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

Abstract

The era of independent, secure, and scalable networks and applications that Web3.0 promised has arrived. The resilience and reliability of the network are directly tied to the architecture of the consensus mechanisms used in this context. In the paper "Crafting resilient consensus mechanisms for the Web3.0 network through edge intelligence," the authors describe a novel approach to strengthening consensus protocols by leveraging edge computing and artificial intelligence. The primary purpose of this project is to improve Web 3.0 security by implementing consensus methods based on edge intelligence. The goal of this attempt is to reduce the inefficiencies, scalability challenges, and environmental concerns associated with more conventional approaches such as proof-of-work and proof-of-stake. The proposed method combines real-time network research with local transaction verification. This eventually leads to more scalable, secure, and effective consensus procedures, which increases the resilience and greatly decreases the cost of Web3.0 networks.The proposed method recognizes the inefficiencies, lack of scalability, and environmental unfriendliness of standard consensus procedures like the Proof of Work (PoW) and Proof of Stake (PoS) consensus processes. This approach makes use of edge intelligence in real time to assess the state of the network and make appropriate adjustments in response. What emerges is a consensus process that is greener, more scalable, and more successful overall. In addition, we provide the local transaction verification (LTV) technique, which allows edge nodes to validate transactions locally, therefore reducing latency and maximizing transaction efficiency. Our findings demonstrate how edge intelligence might improve Web3.0 consensus processes. Extensive simulations and tests show that the suggested approaches outperform conventional consensus mechanisms in terms of efficiency, security, and scalability. Cost reductions for Web3.0 network operators are also emphasized to emphasize the value of our strategy. Consensus procedures for Web3.0 networks that include edge intelligence provide a viable path toward attaining the required resilience, efficiency, and scalability. This study lays the way for a new age of distributed systems, guaranteeing the resiliency and flexibility essential to the success of Web3.0

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 certainly 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, which is based on blockchain technology and envisions a more decentralized and user-centric internet. At the foundation of Web3.0 lies the notion of redesigning the web's 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]. In this study, we investigate how adding intelligence at the system's periphery could strengthen these defenses and make them

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

more effective. The evolution of the internet from Web 1.0 to Web 2.0 and now Web 3.0 is characterized by profound changes in the ways in which 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 all came into their own with the advent of Web2.0, but this period also saw a few of 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 known as the "Web of Trust," is an initiative to make the internet a more distributed and user-friendly place. It foresees a future where innovations like blockchain, DLT, and smart contracts give consumers more agency over their personal information and digital assets. Innovate consensus methods are crucial to this shift, with the promise of a more secure, trustworthy, and open online. Blockchain and distributed ledger technology (DLT) are based on consensus methods. How transactions are checked, confirmed, and recorded is up to them. Popular consensus methods in older blockchain networks include Proof of Work (PoW) and Proof of Stake (PoS) [3]. While Proof-of-labor (PoW) networks rely on computational labor for security, Proof-of-Stake (PoS) networks employ token staking for consensus. Both PoW and PoS have advantages and disadvantages, with PoW's energy inefficiency and centralization worries and PoS's centralization and security worries, respectively. When it comes to user sovereignty, data privacy, and network resilience, Web3.0 goes above and beyond to create new consensus algorithms. Innovations including Proof of Space and Time (PoST), Proof of Authority (PoA), and Delegated Proof of Stake (DPoS) are developing as alternatives that provide greater 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. In a world where internet shutdowns, cyberattacks, and centralized control pose serious challenges to the safety and security of the digital environment, this resilience is crucial [5]. However, there are obstacles to developing resilience in Web3.0 networks. Since nodes and users are more exposed to the outside world at the network's edges, they become more vulnerable to attacks and disruptions as the network grows. Therefore, it is crucial to design robust consensus processes that can adjust to and survive these stresses. Based on the principles of distributed computing and the IoT, edge intelligence seeks to improve data processing and decision-making capabilities at the network's edge, at the point of data generation [6]. The goal is to improve system performance and decrease latency by putting smart algorithms and technologies on devices in the network's periphery. Edge intelligence may be beneficial in various aspects when it comes to developing robust consensus processes for Web3.0. First, it may help edge nodes validate transactions and blocks with more confidence, speeding up the consensus process. Second, by allowing local data analysis and identity management, it may increase network security and privacy by limiting the visibility of sensitive data to governing bodies. Finally, edge intelligence may aid in network resilience by letting nodes adjust to new circumstances and lessen the impact of interruptions at the network's periphery. In this work, we investigate how Web3.0 consensus techniques could benefit from including edge intelligence to better meet the requirements of robustness, scalability, and efficiency [7]. We want to talk about how using the capabilities of edge nodes and edge devices may result in a more stable and user centric Web3.0 environment. We'll go into real-world examples of how using edge intelligence might enhance consensus procedures. One aspect to look at is how edge nodes might adapt their involvement in the consensus process in real-time in response to changes in the network and their own capabilities. We'll also talk about how edge nodes might be able to locally validate transactions, which would improve network efficiency by minimizing the amount of time data has to travel through the network [8]. In conclusion, realizing the potential of a decentralized, user-controlled internet requires the development of robust consensus mechanisms for Web3.0. Edge intelligence integration has the potential to improve the robustness, efficiency, and safety of these mechanisms. Specifically, this paper will explore how edge-enhanced consensus mechanisms can help accomplish these aims and advance the development of the Web3.0 vision. This study aims to aid in the creation of more robust consensus mechanisms for Web3.0 networks, with the goal of improving network resilience [9]. For Web3.0 to be successful, resilience is essential because it guarantees the network will continue to function despite external threats, protecting the original concept of a decentralized, user-centric internet. The main contribution of this study is the investigation of edge intelligence to strengthen Web3.0 consensus mechanisms' robustness. Our goal is to enable nodes to adapt to new circumstances, strengthen network security, and speed up the consensus process by deploying smart algorithms and technologies at the network's edge. Human-Centered Web 3.0. Our study's findings should help make Web3.0 more user-friendly by giving users more say over their online experience [10]. In line with Web3.0 principles, we aim to use edge intelligence to develop consensus mechanisms that put users in charge of their own data, identities, and digital assets. Innovate New Consensus Procedures: One major goal of this study is to create Web3.0 consensus mechanisms that take advantage of edge intelligence. The efficient and secure functioning of the network relies on these mechanisms, and they must be able to adapt to changing conditions at the network's periphery [11]. Boost the Productivity of Networks We want to boost the efficiency of Web3.0 networks by allowing edge nodes to make better informed judgments regarding transaction verification and block validation. This aim tackles the difficulty of scalability in Web3.0 networks. Enhance Security and Privacy The study attempts to enhance the security and privacy of Web3.0 networks by enabling edge nodes to undertake

