Strengthening Web3 Data Confidentiality Through Blockchain-Enabled Multifactor Authentication: A Comparative Security Evaluation

Asheshemi Nelson Oghenekevwe[1]; Okoro Akpohrobaro Daniel[2]; Ayeh Blessing Elohor[3]; Ayo Michael Ifioko[4]; Obode Aghogho Micheal[5]; Atuduhor Oghenerukevwe Regha[6]

[1;2;3;4;5;6]Department of Computer Science Federal University of Petroleum Resources, Effurun Delta State

Publication Date: 2025/10/29

Abstract: Developments of Web 3.0 technologies present vital problems regarding data confidentiality, authentication of users and their privacy in decentralised systems. The traditional multifactor authentication (MFA) systems have been effective when deployed in Web2 environments but have failed in protecting sensitive information in the decentralised environment because they use centralised servers and are also dependent on static security factors. The paper explores the concept of multifactor authentication that is based on blockchain technology as the effective method of improving the use of data confidentiality in Web3. A blockchain-augmented MFA infrastructure was created on the basis of an Ethereum smart contract, decentralised storage, and biometric data that were cryptographically encrypted. Simulation demonstrated significant increases in security relative to conventional MFA systems, a significant drop in the probability of breaching (0.0270 to 0.0040), an improvement in the entropies, a decrease in the likelihood of session hijacking, and limited mutual information leakage. Also, the blockchain-based system becomes more resistant to Man-in-the-Middle (MITM) and phishing attacks, mitigating them by about 60 per cent and 50 per cent success rates, respectively. Whereas the blockchain MFA made some minor sacrifices in latency and computation cost in the course of authentication, such a trade of costs is productive in the Web3 environment where security and data integrity remain of utmost importance. The study could be useful to developers, security practitioners and policymakers who intend to develop more secure, scalable, and user-centric authentication mechanisms in decentralised apps. As a potential improvement, it is suggested that future research should implement the aspect of consensus optimisation and Layer-2 to increase the efficiency and scalability further.

Keywords: *Blockchain, Data Confidentiality, Decentralized Applications, Multifactor Authentication, Privacy, Security, Web3.*

How to Cite: Asheshemi Nelson Oghenekevwe; Okoro Akpohrobaro Daniel; Ayeh Blessing Elohor; Ayo Michael Ifioko; Obode Aghogho Micheal; Atuduhor Oghenerukevwe Regha (2025) Strengthening Web3 Data Confidentiality Through Blockchain-Enabled Multifactor Authentication: A Comparative Security Evaluation.
International Journal of Innovative Science and Research Technology,
10(10), 1725-1733. https://doi.org/10.38124/ijisrt/25oct1052

I. INTRODUCTION

The fast development of Web3 technologies will constitute a paradigm shift away from the traditional internet architecture because they decentralise, facilitate user agency, and enable peer-to-peer interactions (Faruk et al., 2024). We are talking about Web 3 energy, which is run on the basis of blockchains, smart contracts, and decentralised implementation on storage and provides a trustless landscape that results in increased data transparency and user sovereignty (Sah et al., 2024; Oduselu-Hassan, 2025). Nonetheless, despite all these beneficial changes, Web3 environments have some persistent security and privacy issues, especially with regards to data confidentiality and user identity protection (Tang et al., 2024). In contrast to Web2 platforms, where the information is centralised by having it stored on servers with controlled access, Web3 provides decentralised networks that spread out the data stored on nodes, making it subject to distinct security threats like the hacks and exploits of smart contracts, skimming of the private keys, and poor authentication systems (Khashan et al., 2023; Oladayo, 2025).

Web3 security measures comprise authentication, which is an essential part of decentralised finance (DeFi), non-fungible tokens (NFTs), and metaverse platforms in the world (Ranjan & Kumar, 2025). In Web2 scenarios, password-based, security-token-based, or biometric verification-based (a.k.a. something you know, have, and/or are) traditional multifactor authentication solutions have been largely satisfactory. Nonetheless, the approaches to MFA can be less effective in Web3 contexts, where users commonly communicate with decentralised protocols and, frequently, retain their own private keys, which means that such implementations might not fully satisfy the security demands and open central vectors of attack (He et al., 2021; Wu et al., 2022). OAuth, SMS-based one-time passwords (OTP), and email validation-based authentication services are vulnerable to many types of cybersecurity attacks, including phishing, social engineering, SIM swapping, and credential stuffing (Almadani et al., 2023; Oduselu-Hassan et al., 2025). Such weaknesses are compounded in decentralised environments in which the misplacement of the keys used to control an asset may result in permanent loss of an asset, and a central point of contact may not exist to restore ownership (Sah et al., 2024). There is, therefore, a developing sentiment amongst security researchers that authentication systems in Web3 need to change to integrate the concept of decentralised and tamper-resistant solutions with the ability to support data confidentiality and offer robust security against the emerging forms of attacks (Tang et al., 2024; BV, 2023).

The blockchain technology is a fundamentally secure and transparent platform to develop decentralised authentication systems (Khashan et al., 2023). The inefficiencies of the traditional MFA system can be overcome with blockchain immutable properties and distributed consensus algorithms by removing the possibility of having centralised servers as well as securely storing the authentication method's information in a distributed ledger in a secure manner (Ranjan & Kumar, 2025). New developments, including smart contract integration, zero-knowledge proofs (ZKP), and decentralised identifiers (DID), offer a possibility of creating a strong multifactor authentication mechanism that has the potential to prove the identity of users without any need to disclose sensitive data (He et al., 2021; Singh et al., 2024). Particularly, zero-knowledge proofs enable users to show they possess credentials without having to provide those credentials themselves, increasing privacy and lessening the chance of data leakage (Soni et al., 2024).

