American Journal of Engineering Research (AJER)
e-ISSN: 2320-0847 p-ISSN : 2320-0936
Volume-14, Issue-3, pp-10-13
www.ajer.org
Research Paper Open Access

Blockchain-Based Authentication – A Security and Performance Evaluation

Nikoloz Katsitadze
Georgian Technical University, Tbilisi, Georgia
Corresponding Author: Nikoloz Katsitadze

ABSTRACT : *Security remains a critical challenge in Web3 systems, where decentralized architectures introduce new vulnerabilities alongside enhanced privacy and control. Authentication, as a fundamental component of security, is crucial across various sectors, ensuring trust and reliability in digital interactions. In this study, the performance of blockchain-based authentication mechanisms has been analyzed, and their efficiency has been quantitatively evaluated. Based on the findings, recommendations are proposed regarding when and in what form transitioning authentication systems to blockchain is most effective, considering security, scalability, and computational efficiency. This research provides a structured approach to optimizing authentication in decentralized environments while addressing the persistent challenges of Web3 security.*
KEYWORDS *Blockchain authentication, Performance analysis, Decentralized identity, Efficiency in blockchain, Blockchain security.*

Date of Submission: 06-03-2025 Date of acceptance: 18-03-2025

I. INTRODUCTION

Open-source code can indeed be a vulnerability in the development of decentralized applications (Web3) since it allows third parties to analyze the code and identify potential weaknesses. While transparency is one of the key principles of Web3, providing greater trust and accountability, it also exposes applications to increased security risks. Malicious actors can examine the source code, search for vulnerabilities, and exploit them before they are discovered and fixed by developers.

Despite these risks, open-source development has significant advantages. Publicly available code enables the community to review, improve, and strengthen security measures, often leading to faster detection and resolution of security flaws. However, this openness also requires developers to adopt proactive security strategies, such as continuous auditing, penetration testing, and incentivized bug bounty programs, to mitigate potential threats.

One of the critical security challenges in Web3 is authentication—the process of verifying user identities. Unlike traditional systems that rely on centralized databases and passwords, decentralized authentication mechanisms use cryptographic keys, zero-knowledge proofs, and blockchain-based identity solutions. While these methods enhance security and privacy, they also introduce new challenges, particularly regarding key management and user experience. Losing a private key, for example, can result in irreversible access loss, making usability considerations just as important as security measures.

Ultimately, while open-source code contributes to the advancement of Web3 applications, it also necessitates a careful balance between transparency and security. Developers must implement robust security practices to ensure that the benefits of open-source development outweigh its risks. Strong authentication mechanisms, regular security assessments, and innovative cryptographic solutions are essential to safeguarding decentralized systems against evolving threats.

II. THE IMPORTANCE OF RESEARCH IN WEB3 AUTHENTICATION SECURITY

This research is significant because security in Web3 systems remains one of the most critical and current challenges in the development of decentralized applications. While Web3 technologies and blockchain offer numerous benefits and security advantages, issues such as authentication play a crucial role in protecting personal data and ensuring the integrity of the system. Therefore, the purpose of this research is to analyze these

challenges and develop recommendations to improve Web3 system security, ensuring that its potential is fully realized.

This study not only addresses the security risks associated with Web3 but also evaluates the effectiveness of authentication mechanisms and their impact on system coordination, responsiveness, and overall security resilience. A scientific approach to studying these issues enables a deeper understanding of how blockchain and other decentralized technologies can be utilized to solve these challenges, offering stronger security guarantees for Web3 systems.

Another reason this research is important is that the security of Web3 systems directly impacts not only technological development but also critical sectors such as finance, logistics, education, and more. When security and authentication function robustly and reliably, it creates a better environment for industrial innovation, ultimately benefiting the broader society.

Moreover, in this research, the efficiency of blockchain-based authentication systems has been evaluated, providing a more fundamental view of the ways in which decentralized systems can evolve and how these systems should be transformed to enhance security while maintaining optimal performance. Our recommendations offer insights into making the right decisions in specific cases, allowing Web3 infrastructure to develop secure and resilient systems on a global scale.

III. SECURE SESSION MANAGEMENT WITH BLOCKCHAIN-BASED AUTHENTICATION

Recently, a method regarding authentication has emerged online, where the blockchain is responsible for user validation. Its schema is shown in Fig. 1.

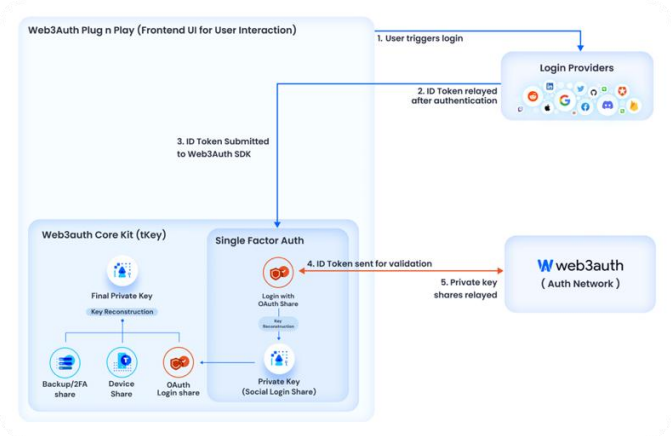

Fig.1. Decentralized Authentication Flow

This diagram (Fig. 1) illustrates a decentralized authentication schema utilizing various service providers such as Google, Facebook, or Apple. It highlights the authentication flow between the user, the service provider, and decentralized components. The process is visualized step by step, showing how user credentials are securely verified in a decentralized manner without relying on a central authority. The diagram showcases the interaction between different decentralized components, ensuring data privacy and enhancing security through distributed systems.

