applied sciences

MDPI

Article

NexoNet: Blockchain Online Social Media with User-Centric Multiple Incentive Mechanism and PoAP Consensus Mechanism

Junzhe Zuo, Wei Guo and Li Ling *

School of Information Science and Technology, Fudan University, Shanghai 200082, China; 21210720082@m.fudan.edu.cn (J.Z.); 21210720136@m.fudan.edu.cn (W.G.)
* Correspondence: lingli@fudan.edu.cn

Abstract: Online social media (OSM) has revolutionized the manner in which communication unfolds, enabling users to spontaneously generate, disseminate, share, and aggregate multimedia data across the internet. Nevertheless, in this exchange of information, OSM platforms assume a dominant, central role, wielding excessive power. Blockchain online social media (BOSM) seeks to mitigate the drawbacks of traditional centralized OSM by leveraging the decentralized nature of blockchain technology, migrating the functionalities of social media into a decentralized realm, and positioning the users at the core of the OSM ecosystem. However, current BOSM models often rely on tokens for incentives and are hampered by the centralized, inefficient blockchain consensus mechanisms, alongside vulnerabilities such as collusion attacks. This paper introduces a novel blockchain system, NexoNet, tailored for decentralized social media, exploring the application of blockchain technology in the realm of online social media from both technical and economic perspectives. The NexoNet quantifies and evaluates user participation within the system, employing a multiple incentive mechanism to equitably distribute value created by users without the need for tokens. Furthermore, we propose the Proof-of-Active-Participation (PoAP) blockchain consensus mechanism, enabling all users to partake in the maintenance of the blockchain system, thus ensuring its security and efficiency. Theoretical analysis and simulations across various scenarios demonstrate that the NexoNet, with extensive user engagement, achieves equitable value distribution through its multiple incentive mechanism. It successfully safeguards against a spectrum of malicious attacks and attains high transaction processing efficiency. The simulation results show that NexoNet achieves an average transaction throughput of 2000 transactions per second (TPS) and a consensus delay of 2.385 s with 100 maintainers in the network. Furthermore, our tests demonstrated that even collusion with users comprising 75% of the total would only allow an additional 30 chances to propose a block. By deeply integrating user behavior with the underlying mechanisms of the blockchain system, the NexoNet fosters a user-centric blockchain social media ecosystem.

Keywords: blockchain; online social media; PoAP consensus mechanism; multiple incentive mechanism

Citation: Zuo, J.; Guo, W.; Ling, L. NexoNet: Blockchain Online Social Media with User-Centric Multiple Incentive Mechanism and PoAP Consensus Mechanism. *Appl. Sci.* **2024**, *14*, 9783. https://doi.org/10.3390/app14219783

Academic Editor: Luis Javier Garcia Villalba

Received: 18 September 2024
Revised: 16 October 2024
Accepted: 24 October 2024
Published: 25 October 2024

1. Introduction

With the rapid development of digitalization and digital media, the methodologies by which individuals acquire information are in a constant state of flux. Distinct from the activities on traditional static and passive web pages, Web 2.0 has emerged as the paradigm of dynamic and interactive knowledge creation on the internet [1]. Users are now able to effortlessly generate, define, publish, share, and collate multimedia data on the web [2]. The year 2008 marked a revolutionary milestone for online social media (OSM), with Mark Zuckerberg launching the most renowned digital social community, Facebook, now known as Meta, alongside other leaders in social media such as Twitter, iMessage, TikTok, YouTube, and Google+ [3]. OSM has fundamentally altered the way people communicate, achieving widespread adoption among users around the world [4].

Presently, OSM platforms have amassed a vast user base and achieved tremendous commercial success. However, in this process of information exchange, these platforms assume a central, dominant role, thereby fostering a centralized model, with users relegated to the periphery. In this model, the platforms wield immense power, while users, as both producers and consumers of content, generate value for the platform but find their rights wholly under the control of the central platforms. This asymmetry in power harbors numerous inherent issues within such centralized model, including but not limited to privacy disclosure [5], copyright infringement [6], unfair distribution of revenue between service providers and users [7], and the selling of sensitive user information to advertising agencies for promotional gains [8]. These challenges have ensnared Web 2.0-based OSM platforms in crises of trust.

Blockchain technology, with its inherent advantages of decentralization, tamper-resistance, traceability, transparency, and censorship resistance, heralds the advent of the new Web 3.0 era on the internet [9]. In response to the myriad issues of traditional, centralized OSM platforms, blockchain technology stands as the epitome of modern decentralized technology and has been employed in the development of a new generation of decentralized online social media [10]. The introduction of blockchain technology has given rise to a new era of BOSM [11], utilizing blockchain to offer social services and address the challenges inherent in centralized OSM platforms. Among the most notable BOSM platforms is Steemit, boasting over one million users around the world. The application of decentralized finance (DeFi) to social media, termed Social Finance (SocialFi), enables every aspect of social media interaction to be tokenized [12]. BOSM leverages the decentralized nature of blockchain to eschew the drawbacks of traditional centralized OSM, migrating the functionalities of social media into a decentralized domain [13] and positioning users engaged in content production and consumption at the core of the social media ecosystem.

Based on the observations of existing OSM platforms, the ability to attract and sustain the active participation of a substantial user base is critical to the success of social media [14]. Influencers, marketers, and advertising agents primarily engage in OSM to generate revenue [15]. Hence, it is imperative for OSM platforms to devise and implement reasonable incentive mechanisms to encourage active user participation. However, token incentives, commonly employed within blockchain contexts, present both opportunities and challenges. While tokens facilitate easier market access, enhanced liquidity, reduced transaction costs, and automated trading processes, their valuation and pricing are fraught with challenges due to the lack of intrinsic value, volatility, and regulatory risks [16].

In this paper, we propose a novel incentive mechanism and Proof-of-Active-Participation (PoAP) consensus mechanism tailored for blockchain online social media, named NexoNet, which endeavors to explore the application of blockchain technology in OSM from both technical and economic perspectives. The NexoNet quantitatively assesses and evaluates users' level of participation by assigning a participation value (PV) to users based on their actions, such as content creation, voting, and engagement. This PV is used in the multiple incentive mechanism to distribute the value generated by users. Moreover, it incorporates the PoAP blockchain consensus mechanism to ensure the security and efficiency of the system. By deeply integrating user actions with the underlying mechanisms of the blockchain system, it aims to create a user-centric blockchain social media ecosystem.

The distinguishable contributions of this paper are as follows:

- We propose a user-centric multiple incentive mechanism that integrates rewards for actively engaged users in social media into the blockchain incentive mechanism to enhance user creativity and ensure the quality of content on the social media platform.
- We propose a novel consensus mechanism, PoAP, based on the operational characteristics of BOSM and the requirements for efficiency and security.
- Based on the multiple incentive mechanism and PoAP, we designed a brand new BOSM system, NexoNet, and conducted a comprehensive analysis on the system model and its operational processes.

The rest of the paper is organized as follows. Section 2 introduces related work on blockchain, social media, and blockchain incentive mechanisms. Section 3 outlines the design goals of the NexoNet. In Section 4, we describe the incentive mechanism based on participation assessment algorithm, and Section 5 details the proposed PoAP consensus mechanism. A theoretical and security analysis of the NexoNet is provided in Section 6. Section 7 reports on the performance evaluation results of NexoNet, and Section 8 summarizes and provides an outlook on the research of this paper.

2. Related Work

Following the official launch of Bitcoin in 2009 [17], blockchain technology has garnered widespread attention; the decentralized model based on blockchain has found extensive applications. Bitcoin, as a pioneering decentralized digital payment system, facilitates peer-to-peer (P2P) transactions without central authorization [18]. In a blockchain system, each newly generated block is appended with the latest transactions. Once all nodes validate its legitimacy, it is linked to the preceding block, and only the transactions appended to the block are executed [19]. Blockchain, serving as a distributed ledger and database, possesses qualities of openness, transparency, decentralization, and immutability, addressing the issue of trust among nodes within decentralized systems and thus facilitating the transformation of information to value on the internet [20]. There has been considerable work applying blockchain technology across various domains, such as securities trading [21], e-commerce [22], and the Internet of Things (IoT) [23]. Zhang et al. [24] proposed a blockchain-based security assessment model for the IoT, combining cryptographic techniques to ensure a secure and trusted environment for agricultural IoT applications.

In recent years, faced with the issue of increasing centralization of power within OSM platforms, blockchain technology, with its inherent decentralization, has gradually been introduced into OSM, effectively alleviating the monopoly problem inherent in centralized OSM platforms. Additionally, by leveraging cryptographic algorithms and the distributed storage technology of blockchain, the privacy of users and the protection of intellectual property in social media can be significantly enhanced [25]. For instance, zero-knowledge proof protocols [26] have been shown to enhance security and privacy in blockchain systems by allowing data verification without revealing the underlying information. Relevant research has implemented and tested zero-knowledge protocols in blockchain for secure identity management. In 2016, Ned Scott founded Steemit, the first successful BOSM community [27]. Steemit advocates for rewarding the platform users with tokens, aiming to provide transparent and precise rewards to individuals who contribute to the community. This involves using tokens to reward content contributors, including creators and content curators, to encourage the production and dissemination of quality content [28]. SocialFi AI and Infuencio, introduced in 2020 and 2022, respectively, are two practical platforms preparing to emerge within the metaverse. They offer a transaction platform based on SocialFi and represent the next generation of marketplaces [12]. The most distinctive feature of blockchain-based platforms lies in their deep integration of social media with tokens and transaction networks on the blockchain. Users are no longer merely participants who post and receive content on the platform; instead, by holding tokens and similar means, they become owners who influence the platform's development. This approach significantly elevates the users' status within the platform [28].

The research of the application of blockchain in social media encompasses several aspects. Arquam et al. [29] developed a user information dissemination behavior model based on the reputation scores of users to verify information spread across social networks on blockchain, but lacked a detailed discussion of real-world application scenarios for the proposed model. Ochoa et al. [30] proposed a framework for using blockchain in the process of detecting false information, employing data mining as a consensus algorithm to verify information published on social networks, which is capable of identifying false information, penalizing disseminators of such information, and rewarding publishers of

truthful information, but has potential limitations related to scalability and performance in handling large volumes of social media data and the complexity of content verification. Calvaresi et al. [31] calculated user reputation scores through contract computations to represent the degree of information exchange between users, thus proposing a reputation-based evaluation mechanism. However, the implementation of smart contracts in such systems adds complexity, particularly in ensuring that reputation is calculated in an unbiased and accurate manner, which complicates the overall system design. Prashanth et al. proposed "SocialChain" [32], which contributes by providing a decentralized framework for social media, enhancing privacy and content ownership, but its main limitation is the lack of scalability and a robust incentivization model. Pavlyshyn et al. [33] discusses how blockchain-based social media can mitigate issues like misinformation and centralized control, but also addresses challenges such as the scalability of integrating large social media datasets and ensuring user privacy within a decentralized structure.

