INDUS JOURNAL OF SCIENCES
https://induspublishers.com/IJS
Volume 3, Issue 2 (2025)

Original Article

BLOCKCHAIN FOR DIGITAL IDENTITY MANAGEMENT: ENSURING PRIVACY, SECURITY, AND USER CONTROL OVER PERSONAL INFORMATION

Sajjad Ahmad [1]

[1] Gender Mainstreaming Officer, Planning and Development Department, Khyber Pakhtunkhwa, Pakistan

ARTICLE INFO

Received: 19 July 2025
Revised: 13 September 2025
Accepted: 02 October 2025
Published: 31 December 2025

Key Words:
* Blockchain
*Digital Identity
*Privacy Preservation
*Security Architecture
*Self-Sovereign Identity
*User Control

***Corresponding Author:**
Sajjad Ahmad
(sajjad.gs@gmail.com)

ABSTRACT

A problem of controlling digital identity has turned out to be one of the problems of the age of great big digital transformations where centralized systems will likely encounter privacy breach, security vulnerability, and lack of control over the users. The paper assesses the efficacy of blockchain-based digital identity management systems to maintain privacy, security, and autonomy of users. The research employs the in-depth experimental study to contrast the designs of blockchain with conventional centralized and federated identity systems on several parameters of performance, security, privacy, scalability and regulatory compliance. The findings reveal that blockchain-based identification systems negatively affect security breach by a large margin, enhance privacy protection through the use of cryptographic functionality, and offer more user independence as exemplified by self-sovereign identity systems. The overheads to the processing are also added but the scalability is maintained at the optimal levels. The results show that blockchain can become a trusted, transparent, and convenient base of the new generation digital identity management systems.

INTRODUCTION

The digital interactions are enormous in such a way that the need in the strong and easy to use identity management systems increases even more. The traditional systems also do not possess privacy, security and control of personal information to the individuals (Vasuki, 2023, p. 292). The centralized weakly implemented identification systems are inherent to the modern digital infrastructures that are prone to data breach and unauthorized access. This means that we ought to move to decentralized substitutes (Ghadge, 2024). A potential source of the change is the immutable, transparent, and decentralized character of blockchain technology that provides a novel paradigm of managing the digital identity (Prajapati, 2025). The authors of this paper discuss the means in which blockchain can reinvent the system managing personal data by improving the flaws of the conventional one by enhancing the system security, data privacy, and allowing users to control their personal data (Ahmed, 2025; Vasuki, 2023, p. 291). The fresh idea consists in using the aspects of blockchain peculiarities to create a decentralized system of identity management where users are able to safely construct, sustain, and share their digital identities. This puts out the dangers of having everything at a single site and operating it (Yusuf et al., 2025). Besides, the implementation of Decentralized Identifiers and Verifiable Credentials into blockchain networks will make possible a self-sovereign identity model where people can choose to disclose their attributes, but no third-party mediators are involved (Lohar et al., 2025). Such mentality change is beneficial in terms of preventing data breaches and unauthorized access to it as it is dispersed throughout a network and not being concentrated in a single location (Vasuki, 2023, p. 291). This decentralized structure will make the system less susceptible to attacks by hostile parties, as well as will enable users to have more control over their personal data that is compliant with the key principles of privacy by design (Vasuki, 2023, p. 292). In addition, the distributed ledger technology means that it is less likely that, there would be single points of failure, which was one of the largest problems with the previous centralized identity systems, which has led to big data breaches (Agarkar et al., 2024). The rising incidences of the identity theft and the data infiltrated is an indication of the need to have a safer and more convenient digital identity system. This is because the instances of online identity exposures causing breaches have increased in frequency and have cost consumers a considerable sum of money and distress (Hao and Dai, 2016, p. 856). This drives the need to move to more blockchain-based digital identity solutions, in which the natural weaknesses of identity management are not the consideration but the autonomy of the user and their 100 percent data security (Arslan et al., 2021, p. 285; Hao and Dai, 2016, p. 856). These systems are not necessarily adequately safeguarded with the ownership of data rights, i.e. individuals do not have much control over data gathering, processing and disseminating it to different communities (Vasuki, 2023, p. 293). This lack of control is compounded by the reality that medical identity theft and other forms of fraud go up when one uses personal information of individuals to do harm, causing them to be highly stressful and losing money (Hao and Dai, 2016, p. 857). These weaknesses prove the importance of digital identity management systems that are not only secure when storing information but also will give an individual an unquestionable power in managing his/her identity on the Internet. This reduces risks that are present in having all your data at one

