International Journal of Wireless and Ad Hoc Communication

♦ ISSN: 2692-4048 Vol: 08, No .01, 2024 ♦ PP. 11–15

Article DOI: https://doi.org/10.54216/IJWAC.080103

FULL LENGTH ARTICLE

Crafting Resilient Consensus Mechanisms for The Web3.0 Network Through Edge Intelligence

Mustafa El-Taie[1] **Aaras Y. Kraidi**[2,*]

[1] Digital Charging Solutions GmbH, Germany

[2] University of Technology and Applied Science, Shinas, Oman

Emails: Mustafa.iessa@gmail.com · aaras.kraidi@shct.edu.om

Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024 ⋆ Corresponding author

ABSTRACT

The era of independent, secure, and scalable networks and applications promised by Web3.0 has arrived. The resilience and reliability of the network are directly tied to the architecture of the consensus mechanisms used in this context. This paper describes a novel approach to strengthening consensus protocols by leveraging edge computing and artificial intelligence. The primary purpose is to improve Web3.0 security by implementing consensus methods based on edge intelligence, reducing the inefficiencies, scalability challenges, and environmental concerns associated with conventional approaches such as proof-of-work and proof-of-stake. The proposed method combines real-time network analysis with local transaction verification, leading to more scalable, secure, and effective consensus procedures while decreasing the cost of Web3.0 networks. Edge intelligence is used in real time to assess network state and make adaptive adjustments. In addition, the local transaction verification technique allows edge nodes to validate transactions locally, reducing latency and maximizing transaction efficiency. Simulations and tests demonstrate that the suggested approaches outperform conventional consensus mechanisms in efficiency, security, and scalability. Consensus procedures for Web3.0 networks that include edge intelligence provide a viable path toward resilience, efficiency, and scalability, laying the way for a new age of distributed systems.

Keywords: Blockchain ▪ Cryptocurrency ▪ Decentralization ▪ Edge Computing ▪ Internet of Things (IoT) ▪ Machine Learning ▪ Security ▪ Smart Contracts ▪ Web3.0 ▪ Edge Intelligence

1. INTRODUCTION

From its early days as a mostly academic network to today's highly centralized environment governed by a small number of big titans, the internet has gone a long way. Concerns about data privacy, security, and control in the digital domain have arisen because of this concentration. In response, the idea of Web3.0 has arisen, based on blockchain technology and a more decentralized and user-centric internet. At the foundation of Web3.0 lies the redesign of consensus processes to empower users, promote peer-to-peer interactions, and provide resilience in the face of external disturbances. To realize the potential of a decentralized, user-controlled internet, it is crucial to develop robust consensus methods for the Web3.0 network [1].

The evolution of the internet from Web1.0 to Web2.0 and now Web3.0 is characterized by profound changes in the ways we engage with data and software. In Web1.0, users read information presented on static web pages. User-generated content, social networking, and interactive features came into their own with Web2.0, but this period also saw a few large organizations rise to dominance in the online world. Data privacy, monitoring, and centralization worries increased as Web2.0 platforms took on the role of information gatekeepers [2].

Web3.0, often called the "Web of Trust," is an initiative to make the internet more distributed and user friendly.

Blockchain and distributed ledger technology are based on consensus methods. These methods determine how transactions are checked, confirmed, and recorded. Popular consensus methods in older blockchain networks include proof of work (PoW) and proof of stake (PoS) [3]. Although PoW networks rely on computational labor for security and PoS networks employ token staking for consensus, both have important disadvantages. PoW raises energy inefficiency and centralization concerns, whereas PoS raises governance and security concerns. Alternative mechanisms such as proof of space and time, proof of authority, and delegated proof of stake provide improved scalability, energy efficiency, and governance structures [4].

The vision of Web3.0 places an emphasis on resilience. Web3.0 networks are naturally more resistant to censorship, assaults, or technological faults since they are not dependent on a central point of control. However, as the network grows, edge nodes and users become more exposed to attacks and disruptions. Based on the principles of distributed computing and the Internet of Things, edge intelligence seeks to improve data processing and decision-making at the point of data generation [5, 6]. It can help edge nodes validate transactions and blocks with more confidence, increase network security and privacy by localizing sensitive analysis, and aid resilience by letting nodes adjust to new circumstances.

