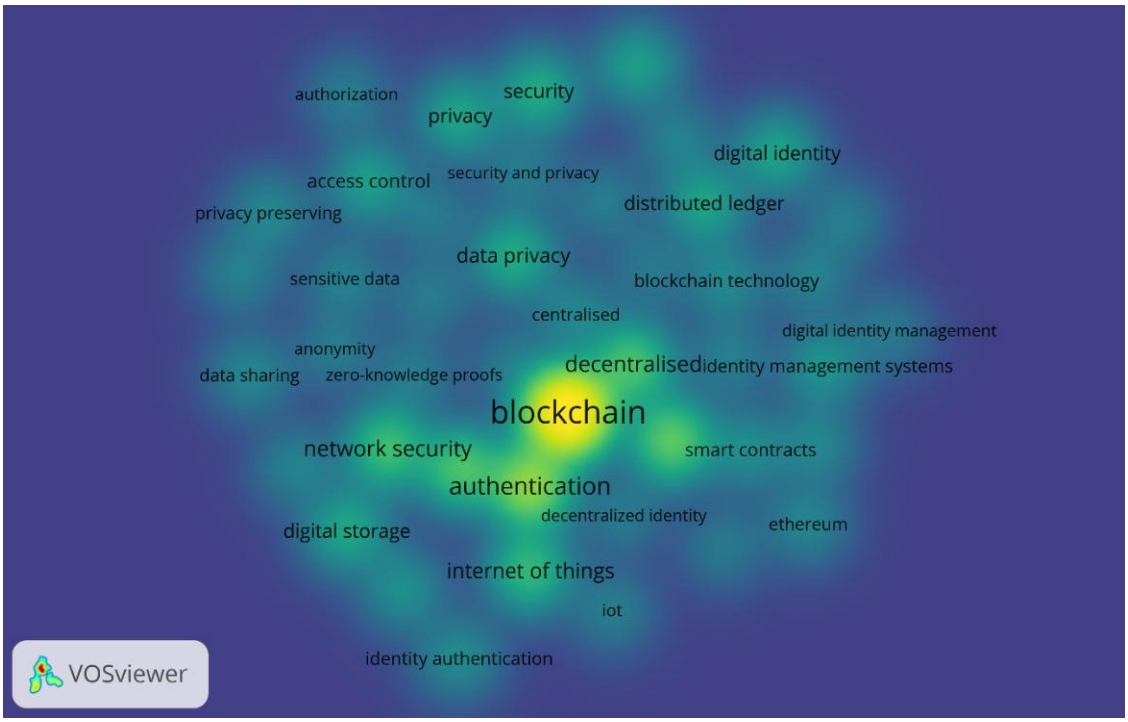

Figure 3. Density Visualization
Source: Data Analysis Result, 2025

Figure 3 highlights the most intensively researched topics in blockchain identity management by showing areas of higher keyword concentration in warmer colors. The brightest and most central hotspot is "blockchain", confirming its role as the conceptual nucleus of the field. Closely surrounding it are "authentication," "decentralised identity management systems," "network security," and "data privacy," indicating that the literature strongly converges on securing identity verification processes through decentralized architectures. This pattern suggests that ensuring trustworthy

authentication and robust security remains the dominant concern in blockchain-based identity research. Beyond the core, moderately dense regions appear around privacy-preserving mechanisms, such as zero-knowledge proofs, anonymity, and access control, as well as application-oriented themes including digital identity, smart contracts, and Internet of Things (IoT). Their lower but visible density indicates established yet still developing research streams that extend the core identity–security focus toward advanced cryptographic techniques and real-world deployment contexts.

