A Qualitative Review of Zero-Knowledge Proofs and Biometrics in Decentralized Identity Systems

Kedimotse Baruni[1], Sthembile Ntshangase[1], Harvest Ngobeni[1], Lesego Moatshe[1] and Nomalisa Ndhlovu[1]

[1] The Council for Scientific and Industrial Research, Pretoria, South Africa
kbaruni@csir.co.za

Abstract. This paper presents a qualitative review of the integration of Zero-Knowledge Proofs (ZKPs) and biometrics in Decentralized Identity (DID) systems. It explores how these technologies address key challenges in digital identity management, including privacy preservation, security enhancement, and regulatory compliance. Using three research questions, the study systematically reviews the recent literature to identify the problems these technologies solve, the sectors where they are applied, and the standards that govern their implementation. The review further reveals that ZKPs-DID is the most widely adopted method, dominating finance and governance applications, while Bio-DID focuses on healthcare and education under GDPR, and BioZK-DID combines biometrics with ZKPs for enhanced security but with limited regulatory guidance. The findings reveal that ZKPs enable privacy-preserving verification, while biometrics offer robust user-specific authentication. Integration within DID systems is particularly relevant in sectors such as finance, healthcare, governance, and education. However, challenges remain in scalability, interoperability, and regulatory alignment. This paper contributes new insights by proposing technical guidelines, policy recommendations, and future research directions to support the ethical and effective deployment of ZKP-biometric-enabled DID systems.

Keywords: Zero-Knowledge-Proofs, Biometrics, Decentralized Identity Systems, Privacy, Security, Regulations, Standards, Sectors, Applications.

1 Introduction

Digital identification has become increasingly essential in today's interconnected world, where secure and private identity management is a top priority[1][2]. Traditional systems that rely on centralized databases are particularly vulnerable to data breaches because all sensitive information is stored in a single location [3]. This centralization creates a single point of failure, making personal data more susceptible to unauthorized access and misuse. In contrast, decentralized identity (DID) systems offer several advantages, such as enhanced user control, improved resilience, and reduced dependency on centralized authorities [4]. Blockchain-based DID systems support self-sovereign identity (SSI), allowing individuals to manage their identity data independently [5]. These systems rely on Decentralized Identifiers (DIDs) and Verifiable Credentials

(VCs) [6], which enable secure and privacy-preserving data exchange. Examples like ShoCard, Authenteq, and IDchainZ show practical applications in finance, healthcare, and government services [6]. However, DID systems often lack robust security due to decentralization, a gap that biometrics can address [7]. Biometrics offer a promising solution to these challenges by providing a unique, user-specific method of identity verification that enhances both security and usability [8] . It also increases the robustness of security in many various applications/sectors such as authentication systems and border control [7][9]. While biometrics enhance authentication, they raise significant privacy concerns that can be mitigated using ZKPs [10]. A key challenge in DID systems is enabling identity verification without exposing sensitive personal data [11], which ZKPs also address. ZKPs allow users to prove their identity without revealing biometric information, reducing risks such as unauthorized access, identity theft, and data breaches.

ZKPs have gained traction as a cryptographic method to verify identity attributes without revealing the underlying data [12]. This is particularly valuable in privacy-sensitive applications, where users must prove eligibility without disclosing personal information. ZKP methods such as zk-SNARKs and Bulletproofs are being explored to enhance the privacy guarantees of DID systems [13]. The integration of ZKPs and biometrics enables secure, user-specific verification while maintaining confidentiality and system integrity [11]. This integration must, however, align with international standards and regulations, such as those proposed by the W3C for DIDs and VCs, ISO/IEC standards for biometrics, and GDPR-like data protection frameworks, to ensure interoperability, legal compliance, and ethical deployment [5].

This qualitative review is guided by the following three research questions:

- RQ1: What problems do ZKPs and biometrics solve in DID systems?
- RQ2: Which sectors apply these technologies?
- RQ3: What regulations and standards support their implementation?