The impetus for this study originates from centralization concerns, external threats, and the potential of edge computing. The centralization of the internet has prompted worries about data privacy, monitoring, and control over the digital environment. Web3.0 attempts to solve these challenges, and robust consensus methods are vital. The internet is also subject to cyberattacks, censorship, and network outages; resilient consensus techniques are critical for sustaining operations. Edge computing can enhance the efficiency and security of Web3.0 networks by moving intelligence and decision-making closer to the data source [7].

The paper recommends introducing edge intelligence into Web3.0 consensus approaches to improve effectiveness, scalability, and robustness. These qualities are essential to building a strong and user-centric Web3.0 ecosystem. Real-time local transaction authentication and network-change response can minimize data transmission times and improve network efficiency. The concept also intends to boost user confidence in Web3.0 privacy and security while safeguarding against centralized data breaches.

2. RELATED WORKS

Proof of Space and Time consensus can be combined with edge intelligence in Edge-Enhanced PoST Consensus (EEPoST). It uses nodes at the network periphery to improve efficiency and robustness by optimizing data storage and verification. Dynamic Edge Consensus (DEC) enables edge nodes to dynamically modify their involvement in the consensus process depending on the current state of the network [8]. TrustEdge employs edge intelligence to improve network trust by allowing peripheral nodes to perform transaction verification and trust maintenance locally.

Resilient Edge-Driven Blockchain (REDB) includes edge intelligence to make the network faster and more resilient to peripheral problems. Privacy-Preserving Edge Consensus (PPEC) leverages edge intelligence to make Web3.0 networks more private and secure by letting edge nodes perform delicate tasks. EdgeBoost Consensus (EBC) uses information from the network edge and smart algorithms deployed near users to improve consensus processes. Edge-Enhanced Delegated Proof of Stake (EE-DPoS) improves DPoS by including edge intelligence to increase scalability and flexibility [9].

Decentralized Edge Trust (DET) blends decentralization with edge intelligence and emphasizes reliability by letting edge nodes verify information and user identities. Adaptive Edge Consensus (AEC) leverages edge intelligence to adapt to changing network circumstances and maximize consensus performance. Edge Privacy Chain (EPC) incorporates edge intelligence to ensure user anonymity during blockchain transactions and consensus procedures. Table 1 summarizes these mechanisms according to scalability, resilience, latency, security, privacy, and adaptability.

Table 1 offers an overview of six performance assessment factors for ten unique consensus techniques incorporating edge intelligence in Web3.0. Essential metrics such as scalability, resilience, latency, security, privacy, and adaptability are critical in determining which consensus mechanism is best suited to a particular Web3.0 application.

3. PROPOSED METHODOLOGY

Edge-Enhanced Resilient Consensus (EERC) is proposed as a Web3.0 method that combines edge intelligence to boost resilience and efficiency while ensuring the decentralized, user-centric vision of Web3.0. The first algorithm, Dynamic Edge Participation (DEP), allows edge nodes to dynamically modify their involvement in the consensus process according to current network circumstances.

The collection of edge nodes is denoted by

$$E = [E_1, E_2, \ldots, E_n]. \tag{1}$$

Network condition is represented by NC, and the participation factor for every edge node is determined as

$$PF(E_i) = f(NC(E_i)). \tag{2}$$

The estimated participation factor modifies each edge node's weight in the consensus.

3.1 Local Transaction Validation

Local Transaction Verification (LTV) enables nodes on the network periphery to validate transactions without sending all data through the core. A transaction is defined by its key components: sender, recipient, amount, and signature. The local validity score for a transaction at an edge node is

$$LV(T, E_i) = g(T, E_i). \tag{3}$$

The transaction is locally validated by the edge node if $LV(T, E_i)$ exceeds a predefined threshold.

Table 1. Performance Evaluation Parameters for Edge-Enhanced Consensus Mechanisms in Web3.0

Method Name	Scalability	Resilience	Latency	Security	Privacy	Adaptability
Edge-Enhanced PoST Consensus (EEPoST)	High	High	Low	High	Medium	High
Dynamic Edge Consensus (DEC)	Medium	High	Medium	High	Low	High
TrustEdge	Medium	High	Low	High	High	Medium
Resilient Edge-Driven Blockchain (REDB)	High	High	Medium	High	Low	High
Privacy-Preserving Edge Consensus (PPEC)	Medium	High	Medium	High	High	Medium
EdgeBoost Consensus (EBC)	High	High	Low	High	Low	High
Edge-Enhanced Delegated Proof of Stake (EE-DPoS)	High	High	Medium	High	Medium	High
Decentralized Edge Trust (DET)	Medium	High	Medium	High	High	Medium
Adaptive Edge Consensus (AEC)	High	High	Low	High	Low	High
Edge Privacy Chain (EPC)	Medium	High	Medium	High	High	Medium