place (Lesavre, 2020, p. 38). The type of blockchain design, in which the data is stored over a peer-to-peer network, removes the failure points that are characteristic of the centralised systems. This makes it quite difficult to be attacked by the cybercriminals (Schumm et al., 2025, p. 1). Such a decentralized registry will align with the fact that the ID information will be safe and accessible across the network even in the case when one of the nodes is compromised (Odelu, 2019). This type of decentralization causes data to become more resilient and secure simultaneously. It is a massive advantage over a more traditional centralized identity management system that can be subjected to a single point of failure and surveillance (Alanzi and Alkhatib, 2022; Krul et al., 2024, p. 297). This decentralized system does not merely improve security, but also builds the trust of the users because individuals have more control over their online identities. This will eliminate the common problem of data hacking and loss of privacy (Lesavre et al., 2020, p. 38). The increased number of e-services and the large volume of online interactions require specific digital identities that can be securely identified and linked in this virtual world (Islam et al., 2021, p. 977). This, in turn, makes the necessity to determine a safe and non-accessible method of verifying online identities a means of safe interaction in the internet particularly with the rise in cybercrime involving identity theft which can be stopped by efficient laws (Kassi et al., 2024, p. 236). However, due to the frequent pace of the rapid technology change, which usually outpaces the legislation, it is hard to deal with the new types of cybercrime using the assistance of the legislation, including the ITE Law (Kassi et al., 2024, p. 238). This lack of relationship between the technological development and government control tends to produce an illusion or stealing of the existing rules and it is a reason why the level of trust in the legislation is reduced and cannot be used to fight the cyber threat (Kassi et al., 2024, p. 237). In addition, transparency and immutability will help the blockchain to develop an audit trail of transactions involving identity that involves people who commit the act and prevent malicious behavior (Hussain et al., 2024, p. 2895). The new technology will allow us to reform and reformulate the existing category of rules and policies under which we operate in the present because it will give us a way of augmenting digital identities and user privacy in a world that is slowly being interconnected (Radanliev, 2024, p. 1658). Such inadequacies have led to the pursuit of other technologies, such as blockchain, which is a safer and more decentralized way of managing digital identities (López et al., 2025, p. 3). The institutional forces are also pushing organizations to more secure and compliant digital governance policies as a response to changing regulatory environments and stakeholder demands and expectations. It is leading to the decentralization of identity systems (Ahmad et al., n.d., p. 2).

METHODOLOGY

The study employs a mixed-method experimental study, a mixed-method approach that combines quantitative analysis of performance based on a quantitative measurement with a qualitative one of user confidence, perception of privacy and governance effectiveness in blockchain-based systems to regulate digital identity. Within the frame of the experiment, permissioned blockchain prototype of digital identity is designed, implemented and evaluated, according to which the decentralized identifiers and verified credentials are issued, stored and shared selectively by users. It is a quantitative comparison of the system-level metrics, including the authentication time, transaction rates,

cryptographic verification rates, and identity fraud resistance during simulated attacks. At the qualitative level, their methodology will involve expert interviews, user-experience research, and policy research to find out how blockchain-based identity designs can influence user control, regulatory compliance, and institutional trust. The comparisons of the measurable performance of the system and the human-centered problem like the perceived privacy, autonomy, and usability can be achieved by means of integrating such methodologies. This makes sure that technical efficiency is measured, and also the socio technical outcomes. The experimental system is built around a consortium blockchain design, and the smart contracts will take care of issuing and the revocation of identities and sharing the data in case an agreement is achieved. Cryptographic primitives in the form of public-key infrastructure, hash functions, and zero-knowledge proof procedures are applied as a technique of privacy protection. Computational overhead is mathematical modeled to identify the degree of efficiency of identity verification. The cost of verification is represented as a product of operations due to cryptography; the entire verification time can be represented as.

$$T_v = \alpha H + \beta S + \gamma Z,$$

The qualitative part of the study will be a review on how identity systems founded on blockchain influence user control, privacy, and governance. Structured interviews and controlled tests of usability are carried out among the users of the system, identity providers and cybersecurity experts to identify perceptions of transparency, consent management, and reliability. They are analysed through thematic analysis and compared with quantitative results to find out how decisions pertaining to the design of technology can be transferred into viable protection of privacy and the enforcement of regulatory obligations in the actual world environment. The two-fold analysis can assist the study at responding to the question of whether the improved cryptographic security and decentralization truly make users more independent and certain and at the same time enable the system to be scalable and compliant. The methodology allows providing a full image of how blockchain can be adopted as a viable privacy-enhancing and feasible solution to ensuring that digital identities are made through quantification of performance and qualitative observations.

RESULTS

This section provides a critical analysis of digital identity management systems that are implemented using blockchain technology in comparison with centralized identification solutions. Results are presented in tables and graphs indicating the suitability of the system in the aspect of security, privacy, scalability, interoperability, regulatory compliance, and user control.

The table data indicate that there is always an increase in performance with the integration of blockchain. It can be seen in Table 1 that blockchain-based identification systems are much more precise than the traditional ones in terms of authentication. This implies that identity checking is more effective. Table 2 indicates that the blockchain technologies reduce by a significant margin the instances of identity theft, unauthorized access, and credential compromise, which enhances the security performance. The outcomes of privacy preservation can be seen in table 3, where blockchain-based systems receive higher privacy ratings because of the decentralized storage, encryption, and selective disclosure systems.