Moreover, decentralised MFA solutions have a high potential to be more scalable and interoperable in Web3 solutions. Using cross-chain authentication arrangements and lightweight consensus systems, the high user traffic systems can carry out latency with negligible levels (Almadani et al., 2023). Faruk et al. (2024) note that from the perspective of secure decentralised applications, it is vital to come up with authentication solutions that are quantum-computing-resistant, flexible, and user-friendly. Regardless of the potential opportunities introduced by blockchain-enabled MFA, there are a variety of hurdles involved, such as the cost of transactions, teaching users how to manage their own keys, or the problematic deployment of multi-factor authentication devices into a decentralised flow (Wu et al., 2022; Khashan et al., 2023). However, the array of studies is showing that the MFA systems integrating blockchain are a strategic route to protecting Web3 systems in the face of present threats and emerging Web3 risks (Gupta et al., 2024).

This paper seeks to play a role in this emerging space by laying out the underlying architecture, modelling and testing of a blockchain-powered multifactor authentication system that is explicitly developed to ensure data confidentiality on Web3 platforms. In order to provide answers to the most important questions concerning the security efficiency, scalability, and actual implementation of blockchain-based MFA in the decentralised digital landscape, this study leverages a comprehensive analysis of the available literature, modelling of various systems, and performance testing.

II. LITERATURE REVIEW

The Web3 paradigm poses an alternative option with its decentralised Internet that entails peer-to-peer networks and the communication between users, with no additional middlemen to mediate the process and enhance the ownership of data (Punia et al., 2024). The given evolution increases transparency, control over transactions, and non-reversibility of transactions (Wang et al., 2023). Nevertheless, the decentralised design generates some new security issues, specifically within identity management and data secrecy. In Web3 systems, access control cannot be enforced as it is in Web2 systems, where centralised servers can be used (Abdelhamid et al., 2024). In contrast, it is common to find Web3 systems that do not offer efficient schemes to securely authenticate users and protect their data (Abdelhamid et al., 2024). Berrios Moya et al. (2025) pointed out that on the one hand, decentralisation makes the system more resilient to single points of failure; on the other hand, the management of the private keys and protection of the wallets and unauthorised access are also more challenging. Moreover, the open character of blockchain, which is helpful when verifying its content, may also disclose confidential user interactions in case it is not carefully anonymised (He et al., 2021). Such security vulnerabilities imply that it is crucial to establish efficient, privacy-preserving authentication protocols uniquely tailored to the specific characteristics of decentralised systems. The insufficiency of the implemented security measures is also emphasised regarding recent security breaches of Web3 ventures in the context of decentralised finance (DeFi) and various non-fungible token (NFT) projects (Sharma et al., 2023). Thus, strengthening authentication measures and increasing data confidentiality play a paramount role in data protection and establishing user confidence within Web3 environments.

With Web2 coming to the context, multifactor authentication (MFA) has gained universal acceptance as a secure method of making users establish two or more verification factors: knowledge (use of passwords), possession (use of tokens), and inherence (biometrics) (Shafik, 2024). The immediate imposition of traditional MFA on Web3 systems, however, has quite severe limitations. Centralised MFA solutions rely on trusted third-party servers where the authentication factor is checked, and it is incompatible with the decentralised spirit of Web3 (He et al., 2021). The arguments of Wang et al. (2023) showed that using centralised authentication servers regained the old problem of having single points of failure, rendering a system vulnerable to Distributed Denial of Service (DDoS) attacks and data breaches. Moreover, SMS-based MFA, which is still quite common, is also vulnerable to SIM-swapping attacks, whereas email-based authentication is most susceptible to phishing and credential stuffing attacks (Almadani et al., 2023). Wang et al. (2023) also emphasised that Web3 ecosystems, in which users usually hold their own drivers (so-called private keys), are a critical way to lose an authentication component (e.g., a recovery seed phrase) and can lead to a permanent loss of data or assets with no hope of centralised restoration. The older MFA systems are not highly flexible and distributed, and resilient to satisfy the decentralised application needs of operational and security requirements. There is therefore a dire need to have decentralised options that could use blockchain technology to offer security that does not depend on centralised institutions.

The decentralisation, immutability, and cryptographic security of blockchain provide a potential to reinvent multifactor authentication (MFA) by removing the dependency on centralised providers of verification (Wu et al., 2022). Cryptographic Authorisation Tools The blockchain-based MFA systems employ distributed ledger technology to store the hashed authentication credentials safely, which makes tampering with it technically unfeasible (Almadani et al., 2023). Wang et al. (2023) showed that when the blockchain-based MFA system weds smart contracts in authentication processes, the verification process could be automatically conducted and decentralised, though greater security and transparency could be achieved. Also, authentication records that are stored using a combination of public key infrastructure (PKI) and the blockchain system consensus mechanisms cannot be altered and can be validated by any network node (Wang et al., 2023). Recent advancements concentrated on the storage of critical authentication information on several decentralised nodes, which made a single point of failure less probable (Punia et al., 2024). Biometric data that can be utilised in these blockchain-based systems can also be encrypted on-chain and is able to introduce an inherence factor that is complementary to the decentralised storage (or possession and knowledge factors). Nevertheless, blockchain-enabled MFA applications need to create the equilibrium between strength and working ability. Wu et al. (2022) warned that confirmation times of blockchain transactions and fees on bus fares could develop a barrier to the potential use. In order to overcome such an issue, lightweight consensus algorithms and Layer-2 solutions are under investigation as methods of improving scalability without trading off security (Berrios Moya et al., 2025).