3.5 Co-Authorship Network

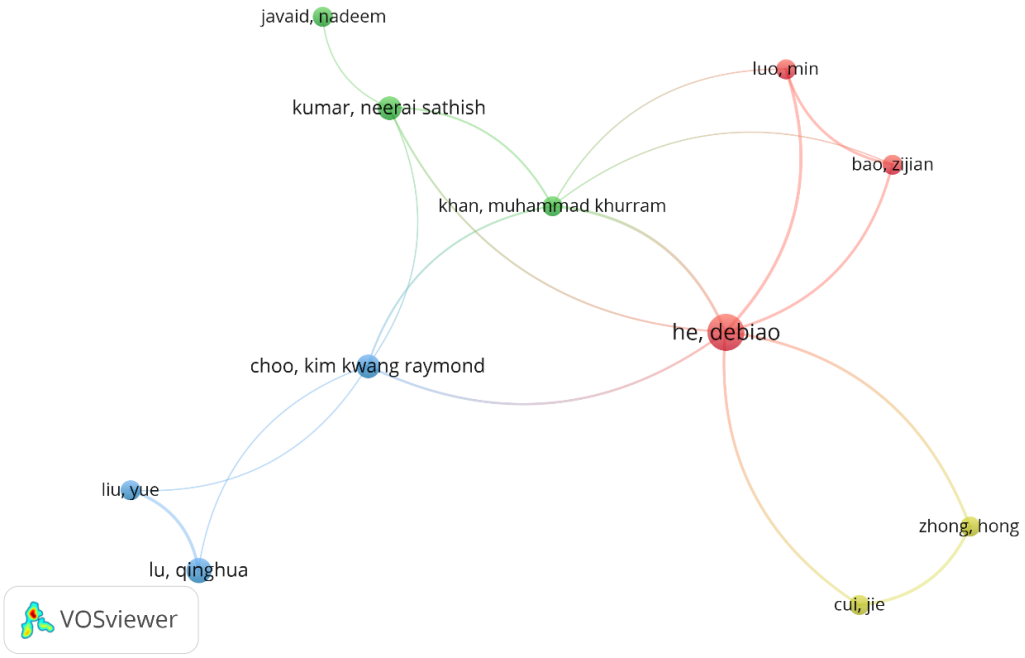

Figure 4. Author Visualization
Source: Data Analysis Result, 2025

Figure 4 reveals a moderately fragmented yet interconnected research community in blockchain identity management, structured around several small collaboration clusters. He, Debiao emerges as the most central and influential author, acting as a key bridge connecting multiple groups, including collaborators such as Luo, Min, Bao, Zijian, Zhong, Hong, and Cui, Jie. This central positioning indicates a leadership role in shaping research directions and facilitating knowledge flow across sub-networks. Other clusters, such as those led by Kumar, Neeraj Sathish and Choo, Kim-Kwang Raymond, show more localized collaboration patterns, suggesting parallel research streams with limited cross-cluster integration.