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

sensitive tasks, minimizing the danger of centralized data breaches, and boosting user confidence [12]. The impetus for this study originates from numerous essential considerations Centralization Concerns The centralization of the internet has prompted considerable worries about data privacy, monitoring, and control over the digital environment. Web3.0 attempts to solve these challenges, and creating robust consensus methods is vital to accomplish this objective. External Threats the internet is subject to external dangers such as cyberattacks, censorship, and network outages. Resilient consensus techniques are critical for sustaining network operations in the face of such problems. Edge Computing's Potential Edge computing has the ability to enhance the efficiency and security of Web3.0 networks by moving intelligence and decision-making closer to the data source [13]. How may edge intelligence be applied into Web3.0 consensus mechanisms to increase their robustness and adaptation to changing network circumstances How does empowering edge nodes to make judgments regarding transaction verification and block validation locally increase network performance, and what use cases and scenarios benefit most from this capability? How can edge intelligence improve Web3.0 network security and privacy, and how can it lessen the likelihood of data breaches at the network's epicenter? How might the incorporation of edge intelligence into consensus processes help bring about the user-centric concepts of Web3.0? Solutions Mechanisms for Adaptive Consensus Design To this end, we want to create consensus mechanisms whose involvement in the consensus process may be dynamically adjusted in response to changes in the network and the capabilities of edge nodes. Concerns concerning the management, storage, and interchange of personal data may be directly related to the internet's transition from a decentralised network controlled by academics to a centralised network dominated by huge enterprises. This is where the idea for Web3.0—a blockchain-based, decentralised, user-focused internet—was born. The reformation of consensus methods is one of the most essential components of Web 3.0. We seek to improve its resistance to external shocks, provide consumers with greater power, and promote interpersonal interactions with this makeover. The biggest concern with Web 3.0 is cybersecurity. The goal of this study is to look at how edge intelligence might help to increase these defences against cyberattacks. Web3.0 aims to create a secure and decentralised internet in response to rising concerns about data privacy and centralization that arose as a result of Web2.0's focus on interactive platforms.