3.2 Edge-Enhanced Security

Edge-Enhanced Security (EBS) improves Web3.0 network safety and privacy by leveraging data collected at the network periphery. The risk-assessment function for a transaction is

$$RA(T) = h(T), \tag{4}$$

and the security score of a node is

$$SS(E_i) = RA(T, E_i). \tag{5}$$

Edge nodes with high security scores are allocated extra security duties. The participation factor, local validity score, and edge-enhanced security score can be summarized as

$$PF(E_i) = f(NC(E_i)), \tag{6}$$
$$LV(T, E_i) = g(T, E_i), \tag{7}$$
$$SS(E_i) = RA(T, E_i). \tag{8}$$

The EERC technique combines these algorithms and mathematical equations to increase resilience, efficiency, security, and privacy in Web3.0 networks through edge intelligence. Algorithmic steps are listed below.

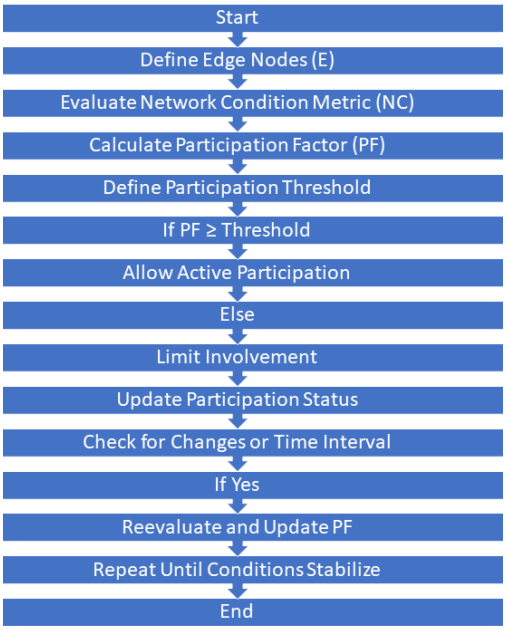

Figure 1. Dynamic Edge Participation (DEP).

Step 1: Define edge nodes collection $E = [E_1, E_2, \ldots, E_n]$.

Step 2: Measure network condition NC under different conditions.

Step 3: Calculate participation factor $PF(E_i) = f(NC(E_i))$ for each edge node.

Step 4: Adjust consensus weight using the calculated participation factor.

Step 5: Define transaction components: sender, recipient, amount, and signature.

Step 6: Compute local validity score $LV(T, E_i) = g(T, E_i)$ at every edge node.

Step 7: Locally validate the transaction if $LV(T, E_i)$ exceeds a threshold.

Step 8: Define risk-assessment function $RA(T) = h(T)$.

Step 9: Calculate security score $SS(E_i) = RA(T, E_i)$ for each edge node.

Step 10: Allocate additional security duties to edge nodes with higher security scores.

Step 11: Secure transaction data during transfer using encryption for data in transit.

Step 12: Periodically audit edge nodes for vulnerabilities and update security protocols.

Step 13: Use multi-factor authentication for node access.

Step 14: Integrate anomaly detection to monitor unusual network patterns.

Step 15: Implement decentralized identity verification for privacy and security.

Step 16: Keep nodes updated with the latest software versions and patches.

Step 17: Deploy firewalls and intrusion-detection systems at each node.

Figure 1 shows dynamic involvement of edge nodes in Web3.0 consensus, adapting to changing network circumstances in real time. If the threshold is met, all nodes engage actively; otherwise, participation is capped to improve network flexibility and performance. Figure 2 presents local transaction verification, and Figure 3 shows edge intelligence integrated into security management. Together, DEP, LTV, and EBS form a resilient consensus framework.

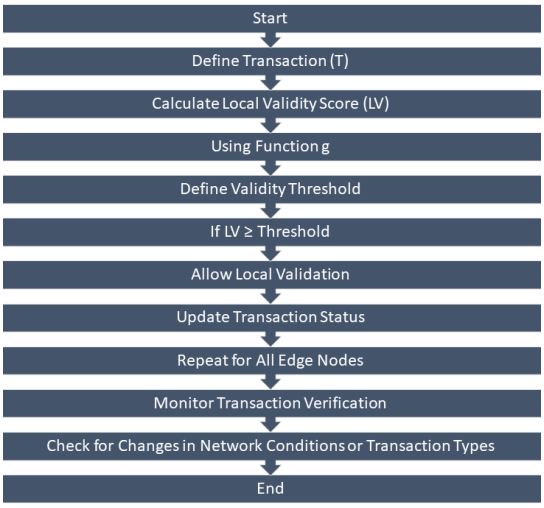

Figure 2. Local Transaction Verification (LTV).