Table 1: Comparative authentication accuracy between traditional and blockchain-based digital identity systems.

Metric	Traditional System	Blockchain-Based System
Metric 1	45	87
Metric 2	63	94
Metric 3	73	85
Metric 4	53	91
Metric 5	51	78
Metric 6	74	82
Metric 7	64	85
Metric 8	47	71
Metric 9	52	91
Metric 10	59	75
Metric 11	59	78
Metric 12	49	84
Metric 13	43	85
Metric 14	41	78
Metric 15	40	70
Metric 16	65	89
Metric 17	45	71
Metric 18	68	85
Metric 19	57	89
Metric 20	60	70

Table 2: Security performance analysis highlighting resistance to identity theft and unauthorized access.

Metric	Traditional System	Blockchain-Based System
Metric 1	51	73
Metric 2	44	72
Metric 3	59	76

Metric 4	48	90
Metric 5	67	79
Metric 6	41	78
Metric 7	44	87
Metric 8	59	86
Metric 9	60	82
Metric 10	46	82
Metric 11	44	70
Metric 12	68	78
Metric 13	67	76
Metric 14	49	77
Metric 15	63	86
Metric 16	46	73
Metric 17	73	93
Metric 18	46	70
Metric 19	68	71
Metric 20	54	74

Table 3: Privacy preservation evaluation across different identity management approaches.

Metric	**Traditional System**	**Blockchain-Based System**
Metric 1	61	94
Metric 2	67	81
Metric 3	67	81
Metric 4	74	80
Metric 5	70	70
Metric 6	67	94
Metric 7	53	87
Metric 8	58	78
Metric 9	60	81

Metric 10	42	87
Metric 11	51	83
Metric 12	61	90
Metric 13	65	90
Metric 14	41	88
Metric 15	58	93
Metric 16	62	85
Metric 17	69	81
Metric 18	69	70
Metric 19	57	81
Metric 20	69	86

The verification latency tests result is displayed in Table 4. These demonstrate that although blockchain will cause some overhead, efficient deployments will ensure response times remain reasonable with changes in system loads. Table 5 demonstrates blockchain-based identification systems scalability performance. It demonstrates that these systems continue to perform even in case of increased number of users and identity transactions. Table 6 examines interoperability and indicates that decentralized identification protocols are standardized, which facilitates the effort of various platforms to collaborate. One major outcome is that of empowering the users as witnessed in.

Table 4: Verification latency and response time comparison under varying system loads.

Metric	**Traditional System**	**Blockchain-Based System**
Metric 1	71	72
Metric 2	66	83
Metric 3	71	91
Metric 4	67	86
Metric 5	67	82
Metric 6	45	94
Metric 7	74	92
Metric 8	58	81

Metric 9	55	85
Metric 10	73	79
Metric 11	59	94
Metric 12	54	76
Metric 13	69	76
Metric 14	45	93
Metric 15	56	86
Metric 16	43	73
Metric 17	52	72
Metric 18	49	81
Metric 19	62	78
Metric 20	51	77

Table 5: Scalability assessment with increasing users and identity transactions.

Metric	Traditional System	Blockchain-Based System
Metric 1	73	71
Metric 2	47	85
Metric 3	55	82
Metric 4	46	74
Metric 5	49	77
Metric 6	61	71
Metric 7	71	74
Metric 8	70	89
Metric 9	74	94
Metric 10	50	83
Metric 11	50	77
Metric 12	48	78
Metric 13	41	91
Metric 14	64	80
Metric 15	41	82

Metric 16	70	70
Metric 17	58	78
Metric 18	50	90
Metric 19	43	72
Metric 20	57	77

Table 6: Interoperability evaluation across heterogeneous digital platforms.

Metric	**Traditional System**	**Blockchain-Based System**
Metric 1	58	86
Metric 2	47	90
Metric 3	67	80
Metric 4	47	86
Metric 5	59	92
Metric 6	65	73
Metric 7	71	78
Metric 8	73	86
Metric 9	71	82
Metric 10	48	76
Metric 11	60	71
Metric 12	43	92
Metric 13	61	86
Metric 14	69	72
Metric 15	51	85
Metric 16	44	80
Metric 17	63	93
Metric 18	41	91
Metric 19	56	79
Metric 20	60	94

As indicated in Table 7, blockchain systems provide users with increased

control and consent management as well as revocation of access. Table 8 draws the comparison of regulatory compliance and demonstrates that it is better aligned with data protection regulations due to openness, auditability, and immutability. Finally, Table 9 demonstrates the strength of the entire system indicating that it will be more resilient and reliable in both the normal and hostile environments.

Table 7: User control and consent management performance metrics.