The integration of DID systems that incorporate biometrics and ZKPs represents a novel and emerging approach to secure digital identity management and connecting technical understanding with practical applications and regularity issues. It is particularly timely given the global surge in digital identity initiatives and increasing concerns over data privacy. With regulations like GDPR and emerging digital ecosystems such as DeFi and e-health, there is a pressing need for authentication methods that are both secure and privacy-preserving. The integration addresses current challenges in identity theft, surveillance, and regulatory compliance, making this topic highly relevant to both academia and industry.

The structure of the paper is as follows: the following section reviews existing literature, the third section outlines the research methodology, the fourth section discusses the findings and results, the fifth section outlines recommendations and proposals and the sixth section concludes this study.

2 Literature Review

To build a comprehensive understanding of the integration of biometrics and ZKPs within DID systems, this section reviews existing scholarly work and technological developments in the field and highlights their applications and the standards that guide their implementation.

The work of [14] introduces the BioZero framework, a privacy-preserving biometric authentication system integrated within the decentralized identity system. It uses homomorphic encryption and ZKPs to ensure that biometric data is never exposed during verification. This system mitigates risks of biometric data leakage and identity theft, and is particularly relevant in healthcare, finance, E-commerce, and identity management. While this approach is technically robust, it lacks explicit reference to regulatory standards, which limits its practical deployment in compliance-sensitive sectors [14].

The work of [15] explores the integration of blockchain-based decentralized identity with biometric authentication to mitigate security issues, such as data breach risks and streamline verification. However, challenges, such as blockchain scalability limits, efficient handling of large biometric datasets, and interoperability demands standardized protocols for DID systems. In addition, this work introduces privacy risks that can be addressed using ZKPs. It also underscores a critical gap between technological innovation and regulatory alignment.

The work of 16] proposed identity authentication architecture based on blockchain and ZKPs. The architecture provides a high level of security and privacy protection and achieves decentralized management of identity information. ZKPs are utilized for digital identity management to maintain privacy and safeguard sensitive data. This technology can be used in digital identity management and health care services to protect the identity of the end user. Although this work achieves decentralized management and privacy protection, the absence of regulatory mapping weakens its applicability in regulated domains like healthcare.

The work of [17] proposed peer-supervised SSI framework that integrates ZKP-blockchain-based oversight, and a peer review mechanism. The framework allows users to manage their digital identity securely and privately while enabling service providers and regulatory authorities to interact with the identity under strict, cryptographically enforced conditions. This technology is used for digital identity management to preserve privacy and protect sensitive data. This work stands out for its regulatory foresight, proposing a three-party oversight system to ensure accountability and traceability.

The work of [18] presents a blockchain-based biometric authentication protocol, which uses fuzzy commitment schemes (FCSs) to allow for identity verification without revealing biometric templates to any third party. The system supports decentralized and cross-device authentication while maintaining user privacy by storing the encrypted biometric commitments on the chain through smart contracts. Authentication works off-chain; a new biometric sample gets matched against the on-chain commitment through ECC decoding. The setup, therefore, enables avoiding centralized storage, enhanced revocability, and is compliant with several privacy principles, such as data

minimization. This work suggests addressing the challenge of scalability and interoperability in future work, which is lacking in this work.

The work of [19] introduces a blockchain-based Multi-Factor Authentication (MFA) approach that uses zero trust principles. It uses ZKPs (zk-SNARKs) to protect user privacy in a decentralized setup. The approach uses a Distributed Authentication Mechanism (DAM) with smart contracts and non-transferable NFTs (based on a modified ERC-721 standard) to verify identity privately, but its reliance on ERC-721 may create interoperability challenges with other systems.

This work of [20] explores the integration of ZKPs and decentralized blockchain technology to address digital identity and financial security challenges in DeFi. It emphasizes ZKPs' ability to verify user attributes (e.g., age, citizenship) without revealing sensitive data, thus preserving privacy while ensuring compliance with regulations like GDPR, KYC, GDPR and AML. These regulations and compliance make this framework suitable for financial applications that mitigate risk, such as identity theft, fraud, and smart contract vulnerabilities.

The work in [21] presents a Blockchain-based Digital Identity Management System (BDIMS) designed to enable users to issue secure and verifiable digital credentials. BDIMS incorporates a QR code feature for real-time identity checks and utilizes ZKPs' identity attributes without disclosing the full information. This work reviews several BDIMS found in existing literature, including Sorvrin, SORA, MyData, and uPort. It underscores the critical role of regulations and standards in ensuring the effectiveness and trustworthiness of these systems. The work also highlights the significance of GDPR compliance, particularly in the context of the MyData BDIMS. However, this work lacks a unified standardization strategy.