In blockchain systems, tokens are commonly employed as incentives for users. Adhering to the principles of token economics [34], this model economically incentivizes constructive behaviors, such as generating contents, by rewarding with tokens (typically in the form of cryptocurrency), thus endowing users' knowledge participation activities with both social and economic dimensions [35]. However, cryptocurrencies pose significant risks to users due to their high volatility and the lesser degree of regulation compared to traditional financial markets, which is not suitable for providing a stable medium for transactions [16]. Tang et al. [36] identified and analyzed collusive behaviors among users in BOSMs. Real data for Steemit are used as a case study herein to examine the collusion of users in BOSMs, and two user collusion behaviors (group voting and vote buying) are defined and measured. Guidi's research [37] assessed the wealth distribution in BOSMs, and revealed the "rich get richer" phenomenon in Steemit, demonstrating the uneven distribution of wealth on the platform. Kim et al. [34] argued that token incentive mechanisms risk leading to a monopoly and dominance by a minority of users within the community. Song et al. [38] proposed a Proof of Contribution consensus mechanism, which rewards users who contribute to the system in a non-monetary manner, thereby avoiding the pitfalls associated with token-based incentives. In this paper, to circumvent the issues arising from token-based incentive mechanisms, the NexoNet integrates a non-token incentive mechanism to encourage user participation, aiming to create a fair and valuable user-centric multiple incentive mechanism.

In recent years, several consensus mechanisms have been introduced to enhance the efficiency, scalability, and trustworthiness of blockchain applications, including those used in social media. Proof of Reputation (PoR) [39] assigns greater validation power to nodes with a proven reputation, making it particularly suitable for social media platforms where trust is central. However, this mechanism can lead to the concentration of validation power among a few highly reputable nodes, potentially centralizing the system. Proof of Participation and Fees (PoPF) [40], on the other hand, rewards users based on their activity and the fees they generate, encouraging engagement in decentralized social media networks. While PoPF incentivizes participation, its reliance on fee structures may lead to inequity between users with different resource levels. Delegated Proof of Stake (DPoS) [41], where token holders vote for validators, offers a democratic approach, but it may still result in the centralization of power among popular validators. This can be a drawback for social media platforms aiming for true decentralization. Lastly, Proof of History (PoH) [42], as used by Solana, enhances transaction speed through timestamping, making it ideal for real-time social media applications. However, PoH is still relatively new, and its long-term stability and security require further validation.

The current state of blockchain in social media focuses on decentralizing platform control, enhancing user privacy and content ownership, and integrating token-based economies for content monetization. However, it lacks a comprehensive approach to fully integrating blockchain's consensus and incentive mechanisms with the specific needs of

social media platforms, particularly in addressing challenges like scalability, governance, and misinformation management.

3. Design of NexoNet System

This section provides a theoretical framework of the NexoNet proposed in this paper, encompassing an introduction and analysis of the design of the NexoNet model and addressing the threat model.

3.1. Design Goal

Based on the above analysis of the current state of OSM and blockchain incentive mechanisms, the NexoNet we proposed should meet the following design goals:

- Data Security and Information Autonomy: Users' transaction data should be recorded on the blockchain, utilizing blockchain and cryptographic technologies to ensure data transparency, immutability, traceability, verifiability, and resistance to censorship. Furthermore, there should be no centralized organization storing and controlling users' personal information in any form. Users' private information should be distributed and stored locally, and when participating in network activities, necessary personal information is provided in an encrypted form using private keys.
- Effective Incentive: Designing an effective and fair incentive mechanism to encourage user participation in the system is a primary focus of this research. In the NexoNet, users' participatory actions in the network should be recorded and stored on the blockchain. A multiple incentive mechanism reasonably assesses and quantifies user participation, rewarding users accordingly to encourage participation.
- User-Centricity: All platform regulations during its operation are autonomously decided by its users, with each user being an owner of the system. Users participate in the system's daily operations and decision-making processes through voting, sharing in all value and profits generated by the system.
- System Security and Efficiency: As a public blockchain system, the blockchain consensus mechanism must be able to tolerate various forms of attacks in a completely open network environment. Therefore, in the face of massive node participation, the blockchain system must be resilient against all types of attacks and maintain efficiency and scalability.

In the subsequent sections of this paper, through the introduction and evaluation of the incentive mechanism based on user participation assessment algorithm and the PoAP consensus mechanism, how the NexoNet fulfills the design goals set forth in this section will be demonstrated.

3.2. System Model

The NexoNet, as a BOSM, relies on blockchain technology and engages users in content creation and purchasing activities within the platform. NexoNet comprises four main roles: users, blockchain system, maintainers, and decentralized application (DApp). The system model is shown in Figure 1, while facilitating social media functionalities, it also embodies the characteristics of decentralization, traceability, and security efficiency. In the proposed NexoNet, maintainers are responsible for the technical maintenance of the blockchain system, such as verifying transactions and generating blocks. However, their authority is strictly limited, and they are subject to the PoAP consensus mechanism and user voting. Users do not directly partake in the blockchain consensus mechanism, such as transaction verification and block generation, to prevent imposing additional burdens on them, like the need for more advanced hardware or increased complexity in usage. Therefore, in the NexoNet, tasks related to the operation and maintenance of the blockchain, such as running the consensus mechanism, are delegated to maintainers in the system. Users participate in the consensus by voting for maintainers, thereby engaging in the system's governance and benefiting from incentive mechanism.

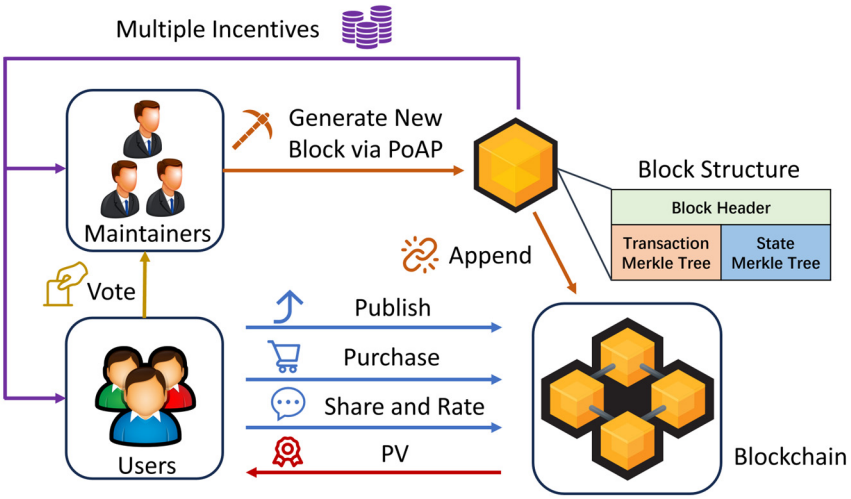


Figure 1. System model of the NexoNet.

The functionalities of each role are described as follows:

Users: As the protagonists of the NexoNet, users are the source of all value within it. Users assume dual roles: as system users, they can be content producers, publishing content that they create; as content consumers, they can purchase and evaluate content. As owners of the system, users participate in its operation and maintenance through voting, thereby influencing its development direction.

Blockchain system: The blockchain serves as the technological foundation of the NexoNet, responsible for storing users' transaction and state information in a decentralized manner and using Merkle trees to store these data within blocks. Cryptography and blockchain structure ensure the traceability and immutability of system information. With each new block's generation, the system's intrinsic multiple incentive mechanism rewards users and maintainers who contribute to the system.

Maintainers: Maintainers equipped with necessary hardware and maintaining an online presence, are responsible for the daily maintenance of the blockchain system and supporting various system functions. Their duties include transaction verification and forwarding, block generation, decentralized storage, maintenance of content and account information, and responding to users' transaction requests.

DApp: DApp is the interface for user–system interaction, facilitate account management and system interaction for users, such as scanning, generating, and purchasing content. DApp transmits user data to blockchain maintainers and return information from the blockchain to users for visualization.

The workflow of the NexoNet is described as follows:

1. Content publication and interaction: Users can publish content and purchase, reward, and rate content in the NexoNet through transactions sent via DApp. DApp forwards these transactions to maintainers, who serialize them and broadcast them across the network to all maintainers. All maintainers store the received valid transactions in a transaction pool.
2. Voting and consensus: At the start of each voting cycle, users vote for the maintainers they trust. Upon receiving votes, maintainers initiate the PoAP consensus mechanism, electing a committee and a block proposer through a cryptographic sortition algorithm. The proposer then proposes a new block to all committee members for a four-phase consensus process.
3. Block verification and broadcasting: After the committee generates a block, it is broadcast to all maintainers for verification. If the block is verified by a majority of maintainers, it is added to the blockchain. The new block updates the status information of all users and maintainers in the system, based on the transaction

Merkle tree and the state Merkle tree. This includes updates to user account balances, content purchased, and PV.

4. Status updates and reward distribution: Maintainers return the updated status to DApp, allowing users to check transaction state, consensus mechanism outcomes, and the distribution of rewards from the system's incentive mechanism through DApp.

3.3. Threat Models

Within the proposed NexoNet's incentive mechanism and PoAP consensus mechanism, several types of attacks could potentially endanger system security:

- Rapid content publication attack: In the NexoNet, publishing and purchasing content allows users to accumulate PV, which can be used to participate in the consensus mechanism by voting. Thus, users might publish a vast number of low-quality works in a short timeframe, attempting to quickly amass substantial PV to participate in consensus voting and illicitly gain economic benefits. Such behavior could severely compromise the fairness of the system's user participation assessment algorithm, diminish the system's reputation, and increase network latency.
- Collusion attack: The maintenance and updating of the blockchain are conducted by maintainers within NexoNet. To reflect the decentralized nature of the system, which is governed by user autonomy, users vote for maintainers to determine their weight in the consensus mechanism, thereby supporting their involvement in subsequent block generation and validation. To obtain additional user votes and the right of bookkeeping in the consensus mechanism, maintainers might collude with some users, bribing them for more votes to gain greater authority over new block decisions and earn more from the blockchain system incentives mechanism.
- Byzantine attack: During the execution of the blockchain consensus mechanism, some maintainers might exhibit various erroneous conditions or malicious behaviors, including denial of service, incorrect generation and verification of blocks, and other Byzantine faults. Such attack could severely impact the operation of the blockchain consensus mechanism, for instance, reducing the efficiency of consensus operation or even causing the consensus mechanism to fail.

4. User-Centric Multiple Incentive Mechanism

To encourage active user participation within the system while aiding the development of blockchain technology to overcome its reliance on cryptocurrencies, and avoid the inherent flaws of cryptocurrency, the proposed NexoNet employs a novel blockchain multiple incentive mechanism based on user participation assessment. This mechanism quantifies users' participatory behaviors within the system into PV, which are recorded on the state Merkle tree. This serves as a fair method for evaluating users, incentivizing them to make further contributions to the system.

4.1. Design of Multiple Incentive Mechanism

For OSM, the extent of users' active participation is a crucial determinant of a community's success [43]. The more positive feedback users receive from the system, the more likely they are to continue participating actively [44]. Therefore, the user participation assessment algorithm, based on users' participatory behaviors within the NexoNet, assesses their level of participation to the blockchain and quantifies this into PV recorded on the blockchain system.

Blockchain system often combine economic incentives with consensus mechanism to attract more user participation [38]. For example, the Bitcoin system, as the first to use the issuance of cryptocurrency as an incentive mechanism, attracted a vast number of users to join mining activities due to its high value. However, this cryptocurrency-based economic incentive also sparked a vicious competition for computational power, running counter to the blockchain's original intention of decentralization.