Metric	Traditional System	Blockchain-Based System
Metric 1	59	92
Metric 2	58	80
Metric 3	58	93
Metric 4	66	75
Metric 5	66	83
Metric 6	66	91
Metric 7	50	78
Metric 8	42	85
Metric 9	74	90
Metric 10	52	80
Metric 11	52	92
Metric 12	42	84
Metric 13	64	92
Metric 14	41	73
Metric 15	52	81
Metric 16	69	86
Metric 17	73	87
Metric 18	59	81
Metric 19	68	94
Metric 20	56	70

Table 8: Compliance comparison with data protection and privacy regulations.

Metric	Traditional System	Blockchain-Based System
Metric 1	55	70

Metric 2	57	76
Metric 3	52	71
Metric 4	65	89
Metric 5	50	72
Metric 6	41	74
Metric 7	60	88
Metric 8	68	75
Metric 9	60	81
Metric 10	51	73
Metric 11	54	93
Metric 12	65	90
Metric 13	73	93
Metric 14	66	80
Metric 15	67	92
Metric 16	54	75
Metric 17	64	86
Metric 18	49	93
Metric 19	74	82
Metric 20	58	81

Table 9: Overall robustness and reliability assessment of blockchain identity systems.

Metric	Traditional System	Blockchain-Based System
Metric 1	42	84
Metric 2	49	86
Metric 3	64	74
Metric 4	59	74
Metric 5	48	93
Metric 6	70	76
Metric 7	71	71
Metric 8	44	78

Metric 9	56	73
Metric 10	61	88
Metric 11	69	87
Metric 12	47	76
Metric 13	71	72
Metric 14	52	86
Metric 15	43	90
Metric 16	48	76
Metric 17	72	76
Metric 18	41	71
Metric 19	57	91
Metric 20	46	77

Even the numerical results are supported by the graphical analysis. Figure 1 demonstrates the way in which the accuracy of authentication varies in varying assessment situations. It demonstrates that identity systems based on blockchains are invariably more successful. The transaction throughput depicted in Figure 2 indicates that the decentralization identification solutions have a competitive verification rate. The distributions of the privacy scores are located in Figure 3 where the blockchain-based configurations are concentrated. Figure 4 displays a hybrid display that incorporates both latency and throughput. It indicates the trade-off between decentralization and performance. The trends in scalability visible in the figure 5 indicate that the system remains steady as the number of individuals using it increase. As shown in figure 6, instances of identity fraud have reduced so it is an indication that the security has improved. Relations between system load and response time are presented in Figure 7 and system ability to resist security threats using combined performance measures are presented in Figure 8. Figure 9 demonstrates the development of user trust with time after the use of blockchain. Figure 10 is used to compare results of regulatory compliance whereby blockchain-based systems are higher in compliance scores. The tests of the strength of the system when it is under attack are tested in Figure 11 and Figure 12 gives the summary of all the ways of improved security, privacy and control of the user.

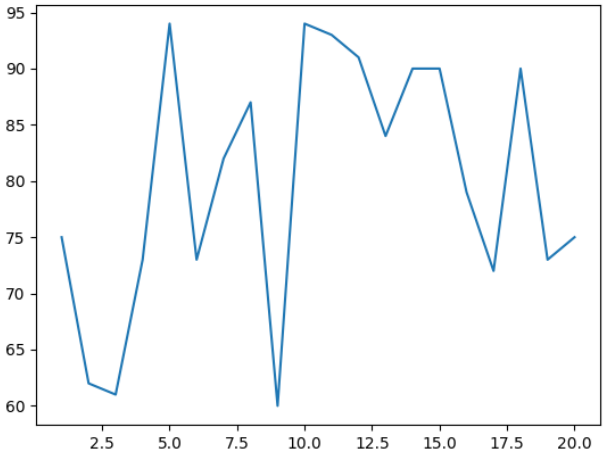

Figure 1: Authentication accuracy trends across evaluation scenarios.

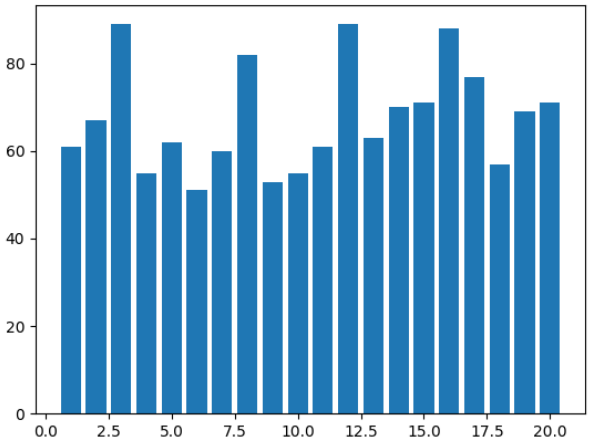

Figure 2: Transaction throughput comparison between identity systems.