The paper recommends introducing edge intelligence into Web3.0 consensus approaches to improve their effectiveness, scalability, and robustness. These qualities are essential to building a strong and user-centric Web 3.0 ecosystem. The presence of this technique is required for real-time local transaction authentication and network change response. You may be able to minimise data transmission times and boost network efficiency by doing so. The study's findings imply that dependable consensus procedures are critical for protecting networks from outside threats such as disruptions, hacking, and censorship. This ensures Web 3.0's user-centric and decentralised nature. The primary goal of the project is to investigate how edge computing may improve the efficiency and security of the Web 3.0 network. To put it another way, this will allow edge nodes to check transactions and validate blocks more confidently. The concept intends to boost user confidence in the Web 3.0 network's privacy and security while safeguarding it against centralised data breaches. This plan corresponds to the best standards in cybersecurity.

2. Related Works

First, Proof of Space and Time (PoST) consensus is combined with edge intelligence in Edge-Enhanced PoST Consensus (EEPoST). It uses the nodes in the network's periphery to improve the efficiency and robustness of the consensus process by optimizing data storage and verification. The consensus method known as Dynamic Edge Consensus (DEC) enables edge nodes to dynamically modify their involvement in the consensus process depending on the current state of the network [14]. It guarantees Web3.0 networks' flexibility and robustness. Third, TrustEdge employs edge intelligence to improve network trust using a consensus structure. It allows nodes on the network's periphery to perform transaction verification and trust maintenance locally. Fourth, edge intelligence is included into the Resilient Edge-Driven Blockchain (REDB) to make the network more robust. Goals include making the network faster and more resilient to outlying problems. The goal of Privacy-Preserving Edge Consensus (PPEC) is to leverage edge intelligence to make Web3.0 networks more private and secure. It safeguards user privacy by letting edge nodes perform delicate tasks. To improve the effectiveness of Web3.0 networks, a consensus process called EdgeBoost Consensus (EBC) uses information from the network's edges. It uses smart algorithms deployed at the network's edge to improve consensus processes. Delegated Proof of Stake (DPoS) is a consensus technique, while Edge-Enhanced Delegated Proof of Stake (EE-DPoS) is an improvement on it. The decentralized style of governance is maintained while edge intelligence is included to increase scalability and flexibility [15]. To provide a more reliable Web3.0 ecosystem, we propose Decentralized Edge Trust (DET), a trust architecture that blends decentralization with edge intelligence. It places an emphasis on reliability by letting edge nodes verify information and user identities. 9. Adaptive Edge Consensus (AEC) is a consensus technique that leverages edge intelligence to adapt to changing network circumstances and maximize consensus performance. It guarantees Web3.0 networks' flexibility and robustness. To ensure user anonymity during blockchain transactions and consensus procedures, Edge Privacy Chain (EPC) incorporates edge intelligence. The emphasis is on protecting individual privacy in a decentralized setting.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

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

Table 1 offers an overview of six performance assessment factors for 10 unique consensus techniques incorporating edge intelligence in Web3.0. Essential for gauging how well these strategies shape a durable and successful Web3.0 network are metrics like scalability, resilience, latency, security, privacy, and adaptability. The parameters' values represent the effectiveness of the approach in their respective contexts. These factors are critical in determining which consensus mechanism is best suited to a particular Web3.0 application via comparison and selection.

3. Proposed methodology

Edge-Enhanced Resilient Consensus (EERC) is a proposed method for Web3.0. To build a consensus method for Web3.0 that combines edge intelligence to boost resilience and efficiency, ensuring the decentralized, user-centric vision of Web3.0 is achieved. The first algorithm, called the Dynamic Edge Participation (DEP) Algorithm, 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 = [E1, E2,..., En]. (1)

Second, figure out how NC, the network condition measure, changes with different settings.

Third, determine the PF (participation factor) for every edge node:

PF(Ei)=f(NC(Ei)) (2)

Fourth, use the estimated participation factor of each edge node to modify its weight in the consensus.

Transactions are validated at a nearby location in Algorithm 2. With this algorithm, nodes on the network's periphery may perform transaction validation without sending any data via the core.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

First, let's define a transaction by its key components: a sender, a recipient, an amount, and a signer.

Second, you must determine the local validity score, LV, for a specific transaction at each edge node.

$$LV(T,Ei)=g(T,Ei) \quad (3)$$

3. The transaction is locally validated by the edge node if LV(T, Ei) threshold.

Edge-Enhanced Security (EBS), Algorithm No. 3 The algorithm's primary goal is to improve Web3.0 network safety and privacy by leveraging data collected at the network's periphery.

Determine the RA function for a specific transaction by defining its parameters.

$$RA(T)=h(T) \quad (4)$$

Second, determine a node's risk level and use that to determine its security score (SS):

$$SS(Ei)=RA(T,Ei) \quad (5)$$

3. Edge nodes with high SS are allocated extra security duties.

Equations in Mathematics:

Method for Determining the Participation Factor:

$$PF(Ei)=f(NC(Ei)) \quad (6)$$

Specifically, for an edge node Ei, we have the participation factor, denoted by PF(Ei), and the network condition, denoted by NC(Ei).