The incentive mechanism in NexoNet offers several functional advantages by utilizing blockchain technology. First, the decentralized nature of the blockchain ensures that PV are stored and managed transparently, preventing any central authority from manipulating the system. Unlike traditional centralized platforms, where the allocation of rewards might be controlled by the platform operator, NexoNet provides a fair and transparent reward distribution based on users' actual contributions. The immutability of blockchain records guarantees that users' earned incentives cannot be altered or disputed after they are recorded. Furthermore, blockchain automates the reward distribution process, ensuring that users are fairly compensated without the need for intermediaries. In the NexoNet proposed in this paper, a multiple incentive mechanism is employed to motivate users in four main aspects without the use of token or cryptocurrency:

- Content revenue incentive: Upon publishing content, creators set a price for their work, allowing other users to purchase it. All earnings from the content, including purchases and rewards from other users, are maintained in a content reward pool. A portion of this reward pool becomes the original author's income, while the rest supports system maintenance.
- PV incentive: Users earn PV rewards both by publishing content as creators or by engaging as readers through purchasing and evaluating content. This serves as proof of active participation within the system. Authors of high-quality works can receive additional PV rewards.
- Blockchain system incentive: Users partake in the blockchain consensus mechanism by voting for blockchain maintainers. Upon the successful generating of a block by the voted maintainer, voters can receive a portion of the transaction fee from the block as a reward.
- Other value incentives: Generating high-quality content increases users' exposure, enhancing their personal value. Highly active users in the NexoNet gain greater voting rights, participating in governance to decide the system's development direction. Furthermore, user-generated content receives social value feedback from other users, such as appreciations and rewards.

In the context of OSM applications, the content produced by users constitutes the core value of the entire blockchain system. To encourage active user participation, this paper proposes user participation assessment algorithm. This algorithm encompasses generating content, purchasing content, and content quality assessment, rewarding users directly in the form of PV.

4.2. Participation Assessment Algorithm

4.2.1. The Behavior of Publishing Content

In OSM, user-generated content is a critical element that attracts users. The richness of content within a OSM platform determines its appeal to users. Only when the quantity and quality of content are assured can more users be attracted and retained, thereby fostering the development of OSM. Publishing content is one of the primary ways for users to earn PV in the NexoNet. The more content a user publishes, the more PV they are rewarded with by the system.

While users can earn PV by publishing content, measures must be in place to counteract malicious users who might publish a large volume of false or low-quality content in a short period to gain undue PV. To address this, the acquisition of PV must be constrained. The hyperbolic tangent function $\tanh x = (e^x - e^{-x})/(e^x + e^{-x})$ exhibits the following characteristics: for $x \geq 0$, x is monotonically increasing, and the function's upper bound is 1. By considering the interval between content publications ΔT as the function's independent variable and the PV gained as the dependent variable, the PV obtained will significantly decrease as the interval between published content shortens, eventually approaching zero. Therefore, after publishing content, users must wait for a system-defined interval before

they can publish again to restore their PV to its original level. The method for calculating the PV gain for publishing content, GCP (Generate Content Participation), is shown in (1).

$$\begin{cases} \tau_1 = \frac{\Delta T}{\omega_1}, \\ \tanh\tau_1 = \frac{e^{\tau_1} - e^{-\tau_1}}{e^{\tau_1} + e^{-\tau_1}}, \\ GCP = \sum_1^{n_1} \alpha_{gcp} \times \tanh\tau_1 \end{cases} \tag{1}$$

n_1 represents the number of contents published by a user. α_{gcp} signifies the upper limit of PV that can be obtained from a single content publication. $\Delta T = (T_i - T_{i-1})$ denotes the time interval between content publications by a user. ω_1 is a variable system parameter, which can be adjusted to set the interval time for publishing content.

Figure 2 illustrates the relationship between the GCP a user can obtain from publishing content and the time interval ΔT between their content publications. If we set $\omega_1 = 1$ s, when the interval time $\Delta T = 0.5$ s for publishing content, the PV obtained by the user is only $0.460\alpha_{gcp}$. When a user publishes multiple contents in a much shorter time interval, the PV obtained for each piece of content will significantly decrease. Meanwhile, when the time interval $\Delta T = 3$ s for publishing content, the PV for publishing content can approximately return to its maximum value α_{gcp}.

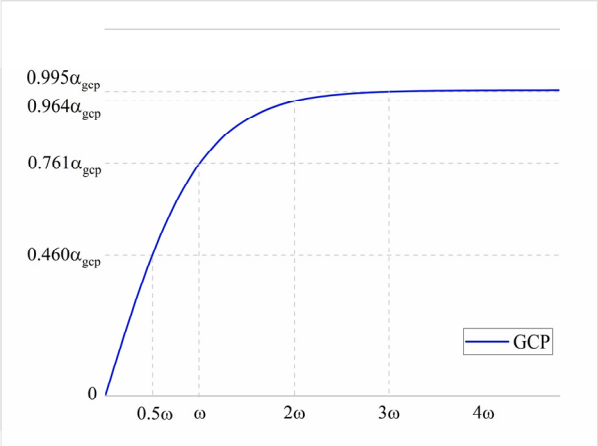


Figure 2. Effect of the hyperbolic tangent function on the PV.

4.2.2. The Behavior of Purchasing Content

Users within the NexoNet may purchase content by sending transactions to unlock desired content, with the paid amount flowing into the content's revenue pool, serving as direct financial remuneration for the creators. The acquisition of content represents a pivotal avenue through which the NexoNet actualizes its value. Purchasers gain access to the desired content, thereby fueling the creative zeal of authors and augmenting the vibrancy of user participation in the system. Consequently, the act of purchasing content is also regarded as a method of contributing to the system through participatory behavior. Upon confirmation of a purchase transaction, users are eligible to receive the system's Purchase Participation (PP) reward.

$$\begin{cases} \tau_2 = \frac{\Delta T}{\omega_2} \\ \tanh\tau_2 = (e^{\tau_2} - e^{-\tau_2})/(e^{\tau_2} + e^{-\tau_2}) \\ PP = \sum_1^{n_2} \alpha_{pp} \times \tanh\tau_2 \times price_i \end{cases} \tag{2}$$

n_2 denotes the number of contents a user publishes. α_{pp} signifies the maximum PV attainable from a single publication. Similar to (1), for the participation of publishing content, the hyperbolic tangent function $\tanh\tau_2$ is employed to curtail the frequency of content purchases, aiming to restrain the malicious behavior to amass PV through voluminous purchase transactions. Should the interval between two successive purchases by a user

be notably short, the quantity of PV rewards PP received will be diminished and thus mitigate the profitability of such actions. The term $price_i$ represents the amount paid by a user per content purchase, indicating that acquiring works of higher value garners greater PV rewards, thereby encouraging the circulation of high-value content in the NexoNet.

4.2.3. The Quality of Content

The value enhancement brought to the OSM by high-quality content is immeasurable. To incentivize the publication of high-quality content and increase the earnings of creators of premium content, the design of the participation assessment algorithm incorporates the quality of the content published by users as a crucial criterion for assessing their participation level. The higher the quality of the content published, the greater the value contributed to the system, and thus, the higher the PV reward conferred to the user.

In BOSM, the quality of content is measured by its popularity. The content popularity is calculated based on the reactions from other users within a certain period after the content is published. The calculation of content popularity includes two components: shares and ratings. The measurement begins from the moment the content is published by the user and continues until the evaluation period ends. After an evaluation period, users can earn quality participation (QP) from the content they have published.

$$\begin{cases} SP = \sum_1^{n_3} \alpha_{share} \times share_i \\ RP = \sum_1^{n_4} \alpha_{rating} \times rating_i \times \log\left(\frac{rating_{num}}{rating_{thresh}}\right) \\ QP = \frac{SP+RP}{T_{epoch}} \end{cases} \tag{3}$$

The QP consists of the share participation (SP) reward and the rating participation (RP) reward within the evaluation period (T_{epoch}). In the SP, n_3 represents the number of pieces of content published by the user that have been shared, and α_{share} is the coefficient for calculating the share participation value.

In the rating participation reward (RP), the term $rating_i$ represents the average rating value given by other users, $rating_{num}$ represents the number of times the content has been rated, and α_{rating} is the coefficient corresponding to the rating value. In the rating calculation process, whether a large number of users have evaluated the content is a reflection of the content's popularity, and also indicates the objectivity and fairness of the rating. Therefore, it is necessary to consider both the value of the rating and the number of users who have rated the content. A logarithmic function is used in the calculation, and only when the number of ratings exceeds $rating_{thresh}$ is the rating considered valid.

The QP calculation is conducted within the evaluation period (T_{epoch}) set by the platform, where the length of the period is measured in the number of blocks. The tipping and rating activities of users during the period reflect the popularity of the published content, and the content's quality is assessed based on its popularity.

Thus, the user participation assessment algorithm in the NexoNet comprises three components, corresponding to publishing content, purchasing content, and content quality. Every time a new block is to be generated successfully by consensus mechanism, all the maintainers in the blockchain will calculate the PV of every user in the NexoNet using the participation assessment algorithm.

$$PV = GCP + PP + QP \tag{4}$$

This trifold approach assesses and quantifies the participation of each user in the NexoNet; incentivizes user to actively participate in by encouraging active publication and the purchasing of works; and the creation of high-quality content, facilitating user to obtain greater PV reward.

5. The PoAP Consensus Mechanism

In the NexoNet, user transactions trigger updates to the system state, which are facilitated through the consensus mechanism. The operation of this mechanism involves transaction forwarding and verification, and block proposing and validation, thereby imposing certain demands on the hardware capabilities for the nodes. Considering that most users of the NexoNet may participate via a mobile or computer-based DApp without the capacity to run the consensus mechanism, the operation of the consensus mechanism is conducted by blockchain maintainers within the system. These maintainers, composed of capable users who volunteer, are responsible for maintaining and updating the system state, ensuring the functionality of the system and responding to user transaction requests.

Given the openness of the public blockchain in the design of the NexoNet, the potential behaviors of nodes are arbitrary. For instance, nodes may join or leave the network at any time and exhibit malicious behaviors such as dropping messages, fabricating messages, or ceasing operation, known as Byzantine faults. Furthermore, during network communication, messages may encounter errors, delays, duplication, or arrive out of order. Hence, an efficient consensus mechanism is requisite in the operation of the NexoNet to ensure data consistency across nodes and maintain the system's security and decentralization, while also ensuring the efficiency of consensus mechanism.

In the blockchain system that we proposed, nodes are interconnected via a peer-to-peer network and disseminate messages through broadcasting, utilizing gossip protocol. Users are able to perform operations, such as sending transactions, and receive data from the blockchain ledger, without directly participating in the consensus algorithm. Maintainers, on the other hand, are tasked with processing transactional information within the network and maintaining the blockchain ledger and network integrity.

5.1. The PoAP Consensus Process

Byzantine Fault Tolerance (BFT) serves as a universal solution for addressing fault tolerance issues within distributed systems, as exemplified by the PBFT consensus algorithm [45]. PBFT necessitates multiple phases of node communication to reach consensus, resulting in a relatively high communication complexity of $O(n^2)$, and is thus typically employed within permissioned blockchain networks with a smaller scale of nodes [46]. Owing to the performance challenges associated with the application of PBFT in large-scale blockchain systems, this paper introduces the PoAP consensus mechanism, which builds upon the foundation of PBFT, addresses its limitations, and is used in conjunction with the specific application scenario of the NexoNet.

The PoAP consensus mechanism is divided into two stages: the election stage and the execution stage, as depicted in Figure 3. During the election stage, users vote for maintainers they trust, followed by the selection of committee members through a cryptographic sortition algorithm. In the execution stage, the proposer generates and proposes a new block, which are then verified through voting by committee members, culminating in the collective update of the blockchain state by all maintainers.