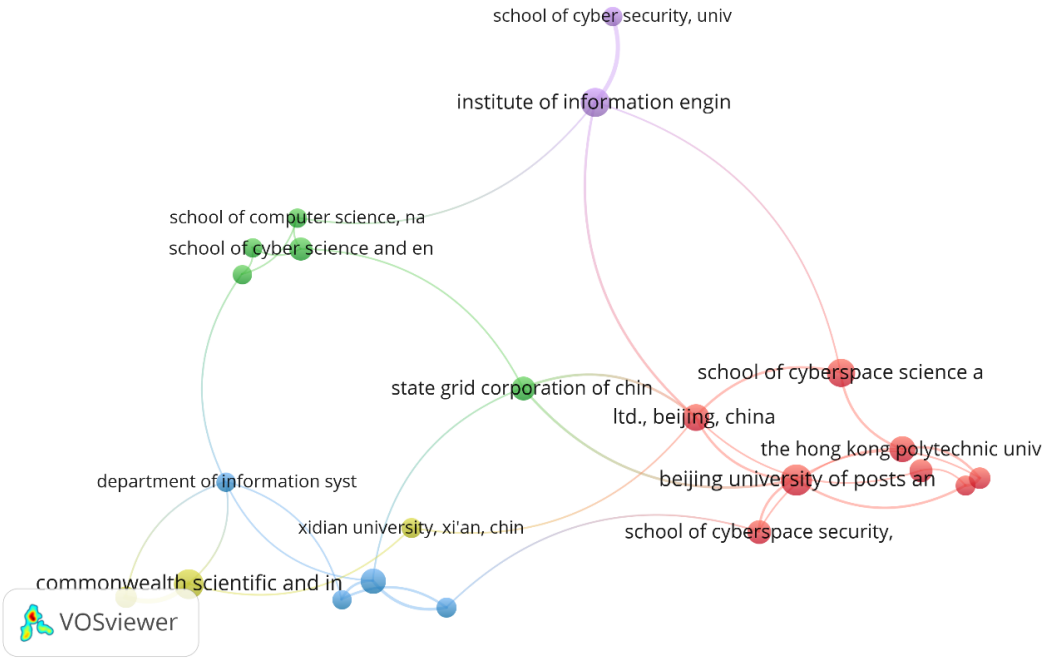

Figure 5. Affiliation Visualization
Source: Data Analysis Result, 2025

Figure 5 shows that research on blockchain identity management is dominated by a small number of highly connected academic and applied institutions, primarily centered in China and the Asia–Pacific region. Beijing University of Posts and Telecommunications and affiliated entities such as the School of Cyberspace Science and School of Cyberspace Security form the most prominent hub, indicating their leading role in coordinating research and collaborations. Strong linkages with institutions like The Hong Kong Polytechnic University, Xidian University, and the State Grid Corporation of China suggest an ecosystem where academic research is closely connected with applied and industry-oriented organizations. Meanwhile, peripheral yet connected nodes such as cybersecurity schools and information engineering institutes reflect specialized contributions rather than broad coordinating roles.

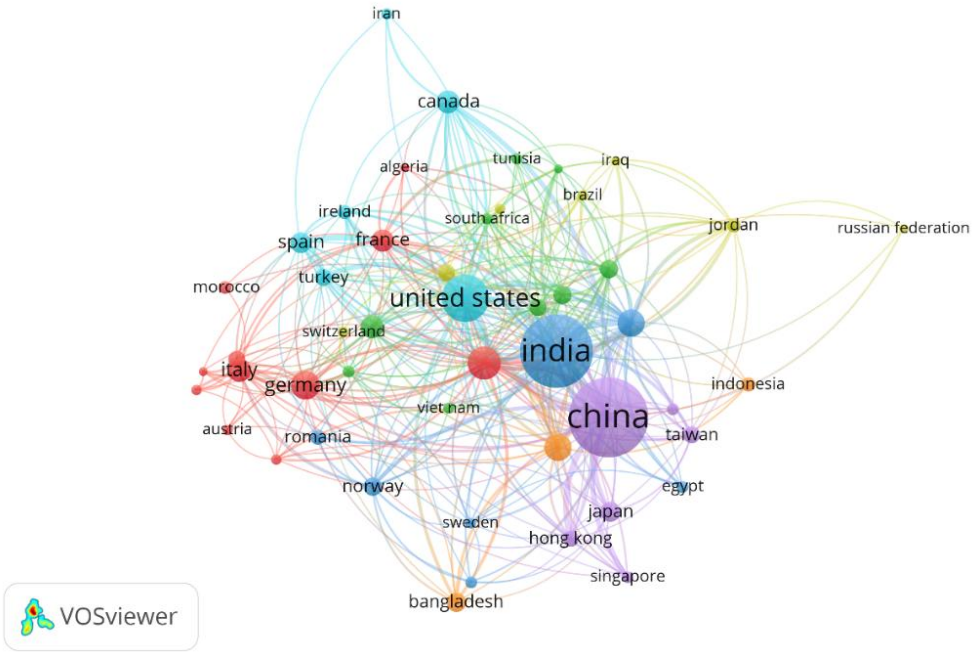

Figure 6. Country Visualization
Source: Data Analysis Result, 2025

Figure 6 network demonstrates that research on blockchain identity management is globally distributed but structurally centered around a few dominant hubs, notably China, India, and the United States. China and India appear as the largest and most interconnected nodes, indicating both high research productivity and extensive international collaboration, particularly with countries across Asia, Europe, and the Middle East. The United States functions as a major bridging actor, linking Western research communities (e.g., Europe and Canada) with Asian partners, thereby facilitating cross-regional knowledge exchange. European countries such as Germany, Italy, France, Spain, and Switzerland form a dense collaborative sub-network, reflecting strong intra-regional cooperation and methodological contributions, often connected to security, privacy, and cryptographic aspects of identity management. Meanwhile, emerging contributions from Southeast Asia (Indonesia, Vietnam, Singapore), Africa (Egypt, South Africa, Morocco), and the Middle East (Jordan, Iraq, Iran) indicate the growing global relevance of blockchain-based identity solutions, particularly in contexts of digital governance and infrastructure development.