The work of [22] propose a ZKP-based Anonymous Biometric Authentication (ZABA) scheme specifically designed for e-health systems, addressing critical concerns around data privacy and secure identity verification. Their approach integrates ZKPs with multimodal cancellable biometrics, including fingerprint, face, and iris data, to enhance authentication robustness while preserving user anonymity. This work contributes significantly to the field by demonstrating how ZKPs can be effectively combined with biometric modalities to achieve secure, anonymous, and efficient authentication in sensitive domains like healthcare.

The work of [23] combine DID systems with ZKPs to allow users to reveal only necessary identity attributes. This fine-grained control supports self-sovereign identity and aligns with modern privacy standards. To implement ZKPs, zk-SNARKs were utilized to enable fast and efficient proof generation and verification while keeping computational demands low. The proposed framework demonstrates strong potential for secure, privacy-preserving identity management across sectors requiring fine-grained control over personal data disclosure, such as healthcare, finance, and education.

Based on the reviewed literature, several key trends emerge in the integration of ZKPs and biometrics within DID systems. Privacy preservation stands out as a dominant theme, with ZKPs enabling identity verification without exposing sensitive data. In addition, strengthening the security is also a focus of this study which is achieved through the uniqueness of biometric traits combined with robust cryptographic protocols. However, regulatory alignment appears inconsistent; while some studies reference

frameworks such as GDPR and ISO/IEC standards, others lack clear regulatory grounding. Additionally, scalability and interoperability remain unresolved challenges, particularly in implementations that rely heavily on blockchain technologies.

The reviewed literature also highlighted several critical areas for future development in DID systems integrating biometrics and ZKPs. First, there is a clear need for standardized frameworks that harmonize technical robustness with regulatory compliance, ensuring interoperability and legal alignment across implementations. Second, while current research predominantly focuses on finance and healthcare, broader cross-sector validation is necessary. Emerging domains such as education, the Internet of Things (IoT), and electronic voting remain underexplored and warrant further investigation. Lastly, user-centric design considerations are often overlooked; many systems lack attention to usability and accessibility, which are essential for widespread adoption and practical deployment in real-world environments.

3 Research Methodology

This research utilized a secondary data analysis approach to examine how ZKPs and/or biometric technologies are integrated into DID systems across different industries, with a particular focus on the standards guiding these implementations. The methodology was designed to ensure a systematic and rigorous review of existing academic literature relevant to the research focus. It consisted of four key stages: dataset collection, source selection, exclusion criteria, and content screening.

Relevant literature was gathered from reputable academic databases, including Google Scholar, IEEE Xplore, and the ACM Digital Library. The search employed targeted keywords such as “Biometrics,” “Decentralized Identity,” “Zero-Knowledge Proofs,” and its abbreviation “ZKPs.” These terms were chosen to capture a comprehensive range of studies addressing the intersection of ZKPs and biometrics in DID systems. The initial search yielded approximately 383 papers, ensuring broad coverage of the topic.

To maintain quality and relevance, the review focused exclusively on peer-reviewed journal articles and conference proceedings. These sources were selected for their contribution to understanding technological applications, regulatory frameworks, and problem domains aligned with the research questions. After preliminary screening, only studies directly addressing ZKPs and/or biometrics within DID systems were retained.

Publications dated prior to 2021 were excluded to ensure the findings remain up-to-date. The remaining articles underwent a rigorous screening process, beginning with titles, abstracts, and conclusions, followed by full-text analysis. This process applied exclusion criteria based on relevance to the three research questions: (1) problems addressed by ZKPs and biometrics in DID systems, (2) sectors applying these technologies, and (3) regulations and standards supporting implementation. After applying these criteria, the dataset was narrowed to 10 papers, which provided detailed insights into the categories defined by the research questions. These papers were analysed to extract information on problems addressed, application domains, and regulatory considerations.