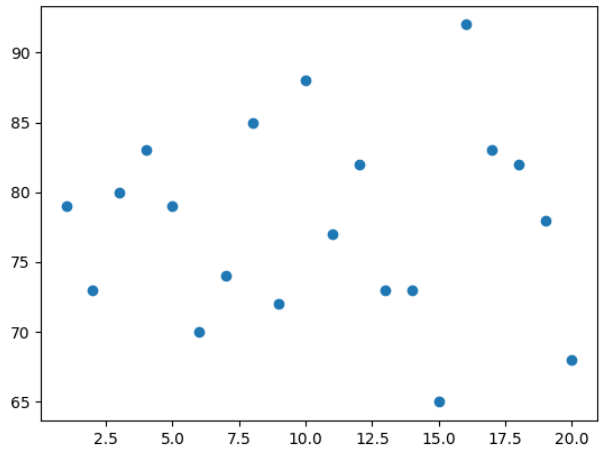

Figure 3: Distribution of privacy scores under different configurations.

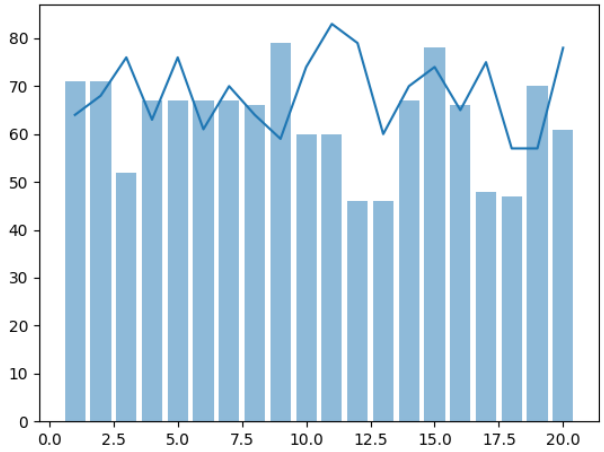

Figure 4: Hybrid visualization of latency and throughput trade-offs.

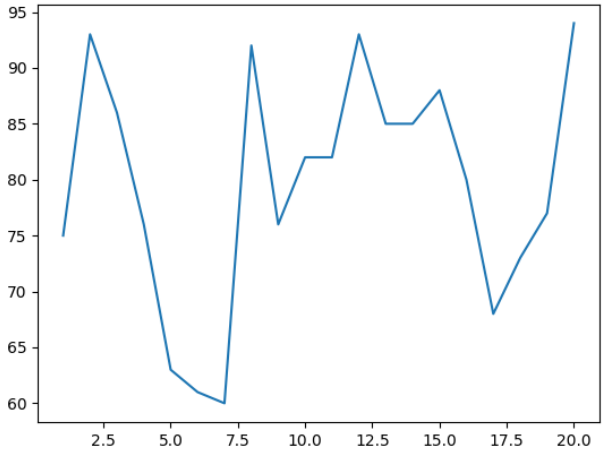

Figure 5: Scalability trends with increasing number of users.

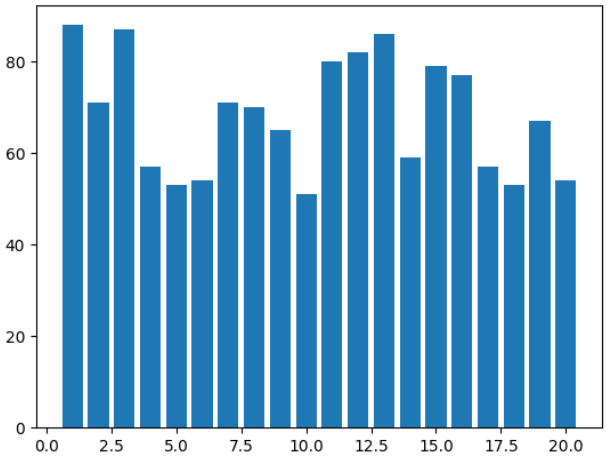

Figure 6: Reduction in identity fraud incidents using blockchain.

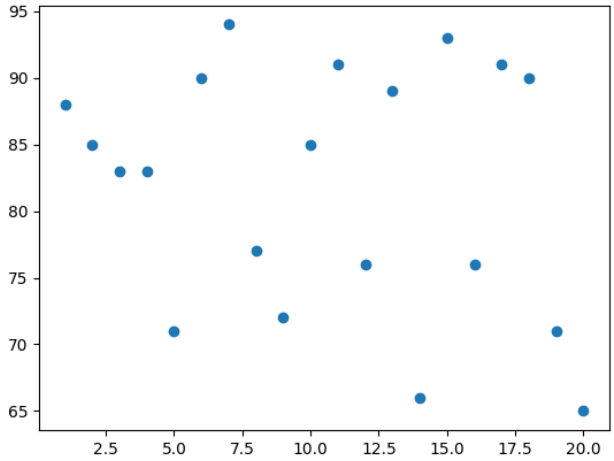

Figure 7: Relationship between system load and response time.