3.6 Discussion

a. Practical Implications

The findings of this bibliometric study offer several practical implications for policymakers, system designers, and technology practitioners involved in blockchain-based identity management. First, the strong concentration of research around authentication, decentralized identity management systems, security, and privacy indicates that these dimensions are considered foundational for real-world deployment. Practitioners developing digital identity solutions particularly for e-government, finance (e-KYC), healthcare, and IoT should therefore prioritize privacy-by-design architectures, integrating mechanisms such as zero-knowledge

proofs, selective disclosure, and robust access control. Second, the prominence of application-oriented keywords (e.g., smart contracts, Ethereum, IoT) suggests that blockchain identity solutions are moving beyond conceptual design toward implementation on specific platforms, highlighting the need for interoperability standards and compliance with existing digital infrastructure. For policymakers, the growing emphasis on data privacy and anonymity signals the importance of aligning blockchain identity initiatives with regulatory frameworks such as data protection and cybersecurity laws, especially in cross-border digital identity use cases.

b. Theoretical Contributions

From a theoretical perspective, this study contributes to the blockchain and identity management literature by systematically mapping the intellectual structure, thematic evolution, and collaboration patterns of the field over a 15-year period. The results demonstrate that blockchain identity management research is theoretically anchored at the intersection of distributed systems, security and privacy theory, and identity and access management (IAM). The evolution from core concepts (blockchain, authentication) toward advanced privacy-preserving mechanisms (zero-knowledge proofs, anonymity) reflects a theoretical shift from infrastructure-centric views to trust-minimization and user-centric identity paradigms, such as self-sovereign identity. Additionally, the identification of geographically concentrated yet globally connected collaboration networks enriches the understanding of how knowledge production in this field is shaped by regional research leadership, particularly from Asia, while still relying on international scientific exchange. As such, this study provides a structured knowledge base that future researchers can use to position new theoretical models, integrate interdisciplinary perspectives, and identify underexplored conceptual linkages.

c. Limitations and Future Research

Despite its contributions, this study has several limitations that should be acknowledged. First, the analysis is constrained by the choice of bibliographic database(s) and search query, which may exclude relevant studies published outside indexed journals or in non-English outlets. Second, bibliometric techniques focus on quantitative patterns of publications and citations, and therefore cannot fully capture the qualitative depth, technical rigor, or contextual nuances of individual studies. Third, keyword-based analyses are sensitive to author terminology, which may lead to partial fragmentation of closely related concepts (e.g., variations of decentralized or self-sovereign identity). Future research could address these limitations by combining bibliometric mapping with systematic literature reviews or qualitative content analysis, expanding data sources, and conducting longitudinal comparisons across shorter time windows. Such extensions would allow for deeper theoretical synthesis and more precise identification of emerging research frontiers in blockchain identity management.

4. CONCLUSIONS

This study provides a comprehensive bibliometric mapping of blockchain identity management research from 2010 to 2025,

revealing a rapidly evolving and increasingly interconnected scholarly landscape. The findings show that the field is conceptually centered on blockchain-enabled authentication and decentralized identity systems, with a clear progression toward privacy-preserving mechanisms and application-oriented use cases. Collaboration patterns highlight the pivotal role of Asia (particularly China and India) supported by strong transcontinental linkages with the United States and Europe, underscoring the global relevance of blockchain-based identity solutions. By elucidating the intellectual foundations, thematic evolution, and research frontiers of the field, this study offers a structured knowledge base that can guide future theoretical development, inform practical implementation, and support evidence-based policymaking in digital identity ecosystems.

REFERENCES

[1] Y. Liu, D. He, M. S. Obaidat, N. Kumar, M. K. Khan, and K.-K. R. Choo, "Blockchain-based identity management systems: A review," *J. Netw. Comput. Appl.*, vol. 166, p. 102731, 2020.

[2] P. Dunphy and F. A. P. Petitcolas, "A first look at identity management schemes on the blockchain," *IEEE Secur. Priv.*, vol. 16, no. 4, pp. 20–29, 2018.

[3] S. El Haddouti and M. D. E.-C. El Kettani, "Analysis of identity management systems using blockchain technology," in *2019 International Conference on Advanced Communication Technologies and Networking (CommNet)*, 2019, pp. 1–7.

[4] M. Natti, "Reducing Oracle RAC Wait Events by Using Instance-Specific Block Allocation for Production Applications," *Eastasouth J. Inf. Syst. Comput. Sci.*, vol. 1, no. 01 SE-Articles, pp. 65–68, Aug. 2023, doi: 10.58812/esiscs.v1i01.447.

[5] T. Rathee and P. Singh, "A systematic literature mapping on secure identity management using blockchain technology," *J. King Saud Univ. Inf. Sci.*, vol. 34, no. 8, pp. 5782–5796, 2022.