4 Results and Discussions

This section presents findings from the qualitative review of academic literature on the integration of ZKPs and biometrics within DID systems, as shown in Table 1. The analysis is structured around the three research questions (RQ1, RQ2 and RQ3) to ensure clarity and relevance.

RQ1: What problems do ZKPs and biometrics solve in DID systems? The review reveals that ZKPs and biometrics jointly address critical challenges in identity management, including privacy preservation, security enhancement, and decentralized user control. ZKPs enable verification without exposing sensitive data, mitigating risks of identity theft and data breaches. Advanced cryptographic techniques such as zk-SNARKs and Bulletproofs further improve scalability and efficiency, making these solutions suitable for high-throughput environments like decentralized finance (DeFi). Biometrics complement ZKPs by providing strong identity assurance and reducing impersonation risks, though they introduce new concerns around secure storage and ethical use of biometric data.

RQ2: Which sectors apply these technologies? Applications span multiple domains, including finance, healthcare, governance, education, and e-commerce, where secure and privacy-preserving identity verification is essential. ZKP-DID emerges as the most prevalent approach, appearing in the majority of studies and primarily applied in finance and governance to address fraud prevention and compliance challenges. Bio-DID is less common but plays a significant role in healthcare and education, where GDPR compliance and user sovereignty are critical. BioZK-DID, which integrates both ZKPs and biometrics, appears in fewer studies but demonstrates strong potential for enhancing security in sensitive sectors such as e-health and identity management systems.

RQ3: What regulations and standards support their implementation? Regulatory alignment remains inconsistent across implementations. While some frameworks reference GDPR, AML/KYC, and ISO/IEC biometric standards, others lack explicit compliance strategies, limiting their applicability in compliance-sensitive sectors. Emerging proposals, such as three-party oversight models, aim to ensure accountability and regulatory coverage, but harmonized global standards are still absent. This gap underscores the need for interoperability frameworks that integrate technical robustness with legal compliance.

The integration of ZKPs and biometrics in DID systems represents a transformative approach to secure, privacy-preserving, and user-centric identity management. However, several challenges persist. Scalability and interoperability remain major technical hurdles, as blockchain-based systems often face performance bottlenecks and lack standardized protocols for cross-platform compatibility. Regulatory fragmentation further complicates adoption, with varying interpretations of privacy laws and insufficient global harmonization. Additionally, usability and accessibility are rarely addressed in existing literature, despite their importance for widespread adoption across diverse populations.

These findings highlight the need for future research to focus on lightweight ZKP protocols optimized for mobile and edge devices, enabling resource-efficient verification in decentralized environments. Interoperability frameworks must be developed to

allow seamless identity verification across platforms and jurisdictions. Ethical considerations surrounding biometric surveillance require urgent attention, with safeguards to prevent misuse and protect user rights. Finally, designing user-centric identity architectures that balance privacy, usability, and security will be critical to achieving global adoption.

Table 1. Methods, Addressed Problems, Sectors/Applications and Governing Standards

Methods [Ref]	Problems Addressed	Application/Sectors	Regulations
ZKP-DID [20]	Identity theft and fraud	Finance, Healthcare, Voting, Supply Chains	GDPR, KYC, AML
ZKP-DID [21]	Privacy preservation	Healthcare, Education	GDPR
Bio-DID [15]	Data breach risks, streamlined verification, user control & self-sovereignty	Identity Management Systems in Healthcare and Education	GDPR
ZKP-DID [19]	Privacy preservation and scalability using zk-SNARKs	Finance (DeFi), Health, Governance & Public Services	Not specified
ZKP-DID [17]	Privacy preservation, data breach risks, excessive data requests and misuse	Identity Management Systems	Novel three-party oversight ensuring complete regulatory coverage and accountability
ZKP-DID [16]	Privacy preservation	Banking, Digital Identity Management, Healthcare	Not specified
BioZK-DID [14]	Privacy preservation, security (Sybil attacks), scalability	Healthcare, Finance, E-commerce, Identity Management	Not specified
Bio-DID [18]	Privacy preservation, security	Identity Management Systems	GDPR
BioZK-DID [22]	Privacy preservation, security	e-Health	Not specified
ZKP-DID [23]	Privacy preservation	Healthcare, Finance, Education	Not specified

5 Recommendations and Proposals

To enhance the practical relevance and future direction of integrating ZKPs and biometrics in DID systems, this section outlines key recommendations and proposals. The technical guidelines for implementation, policy and regulations proposals include recommendations for researchers, policy makers and industry practitioners.