5.1.1. The Election Stage of PoAP

The NexoNet is a public blockchain system, with user autonomy at the core of its design philosophy. All users are empowered to participate in the maintenance of the blockchain system: users can apply to become maintainers, or vote for maintainers they trust to elect committee members who execute the consensus mechanism. Voting for maintainers is conducted through voting transactions, with the voting weight determined by the number of PV held by each voter. This implies that the more actively a node participates in the system, the greater its influence during the consensus process, enabling it to exert a more significant impact, and garner more rewards from the incentive mechanism. To introduce randomness in the election process and prevent collusion attacks or the accumulation of power by maintainers, the PoAP consensus mechanism employs a cryptographic sortition algorithm. This randomness ensures that even maintainers who receive a high

number of user votes cannot consistently dominate the block proposal process, as their election as proposers is randomized. This system guarantees that the control of the network remains decentralized and user-driven, preventing any single entity from accumulating excessive influence over the blockchain. The election stage proceeds as detailed below:

User voting: Users cast their votes for their chosen maintainers using voting transactions by staking their PV. In a voting round, users are required to stake all the PV, with the staked amount being fully allocated to the target maintainer's voting pool, as shown in (5). $Vote_i$ represents the voting pool of the maintainer. m is the number of voting users; if user u_j votes for the target maintainer m_i, then $Vote_{ij} = 1$, otherwise $Vote_{ij} = 0$. PV_j represents the user's PV.

$$Vote_i = \sum_{j=1}^{m} PV_j \times Vote_{ij} \tag{5}$$

Committee election: After user voting, each maintainer receives votes denoted by $Vote_i$. To introduce randomness in the election process and prevent collusion attacks that could compromise system security, and to avoid fault from a single proposer during block proposing that could reduce consensus efficiency, PoAP employs a cryptographic sortition algorithm [47] during the committee election. Maintainers compute their hash values: $\langle \text{hash}, \pi \rangle \leftarrow \text{VRF}_{\text{sk}}(\text{seed})$ using a VRF random function and divide the [0,1) interval into continuous segments I^j.

$$I^j = \left[\sum_{k=0}^{j} B(k; Vote_i, p), \sum_{k=0}^{j+1} B(k; Vote_i, p) \right), \quad j \in \{1, \ldots, Vote_i\} \tag{6}$$

Here, p represents the probability of vote selection in consensus. If $\text{hash}/2^{hashlen}$ falls within interval I^j, then the maintainer's weight for this round of consensus is j, and the sortition result can be verified by other maintainers. The weight j of each maintainer are sorted, and members whose $j > 0$ are selected as committee members, with the number of selected vote values determining their weight on the committee. If no vote value is selected, they remain as maintainers. The committee elected through this cryptographic sortition participates in the subsequent execution of consensus.

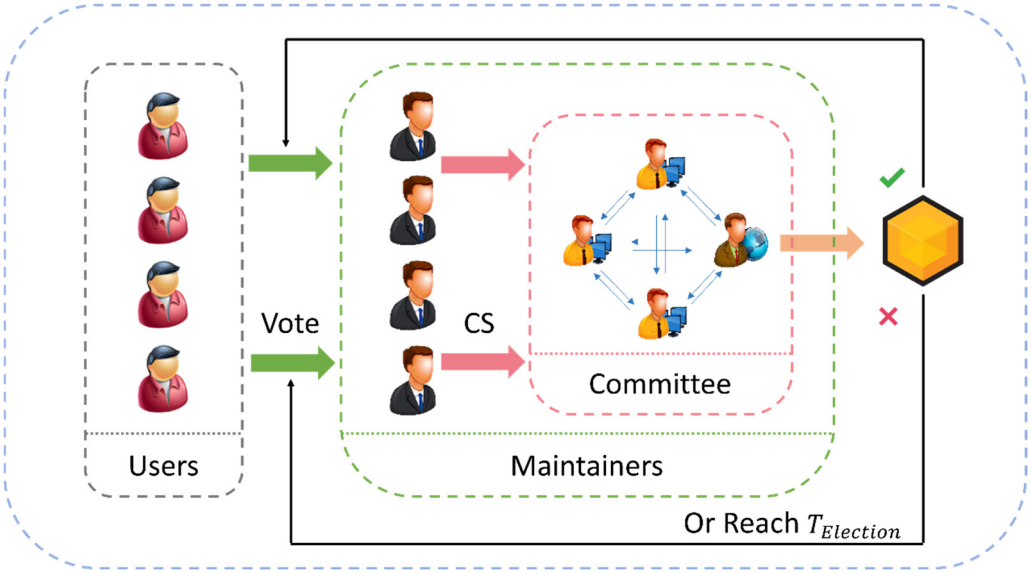


Figure 3. The PoAP consensus process.

5.1.2. The Execution Stage of PoAP

Within the committee, the top maintainers by weight act as proposer for consensus. Among the blocks proposed by multiple proposers, the block proposed by the proposer with the highest weight is selected as the target for this round of consensus execution, and blocks from other proposers are discarded. If the highest-weight proposer fails to propose

a correct block, the next proposer in line takes over as the proposer of a new block. During the verification process, the committee votes on the proposed block, with the weight of each vote determined by the number of user votes received during the election stage. Figure 4 illustrates the four phases of the PoAP consensus execution stage.

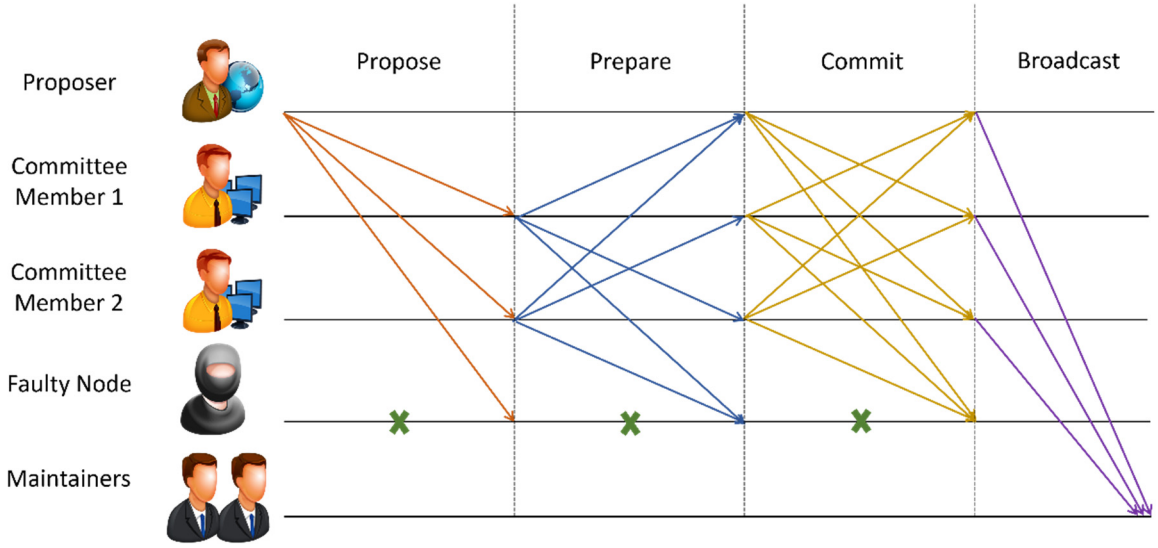


Figure 4. The execution stage of PoAP.

Propose Phase: The committee member with the highest weight is selected as the proposer, who is responsible for generating and proposing a new block and then broadcasting the block to all committee members.

Prepare Phase: All committee members verify the proposed block, including verifying whether the proposer has the highest weight, and whether the block's signatures, transactions, and other information are correct. Upon successful verification, members cache the newly generated block and broadcast and prepare signature packets, while also verifying and storing the packets from other committee members. Within the designated period for this phase, if the collective voting weight for the same block exceeds two-thirds of the total voting weight, i.e., satisfies inequality (7), the committee member successfully moves to the next phase. Here, M represents the number of honest committee members, while $(Vote_{all} \times p)$ represents the total weight as determined by the cryptographic sortition algorithm.

$$\sum_{i=1}^{M} weight_i > \frac{2}{3}(Vote_{all} \times p) \tag{7}$$

Commit Phase: Following the prepare phase, members broadcast commit signature packets while verifying and storing the packets from other committee members. Similar to the prepare phase, within the designated period for this phase, if the collective voting weight for the same block exceeds two-thirds of the total weight, the block proposed in this round is successfully committed.

Broadcast Phase: After the block is successfully committed by the committee members, it is broadcast to all the maintainers in the system. After the verification of the block, each maintainer appends this block to the blockchain and updates user state based on the newly generated block.

Maintainers not selected through cryptographic sortition assume the role of validators, responsible for verifying the newly generated block, adding the correct block to the blockchain, and updating user data. Because the election transactions sent by users consume considerable network bandwidth resources, committee elections are conducted

periodically, with each elected committee responsible for the generation of blocks for the subsequent $T_{election}$ length.

Upon finality of the consensus, if the voting period for $T_{election}$ blocks is reached, a new round of voting by all users commences to elect committee members for the next epoch. If a new voting epoch is not reached, cryptographic sortition is directly conducted within the committee to select the proposer for the next round of consensus, with each member eligible to serve as a proposer only once during each epoch. If the consensus fails, the committee is elected immediately.

5.2. Distribution of Blockchain System Incentive

The transaction fee contained within the newly generated blocks constitute an integral part of the multiple incentive mechanism, namely the blockchain system incentive. The design of a blockchain system incentive can encourage voter enthusiasm, thereby enhancing the security and decentralization of the NexoNet. Furthermore, a blockchain system incentive also serves as a means to motivate maintainers to actively and correctly participate in the consensus mechanism and actively maintain the blockchain system.

The blockchain system incentive mechanism is funded by the transaction fee from each block's included transactions, necessitating a fair distribution of the revenue generated from system maintenance. Meanwhile, committee members and the proposer, as key roles in the process of consensus, ensure the smooth functioning of the blockchain system. Therefore, all three roles should proportionately share in the revenue brought about by the blockchain system incentive.

5.2.1. Incentive Distribution for User

For users, staking their entire PV for voting in each consensus round allows them, should their chosen maintainer successfully propose a new block, to convert the staked PV into the transaction fee as a blockchain system incentive proportionally. If the chosen maintainer is not selected, they will not receive an incentive from this block, and the staked PV will be returned. Among all users who successfully voted for the proposer, the incentive is distributed based on each user's share of the total votes received by the proposer.

$$Tu_i = Tf \times \gamma_1 \times \frac{PV_i}{\sum_{j=1}^{m_1} PV_j} \tag{8}$$

Tf represents the transaction fee contained in the block generated during this consensus round, γ_1 denotes the proportion of block transaction fee distributed to users, m_1 is the number of users voting for the proposer, and Tu_i represents the transaction fee earned by users who voted for the proposer. Should the maintainer voted for by the user engage in incorrect block proposing or verification, the user's staked PV will be confiscated by the system. Thus, if a maintainer has a history of malicious behavior, it becomes increasingly unlikely for them to receive votes from users or be elected as a committee member in subsequent rounds. The introduction of this penalty mechanism significantly reduces the probability of maintainers compromising the operation of the blockchain system's consensus mechanism through malicious behavior.

5.2.2. Incentive Distribution for Committee

Committee members are responsible for verifying blocks proposed by the proposer and voting on blocks during the consensus execution stage. The block includes a confirmation information list from the previous block, detailing the correct voting committee members and their respective weights. Only committee members whose correct votes are included in this list will receive incentive. The incentive distribution for committee members is shown below, where each member's share is directly proportional to their voting weight.

$$Tc_i = Tf \times \gamma_2 \times \frac{weight_i}{\sum_{j=1}^{m_2} weight_j} \tag{9}$$

Here, γ_2 represents the proportion of transaction fee distributed to the committee, m_2 is the number of committee members who correctly verified the block, and Tc_i indicates the amount of transaction fee distribution earned by committee members who correctly voted on the block. Committee members who fail to correctly verify a block will not receive rewards from that round's block.