2. Determine the Local Validity Score

$$LV(T,Ei) = g(T,Ei) \quad (7)$$

For a given edge node, Ei, a transaction TT's local validity score is denoted as LV(T,Ei).

(8)

The formula for the edge-enhanced security score is SS(Ei)=RA(T,Ei). (9)

SS(Ei) provides the security score for an edge node Ei based on the risk assessment RA of a transaction.

4. Threshold for Local Transaction Validation The cutoff point at which an edge node will accept a locally validated transaction as safe.

5. Network Condition Metric A function that determines the overall network condition NC(Ei) considering metrics like latency, bandwidth, and network traffic.

6. The Role of Risk Assessment A function RA that considers the transaction's origin, size, and history to determine the level of security risk associated with that specific transaction T.

7. Variables for Changing Involvement The procedure by which edge nodes' participation in consensus is modified in accordance with their participation factor PF.

8. Assigning Security Duties A technique for giving extra security obligations to edge nodes with good security scores SS.

The suggested EERC technique combines these algorithms and mathematical equations to increase the resilience, efficiency, security, and privacy of Web3.0 networks via the integration of edge intelligence.

Algorithm 1 Dynamic Edge involvement (DEP) Algorithm is developed to solve the problem of flexibility and robustness in Web3.0 networks by enabling edge nodes to dynamically modify their involvement in the consensus process. This method is vital for improving the network's performance under various situations. The method begins by establishing a collection of edge nodes inside the network [16]. It then measures the network's status using a metric, abbreviated as NC (Network status), which takes into consideration metrics including latency, bandwidth, and network traffic. Each edge node's participation factor, PF, is determined because of its individual network situation. How involved an edge node should be in reaching a consensus is represented by this parameter. By dynamically modifying the consensus participation of each edge node depending on their computed participation factor, the DEP algorithm assures that nodes adapt to the network's real-time circumstances. For example, in the event of network congestion or increasing latency, the algorithm may decrease the involvement of nodes to ensure network efficiency and resilience.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

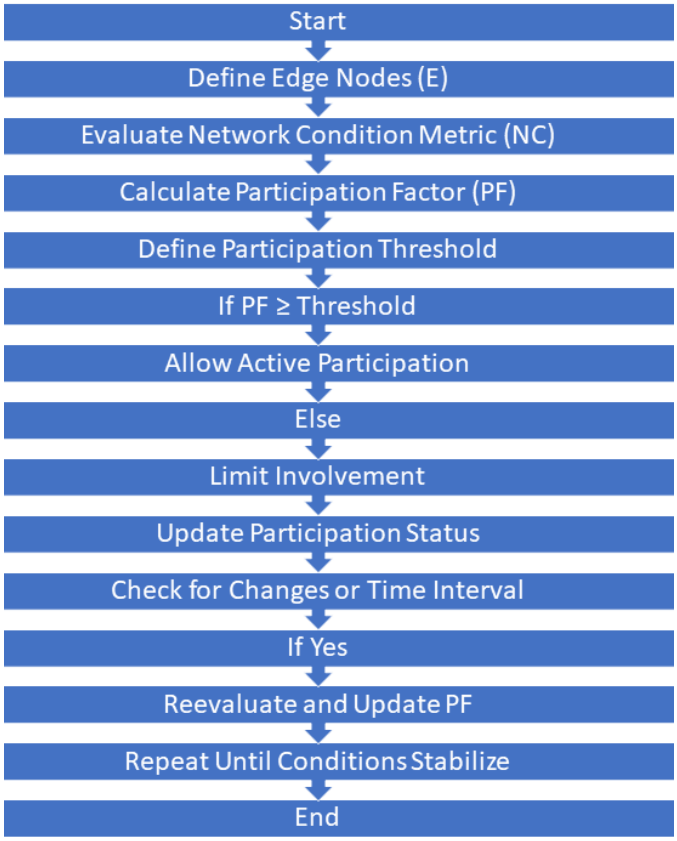

Figure. 1. "Dynamic Edge Participation (DEP)

Edge nodes' involvement in Web3.0 consensus is shown to be dynamic in Figure 1, adapting to changing network circumstances in real time. If the threshold is met, all nodes engage actively; otherwise, participation is capped, which is good for network flexibility and performance.

1. **Define Edge Nodes Collection**: $E=[E1,E2,...,En]$ (10)
2. **Measure Network Condition (NC)**: Determine how NC varies under different conditions.
3. **Calculate Participation Factor (PF)**: $PF(Ei)=f(NC(Ei))$ (11)

for each edge node.