- For researchers
    - Investigate hybrid models combining ZKP and biometrics for enhanced security.
    - Employ zk-SNARKs or Bulletproofs for efficient and scalable privacy-preserving verification.
    - Explore lightweight cryptographic protocols for scalability in resource-constrained environments.
    - Consider quantum-safe cryptographic protocols for ZKP and biometrics implementations.
    - Use multimodal biometric systems (e.g., fingerprint + iris) to improve authentication robustness.
    - Implement decentralized consent protocols to ensure user control over biometric data.
- For policy makers
    - Establish global standards for privacy-preserving identity systems.
    - Develop standards for biometric data handling in decentralized systems aligned with data protection regulations, such as, POPIA, ISO/IEC 24745 and GDPR.
    - Mandate compliance frameworks that integrate GDPR, AML, and KYC requirements.
    - Encourage cross-border regulatory harmonization to support interoperability and legal compliance.
    - Promote ethical guidelines for biometric data usage, including transparency, consent, and data minimization.
- For industry practitioners
    - Adopt ZKP-DID solutions in finance and healthcare to mitigate fraud and privacy risks.
    - Implement biometric safeguards and ensure regulatory interoperability before deployment.
    - Leverage smart contracts for secure and automated identity verification workflows.
    - Ensure secure storage and revocation mechanisms for biometric data to prevent misuse.

6 Conclusion

This review examined the intersection of ZKPs, biometrics, and DID systems, addressing three core research questions on problems ZKPs and biometrics solve in DID systems, sectors that apply these technologies, regulations and standards that support their implementation. The findings reveal that ZKPs and biometrics jointly tackle critical issues such as privacy preservation, security enhancement, and decentralized user control. These technologies are increasingly applied in finance, healthcare, governance, and education, with emerging use cases in e-commerce and e-health. However, regulatory compliance remains inconsistent; while some systems reference GDPR and

ISO/IEC standards, others lack clear legal grounding, limiting interoperability and global adoption. Additionally, usability and accessibility challenges persist, which could hinder widespread deployment. To address these gaps, this study proposed technical and policy recommendations, including zk-SNARKs for scalable verification, multimodal biometrics for robust authentication, and decentralized consent protocols for user control. Aligning technological innovation with ethical and legal standards is essential to building trustworthy digital ecosystems.

Future research should prioritize practical validation of the proposed intersection of ZKPs, biometrics, and DID systems. Developing a basic prototype or proof-of-concept implementation will allow researchers to test the feasibility, scalability, and usability of these integrated technologies in real-world scenarios. This step is critical to move from theoretical soundness to empirical evidence, ensuring that the hypothesis holds under practical constraints. Additionally, research should continue to advance lightweight ZKP protocols optimized for mobile and edge devices, explore interoperability frameworks for seamless cross-platform identity verification, and examine the ethical implications of biometric surveillance to propose robust safeguards. Finally, designing user-centric identity architectures that balance privacy, usability, and security will be essential for global adoption.