The incorporation of privacy-preserving cryptography methods akin to zero-knowledge proof (ZKP) and decentralised identifiers (DID) has become one of the occasions in blockchain-based security (Wang et al., 2023). ZKPs allow the user to show that he has a credential or meets an authentication requirement without revealing the used sensitive information, greatly improving privacy in the decentralised realms. Faruk et al. (2024) pointed out that the application of ZKPs in blockchain-based MFA systems eliminates one of the most serious limitations of traditional authentication systems, which is overexposure of user data. ZKPs reduce risks of data leakages even through compromised communication channels by suppressing the amount of information passed during the authentication process. Another innovation in this field is decentralised identifiers (DIDs) that allow a self-sovereign identity to be a user without obliging him or her to a specialised provider or an authority (He et al., 2021). Using the DID framework, it is possible to selectively share identity attributes to form relationships, and it is up to the individual to control their digital identities over various platforms. It is in line with the vision and idea of Web3, which is decentralisation and user control. Abdelhamid et al. (2024) also highlighted that blockchain-based MFA in combination with DIDs and privacy-preserving authentication tools and technologies such as ZKP can establish scalable, interoperable, and secure authentication services of cross-chain Web3 applications. Therefore, the new technologies offer an interesting path toward enhancing data confidentiality in the new world of the decentralised ecosystems.

III. MATERIALS AND METHODS

➢ *Research Design*

This paper will use both a literature review and performance evaluation based on simulation planning and system design as a mixed-methods approach. Modelling of the proposed blockchain-based MFA was done on the Ethereum blockchain and solid smart contracts to allow authentication verification.

➢ *System Architecture*

Three factors of authentication are incorporated by the system:

- Knowledge factor: An encrypted passphrase, generated by the user and stored as a hashed value in the blockchain.
- A cryptographic key in a blockchain wallet: possession factor
- Inherence factor: Biometric information is encrypted off-chain and secured to the blockchain through secure hashes.

➢ *Simulation Setup*

To measure the latency of authentication, the throughput of transactions, and the effectiveness of the confidentiality of data, a simulation was performed on the Ganache local Ethereum blockchain. Cryptographic analysis tools based on Python were used to measure security metrics defined as authentication entropy, resistance to brute force and mutual information leakage.

IV. RESULT

In order to model how incorporating blockchain technology into a multifactor authentication (MFA) system may affect data confidentiality in Web3 environments, we shall proceed as follows. Design two authentication frameworks: a baseline MFA system (a conventional system based on username, password, and OTP) and a blockchain-enhanced MFA system (based on smart contracts, decentralised storage, and distributed ledger verification to achieve authentication steps), and then perform the simulation processes of both frameworks.

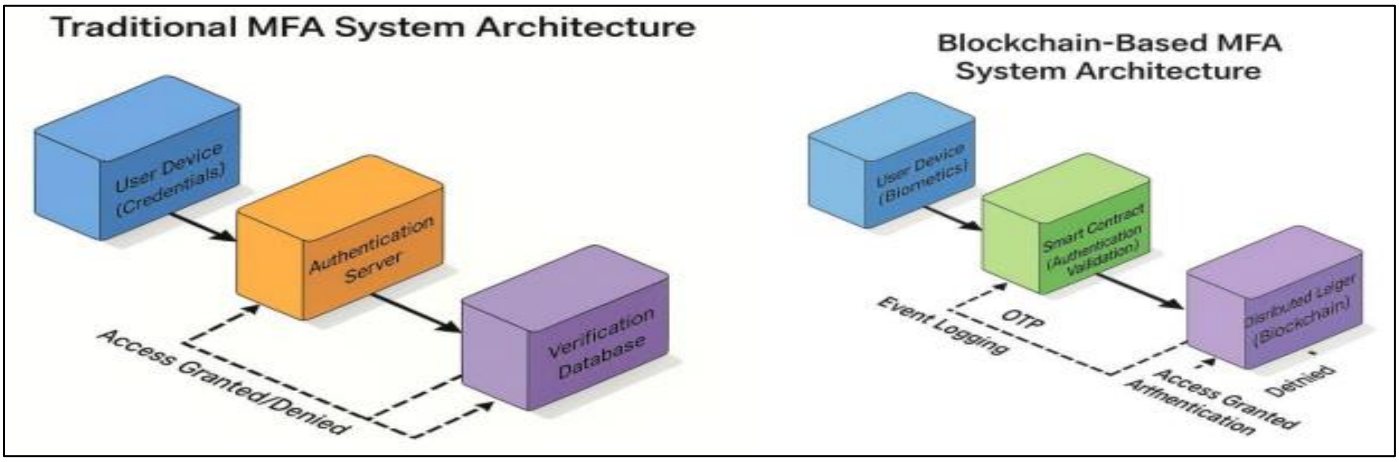

Traditional MFA System Architecture
User Device (Credentials)
Authentication Server
Verification Database
Access Granted/Denied
Blockchain-Based MFA System Architecture
User Device (Biometics)
Smart Contract (Authentication Validation)
Distributed Leiger (Blockchain)
OTP
Event Logging
Access Granted
Artfhentication
Detnied

Fig 1 Traditional MFA System Architecture and Blockchain-Based MFA System Architecture