It becomes possible for the user's information and session to be stored not in a centralized system, but directly on the blockchain, ensuring future verification of the individual with any service. Each time, the client receives a confirmation from the service to validate them, as was done in previous scenarios. However, now everything is decentralized in this regard, and token theft will no longer lead to a leak of user data.

In Fig 1, it is shown how a WEB2 application interacts with the blockchain and requests the opening of a session for the individual. To do so, it provides the necessary information. If the verification process for the individual requires more than one step (this point may be optional for different business processes), the blockchain returns a so-called "Challenge" to the application, and this process becomes part of the second step. Once the user confirms the second step using the private key they generated, the record is made.

IV. PERFORMANCE COMPARISON OF SYSTEM DELAY

Such service providers will impact the system's latency, as a new component is introduced into the ecosystem. Let's calculate the changes we should expect in terms of performance. To calculate the system's speed reduction, several factors must be considered that directly affect the process:

- WEB2 application request speed (RT_web2): This is the time required to send a request from the application and return the data without the decentralized service on the blockchain.
- Blockchain request speed (RT_blockchain): Transactions on the blockchain are slower because they require data confirmation and consensus within the network.
- Additional steps in multi-step authorization (T_multistep): The inclusion of "Challenge" and "Response" phases in the system increases the operation length."
  Speed reduction calculation can be done as follows:

$$\text{Total Delay} = \frac{RT_{\text{web2}} + RT_{\text{blockchain}} + T_{\text{multistep}}}{RT_{\text{web2}}}$$

Fig.2. Latency Increase Ratio Formula

Using Fig 2, a simple example calculation: Let's assume that:

- RT_web2 = 0.1 seconds (for the WEB2 system).
- A blockchain transaction (RT_blockchain) takes an average of 1 second.
- Multi-step authentication (T_multistep) takes 0.5 seconds.

Now, let's substitute these values into the formula and analyze the results:

$$\text{Total Delay} = \frac{(0.1 + 1 + 0.5)}{0.1} = \frac{1.6}{0.1} = 16$$

Fig.3. Latency Increase Ratio Formula with Result

The system's speed will decrease by a factor of 16 compared to the WEB2 system.

When using the fastest blockchains, the system will be significantly faster, but it will still depend on the following factors:

- Blockchain execution time (RT_blockchain): The fastest blockchains, such as Solana, Avalanche, or Polygon, can perform transactions within 50 milliseconds to 500 milliseconds (0.05–0.5 seconds).
- WEB2 request time (RT_web2): The WEB2 request time will remain the same, let's say 0.1 seconds.
- Multi-step authentication (T_multistep): Additional authentication steps may range from 0.2 to 0.5 seconds (depending on the blockchain's speed).

Let's change the variables and calculate the coefficient using the same formula for the fastest blockchain:

$$\text{Total Delay} = \frac{0.1 + 0.05 + 0.3}{0.1} = \frac{0.45}{0.1} = 4.5$$

Fig.4. Latency Calculation Formula for the Fastest Blockchain

Using the fastest blockchain, the system's speed will decrease by a factor of 4.5 compared to WEB2, which represents a significant improvement over the 16-fold decrease.

Of course, this data will change as it depends on the specific blockchain, network load, and the authentication method. For a more accurate model, the speed reduction coefficient can be calculated using this formula.

V. CONCLUSION

The decentralized approach that utilizes blockchain for user verification and session management offers a high level of data security, control over personal information, and robust protection of user uniqueness. By leveraging blockchain's transparency and immutability, users can maintain greater control over their data, and the system ensures that no sensitive information is at risk of being compromised. These advantages make decentralized authentication and session management especially beneficial in environments where data privacy and security are paramount.

However, this approach comes with its own set of challenges, particularly in terms of system performance. The process of verifying users and managing sessions through a blockchain network can result in significant delays, especially when combined with multi-step authorization processes. Blockchain transactions are inherently slower due to the need for network consensus and validation, which introduces latency into the system. This can be particularly noticeable when using slower blockchains or when the network is under heavy load.

Given these factors, while the decentralized approach is highly secure, it may not be suitable for all applications, particularly those where system speed and real-time responses are critical. For sensitive services or processes, where security is a critical factor, this approach can be highly effective, but it should be employed strategically and sparingly. Specifically, it is recommended that decentralized authentication and session management be limited to critical stages in the system's operation, where security outweighs the need for speed.

In cases where both speed and security are essential, it is crucial to find a balance. Hybrid models that combine the strengths of centralized and decentralized approaches can be considered, or optimizations may be applied to reduce the impact of blockchain transactions on overall system performance. By carefully selecting when and where to implement blockchain-based solutions, the system can achieve a secure, fast, and efficient user experience, without compromising the performance of the entire application.

Recommendation: In systems where security is paramount but speed is also a factor, use decentralized authentication and session management selectively. Consider hybrid approaches or optimization techniques to balance security and speed, ensuring that the system remains responsive while maintaining a high level of protection for user data.

REFERENCES

[1]. Gök, R. (2025). Spillovers between cryptocurrency, DeFi, carbon, and energy markets: A frequency quantile-on-quantile perspective. The Quarterly Review of Economics and Finance, 100, March 2025.
[2]. Katsitadze, N.: DeFi and NFT Adoption in Blockchain Financial Analysis Using Transaction Data. American Journal of Engineering Research (AJER), vol. 14, no. 3, pp. 6–9. AJER Publications.
[3]. Morchiladze, A.: Pricing Strategy Comparison in Blockchain-Based Distributed Energy Systems. Journal of Business, vol. 9, no. 2, pp. 29, 2020.
[4]. Vairam, T., Srijeimathy, M.: Investigation of Blockchain for Security and Transparency in Intelligent Transportation Systems. Procedia Computer Science, vol. 252, pp. 851–861, 2025.