References

1. M. Robles-Carrillo, *Digital identity: an approach to its nature, concept, and functionalities*, International Journal of Law and Information Technology, vol. 32, pp. eaae019, 2024.
2. C. S. Ntshangase et al., *Solving the privacy and security challenge using ZKP: Its positive impact on the economy*, 2024.
3. V. Listi, *Securing Digital Identity Blockchain-Based Anonymous Authentication with Zero-Knowledge Proofs*, 2025.
4. A. Goel and Y. Rahulamathavan, *A Comparative Survey of Centralised and Decentralised Identity Management Systems: Analysing Scalability, Security, and Feasibility*, Future Internet, vol. 17, no. 1, 2024. DOI: 10.3390/fi17010001.
5. C. Brunner et al., *DID and VC: Untangling Decentralized Identifiers and Verifiable Credentials for the Web of Trust*, 3rd International Conference on Blockchain Technology and Applications, pp. 61, 2020. DOI: 10.1145/3446983.3446992.
6. R. Nokhbeh Zaeem et al., *Blockchain-Based Self-Sovereign Identity: Survey, Requirements, Use-Cases, and Comparative Study*, IEEE/WIC/ACM International Conference on Web Intelligence, pp. 128, 2021. DOI: 10.1145/3486622.3493917.
7. M. Ghafourian et al., *Combining blockchain and biometrics: A survey on technical aspects and a first legal analysis*, arXiv Preprint arXiv:2302.10883, 2023.
8. S. H. G. Salem et al., *Blockchain-based biometric identity management*, Cluster Computing, vol. 27, no. 3, pp. 3741–3752, 2024.
9. K. Baruni et al., *Age invariant face recognition methods: A review*, 2021 International Conference on Computational Science and Computational Intelligence (CSCI), 2021.
10. Y. Ali Zouaghi et al., *Privacy preserving biometric authentication based on fully homomorphic encryption, blockchain, and IPFS data storage*, Multimed Tools Appl, 2025. DOI: 10.1007/s11042-025-20817-y.

11. S. Prasad, N. Tiwari, and M. Chawla, *Zero-knowledge proofs in biometric authentication systems: A review*, Congress on Smart Computing Technologies, 2023.
12. K. Wang et al., *Hades: Practical decentralized identity with full accountability and fine-grained sybil-resistance*, Proceedings of the 39th Annual Compu Security Applications Conference, 2023.
13. J. Lai et al., *BioZero: An Efficient and Privacy-Preserving Decentralized Biometric Authentication Protocol on Open Blockchain*, arXiv, Sept. 26, 2024. Available: http://arxiv.org/abs/2409.17509.
14. H. A. Oluwadara, *Integrating Blockchain and Biometric Authentication for Decentralized Identity Management Systems*, 2023.
15. Y. Jielin et al., *Research on Identity Data Privacy Protection Based on Blockchain and Zero Knowledge Proofs*, Proceedings of the 2024 7th International Conference on Artificial Intelligence and Pattern Recognition, 2025. DOI: https://doi.org/10.1145/3703935.3703972.
16. J. Liu, Z. Liang, and Q. Lyu, *Empowering Privacy Through Peer-Supervised Self-Sovereign Identity: Integrating Zero-Knowledge Proofs, Blockchain Oversight, and Peer Review Mechanism*, Sensors, vol. 24, no. 24, pp. 8136, 2024. DOI: 10.3390/s24248136.
17. N. A. Alzahab et al., *Decentralized Biometric Authentication based on Fuzzy Commitments and Blockchain*, arXiv, Sept. 17, 2024. Available: http://arxiv.org/abs/2409.11303.
18. J. Jose Diaz Rivera, A. Muhammad, and W. Song, *Securing Digital Identity in the Zero Trust Architecture: A Blockchain Approach to Privacy-Focused Multi-Factor Authentication*, IEEE Open J. Commun. Soc., vol. 5, pp. 2792, 2024. DOI: 10.1109/ojcoms.2024.3391728.
19. A. D. Soyele et al., *Enhancing Digital Identity and Financial Security in Decentralized Finance (DeFi) through Zero-Knowledge Proofs (ZKPs) and Blockchain Solutions for Regulatory Compliance and Privacy*, 2024.
20. M. H. K. Rupok and K. M. A. Hasan, *BDIMS: A Blockchain Based Digital Identity Management System with Zero Knowledge Proof*, Proceedings of the 3rd International Conference on Computing Advancements, pp. 607, 2024. DOI: 10.1145/3723178.3723258.
21. X. Mao et al., *A ZKP-based anonymous biometric authentication scheme for the E-health systems*, PLoS One, vol. 20, no. 6, pp. e0324289, 2025.
22. H. Yin et al., *A blockchain-based selective disclosure authentication system: A self-sovereign credential scheme combining decentralized identity and zero-knowledge proofs*, International Conference on Ubiquitous Security, 2024.
23. X. Yang and W. Li, *A zero-knowledge-proof-based digital identity management scheme in blockchain*, Computers & Security, vol. 99, 2020. DOI: 10.1016/j.cose.2020.102050.