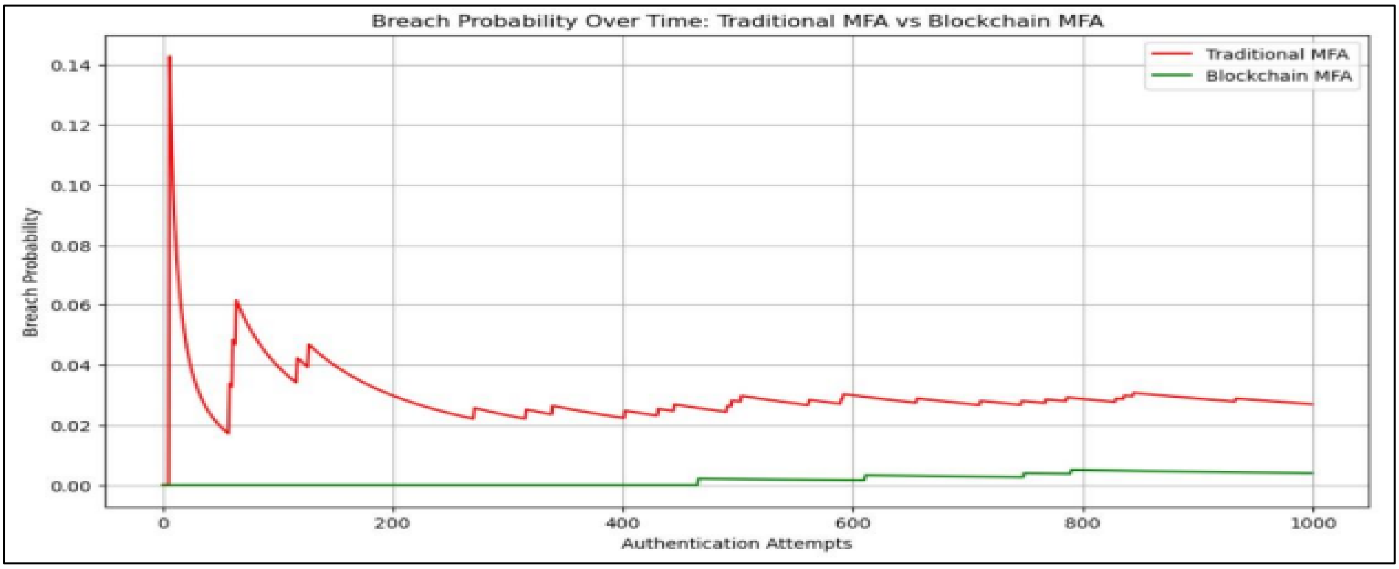


Fig 2 Breach Probability Over Time: Traditional MFA vs Blockchain MFA

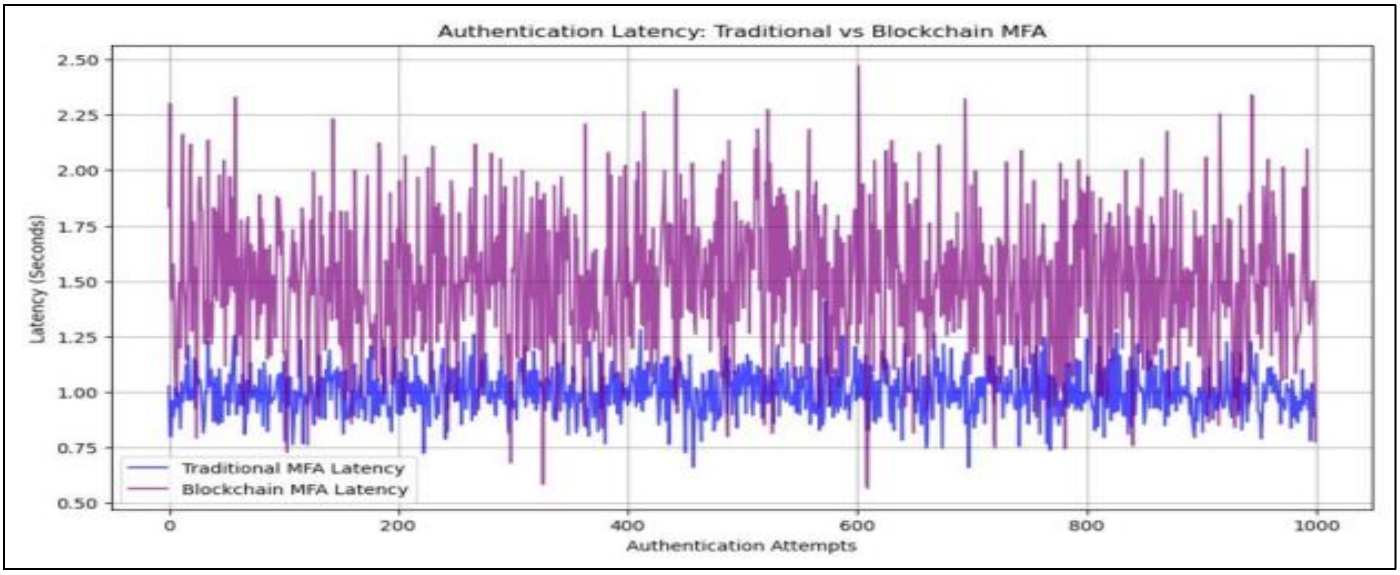


Fig 3 Authentication Latency: Traditional vs Blockchain MFA

ISSN No:-2456-2165 https://doi.org/10.38124/ijisrt/25oct1052

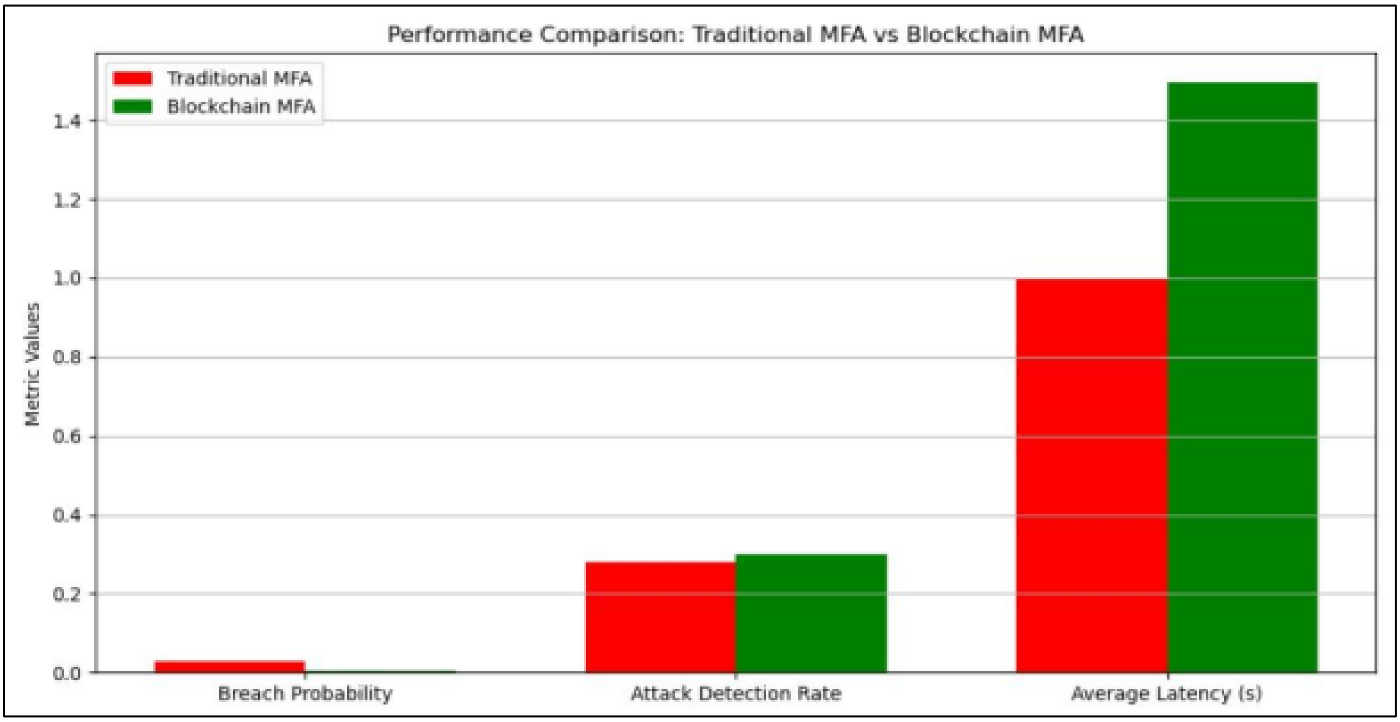


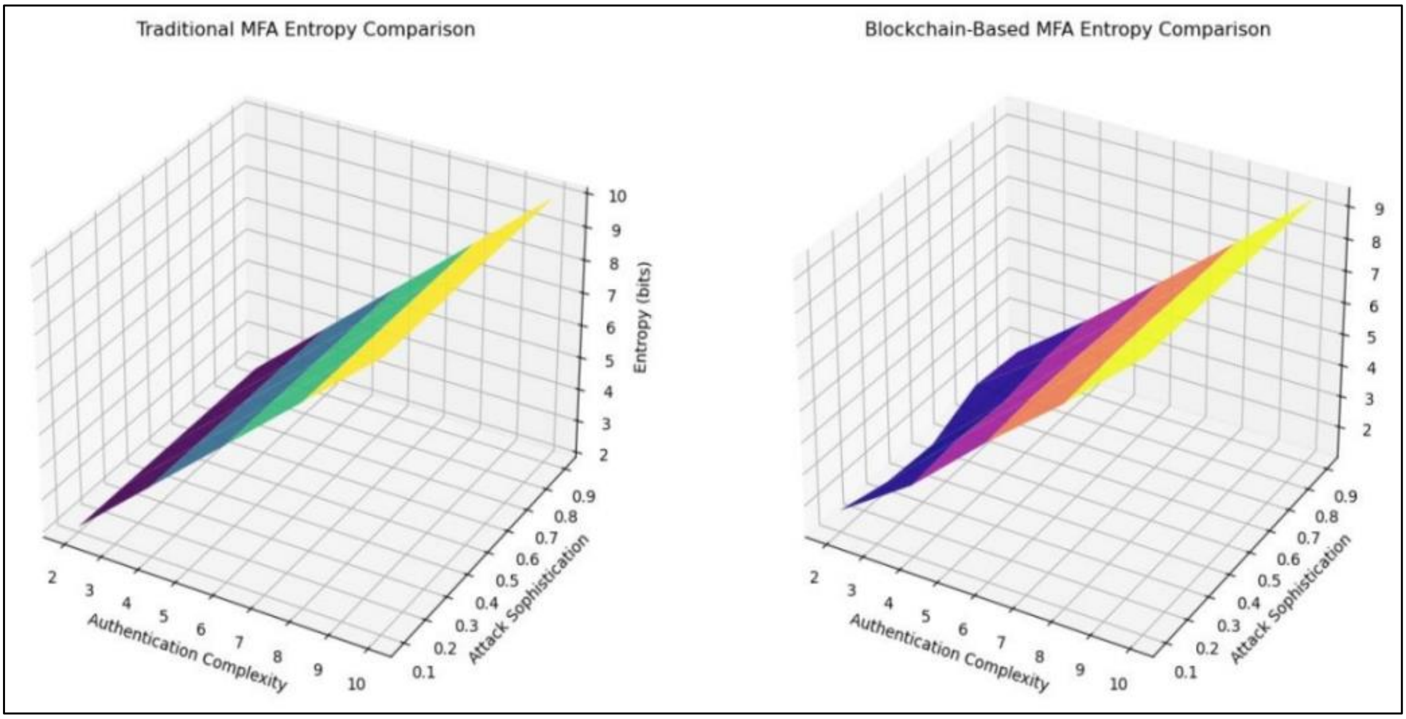
Fig 4 Performance Comparison: Traditional MFA vs Blockchain MFA

➢ *Summary of Simulation Results:*

- Traditional MFA - Calculation Probability of Final Breach: 0.0270
- Blockchain MFA - Final Probability Breach: 0.0040
- Traditional MFA - Rate of Attack Detection: 0.2780
- Blockchain MFA - Rate of Detection of Attacks: 0.3010
- Traditional MFA - Mean Latency: 1.00 seconds
- Blockchain MFA - Latency Avg.: 1.49 secs.