[6] S. Y. Lim *et al.*, "Blockchain technology the identity management and authentication service disruptor: a survey," *Int. J. Adv. Sci. Eng. Inf. Technol.*, vol. 8, no. 4–2, pp. 1735–1745, 2018.

[7] Y. Liu, Z. Zhao, G. Guo, X. Wang, Z. Tan, and S. Wang, "An identity management system based on blockchain," in *2017 15th Annual Conference on Privacy, Security and Trust (PST)*, 2017, pp. 44–4409.

[8] M. R. Ahmed, A. K. M. M. Islam, S. Shatabda, and S. Islam, "Blockchain-based identity management system and self-sovereign identity ecosystem: A comprehensive survey," *Ieee Access*, vol. 10, pp. 113436–113481, 2022.

[9] X. Zhu and Y. Badr, "Identity management systems for the internet of things: a survey towards blockchain solutions," *Sensors*, vol. 18, no. 12, p. 4215, 2018.

[10] C. S. Sung and J. Y. Park, "Understanding of blockchain-based identity management system adoption in the public sector," *J. Enterp. Inf. Manag.*, vol. 34, no. 5, pp. 1481–1505, 2021.

[11] B. Faber, G. Michelet, N. Weidmann, R. R. Mukkamala, and R. Vatrapu, "BPDIMS: A blockchain-based personal data and identity management system," in *The 52nd Hawaii International Conference on System Sciences. HISS 2019: HISS 2019*, 2019, pp. 6855–6864.

[12] L. Lesavre, P. Varin, P. Mell, M. Davidson, and J. Shook, "A taxonomic approach to understanding emerging blockchain identity management systems," *arXiv Prepr. arXiv1908.00929*, 2019.

[13] M. Aria and C. Cuccurullo, "A brief introduction to bibliometrix," *J. Informetr.*, vol. 11, no. 4, pp. 959–975, 2017.

[14] I. Zupic and T. Čater, "Bibliometric methods in management and organization," *Organ. Res. methods*, vol. 18, no. 3, pp. 429–472, 2015.

[15] E. Androulaki *et al.*, "Hyperledger fabric: a distributed operating system for permissioned blockchains," in *Proceedings of the thirteenth EuroSys conference*, 2018, pp. 1–15.

[16] N. Kshetri, "1 Blockchain's roles in meeting key supply chain management objectives," *Int. J. Inf. Manage.*, vol. 39, pp. 80–89, 2018.

[17] L. Klerkx, E. Jakku, and P. Labarthe, "A review of social science on digital agriculture, smart farming and agriculture 4.0: New contributions and a future research agenda," *NJAS-Wageningen J. life Sci.*, vol. 90, p. 100315, 2019.

[18] N. Kshetri, "Can blockchain strengthen the internet of things?," *IT Prof.*, vol. 19, no. 4, pp. 68–72, 2017.

[19] T. McGhin, K.-K. R. Choo, C. Z. Liu, and D. He, "Blockchain in healthcare applications: Research challenges and opportunities," *J. Netw. Comput. Appl.*, vol. 135, pp. 62–75, 2019.

[20] Q. Feng, D. He, S. Zeadally, M. K. Khan, and N. Kumar, "A survey on privacy protection in blockchain system," *J. Netw. Comput. Appl.*, vol. 126, pp. 45–58, 2019.

[21] N. Kshetri, "Blockchain's roles in strengthening cybersecurity and protecting privacy," *Telecomm. Policy*, vol. 41, no. 10, pp. 1027–1038, 2017.

[22] X. Liang, J. Zhao, S. Shetty, J. Liu, and D. Li, "Integrating blockchain for data sharing and collaboration in mobile healthcare applications," in *2017 IEEE 28th annual international symposium on personal, indoor, and mobile radio communications (PIMRC)*, 2017, pp. 1–5.

[23] J. B. Bernabe, J. L. Canovas, J. L. Hernandez-Ramos, R. T. Moreno, and A. Skarmeta, "Privacy-preserving solutions

for blockchain: Review and challenges," *Ieee Access*, vol. 7, pp. 164908–164940, 2019.

[24] M. Shen *et al.*, "Blockchain-assisted secure device authentication for cross-domain industrial IoT," *IEEE J. Sel. Areas Commun.*, vol. 38, no. 5, pp. 942–954, 2020.