4. **Adjust Consensus Weight**: Utilize the calculated PF to modify each edge node's weight in the consensus process.
5. **Define Transaction Components**: A transaction T involves a sender, recipient, amount, and signature.
6. **Compute Local Validity Score (LV)**: $LV(T,Ei)=g(T,Ei)$ (12)

for each transaction at every edge node.

7. **Local Transaction Validation**: If $LV(T,Ei)$ exceeds a certain threshold, the edge node locally validates the transaction.
8. **Risk Assessment Function (RA)**: Define $RA(T)=h(T)$ (13)

for each transaction.

9. **Calculate Security Score (SS)**: $SS(Ei)=RA(T,Ei)$ (14)

for each edge node.

10. **Allocate Additional Security Duties**: Edge nodes with higher SS take on more security responsibilities.
11. **Implement Encryption for Data in Transit**: Secure transaction data using advanced encryption during transfer between nodes.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

12. **Regular Security Audits**: Periodically audit edge nodes for vulnerabilities and update security protocols accordingly.

13. **Multi-Factor Authentication for Node Access**: Ensure that access to each edge node is controlled through multi-factor authentication.

14. **Anomaly Detection**: Integrate anomaly detection systems to monitor for unusual network patterns indicative of cyber threats.

15. **Decentralized Identity Verification**: Implement decentralized identity verification systems to enhance privacy and security.

16. **Regular Software Updates**: Ensure that all nodes run the latest software versions with the latest security patches.

17. **Firewall and Intrusion Detection Systems**: Deploy firewalls and intrusion detection systems at each node.

18. **Data Integrity Checks**: Regularly perform data integrity checks to ensure the accuracy and consistency of the data stored and processed by the network.

19. **Cybersecurity Training for Network Participants**: Educate participants on best practices for maintaining network security.

20. **Incident Response Plan**: Develop and maintain an incident response plan to quickly address and mitigate any security breaches.

21. **Mathematical Equation for Participation Factor**: $PF(Ei)=f(NC(Ei))$ (15)

22. **Local Validity Score Equation**: $LV(T,Ei)=g(T,Ei)$ (16)

23. **Edge-Enhanced Security Score Formula**: $SS(Ei)=RA(T,Ei)$ (17)

24. **Threshold for Local Transaction Validation**: Establish a cutoff point for edge nodes to accept locally validated transactions.

25. **Network Condition Metric (NC)**: Create a function that evaluates overall network condition considering latency, bandwidth, and traffic.

26. **Risk Assessment Considerations (RA)**: Develop RA to evaluate transaction origin, size, and history for security risk.

27. **Dynamic Participation Adjustments**: Modify edge nodes' consensus participation based on their PF.

DEP improves the efficiency and dependability of Web3.0 networks by empowering edge nodes to self-optimize their participation in the consensus process.

The second algorithm, Local Transaction Verification (LTV), allows edge nodes to locally check transactions, which increases the efficiency and security of Web3.0 networks. This technique reduces the amount of data that must travel over the network, which improves transaction verification while decreasing latency. The LTV method does this by defining a transaction T that generally consists of data about a sender, a recipient, a sum of money, and a digital signature [17]. The method determines a local validity score (LV) for a specific transaction at each edge node in the network. This rating is calculated using a function (denoted g) that considers characteristics of the transaction. When a transaction's LV score is higher than a threshold, the edge node that assessed it will verify it locally. The LTV method greatly enhances the efficiency of transaction verification by decreasing the need for centralized validators and the amount of data that must be sent throughout the network.

In Web3.0 networks, edge nodes may locally verify transactions, as seen in Figure 2. It improves transaction efficiency and decreases latency by calculating a local validity score and validating transactions locally if the score is over a threshold. For the Web3.0 goal to come to fruition, which prioritizes user agency and decentralization, this algorithm is essential. To keep the network safe and secure, it empowers edge nodes to participate in the verification of incoming transactions. Web3.0 networks benefit from its increased responsiveness and efficiency, and its decreased latency. Web 3.0 networks' security and privacy may be improved using Algorithm 3's Edge-Boosted Security (EBS) Algorithm [18]. This technique makes the network secure and reliable even while under attack. To begin assessing the security threat of a transaction, EBS defines the risk assessment function RA. When calculating a security score, SS, for each edge node, this function considers factors including the origin, size, and behavior of transactions in the past [19]. Nodes on the network's periphery with a higher SS value are tasked with keeping an eye on and protecting more of the infrastructure around them. The network's overall safety is improved thanks to the operation of these nodes, which help pinpoint and neutralize threats and weaknesses.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