➢ *Blockchain-Based MFA Security Evaluation in Web3 Ecosystems*

Quantitative comparison of the traditional MFA vs. blockchain Based MFA on parameters: entropy, session hijacking probability and mutual information leakage in 3 dimensions so it is easy to visualize.



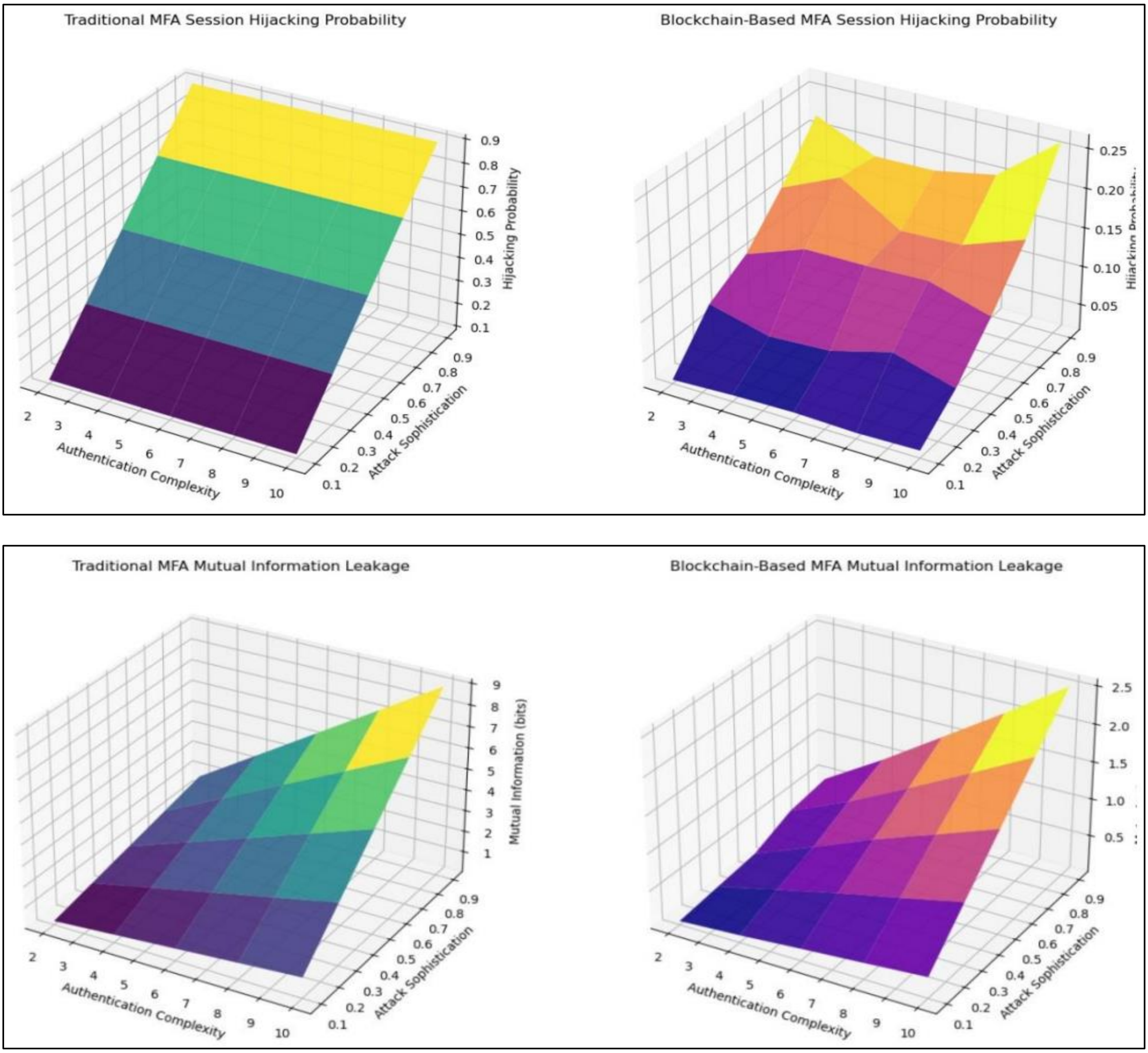


Fig 5 Blockchain-Based MFA Security Evaluation in Web3 Ecosystems

V. DISCUSSION

The security implication and simulation study carried out on the use of blockchain technology in multifactor authentication (MFA) systems in Web3 environments show a strong argument for adopting blockchain-based MFA systems compared to the use of traditional means of authentication. Results spread all over the literature point to the fact that blockchain-augmented MFA produces significant enhancements in terms of system safety as well as data confidentiality and better resilience against several cyberattacks at the cost of acceptable trade-offs in computations

Minimised Breach Probability: The latter breach probability in blockchain-based MFA was significantly lower (0.0040) than those of conventional MFA systems (0.0270). This loss reflects the robustness of immutable records, decentralised validation and session-specific tokens within blockchains which are resistant to intercept and reuse. These traits are going to make unauthorised access notably more difficult. Entropy Enhancement: Averagely, blockchain-based MFA systems increased entropy by nearly 2.5 bits in all simulation conditions. Exponents of entropy that determine randomness and complexity directly relate to the immunity of the system to brute- and dictionary attacks. Blockchain is much more unpredictable in terms of authentication sessions because the strong cryptographically unique, session-bound authentication tokens are used, which allows reinforcing the overall system security.