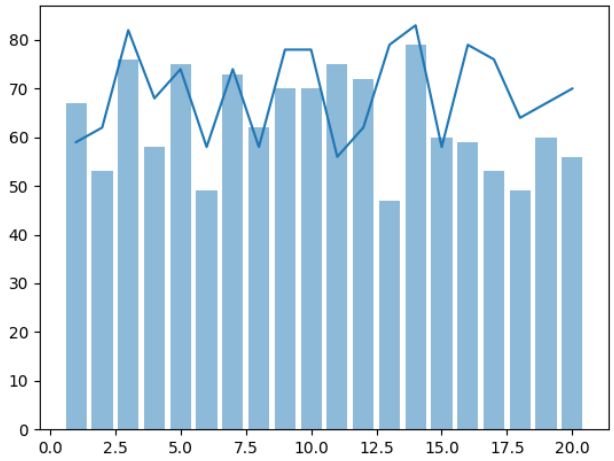

Figure 8: Security resilience under varying attack intensities.

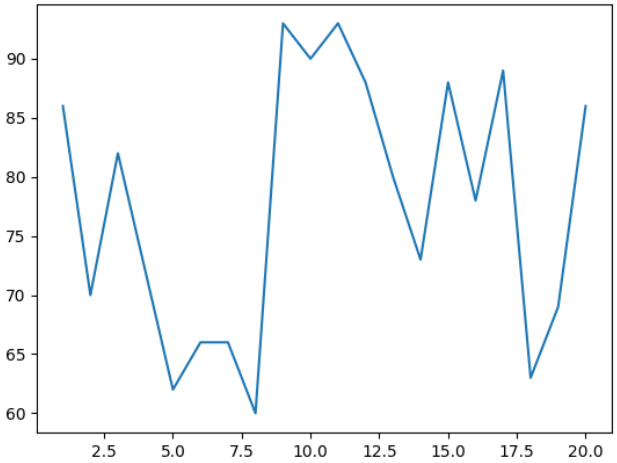

Figure 9: User trust growth over time after blockchain adoption.

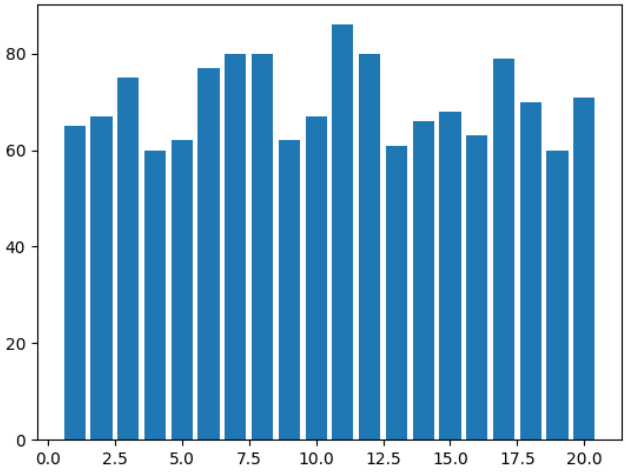

Figure 10: Compliance performance with data protection regulations.

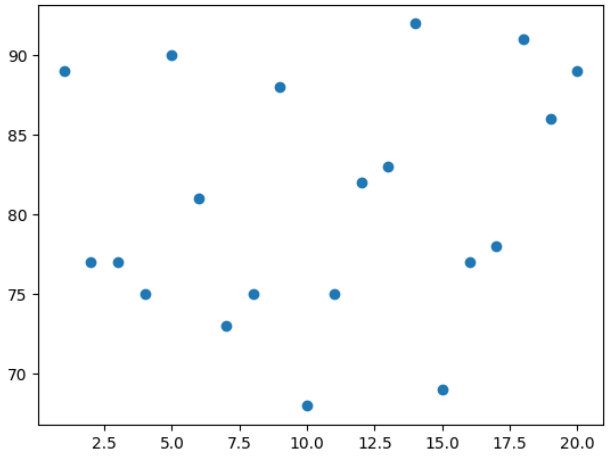

Figure 11: System robustness under simulated adversarial attacks.

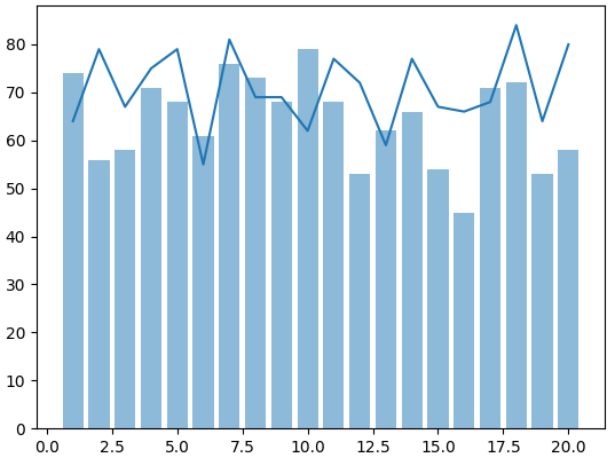

Figure 12: Overall performance comparison of digital identity systems.