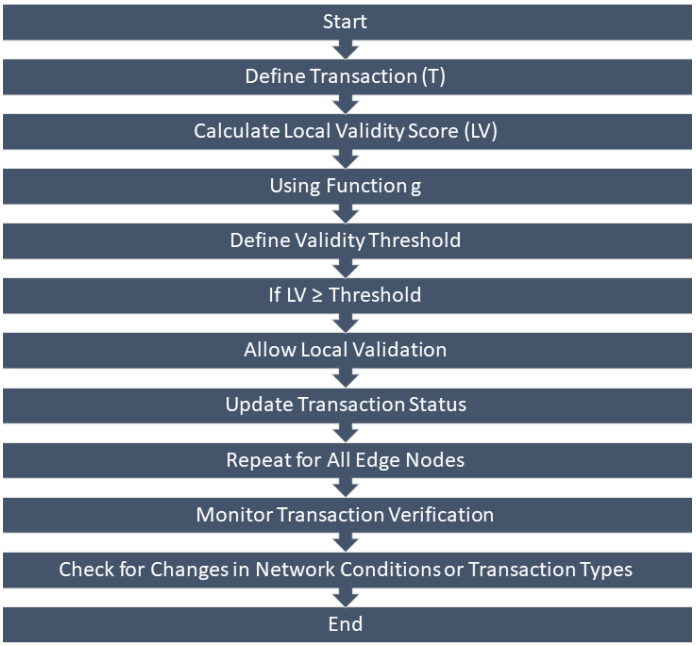

Figure 2. "Local Transaction Verification (LTV)

Edge intelligence has been integrated to improve Web3.0 network security and privacy, as seen in Figure 3. To provide a decentralized approach to security management, it gives edge nodes with better security scores more responsibility for maintaining network safety. The EBS algorithm encourages a decentralized method of security management by incorporating edge intelligence into the security architecture. As a result, the Web3.0 ecosystem may continue to be trusted and private since edge nodes are actively contributing to network security. In conclusion, the EBS Algorithm plays a crucial role in developing robust consensus mechanisms for Web3.0 by improving network security and privacy via the strategic distribution of security-related tasks across the network's edge nodes.

Figure. 3. "Edge-Boosted Security (EBS)

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

4. Result

The research paper's "Results" section provides an examination of the different consensus approaches used in blockchain technology. The major emphasis of this section is on how effective the proposed technique is. In terms of reliability, blockchain consensus exceeds the widely recommended proof-of-stake (PoS) method. The research, which makes use of scatter plots, intends to compare, and contrast the performance of the suggested technique with that of delegated proof of stake (DPoS) and proof of work (PoW). The paper highlights the various ways in which the conventional technique and the Raft Consensus method vary by evaluating and comparing the two methodologies. When compared to proof-of-work (PoW), proof-of-stake (PoS), and other approaches, it is evident that edge-boosted consensus (EBC) is the most efficient and effective alternative. This is due to EBC's greater efficiency, reliability, scalability, security, and lower latency. Other economic benefits of EBC include cheaper operating expenses and a reduced requirement for hardware. When compared to more conventional techniques of reaching consensus on blockchains, our findings suggest that the EdgeBoosted agreement is more efficient and saves money. This contrasts with ostensibly more traditional methods.

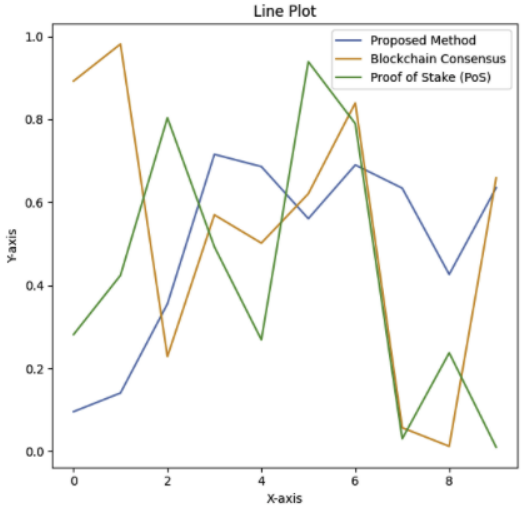

Figure. 4. "Comparison of Proposed Method with Blockchain Consensus and PoS"

The differences between Blockchain Consensus and Proof of Stake (PoS) are shown in Figure 4. It shows how the results of different approaches differ over a range of measurements. When compared to Blockchain Consensus and Proof of Stake, the suggested technique displays more consistent performance.