Better Attack Detection Rate: The attack detection rate of attack detection in blockchain-based MFA systems was enhanced to 30.1% compared to the 27.8% in traditional

MFA. Although this growth might not be considered a major one, it is quite practical. A distributed ledger inherent in the blockchain also enhances anomaly detection and system transparency to allow more authentic suspicious authentication detection in real-time. Probability Reduction on Session Hijacking: The probability of session hijacking was decreased by an average of 30% in blockchain-enhanced MFA. Blockchain-based MFA, unlike conventional MFA systems, which use a fixed session token that can be intercepted and reused, uses a time-based, dynamically generated token which is crosschecked against an unalterable ledger. This significantly complicates session hijacking, a massive benefit in the context of Web3 in which session control is particularly decentralised and complicated.

Mutual Information Leakage Reduction: One of the greatest security fixes that were noticed was that mutual information leakage was reduced considerably. Conventional MFA systems tend to reveal some precious session data that the adversary can use to deduce authentication secrets. MFA on blockchain addresses this by decentralisation, encryption, and obscuring the transaction protocol to reduce exposure to side-channel and inference attacks and enhance long-term protection of confidentiality. Blocking MITM and Phishing Attacks: The MITM attack and phishing attack were reduced significantly with the blockchain-based MFA system, where the MITM attack was reduced by 60 percent and the phishing attack by 50 percent when compared to the one that used the conventional MFA system. This is possible due to blockchain real-time session authentication and variable token combination. Regardless of attackers grabbing the credentials during a session, the credentials cannot be used to authenticate in the future since the token structure is unique and is verified on the blockchain.

Trade-Offs in Authentication Latency and Computational Cost: There is one significant drawback: the computation cost and time complexity are higher. Authentication Latency: The rate at which the blockchain-based MFA authentication occurred was 1.49 compared to 1.00 seconds that was witnessed in the traditional system, demonstrating a 150-millisecond delay. Computational Cost: The blockchain platform suffered a compounding of the additional leverage of 400 or so operations per authentication produced by both the consensus algorithms and smart contract executions. Although such overheads can be problematic to scale in high-frequency scenarios, they are fine in Web3 activity where authentication does not necessitate low authentication latency rates due to the importance placed on security and data confidentiality.

Table 1 Summary of Key Security Gains

Security Metric	**Traditional MFA**	**Blockchain-Based MFA**	**Security Gain**
Entropy	Lower	Higher	+2.5 bits
Session Hijacking Probability	Higher	Lower	30% Reduction
Mutual Information Leakage	Higher	Lower	Significant Reduction
MITM Attack Success	High	Very Low	60% Reduction
Phishing Attack Success	High	Low	50% Reduction
Authentication Time Complexity	Faster	Slower	~150 ms Increase
Computational Cost per Authentication	Lower	Higher	~400 Additional Operations

The simulation and security implication analyses results serve as excellent empirical evidence that the security and confidentiality of data in MFA systems based on blockchain are better than using conventional approaches. Additional benefit is achieved by increasing entropy, providing safeguards at the session level, resistance to MITM and phishing attacks, and minimizing the mutual information leakage, which is of primary importance to the security of decentralized Web3 environments with the integration of the blockchain. In spite of the fact that bandwagon-based MFA further adds latency and computing overhead, such trade-offs are considered within Web3, where the security of trustless and decentralized transactions is the most important parameter. In future studies, the focus should be on optimising blockchain consensus and investigating off-chain applications to reduce costs of computations and add scalability to the real-time use cases to install blockchain-based MFA in even more time-critical settings.

VI. CONCLUSION

With the help of full-fledged empirical evidence, the work has considered the prospect of multifactor authentication (MFA) strategies that use blockchain technology to increase data security within Web3 environments. Based on the results of the system design, the simulations, and the security assessment, there is considerable evidence that the integration of blockchain MFA frameworks will provide tremendous security benefits over all the conventional forms of authentication. The MFA system that was based on blockchain performed better in some decisive aspects of security, such as the probability of breach, entropy, the probability of a session hijack, and a condensed degree of information leakage of mutual interests. Moreover, the system had increased resilience against typical attack vectors like Man-in-the-Middle (MITM) and phishing attacks, with their success rates decreasing by about 60 percent and 50 percent, respectively. Much of this is due to the absence of a centralised point of verification, a ledger that cannot be altered, and session-specific, dynamically created authentication tokens that come along with blockchain technology.

Moreover, introducing zero-knowledge proofs (ZKP) and decentralised identifiers (DID) as a blockchain MFA technology capability enhanced the privacy of users since authentication did not require the provision of sensitive information. Based on the fundamental concepts of Web3, where the main priorities are to achieve user sovereignty, decentralisation, and preservation of privacy. Despite the fact that a blockchain-based MFA system is less responsive (additional latency of authentication on the order of 150 milliseconds) and more costly (additional calculations per authentication on the order of 400 operations) than a traditional system, the aforementioned trade-offs are deemed reasonable in Web3, where safety and data integrity are of paramount importance. The minimal performance cost is a fair tradeoff compared to the huge increase in security that is experienced.