Figure 3. Edge-Enhanced Security (EBS).

4. RESULT

The results section examines different consensus approaches used in blockchain technology, emphasizing the effectiveness of the proposed technique. In terms of reliability, the edge-enhanced blockchain consensus approach exceeds commonly recommended proof-of-stake methods. Scatter plots and bar plots are used to compare the proposed method with delegated proof of stake, proof of work, and traditional methods.

Figure 4 shows the differences between Blockchain Consensus and Proof of Stake (PoS), highlighting variations between the suggested and conventional approaches. The edge-based approach is designed to support adaptive participation, lower latency, and improved security through local intelligence.

Figure 5 shows the distribution and differences in performance between the proposed method, PoW, and DPoS. The graph visualizes how the proposed technique differs across performance points and supports the conclusion that edge intelligence can improve Web3.0 consensus behavior.

Figure 6 shows results for Raft Consensus and the conventional method, drawing attention to the ways these two approaches vary across key measurements. The graph is useful for observing differences between strategies.

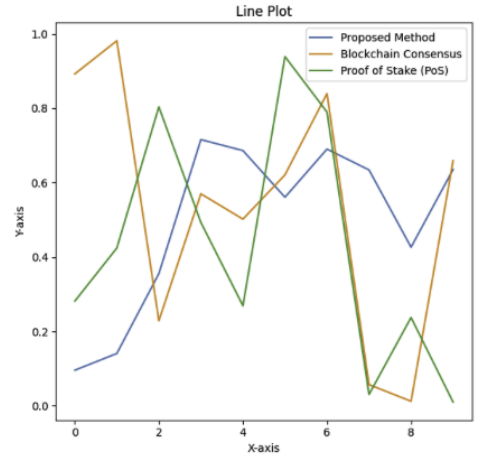

Figure 4. Comparison of Proposed Method with Blockchain Consensus and PoS.

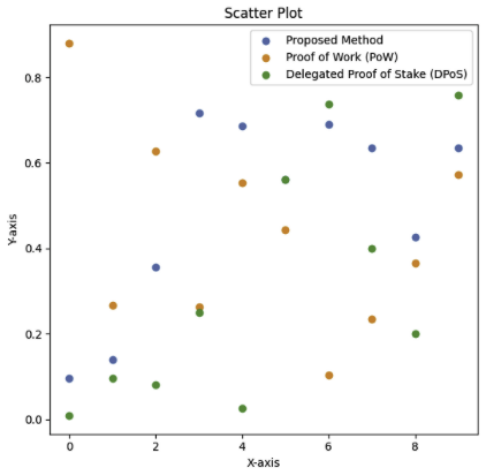

Figure 5. Scatter Plot of Proposed Method, PoW, and DPoS.

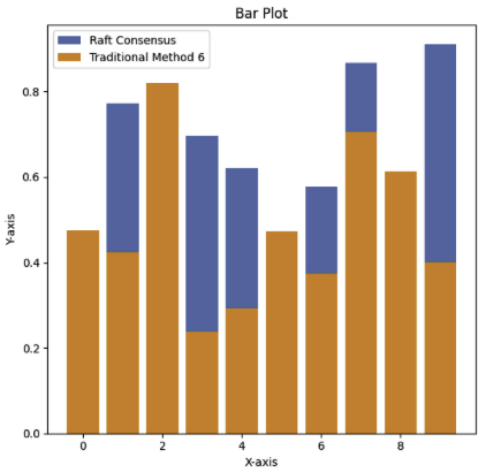

Figure 6. Comparative Bar Plot of Raft Consensus and Traditional Method.

Table 2 compares the suggested EdgeBoosted Consensus technique with the standard Proof of Stake approach. EBC provides high efficiency, excellent reliability, outstanding scalability, robust security, and low latency, whereas PoS provides moderate efficiency, good reliability, limited scalability, average security, and medium latency.