The proposer, tasked with proposing new blocks for each consensus round, plays a critical role in updating the blockchain system state with their correct block generation. The incentive distribution for proposer is shown in (10), where γ_3 denotes the proportion of transaction fee allocated to proposers, and Tp_i represents the amount of transaction fee distribution earned by proposers who correctly submit a block and achieve consensus.

$$Tp_i = Tf \times \gamma_3 \tag{10}$$

In the above equations, the distribution coefficients γ_1, γ_2, and γ_3 must sum up to 1: $\gamma_1 + \gamma_2 + \gamma_3 = 1$. After each successful consensus round, the transaction fee from the newly generated block is distributed according to the above equations among all users and maintainers who correctly participated in the consensus mechanism. This serves as the blockchain system incentive for participating in the NexoNet.

6. Theoretical and Security Analysis

This section provides a theoretical analysis of the NexoNet proposed in this paper, encompassing a theoretical analysis of the system and a security analysis addressing the threat model.

6.1. Theoretical Analysis

6.1.1. Decentralization of the NexoNet

Throughout the operation of the NexoNet, all users joining the system can participate in its various functions through sending transactions. Unlike a traditional centralized OSM, users can engage not only in content publication, consumption, and commenting processes but also accumulate PV to partake in the consensus mechanism, including voting for maintainers and applying to become maintainers themselves. The operational parameters of the system and settings are subject to change through proposals by maintainers. Users have complete control over their personal information, conducting various actions in the system through private key signatures, without interference from any individual or organization in their network transactions, thereby establishing a truly user-autonomous decentralized social media.

6.1.2. Incentive Mechanisms and Distribution

The NexoNet, through the integration of a multiple incentive mechanism with the PoAP consensus mechanism, ensures that the value created by users on the blockchain is genuinely enjoyed by the users themselves, rather than being predominantly controlled by centralized platforms. The multiple incentive mechanism quantifies user behavior into PV; users who create more value in the NexoNet will obtain greater rewards, continuously inspiring users' level of participation with the aim of achieving higher PV and more profits. On the other hand, it encourages users to actively participate in system governance, promoting correct and active involvement in the consensus mechanism process through a blockchain system incentive, including voting for trustworthy maintainers and maintainers executing the consensus mechanism correctly. This can effectively enhance the efficiency of blockchain operation and reduce the likelihood of failures.

Users create value for the system by publishing, purchasing, and rating works, upon which the system, through its multiple incentive mechanisms, fairly distributes its value to all users and maintainers. Leveraging its influence, the NexoNet can attract more users, thereby creating more value to benefit its users. Thus, the multiple incentive mechanism establishes a positive cycle that links user participatory behavior with system value.

6.1.3. Comparative Analysis with Existing BOSMs

We compare the proposed NexoNet system with several existing blockchain social media platforms, including Steemit (available online: https://steemit.com (accessed on 10 September 2024)), Mastodon (available online: https://joinmastodon.org (accessed on 10 September 2024)), Minds (Available online: https://www.minds.com (accessed on 10 September 2024)), and Diaspora (available online: https://diasporafoundation.org (accessed on 10 September 2024)), across key dimensions such as decentralization, data storage, incentive mechanisms, and scalability. The comparison results are summarized in Table 1.

Table 1. Comparison of consensus mechanism.

Platform	NexoNet	Steemit	Mastodon	Minds	Diaspora
Decentralization	Fully	Partial	Federated	Partial	Fully
Data Storage	Swarm Distributed	Blockchain	Instance-controlled	Blockchain	User-controlled
Incentive Mechanism	Multiple Incentives	Token Rewards	None	Token Rewards	None
Scalability	High	Limited	Instance-dependent	Limited	High

From the comparative analysis, it is evident that NexoNet outperforms other platforms in several key areas. In terms of decentralization, NexoNet achieves a higher degree through its PoAP consensus mechanism, allowing users to vote for maintainers and take part in platform governance, unlike Steemit and Minds, which maintain partial decentralization. NexoNet also excels in data storage by leveraging Swarm distributed storage technology, ensuring data security and traceability, and avoiding single points of failure, unlike the more centralized approaches of Steemit and Minds, and the federated structure of Mastodon and Diaspora.

In terms of incentive mechanisms, NexoNet introduces a multiple incentive model that fairly distributes rewards based on user participation and contributions, offering a more comprehensive system compared to Steemit's token-based rewards. Platforms like Mastodon and Diaspora lack built-in economic incentives altogether. Additionally, NexoNet's scalability is a major advantage, supporting large-scale participation and efficient data processing, whereas Steemit, Minds, Mastodon, and Diaspora face limitations due to blockchain performance or node-based configurations. Overall, NexoNet demonstrates significant improvements across these dimensions, making it a promising solution for decentralized social media platforms.

6.2. Security Analysis

6.2.1. Rapid Content Publication Attack

In the participation assessment algorithm, users can accumulate PV by publishing content. Thus, they might exploit this algorithm by publishing a large volume of false or low-quality content to garner extra PV. To counter this type of attack, the NexoNet utilizes the hyperbolic tangent function's properties in the calculation of PV gained from content publication: $GCP = \sum_{1}^{n_1} \alpha_{gcp} \times \tanh\tau_1$. If users publish a vast amount of content in a short period, the quantity of PV they can obtain becomes inversely related to the interval ΔT between publications. The shorter the interval between user publications, the closer the gained PV will approach 0. This design prevents users from benefiting from such malicious behavior by making it impossible to gain any profits from rapidly publishing a large volume of content. Furthermore, publishing content on the system requires the payment of a transaction fee to cover the costs for system use and maintenance, imposing a significant cost on users who publish content extensively, thereby preventing rapid content publication attack.

6.2.2. Collusion Attack

In the PoAP consensus mechanism, maintainers receive votes from users that contribute to their weight in the consensus process. The more votes they receive, the more likely they are to become committee members or a proposer. Therefore, there is a potential for maintainers to collude with users, bribing them for votes to launch a collusion attack.

In the proposed PoAP consensus mechanism, after user voting, the weight of committee members is generated randomly through a cryptographic sortition algorithm. Even if committee members receive more votes by collusion with users, this does not guarantee them greater weight or the privilege to propose blocks in the subsequent consensus process. The randomness of this election algorithm significantly reduces the security risks associated with collusion between maintainers and users. Furthermore, within an election period $T_{election}$, each maintainer has only one opportunity to be elected as a proposer, mitigating the benefits that maintainers can obtain through collusion.

From the perspective of users, they aim to vote for maintainers with a higher probability of becoming proposers to gain a share of the transaction fee distributed in the block. However, due to the randomness of the election, voting for a specific maintainer only offers a small chance of earning transaction fee from the block, and it comes at the cost of all their PV, thus preventing any potential for additional profit. Moreover, if users collude with malicious maintainer nodes, voting for maintainers attempting to attack the blockchain system, their accumulated PV will be forfeited as a penalty for supporting malicious maintainers in the system after the malicious behavior of the maintainer is detected.

6.2.3. Byzantine Attack

Committee nodes might exhibit Byzantine faults during the consensus execution phase, such as proposing or validating incorrect blocks. In the PBFT consensus algorithm, a system with N nodes can tolerate up to f faulty nodes, provided that $N \geq 3f + 1$. In PoAP, when N committee members vote to validate a block, at least M honest committee members need to correctly perform validation, and these correct blocks must receive more than two-thirds of the total committee votes to properly operate the consensus mechanism, as stipulated by (7).

PoAP can tolerate Byzantine fault from committee members whose total weight does not exceed one-third, and due to the randomness introduced by the cryptographic sortition algorithm for committee member weights, it is considerably difficult for members to collude and form a Byzantine attack that exceeds one-third of the weight. Additionally, after the committee reach consensus, the generated block must be verified by other maintainers not elected as committee members. If more than half of the nodes fail to verify the committee-generated block during the verification process, the consensus fails and restarts, prompting users to vote again to elect a new committee. In the event of consensus failure, committee members will be recorded by all nodes in the network, and they are unlikely to receive support in subsequent elections.

Overall, PoAP defends against Byzantine attacks through the introduction of election randomness and the trust relationship between users and maintainers. PoAP with N maintainers and C committee members tolerate up to $f = \left\lfloor \frac{3N-C-2}{6} \right\rfloor$ faulty maintainers; due to the randomness introduced by the cryptographic sortition algorithm, more than f malicious maintainers are needed to launch a Byzantine attack.

6.2.4. Other Common Blockchain Attacks

NexoNet's PoAP consensus mechanism effectively mitigates several common blockchain attacks. For a 51% attack, the randomization introduced by the cryptographic sortition algorithm and user voting significantly increases the difficulty for an attacker to control the consensus process, even if they accumulate substantial participation value (PV). In the case of a Sybil attack, PoAP prevents a single entity from gaining undue influence through fake identities, as voting power is tied to real user engagement, limiting the impact of multiple identities. DDoS attacks are mitigated through prioritization of transactions

based on fees and consensus-driven filtering by maintainers, ensuring that the network continues to process legitimate transactions efficiently. Man-in-the-Middle (MITM) attacks are countered through cryptographic signatures, ensuring that even if communication is intercepted, transactions cannot be tampered with. Additionally, while the model does not directly focus on a private key compromise, NexoNet can integrate existing solutions like multi-signature wallets and decentralized identity systems to reduce the risks associated with private key breaches.

6.2.5. Incentive Mechanism Security and External Protection

While NexoNet's incentive mechanism primarily operates within the blockchain network, leveraging the network's decentralized nature to ensure transparency and immutability, there are additional security considerations regarding how users can safeguard their rewards outside of the network. On-chain incentives benefit from blockchain's inherent protection against tampering and manipulation, but users may also need to secure their incentives when not actively engaged with the system. To mitigate risks such as private key compromise or external attacks, NexoNet can support multi-signature wallets and cold storage solutions. These methods allow users to store their incentives in highly secure, offline environments. Multi-signature wallets, for example, require multiple private keys to authorize a transaction, reducing the risk of a single point of failure. Cold storage solutions, such as hardware wallets, provide an additional layer of protection by keeping private keys offline. By combining NexoNet's on-chain security mechanisms with these external tools, users can ensure their incentives are protected both within and outside the network.

7. Experiment and Analysis

To evaluate the comprehensive performance of the NexoNet, this study utilized a computer equipped with a 12th Gen Intel® Core™ i5-12400 2.50 GHz processor, 16 GB DDR4 memory, 1 TB SSD, manufactured by Dell Technologies Inc., located in Round Rock, TX, USA, and running Windows 11 Professional edition. The system was constructed and subjected to simulation experiments using the Golang programming language. The experiments focused on analyzing both the multiple incentive mechanism and the PoAP consensus mechanism.

Parameters used in the experiments are detailed in Table 2. Within the parameter configuration, the PV calculation parameter α_{gcp}, representing the maximum PV attainable from a single content publication, was set at 10.0. The PV calculation parameter α_{pp} for purchasing content, which is multiplied by the expenditure amount to derive the purchase PV, was set at 1.0. The parameter for reward amounts α_{reward} was set at 2.0, and the rating calculation coefficient α_{rating} at 0.5, with the rating user number threshold $rating_{threshould}$ designated at 40: only ratings from a user count exceeding this threshold are deemed valid. Evaluations of content quality are conducted each period, with the period $T_{evaluation}$ defined as 30 block heights. Parameters ω_1 and ω_2, related to the content publication interval, were set at 1.0, necessitating a 3 s wait before publishing subsequent content to ensure the PV remains unaffected, with the same principle applying to purchase activities.

Table 2. Experiment parameter setting.