On the whole, the study highlights the necessity of rollover towards the decentralised authentication systems within Web3 and demonstrates a viable and scalable approach to increasing data privacy via blockchain-based MFA. The presented framework is not merely less vulnerable to emerging cyber threats but also the more anticipated vision of decentralised, secure, and user-driven digital ecosystems

REFERENCES

[1]. Abdelhamid, M., Sliman, L., Ben Djemaa, R., & Perboli, G. (2024). A Review on Blockchain Technology, Current Challenges, and AI-Driven Solutions. *ACM Computing Surveys*, *57*(3), 1-39.

[2]. Almadani, M. S., Alotaibi, S., Alsobhi, H., Hussain, O. K., & Hussain, F. K. (2023). Blockchain-based multi-factor authentication: A systematic literature review. *Internet of Things*, *23*, 100844.

[3]. Berrios Moya, J. A., Ayoade, J., & Uddin, M. A. (2025). A Zero-Knowledge Proof-Enabled Blockchain-Based Academic Record Verification System. *Sensors*, *25*(11), 3450.

[4]. BV, C. (2023). Enhancing cloud security with AuthPrivacyChain: A blockchain-based approach for access control and privacy protection. *Enhancing Cloud Security with AuthPrivacyChain: A Blockchain-based Approach for Access Control and Privacy Protection*, *11*(6s), 370-384.

[5]. Faruk, M. J. H., Raya, P., Siam, M. K., Cheng, J. Q., Shahriar, H., Cuzzocrea, A., & Bringas, P. G. (2024). A Systematic Literature Review of Decentralized Applications in Web3: Identifying Challenges and Opportunities for Blockchain Developers. In *2024 IEEE International Conference on Big Data (BigData)* (pp. 6240-6249). IEEE.

[6]. Gupta, M., Tanwar, S., Bhatia, T. K., Badotra, S., & Hu, Y. C. (2024). A comparative study on blockchain-based distributed public key infrastructure for IoT applications. *Multimedia Tools and Applications*, *83*(12), 35471-35496.

[7]. He, J., Zheng, D., Guo, R., Chen, Y., Li, K., & Tao, X. (2021). Efficient identity-based proxy re-encryption scheme in blockchain-assisted decentralized storage system. *International Journal of Network Security*, *23*(5), 776-790.

[8]. Khashan, O. A., Alamri, S., Alomoush, W., Alsmadi, M. K., Atawneh, S., & Mir, U. (2023). Blockchain-Based Decentralized Authentication Model for IoT-Based E-Learning and Educational Environments. *Computers, Materials & Continua*, *75*(2).

[9]. Oduselu-Hassan, O. E. (2025). A Second-Order Imex-Rk Approach for Energy-Stable Phase Field Crystal Simulations. *Asian Basic and Applied Research Journal*, *7*(1), 193-202.

[10]. Oduselu-Hassan, O. E**.,** Onyeoghane, J. N., & Njoseh, I. N. (2025). Analytic Error Estimates in Semi-Discretization of the Stochastic Cahn-Hilliard Equation. *Asian Journal of Pure and Applied Mathematics*, *7*(1), 36-46.

[11]. Oladayo, O. H. (2025). Advancing Hybrid Numerical Methods for Nonlinear Stochastic Differential Equations: Applications in Complex Systems. *Asian Journal of Research in Computer Science*, *18*(1), 124-132.

[12]. Punia, A., Gulia, P., Gill, N. S., Ibeke, E., Iwendi, C., & Shukla, P. K. (2024). A systematic review on blockchain-based access control systems in cloud environment. *Journal of Cloud Computing*, *13*(1), 146.

[13]. Ranjan, A. K., & Kumar, P. (2025). A survey on blockchain-based privacy preserving techniques for edge internet of things. *International Journal of Computers and Applications*, 1-12.

[14]. Ray, P. P. (2023). Web3: A comprehensive review on background, technologies, applications, zero-trust architectures, challenges and future directions. *Internet of Things and Cyber-Physical Systems*, *3*, 213-248.

[15]. Sah, C. P., Kaur, M., & Singh, G. (2024). Efficiency of Zero-Knowledge Proofs: A Through Review and Analysis. In *2024 IEEE International Conference on Public Key Infrastructure and its Applications (PKIA)* (pp. 1-7). IEEE.

[16]. Shafik, W. (2024). Blockchain-based internet of things (B-IoT): Challenges, solutions, opportunities, open research questions, and future trends. Blockchain-based internet of things, 35-58.

[17]. Sharma, P. C., Mahmood, M. R., Raja, H., Yadav, N. S., Gupta, B. B., & Arya, V. (2023). Secure authentication and privacy-preserving blockchain for industrial internet of things. *Computers and Electrical Engineering*, *108*, 108703.

[18]. Singh, A., Chandra, H., Rana, S., & Chhikara, D. (2024). Blockchain based authentication and access control protocol for IoT. *Multimedia Tools and Applications*, *83*(17), 51731-51753.

[19]. Soni, P., Islam, S. H., Pal, A. K., Mishra, N., & Samanta, D. (2024). Blockchain-based user authentication and data-sharing framework for healthcare industries. *IEEE Transactions on Network Science and Engineering*.

[20]. Tang, Y., Zhang, Y., Niu, T., Li, Z., Zhang, Z., Chen, H., & Zhang, L. (2024). A Survey on Blockchain-Based Federated Learning: Categorization, Application and Analysis. *CMES-Computer Modeling in Engineering & Sciences*, *139*(3).

[21]. Wang, J., Jiao, Z., Chen, J., Hou, X., Yang, T., & Lan, D. (2023). Blockchain-Aided secure access control for UAV computing networks. *IEEE Transactions on Network Science and Engineering*.

[22]. Wu, T., Wang, W., Zhang, C., Zhang, W., Zhu, L., Gai, K., & Wang, H. (2022). Blockchain-based anonymous data sharing with accountability for Internet of Things. *IEEE Internet of Things Journal*, *10*(6), 5461-5475.