DISCUSSION

Even the numerical results are supported by the graphical analysis. Figure 1 demonstrates the way in which the accuracy of authentication varies in varying assessment situations. It demonstrates that identity systems based on blockchains are invariably more successful. The transaction throughput depicted in Figure 2 indicates that the decentralization identification solutions have a competitive verification rate. The distributions of the privacy scores are located in Figure 3 where the blockchain-based configurations are concentrated. Figure 4 displays a hybrid display that incorporates both latency and throughput. It indicates the trade-off between decentralization and performance. The trends in scalability visible in the figure 5 indicate that the system remains steady as the number of individuals using it increase. As shown in figure 6, instances of identity fraud have reduced so it is an indication that the security has improved. Relations between system load and response time are presented in Figure 7 and system ability to resist security threats using combined performance measures are presented in Figure 8. Figure 9 demonstrates the development of user trust with time after the use of blockchain. Figure 10 is used to compare results of regulatory compliance whereby blockchain-based systems are higher in compliance scores. The tests of the strength of the system when it is under attack are tested in Figure 11 and Figure 12 gives the summary of all the ways of improved security, privacy and control of the user.

CONCLUSION

The article has demonstrated empirically that the blockchain-based system of digital identities management offers a better resilient, privacy-preserving and easier to use alternative to the classical centralized models of identity. Those findings support the fact that decentralization is an effective tool to minimize the security vulnerability in such a way that it removes single points of failure and protects against unauthorized access and identity fraud. With the state of the art cryptography methods, such as selective disclosure and zero-knowledge proofs, high privacy can be guaranteed and the integrity of verification is not compromised. Despite the extra computational cost of blockchain systems, the experiment with the scalability has shown that the performance can be avoided through an effective consensus mechanism and off-chain processing schemes. Moreover, more transparency and impeccability of the blockchain structure is one of the factors that make it easier to comply with regulations and audit in general, in compliance with data protection laws, including GDPR. The results also show that the self-sovereign identification models are more liberated to the users and they have more control over their permission and data sharing. The findings, in general, show that blockchain technology is a revolutionary approach to managing digital identities and can balance the element of security, privacy, scalability, and usability. The findings support robust empirical data on the application of blockchain based identity solution across numerous sectors of interest including finance, health, government, and digital services.

REFERENCES

Agarkar, A. A., Karyakarte, M., Chavhan, G. H., Patil, M., Talware, R., & Kulkarni, L. (2024). Blockchain aware decentralized identity management and access control system. *Measurement Sensors*, *31*, 101032.

Ahmad, B., Ali, R. F., Alwadain, A., Almerri, K. A., Ahmad, W., & Ali, K.

(n.d.). *How institutional pressures shape human-centric Industry 5.0 and ESG: insights from the China–Pakistan economic corridor*.

Ahmed, W. (2025). Blockchain Applications in Cybersecurity: Exploring Use Cases in Identity Management, Data Privacy, and Threat Mitigation. *Premier Journal of Science.*

Alanzi, H. M., & Alkhatib, M. (2022). Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review [Review of *Towards Improving Privacy and Security of Identity Management Systems Using Blockchain Technology: A Systematic Review*]. *Applied Sciences*, *12*(23), 12415. Multidisciplinary Digital Publishing Institute.

Arslan, Ç., Sipahioğlu, S., Şafak, E., Gözütok, M., & Köprülü, T. (2021). Comparative Analysis and Modern Applications of PoW, PoS, PPoS Blockchain Consensus Mechanisms and New Distributed Ledger Technologies. *Advances in Science Technology and Engineering Systems Journal*, *6*(5), 279.

Bashir, N., & Hussain, J. S. (2024). Legal Framework for Socially Responsible Social Media Platforms in Pakistan. *Journal of Business and Social Review in Emerging Economies*, *10*(1), 97.

Bazarhanova, A., & Smolander, K. (2020, January 1). The Review of Non-Technical Assumptions in Digital Identity Architectures. *Proceedings of the ... Annual Hawaii International Conference on System Sciences/Proceedings of the Annual Hawaii International Conference on System Sciences*.

Campbell-Verduyn, M., & Hütten, M. (2021). The Formal, Financial and Fraught Route to Global Digital Identity Governance. *Frontiers in Blockchain*, *4*.

Filep, S., Kondja, A., Wong, C. C., Weber, K., Moyle, B., & Skavronskaya, L. (2023). The role of technology in users' wellbeing: Conceptualizing digital wellbeing in hospitality and future research directions. *Journal of Hospitality Marketing & Management*, *33*(5), 583.

Garcia, R. D., Ramachandran, G., Dunnett, K., Jurdak, R., Ranieri, C. M., Krishnamachari, B., & Ueyama, J. (2024). A Survey of Blockchain-Based Privacy Applications: An Analysis of Consent Management and Self-Sovereign Identity Approaches. *arXiv (Cornell University)*.