Parameter	Value	Parameter	Value
$\alpha_{gcp}, \alpha_{pp}$	10.0, 1.0	ω_1, ω_2	1.0, 1.0
$\alpha_{share}, \alpha_{rating}$	2.0, 0.5	$\gamma_1, \gamma_2, \gamma_3$	0.80, 0.15, 0.05
T_{epoch}	30.0	$T_{election}$	10.0
$rating_{threshould}$	40.0	p	0.2

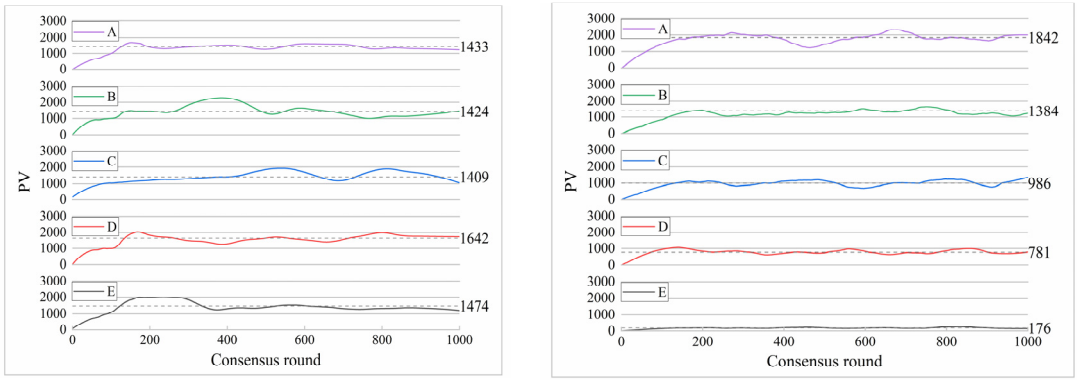
Within the PoAP consensus mechanism, the probability p for cryptographic sortition from the total votes was set to 0.2, with the voting period $T_{election}$ defined as 10 block heights. The parameters for the distribution of block transaction fee rewards, γ_1, γ_2, and γ_3, were established at 0.80, 0.15, and 0.05, respectively. The majority of the block

system incentive, accounting for 0.80 of the total, is enjoyed by users who contribute to the NexoNet. Committee members are allocated 0.15 of the total block rewards based on their weight, and the block proposer are entitled to 0.05 of the overall rewards.

7.1. Evaluation of Participation Assessment Algorithm

In the evaluation of the participation assessment algorithm, the network was assumed to consist of 100 user nodes and 20 maintainer nodes. Users were categorized into five groups based on their levels of participation: A, B, C, D, and E. It was assumed that all users randomly chose maintainer nodes when voting, with each maintainer having an equal probability of being selected as a committee member or proposer.

Figure 5 demonstrates the changes in the average *PV* of each group of users. In Figure 5a, assuming equal levels of participation across the five user groups, we observed the accumulation of *PV* for each group. The average *PV* for each group varied with increasing block height, depicted by different colored curves in the graph. A bar chart represented the mean *PV* for each user group throughout the entire test. It was observed that the average *PV* changes among the five groups with equal levels of participation were relatively similar. The average *PV* for the A, B, C, D, and E groups throughout the test were 1433, 1424, 1409, 1642, and 1474, respectively, without obvious disparities. This demonstrates the fairness of the user participation assessment mechanism within the NexoNet, indicating that all users with similar levels of participation can accumulate an equal amount of *PV*.



(**a**) (**b**)

Figure 5. Changes in the average PV: (**a**) 5 user groups with equal levels of participation; (**b**) 5 user groups with different levels of participation.

Figure 5b shows that Group A users exhibit a significantly higher propensity for content creation, characterized by the frequency and quality of their published content, whereas Groups B, C, and D demonstrate progressively lower capabilities in this regard, with Group E participants only participating in the acquisition and evaluation of content, abstaining from any content publishing. An assessment of the *PV* among these five groups revealed that the average participation scores for Groups A through D throughout the test phase were 1842, 1384, 986, and 781, respectively. In contrast, Group E's participation, limited to content purchase and evaluation without content publishing, was marked by a comparatively diminished level of participation, averaging at a mere 176. From the initiation of the test through to the completion of 1000 rounds of consensus, the mean *PV* for the five groups witnessed a cumulative increase upon joining the system, achieving a dynamic equilibrium within a range commensurate with their creative capacities after approximately 100 rounds of consensus. The average *PV* of each group fluctuated; this fluctuation was attributed to the transformation of the entirety of the staked *PV* into block transaction fee rewards subsequent to the successful voting on the proposer, with

the outcomes of these electoral processes being inherently random, thus instigating the volatility in *PV*.

To further assess the significance of the differences in the *PV* among the five user groups (A, B, C, D, E), an ANOVA (Analysis of Variance) test was conducted. The test compared the average *PV* across the groups to determine if there are statistically significant differences in user participation. The results of the ANOVA test indicated a significant difference between the groups ($F = 50.32$, $p < 0.001$), confirming that user participation levels, as measured by the *PV*, vary significantly across the groups. Group A, characterized by higher content creation activity, displayed a significantly higher *PV* compared to Group E, which primarily engaged in content evaluation and purchasing.

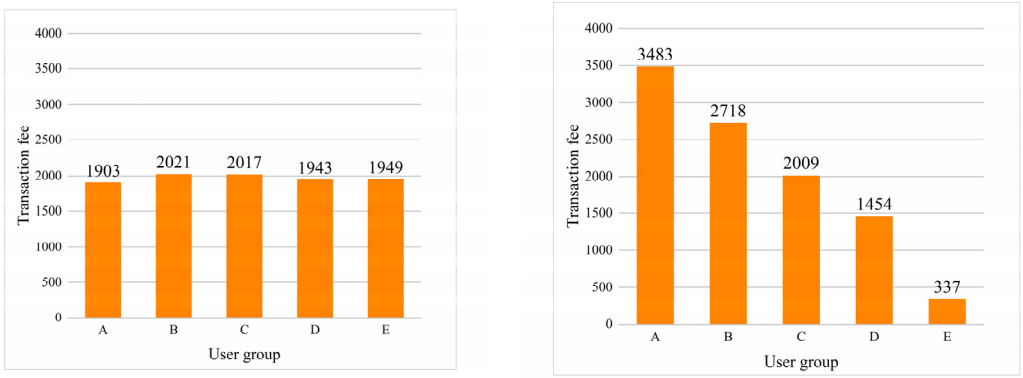
The comparative analysis of the cumulative average *PV* across users of varying creative capacities underscores the efficacy and rationality of the user participation assessment mechanism within the NexoNet, affirming that the accumulation of PV serves as a reflective measure of the user level and participation within the system.

7.2. Evaluation of Multiple Incentive Mechanism

Within the NexoNet, a significant portion of the incentive for users stems from the block transaction fee. Users earn PV through their participation in the system and use it to vote for maintainers. Being elected as a proposer enables them to receive a share of the transaction fee distribution, as delineated in Formula (8). The incentive distribution should reflect the idea that users with higher levels of participation receive greater rewards. This form of positive reinforcement aims to encourage active user participation within the system, fostering a vibrant and thriving BOSM.

To evaluate the fairness of the transaction fee rewards obtained by users through the incentive mechanism, we conducted tests on the distribution of transaction fee to ascertain its fairness. The transaction fee in a block, determined by the proposer based on the pending transactions within the network, were assumed to be a fixed amount for each block during testing. All users randomly selected maintainers when voting, with each maintainer having an equal probability of being elected as a committee member or proposer.

Assuming equal levels of participation among five user groups within the NexoNet, we observed the accumulation of transaction fee for each group, as shown in Figure 6a. The average *PV* for each group increases with each consensus round, with the cumulative change in the transaction fee depicted using different colored curves. It can be noted that among the five groups with equal participation, the average amount of the transaction fee accumulated by each group is quite similar, reaching approximately 2000 in the transaction fee after 1000 rounds of consensus. This demonstrates the fairness of the user incentive mechanism within the NexoNet, indicating that all users with the same level of participation can receive an equal amount of transaction fee rewards.



(**a**) (**b**)

Figure 6. The accumulation of transaction fee: (**a**) 5 user groups with equal levels of participation; (**b**) 5 user groups with different levels of participation.

In Figure 6b, the same user grouping as in the last section is adopted. From the start of the test to the completion of 1000 rounds of consensus, the average transaction fee rewards for the five groups continuously accumulate upon joining the system. After 1000 rounds of consensus, from Group A to Group E, users have, respectively, accumulated average transaction fee rewards of 3483, 2718, 2009, 1454, and 337, with the accumulation of transaction fee rewards aligning with the participation levels of the respective groups.

In the design of the multiple incentive mechanism, the higher the level of user participation, the greater the rewards obtained. However, there should be no distinction in the method of reward distribution among users based on the degree of participation; that is, the relationship between participation level and the amounts of rewards received should be linear. Therefore, this paper tests the transaction fee reward per PV (TpPv) of five user groups with different levels of participation, which represents the amount of the transaction fee reward obtained per unit of PV consumed by the user, serving as a measure of the fairness and decentralization of the incentive mechanism. If the average PV obtained by group i users over 1000 rounds of consensus is denoted as $\overline{PV_i}$, and the total accumulated average transaction fee rewards as $\overline{Tu_i}$, then the TpPv for this group of users in the NexoNet incentive mechanism can be calculated as

$$TpPv_i = \frac{\overline{Tu_i}}{\overline{PV_i}} \tag{11}$$

The average PV for Groups A to E were, respectively, 1842, 1384, 986, 781, and 176, summing to a total average PV: $\overline{PV_{all}} = \sum \overline{PV_i} = 5169$. Assuming that users can obtain an average transaction fee reward $\overline{Tu_i} = 200$ from the transaction fee in blocks generated in each consensus round, then after 1000 rounds of consensus, each group of users would, on average, receive a total transaction fee reward of $\overline{Tu_{all}}$ = 10,000. Theoretically, the average transaction fee reward per unit of PV consumed would be

$$TpPv_{all} = \frac{\overline{Tu_{all}}}{\overline{PV_{all}}} = \frac{10{,}000}{5169} = 1.934 \tag{12}$$

Calculating the $TpPv_i$ values for Groups A through E, as presented in Table 3, reveals some deviation from the theoretical value $TpPv_{all}$ for each group. This deviation arises from the randomness inherent in the voting and election processes, but the deviation introduced by this randomness is minor. Consequently, it can be concluded that users of varying participation levels within the NexoNet are not discriminated against based on their levels of participation; they are awarded a transaction fee commensurate with their level of participation. This ensures that users with higher participation levels do not receive additional rewards, thus preventing a reduction in enthusiasm among new users joining the NexoNet and averting risks of centralization. Hence, the fairness, rationality, and decentralization of the incentive distribution for user within the NexoNet are validated.

Table 3. *TpPv* for each users group.

Theoretical *TpPv*	***TpPv* for Each User Group**				
$TpPv_{all}$	$TpPv_A$	$TpPv_B$	$TpPv_C$	$TpPv_D$	$TpPv_E$
1.934	1.891	1.960	2.038	1.862	1.916

7.3. Evaluation of PoAP

7.3.1. Evaluation of Decentralization

Maintainers derive maximal rewards from the incentive mechanism by becoming a proposer. Hence, assessing whether maintainers have equal opportunities to become a proposer is crucial for evaluating the decentralization of the PoAP consensus mechanism. Within PoAP, maintainers receive votes from users and are allocated consensus weights

via a cryptographic sortition algorithm, with the highest weight conferring the role of the proposer for that consensus round.