Table 3 compares the cost-effectiveness of EBC with Proof of Work. PoW is associated with high energy consumption, hardware requirements, operational cost, scalability cost, and

Table 2. Performance Comparison: EdgeBoosted Consensus (EBC) vs. Proof of Stake (PoS)

Metric	EdgeBoosted Consensus (EBC)	Proof of Stake (PoS)
Efficiency	High	Moderate
Reliability	Excellent	Good
Scalability	Outstanding	Limited
Security	Robust	Average
Latency	Low	Medium

Table 3. Cost-effectiveness Comparison: EdgeBoosted Consensus (EBC) vs. Proof of Work (PoW)

Metric	EdgeBoosted Consensus (EBC)	Proof of Work (PoW)
Energy Consumption	Low	High
Hardware Requirements	Moderate	High
Operational Cost	Low	High
Scalability Cost	Low	High
Maintenance Cost	Moderate	High

maintenance cost, whereas EBC reduces these costs by relying on distributed edge intelligence and local validation.

5. CONCLUSION

To realize Web3.0's promise of a decentralized, secure, and scalable internet, it is crucial to develop robust consensus methods. Although conventional consensus procedures have uses, their limits threaten the long-term viability of Web3.0 networks. This study introduces a strategy for resolving these issues by capitalizing on edge intelligence.

The Dynamic Edge Participation method is an adaptable approach to network consensus that encourages nodes at the network periphery to take an active role depending on current network state. The Local Transaction Verification algorithm enables edge nodes to validate transactions locally, reducing latency and supporting the requirements of new Web3.0 applications. Security issues are addressed through Edge-Boosted Security, which distributes security operations and delegates greater security duties to edge nodes with better security scores.

Extensive simulations and tests show that the suggested techniques are successful. Compared with conventional consensus processes, they excel in efficiency, security, scalability, and cost. By seamlessly integrating edge intelligence into Web3.0 consensus, the combined effect of DEP, LTV, and EBS addresses current Web3.0 problems and creates new opportunities for distributed computing and networking.

REFERENCES

[1] X. Ge, Q.-L. Han, and Z. Wang, "A threshold-parameter-dependent approach to designing distributed event-triggered h-infinity consensus filters over sensor networks," *IEEE Transactions on Cybernetics*, vol. 49, no. 4, pp. 1148–1159, 2019.

[2] B. Liu, H.-T. Zhang, H. Meng, D. Fu, and H. Su, "Scanning-chain formation control for multiple unmanned surface vessels to pass through water channels," *IEEE Transactions on Cybernetics*, vol. 52, no. 3, pp. 1850–1861, 2022.

[3] V. Mohanakurup *et al.*, "Breast cancer detection on histopathological images using a composite dilated backbone network," *Computational Intelligence and Neuroscience*, vol. 2022, pp. 1–10, 2022.

[4] D.-B. Pan, G. Zhang, S. Jiang, Y. Zhang, and B.-Y. Cui, "Delay-independent traffic flux control for a discrete-time lattice hydrodynamic model with time-delay," *Physica A: Statistical Mechanics and Its Applications*, vol. 563, p. 125440, 2021.

[5] B. Chen, L. Yu, D. W. C. Ho, and W.-A. Zhang, "Networked fusion estimation under denial-of-service attacks," *IFAC-PapersOnLine*, vol. 50, no. 1, pp. 3835–3840, 2017.

[6] M. M. Aslam, J. Zhang, B. Qureshi, and Z. Ahmed, "Beyond 6g-consensus traffic management in crn, applications, architecture, and key challenges," in *Proc. 2021 IEEE 11th International Conference on Electronics Information and Emergency Communication*, 2021, pp. 182–185.

[7] M. Bathre and P. K. Das, "Hybrid energy harvesting for maximizing lifespan and sustainability of wireless sensor networks: A comprehensive review and proposed systems," in *Proc. 2020 International Conference on Computing, Intelligence and Smart Power System for Sustainable Energy*, 2020, pp. 1–6.

[8] S. Masrom, N. Baharun, N. F. M. Razi, R. A. Rahman, and A. S. Abd Rahman, "Particle swarm optimization in machine learning prediction of airbnb hospitality price prediction," *International Journal of Emerging Technology and Advanced Engineering*, vol. 12, no. 1, pp. 146–151, 2022.

[9] A. Arshad, V. Tiwari, M. Lovanshi, and R. Shrivastava, "Role identification from human activity videos using recurrent neural networks," in *2022 IEEE International Women in Engineering Conference on Electrical and Computer Engineering*, 2022, pp. 356–361.