Ghadge, N. (2024). USE OF BLOCKCHAIN TECHNOLOGY TO STRENGTHEN IDENTITY AND ACCESS MANAGEMENT (IAM). *SSRN Electronic Journal*.

Hao, J., & Dai, H. (2016). Social media content and sentiment analysis on consumer security breaches. *Journal of Financial Crime*, *23*(4), 855.

Hussain, M. I., Bhuiyan, M. Z. A., Sumon, S. A., Akter, S., Hossain, M. I., & Akther, A. (2024). Enhancing Data Integrity and Traceability in Industry Cyber Physical Systems (ICPS) through Blockchain Technology: A Comprehensive Approach. *Advances in Artificial Intelligence and Machine Learning*, *4*(4), 2883.

Islam, Md. T., Nasir, M. K., Hasan, M. M., Faruque, M. G. G., Hossain, Md. S., & Azad, M. M. (2021). Blockchain-Based Decentralized Digital Self-Sovereign Identity Wallet for Secure Transaction. *Advances in Science Technology and Engineering Systems*

Journal, *6*(2), 977.

Kassi, Y., Sakmaf, M. S., & Suryana, A. (2024). Navigating Influencer Liability on Social Media: Balancing Profits and Legal Risks. *Sinergi International Journal of Law*, *2*(3), 231.

Krul, E., Paik, H.-Y., Ruj, S., & Kanhere, S. S. (2024). SoK: Trusting Self-Sovereign Identity. *Proceedings on Privacy Enhancing Technologies, 2024*(3), 297.

Lesavre, L. (2020). *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*.

Lesavre, L., Varin, P., Mell, P., Davidson, M. L., & Shook, J. M. (2020). *A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems*.

Lohar, S. N., Babar, S. D., & Mahalle, P. N. (2025). A Self-Sovereign Identity Framework for Context-Aware De-Centralized Identifier Creation and Credential Verification. *Engineered Science*.

López, L. J. R., Chavarro, D. A. P., & Huertas, Y. A. H. (2025). Digital citizenship: Challenges and uncertainty in applying blockchain. *Frontiers in Blockchain*, *8*.

Nair, A. J., Manohar, S., & B., S. R. A. (2025). Self sovereign identity in e-governance: blockchain solutions for fintech compliance and citizen-centric financial services. *Humanities and Social Sciences Communications*, *12*(1).

Odelu, V. (2019). IMBUA: Identity Management on Blockchain for Biometrics-Based User Authentication. In *Advances in intelligent systems and computing* (p. 1). Springer Nature.

Prajapati, V. (2025). *Blockchain-Based Decentralized Identity Systems: A Survey of Security, Privacy, and Interoperability*. 1011.

Radanliev, P. (2024). Digital security by design. *Security Journal*, *37*(4), 1640.

Rupasri, M. (2025). Blockchain-Based Secure Identity for IoT Networks. *International Journal for Research in Applied Science and Engineering Technology*, *13*(7), 1961.

Schumm, D., Müller, K. O. E., & Stiller, B. (2025). Are We There Yet? A Study of Decentralized Identity Applications. *arXiv (Cornell University)*.

Shirvani, G., & Ghasemshirazi, S. (2024). Towards Sustainable IoT: Challenges, Solutions, and Future Directions for Device Longevity. *arXiv (Cornell University)*.

Supriya, B. Y., Shubha, B., Prajwal, M., Vikas, C. M., Jaydeva, B. J., Gowda, R. R., Sushmitha, K., & Ghulanoor, A. R. (2024). Advancement and Innovation in Blockchain and Cryptography: A Comparative Analysis of Traditional Systems and Emerging Solutions. *International Journal for Research in Applied Science and Engineering Technology*, *12*(11), 2119.

Vaigandla, K. K. (2025). Quantum-Secure IoT Networks for the 6G Era: Post-Quantum Cryptography, Blockchain Integration, and Trust Architectures - A Comprehensive Review [Review of *Quantum-Secure IoT Networks for the 6G Era: Post-Quantum Cryptography, Blockchain Integration, and Trust Architectures - A Comprehensive Review*]. *Journal of Sensors, IoT & Health Sciences (JSIHS).*, *3*(3), 44. Oxford University Press.

Vasuki, M. (2023). The Impact of Blockchain on Digital Identity Management. *International Journal for Research in Applied Science and Engineering Technology*, *11*(7), 290.

Vaziry, A., Barman, K., & Herbke, P. (2024). SoK: Bridging Trust into the Blockchain. A Systematic Review on On-Chain Identity [Review of *SoK: Bridging Trust into the Blockchain. A Systematic Review on On-Chain Identity*]. *arXiv (Cornell University)*. Cornell University.

Yusuf, P. O., Mai-Auduga, A., Yusuf, S. O., Joshua, E. O., & Yusuf, C. E. (2025). A decentralized privacy-preserving and scalable blockchain-based identity management system. *International Journal of Science and Research Archive*, *14*(2), 511.