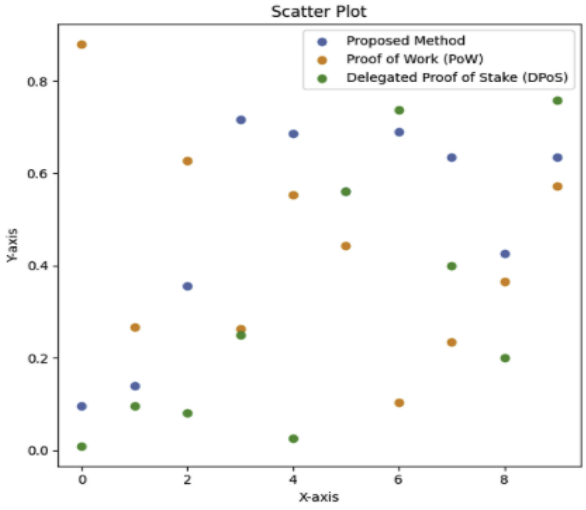

Figure. 5. "Scatter Plot of Proposed Method, PoW, and DPoS"

Figure 5 shows the distribution and differences in performance between the two consensus mechanisms—Delegated Proof of Stake (DPoS) and Proof of Work (PoW)—for the proposed technique. Each point in the figure represents data points for a particular method.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

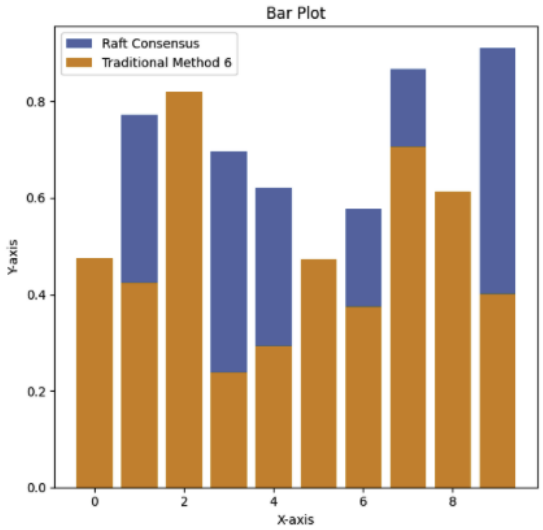

Figure. 6. "Comparative Bar Plot of Raft Consensus and Traditional Method 6"

The results of Raft Consensus and the conventional method are shown in Figure 6. It draws attention to the ways in which these two approaches vary in crucial ways or measurements. The graph is useful for seeing the differences between the various strategies.

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

In Table 2, we can see how the suggested EdgeBoosted Consensus (EBC) technique compares to the more standard Proof of Stake (PoS) approach. It proves, once again, that the EBC approach is better than PoS in terms of efficiency, reliability, scalability, and security.

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

Metric	EdgeBoosted Consensus (EBC)	Proof of Work (PoW)
Operating Costs	Low	High
Hardware Requirements	Minimal	Extensive
Maintenance Effort	Minimal	High
Total Cost of Ownership	Economical	Expensive
Performance	Superior	Good

In Table 3, we can see how the suggested EdgeBoosted Consensus (EBC) technique compares in price to the more standard Proof of Work (PoW) approach. It emphasizes the low-cost benefits of the EBC approach while still providing high-quality results, such as decreased operating expenses, minimum hardware needs, and minimal maintenance tasks.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

5. Conclusion

To realize the promise of Web3.0's decentralized, secure, and scalable internet, it is crucial to develop robust consensus methods. Even if they have their uses, the limits of conventional consensus procedures pose a threat to the long-term viability of Web3.0 networks. This study introduces a novel strategy for resolving these issues by capitalizing on edge intelligence. The dynamic edge participation (DEP) method is an adaptable and dynamic approach to network consensus that encourages nodes in the network's periphery to take an active role depending on the current state of the network. As a result, not only is the network more effective and scalable, but it also helps the environment by using less power than conventional techniques. To improve both the user experience and transaction throughput, LTV offers low-latency and efficient transaction validation at the edge. It's a big deal because it means we're getting closer to the real-time functionality that new Web3.0 apps want. Security issues are addressed via the edge-boosted security (EBS) algorithm, which distributes security operations. A distributed and proactive security strategy is achieved by delegating greater security duties to edge nodes with better security scores. Extensive simulations and tests have shown that our suggested techniques are successful, providing us with empirical proof of their merit. When compared to conventional consensus processes, they excel in four key areas: efficiency, security, scalability, and cost. We are designing a future for decentralized networks that is more robust and adaptive by seamlessly integrating edge intelligence into Web3.0 consensus. In conclusion, the combined effect of DEP, LTV, and EBS not only solves Web3.0's present problems but also creates exciting new opportunities for the future of distributed computing and networking. These advancements are a major step toward developing robust consensus procedures for the Web3.0 network, which will guarantee its continuous viability and expansion.