In the test, 20 maintainers were set, each indiscriminately receiving votes from users, so the chances for all maintainers to be elected as proposer is equal. The test aimed to evaluate the frequency with which each maintainer was elected as a proposer over 1000 consensus rounds, as shown in Figure 7. Theoretically, each maintainer should have an average opportunity of being elected as a proposer 50 times. Due to the randomness introduced by user voting and the cryptographic sortition algorithm, the actual number of times each maintainer became a proposer varied within a certain range from the theoretical value, with a standard deviation of 5.11. This indicates a uniform and systematic distribution of block generation rights among all maintainers. It can be inferred that in the PoAP consensus mechanism, each maintainer has an equal chance of being proposer for the current consensus round, fulfilling the decentralized and fairness criteria of the PoAP consensus mechanism.

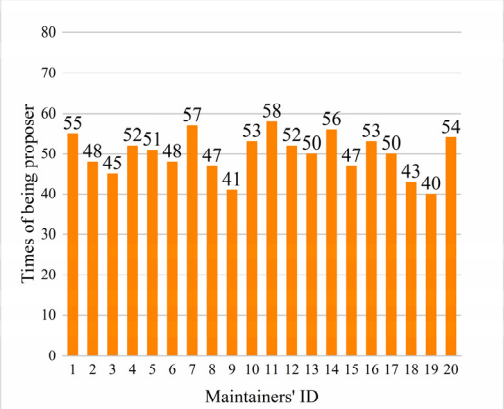


Figure 7. Distribution of block generating maintainers.

7.3.2. Evaluation of Consensus Efficiency

To evaluate the efficiency of the PoAP consensus mechanism, we conducted experiments and compared its performance against the PBFT algorithm. The efficiency of the consensus execution was evaluated by measuring consensus delay and throughput.

Consensus delay is the time taken for the generation of each block. The increase in the number of nodes participating in the consensus led to a higher number of communications required to reach consensus, thereby increasing the consensus latency. Figure 8 indicate a sharp decline in PBFT performance with a large number of nodes, with an average time of 11.607 s when 100 nodes execute consensus. Conversely, PoAP consistently demonstrated lower consensus delay under the same number of maintainer nodes. In the experiments, different cryptographic sortition probabilities p was assigned values in the range of [0.2, 0.3, 0.4], thus altering the number of committee members elected. A higher probability resulted in more committee members being elected. With the increase in nodes, the PoAP consensus delay also increased, with a new block generation taking 2.385 s with 100 maintainers and $p = 0.3$, indicating that PoAP maintains lower consensus delay, allowing users' transactions to be quickly confirmed in the NexoNet.

The transaction throughput refers to the number of transactions processed by a system within a unit of time. It serves as a measure of the system's concurrency capacity and is typically expressed as transactions per second (TPS). The throughput of PoAP at $p = 0.3$ is compared with PBFT, as shown in Figure 9. With the increase in the number of nodes, the throughput of PBFT decreases significantly, while that of PoAP decreases very slowly. The reason is that through committee elections, PoAP achieves consensus among a trusted small group of maintainers, thereby reducing the communication between nodes caused by the increase in node count. Therefore, PoAP outperforms PBFT in terms of throughput.

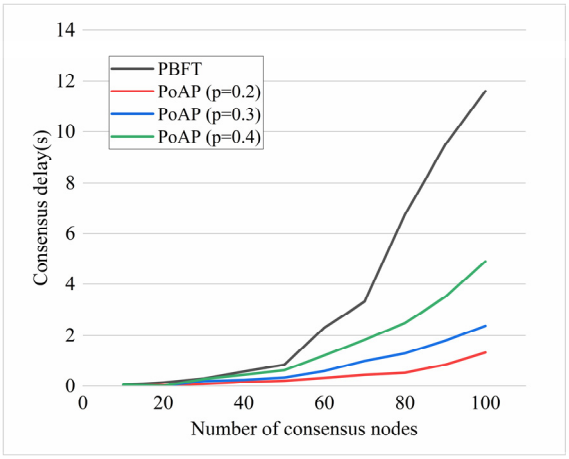


Figure 8. Comparison of consensus delay.

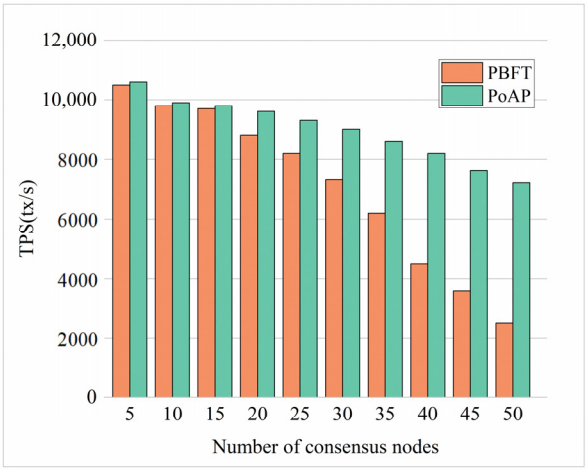


Figure 9. Comparison of TPS.

We compare PoAP with widely used consensus mechanisms in blockchain system such as PoW, PoS, and PBFT in Table 4. It is evident that PoAP surpasses other mechanisms in terms of higher TPS, better scalability, resistance to hard forks, and a well-defined incentive mechanism. As a novel consensus mechanism design, PoAP leverages users' accumulation of *PV* and their voting to perform effectively in the BOSM application scenario, especially in public blockchain with a large user base, showcasing its significant potential for widespread application.

Table 4. Comparison of consensus mechanism.

	PoAP	**PBFT**	**PoW**	**PoS**
TPS	High	Low	Low	High
Scalability	Good	Bad	Good	Good
Fork	Hard	Hard	Easy	Easy
Incentive	Multiple incentive	None	Token	Token

7.3.3. Security Evaluation

To test whether a rapid content publication attack could yield additional profits in the NexoNet, assume four groups of users publish content under different rates. With parameter setting $\omega_1 = 1$, the interval between content publications must satisfy $\Delta T \geq 3$ s to gain the full publication PV: α_{gcp} for each content. These four groups of users employ publication intervals of 1.000 s, 0.500 s, 0.250 s, and 0.125 s, respectively; the resulting transaction fee accumulation is illustrated in Figure 10.

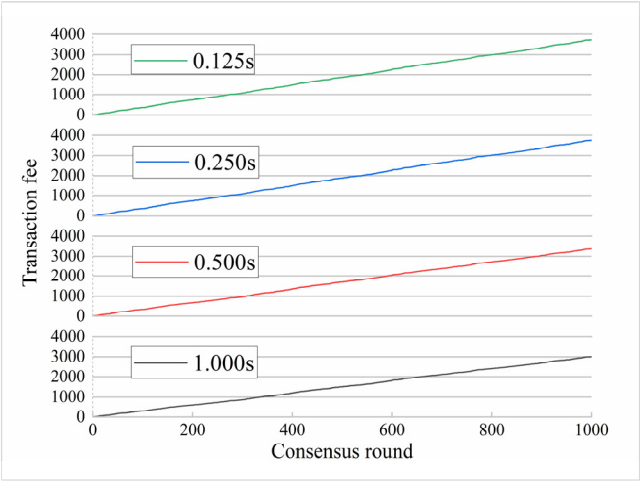


Figure 10. The accumulation of transaction fee for launching rapid content publication attack.

The observations from Figure 10 indicate that due to the characteristic of the hyperbolic tangent function used in Formula (1), increasing the rate of content publication from 1.000 s leads to diminishing increments in transaction fee rewards, even resulting in a decrease when accelerating from 0.250 s to 0.125 s. Given the transaction fee associated with publishing content, users cannot gain additional profits by rapid content publication in a short period. This demonstrates that the introduction of the hyperbolic tangent function in the user participation assessment algorithm successfully prevents rapid content publication attacks.

In the PoAP consensus mechanism, the foundation for a maintainer to become a committee member or a proposer is predicated upon securing a substantial number of votes from users. Thus, there exists a potential vulnerability wherein malicious maintainers could conspire with users to amass a greater volume of votes than their counterparts. To counteract this threat, a cryptographic sortition algorithm is introduced during the committee election, significantly mitigating the risk associated with this type of attack. In the experimental setup, malicious maintainers collude with certain users within the NexoNet, where these conspiring users exclusively cast their votes for the target maintainer. To test the frequency with which the malicious maintainer is elected as a proposer, over 1000 rounds of consensus were conducted. For these tests, an election period length $T_{election} = 10$ is set.

The test results are shown in Figure 11. Given that each maintainer can only be elected as a proposer once within each election period, this constrains the maximum number of times a committee member can be elected as a proposer to 100 over 1000 rounds of consensus. We contrast the scenario of electing the committee member with the highest votes as the proposer directly, without the use of cryptographic sortition algorithms, against the scenario where such algorithms are employed for elections. Theoretically, each maintainer should have an average opportunity to act as the proposer 50 times. When colluding with users with 15% total PV, a malicious maintainer elected directly as the proposer could be elected as a proposer approximately 70 times. This number could rise to approximately 90 when colluding with users with 35% total PV, nearing the theoretical maximum of 100 times. However, by using a cryptographic sortition algorithm into the committee election process, even collusion with users with 75% total PV would only allow an additional 30 chances to propose block, significantly mitigating the risk of collusion attacks against the PoAP consensus mechanism.

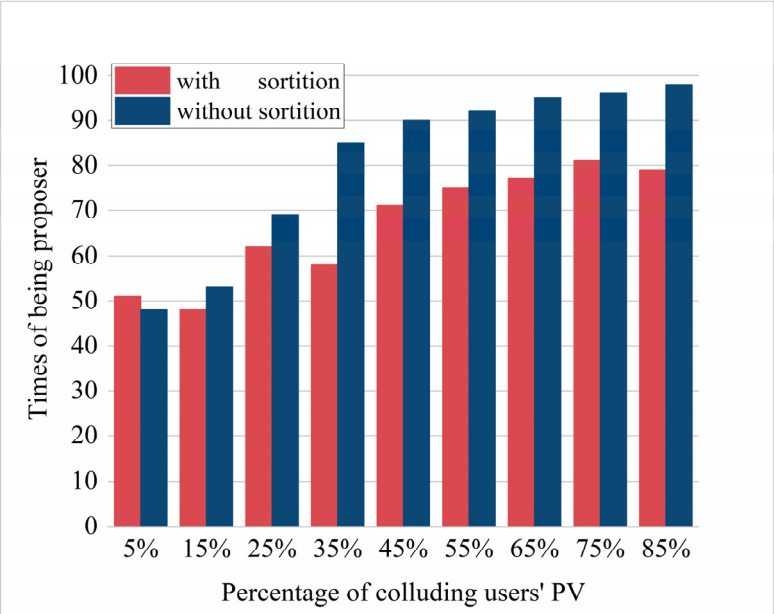


Figure 11. Proposer election results under different levels of collusion attacks.

8. Conclusions

This paper proposes a novel blockchain system, NexoNet, tailored for decentralized social media. Drawing upon an evaluation of users' participation levels within the system, a multiple incentive mechanism is devised to encourage active user participation. Utilizing the results of user participation assessment algorithm, a highly fault-tolerant and efficient consensus mechanism, PoAP, was developed, enabling users to partake in NexoNet through voting. This mechanism equitably distributes all value generated by the system to every participating user via the consensus process. Theoretical analysis and comprehensive experimental evaluations have demonstrated the suitability of the proposed NexoNet for incentivizing user participation in public blockchains with large-scale nodes in a BOSM scenario.