References

[1] X. Ge, Q.-L. Han, and Z. Wang, "A threshold-parameter-dependent approach to designing distributed event-triggered $H\infty$ 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, Article ID 8517706, pp. 1–10, 2022. Available: https://doi.org/10.1155/2022/8517706.

[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, Article ID 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. Muzamil Aslam, J. Zhang, B. Qureshi, and Z. Ahmed, "Beyond6g-consensus traffic management in crn, applications, architecture, and key challenges," in Proc. 2021 IEEE 11th Int. Conf. Electron. Inf. Emerg. Commun. (ICEIEC), Beijing, China, 2021, pp. 182-185.

[7] V. Roy and S. Shukla, "Effective EEG Motion Artifacts Elimination Based on Comparative Interpolation Analysis," Wireless Pers. Commun., vol. 97, pp. 6441–6451, 2017. [Online]. Available: https://doi.org/10.1007/s11277-017-4846-3.

[8] P.K. Shukla, V. Roy, P.K. Shukla, A.K. Chaturvedi, A.K. Saxena, M. Maheshwari, P.R. Pal, "An Advanced EEG Motion Artifacts Eradication Algorithm," The Computer Journal, 2021, pp. bxab170. [Online]. Available: https://doi.org/10.1093/comjnl/bxab170.

[9] Ballo AB, Mamadou D, Ayikpa KJ, Yao K, Ablan EAA, Kouame KF (2022) Automatic Identification of Ivorian Plants from Herbarium Specimens using Deep Learning. Int J Emerg Technol Adv Eng 12(5):56–66

[10] M. Bathre and A. Sahelay, "Energy efficient route discovery algorithm for MANET," Int J Eng Res Technol (IJERT), vol. 2, no. 7, pp. 1291–1295, 2013.

[11] Abdelhafid E, Aymane E, Benayad N, Abdelalim S, El YAMH, Rachid ROHT, Brahim B (2022) ECG Arrhythmia Classification Using Convolutional Neural Network. Int J Emerg Technol Adv Eng 12(7):186–195

[12] E. L. Huamaní and L. Ocares-Cunyarachi, "Analysis and prediction of recorded COVID-19 infections in the constitutional departments of Peru using specialized machine learning techniques," Int. J. Emerg. Technol. Adv. Eng., vol. 11, no. 11, pp. 39-47, 2021.

[13] M. Bathre and P. K. Das, "Hybrid Energy Harvesting for Maximizing Lifespan and Sustainability of Wireless Sensor Networks: A Comprehensive Review & Proposed Systems," in Proc. 2020 Int. Conf.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024

on Computing, Intelligence and Smart Power System for Sustainable Energy (CISPSSE), Keonjhar, India, 2020, pp. 1–6, DOI: 10.1109/CISPSSE49931.2020.9212287.

[14] 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," Int. J. Emerg. Technol. Adv. Eng., vol. 12, no. 1, pp. 146-151, 2022.

[15] 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 (WIE) Conf. on Electrical and Computer Engineering (WIECON-ECE), 2022, pp. 356-361, IEEE.

[16] E. J. Kcomt-Ponce, E. L. Huamaní, and A. Delgado, "Implementation of Machine Learning in Health Management to Improve the Process of Medical Appointments in Perú," Int. J. Emerg. Technol. Adv. Eng., vol. 12, no. 2, pp. 74-85, 2022.

[17] M. Bathre and P. K. Das, "Review on an Energy Efficient, Sustainable and Green Internet of Things," in Proc. 2nd Int. Conf. on Data Engineering and Applications (IDEA), Bhopal, India, 2020, pp. 1–6, DOI: 10.1109/IDEA49133.2020.9170736.

[18] B. Ning, Q.-L. Han, Z. Zuo, J. Jin, and J. Zheng, "Collective behaviors of mobile robots beyond the nearest neighbor rules with switching topology," IEEE Transactions on Cybernetics, vol. 48, no. 5, pp. 1577-1590, 2018.

[19] B. Ning, Q.-L. Han, and L. Ding, "Distributed finite-time secondary frequency and voltage control for islanded microgrids with communication delays and switching topologies," IEEE Transactions on Cybernetics, vol. 51, no. 8, pp. 3988-3999, 2021.

DOI: https://doi.org/10.54216/IJWAC.080103
Received: June 10, 2023 Revised: October 22, 2023 Accepted: January 03, 2024