Looking ahead, there are several areas for potential future implementation and improvement. In practical applications, NexoNet could be integrated into real-world decentralized social media platforms, particularly within the Web 3.0 and metaverse ecosystems, where decentralized user control and content creation are critical. By providing a transparent and equitable incentive mechanism, NexoNet could offer a sustainable and secure foundation for these platforms.

Future work may focus on several key areas. First, optimizing the efficiency of the PoAP consensus mechanism to further reduce consensus delay and improve transaction throughput is essential for scaling the system to larger networks. Second, enhancing the user participation assessment algorithm to incorporate more factors, such as user reputation and long-term contributions, could refine the incentive distribution process. Additionally, further research into integrating advanced security measures, such as improved private key management and stronger resistance to emerging blockchain attacks, will be critical to ensuring NexoNet's long-term security and viability in large-scale applications.

Author Contributions: Conceptualization, J.Z. and L.L.; methodology, J.Z. and L.L.; software, J.Z. and W.G.; validation, J.Z. and W.G.; formal analysis, J.Z.; investigation, J.Z.; resources, J.Z. and L.L.; data curation, J.Z. and W.G.; writing—original draft preparation, J.Z.; writing—review and editing, J.Z. and L.L.; visualization, J.Z.; supervision, L.L.; project administration, L.L. All authors have read and agreed to the published version of the manuscript.

Funding: This research received no external funding.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: The raw data supporting the conclusions of this article will be made available by the authors on request.

Conflicts of Interest: The authors declare no conflicts of interest.

Abbreviations

Acronyms: The following acronyms are used in this manuscript:

OSM	Online Social Media
BOSM	Blockchain Online Social Media
PoAP	Proof-of-Active-Participation (Consensus mechanism)
DeFi	Decentralized Finance
SocialFi	Social Finance
DApp	Decentralized Application
PBFT	Practical Byzantine Fault Tolerance
BFT	Byzantine Fault Tolerance
VRF	Verifiable Random Function
TPS	Transactions Per Second
PoW	Proof-of-Work (Consensus algorithm)
PoS	Proof-of-Stake (Consensus algorithm)
PP	Purchase Participation
GCP	Generate Content Participation
QP	Quality Participation
PV	Participation Value (Represents user's contribution to the platform)

Symbols: The following symbols are used in this manuscript:

α_{gcp}	Maximum PV attainable from a single content publication
α_{pp}	PV calculation parameter for content purchasing
α_{share}	Reward parameter used in calculating rewards
α_{rating}	Coefficient for calculating rating contribution
ΔT	Time interval between content publications
ω_1, ω_2	System parameter controlling the interval time for publishing content
$\tanh \tau$	Hyperbolic tangent function used to control PV gain based on time interval
n	Number of user nodes in the network
m	Number of maintainer nodes in the network
T_{epoch}	The evaluation period of QP
$T_{election}$	Election period for maintainer nodes
p	Probability of vote selection during consensus
$Vote$	Voting pool of the maintainer
$Weight$	Weight assigned to a maintainer during consensus based on votes
Tf	Transaction fee contained in the block
Tu	Transaction fee earned by users who voted for the proposer
Tc	Transaction fee earned by committee members
Tp	Transaction fee earned by proposers
$\gamma_1, \gamma_2, \gamma_3$	Proportions of transaction fee allocated to users, committee members, and proposers
$rating_{num}$	Number of times content has been rated
$rating_{thresh}$	Threshold for rating count to be considered valid

References

1. Shang, S.S.C.; Li, E.Y.; Wu, Y.-L.; Hou, O.C.L. Understanding Web 2.0 Service Models: A Knowledge-Creating Perspective. *Inf. Manag.* **2011**, *48*, 178–184. [CrossRef]
2. Abebe, M.A.; Tekli, J.; Getahun, F.; Chbeir, R.; Tekli, G. Overview of Event-Based Collective Knowledge Management in Multimedia Digital Ecosystems. In Proceedings of the 13th International Conference on Signal-Image Technology and Internet-Based Systems, SITIS, Jaipur, India, 4–7 December 2017; Volume 2018, pp. 40–49.
3. Panger, G. Social Comparison in Social Media: A Look at Facebook and Twitter. In Proceedings of the Conference on Human Factors in Computing Systems, Toronto, ON, Canada, 26 April–1 May 2014; pp. 2095–2100.
4. Chugh, M.; Chugh, N. The Blockchain Technologies in Online Social Media: Insights, Technologies, and Applications. In *Blockchain Technology for Secure Social Media Computing*; IET: Stevenage, UK, 2023.

5. Necaise, A.; Tanni, T.I.; Williams, A.; Solihin, Y.; Kapadia, A.; Amon, M.J. User Preferences for Interdependent Privacy Preservation Strategies in Social Media. *Proc. ACM Hum. Comput. Interact.* **2023**, *7*, 1–30. [CrossRef]
6. Rathore, S.; Sharma, P.K.; Loia, V.; Jeong, Y.-S.; Park, J.H. Social Network Security: Issues, Challenges, Threats, and Solutions. *Inf. Sci.* **2017**, *421*, 43–69. [CrossRef]
7. Qi, T.; Wang, T.; Yan, J. The Spillover Effects of Different Monetary Incentive Levels on Health Experts' Free Knowledge Contribution Behavior. *Internet Res.* **2021**, *31*, 2143–2166. [CrossRef]
8. Chen, Y.; Bellavitis, C. Blockchain Disruption and Decentralized Finance: The Rise of Decentralized Business Models. *J. Bus. Ventur. Insights* **2020**, *13*, e00151. [CrossRef]
9. Park, S.-M.; Kim, Y.-G. A Metaverse: Taxonomy, Components, Applications, and Open Challenges. *IEEE Access* **2022**, *10*, 4209–4251. [CrossRef]
10. Guidi, B.; Michienzi, A. The Decentralization of Social Media through the Blockchain Technology. In Proceedings of the ACM Web Science Conference, Virtual, 21–25 June 2021.
11. Guidi, B. When Blockchain Meets Online Social Networks. *Pervasive Mob. Comput.* **2020**, *62*, 101131. [CrossRef]
12. Imani Rad, A.; Banaeian Far, S. SocialFi Transforms Social Media: An Overview of Key Technologies, Challenges, and Opportunities of the Future Generation of Social Media. *Soc. Netw. Anal. Min.* **2023**, *13*, 42. [CrossRef]
13. Guidi, B.; Michienzi, A. How to Reward the Web: The Social DApp Yup. *Online Soc. Netw. Media* **2022**, *31*, 100229. [CrossRef]
14. Ur Rahman, M.; Guidi, B.; Baiardi, F. Blockchain-Based Access Control Management for Decentralized Online Social Networks. *J. Parallel Distrib. Comput.* **2020**, *144*, 41–54. [CrossRef]
15. Zheng, Y.; Zhao, K.; Stylianou, A. The Impacts of Information Quality and System Quality on Users' Continuance Intention in Information-Exchange Virtual Communities: An Empirical Investigation. *Decis. Support. Syst.* **2013**, *56*, 513–524. [CrossRef]
16. Marin, O.; Cioara, T.; Toderean, L.; Mitrea, D.; Anghel, I. Review of Blockchain Tokens Creation and Valuation. *Future Internet* **2023**, *15*, 382. [CrossRef]
17. Tschorsch, F.; Scheuermann, B. Bitcoin and beyond: A Technical Survey on Decentralized Digital Currencies. *IEEE Commun. Surv. Tutor.* **2016**, *18*, 2084–2123. [CrossRef]
18. Liu, X.; Liu, Y.; Li, H.; Wang, J.; Zhu, J.; Song, H. Multi-Side Incentive Compatible Transaction Fee Mechanism. *Comput. Electr. Eng.* **2024**, *113*, 109050. [CrossRef]
19. Zhan, Y.; Wang, B.; Lu, R.; Yu, Y. DRBFT: Delegated Randomization Byzantine Fault Tolerance Consensus Protocol for Blockchains. *Inf. Sci.* **2021**, *559*, 8–21. [CrossRef]
20. Carrara, G.R.; Burle, L.M.; Medeiros, D.S.V.; de Albuquerque, C.V.N.; Mattos, D.M.F. Consistency, Availability, and Partition Tolerance in Blockchain: A Survey on the Consensus Mechanism over Peer-to-Peer Networking. *Ann. Des Telecommun. Ann. Telecommun.* **2020**, *75*, 163–174. [CrossRef]
21. Notheisen, B.; Willrich, S.; Diez, M.; Weinhardt, C. Requirement-Driven Taxonomy Development—A Classification of Blockchain Technologies for Securities Post-Trading. In Proceedings of the Annual Hawaii International Conference on System Sciences, Grand Wailea, HI, USA, 8–11 January 2019; Volume 2019, pp. 4615–4624.
22. Su, X.; Liu, Y.; Choi, C. A Blockchain-Based P2P Transaction Method and Sensitive Data Encoding for E-Commerce Transactions. *IEEE Consum. Electron. Mag.* **2020**, *9*, 56–66. [CrossRef]
23. Reyna, A.; Martín, C.; Chen, J.; Soler, E.; Díaz, M. On Blockchain and Its Integration with IoT. Challenges and Opportunities. *Future Gener. Comput. Syst.* **2018**, *88*, 173–190. [CrossRef]
24. Zhang, G.; Chen, X.; Zhang, L.; Feng, B.; Guo, X.; Liang, J.; Zhang, Y. STAIBT: Blockchain and CP-ABE Empowered Secure and Trusted Agricultural IoT Blockchain Terminal. *Int. J. Interact. Multimed. Artif. Intell.* **2022**, *7*, 66–75. [CrossRef]
25. Feng, Q.; He, D.; Zeadally, S.; Khan, M.K.; Kumar, N. A Survey on Privacy Protection in Blockchain System. *J. Netw. Comput. Appl.* **2019**, *126*, 45–58. [CrossRef]
26. Moya, C.V.; Bermejo Higuera, J.R.; Bermejo Higuera, J.; Sicilia Montalvo, J.A. Implementation and Security Test of Zero-Knowledge Protocols on SSI Blockchain. *Appl. Sci.* **2023**, *13*, 5552. [CrossRef]
27. Scott, N.; Larimer, D. *Steem Whitepaper: An Incentivized, Blockchain-Based, Public Content Platform*; Steem: New York, NY, USA, 2018.
28. Thelwall, M. Can Social News Websites Pay for Content and Curation? The SteemIt Cryptocurrency Model. *J. Inf. Sci.* **2018**, *44*, 736–751. [CrossRef]
29. Arquam, M.; Singh, A.; Sharma, R. A Blockchain-Based Secured and Trusted Framework for Information Propagation on Online Social Networks. *Soc. Netw. Anal. Min.* **2021**, *11*, 49. [CrossRef]
30. Ochoa, I.S.; de Mello, G.; Silva, L.A.; Gomes, A.J.P.; Fernandes, A.M.R.; Leithardt, V.R.Q. FakeChain: A Blockchain Architecture to Ensure Trust in Social Media Networks. *Commun. Comput. Inf. Sci.* **2019**, *1010*, 105–118. [CrossRef]
31. Calvaresi, D.; Mattioli, V.; Dubovitskaya, A.; Dragoni, A.F.; Schumacher, M. Reputation Management in Multi-Agent Systems Using Permissioned Blockchain Technology. In Proceedings of the 2018 IEEE/WIC/ACM International Conference on Web Intelligence, WI, Santiago, Chile, 3–6 December 2018; pp. 719–725.
32. Prashanth, M.S.; Maheswari, V.U.; Aluvalu, R.; Kantipudi, M.V.V.P. SocialChain: A Decentralized Social Media Platform on the Blockchain. In *Pervasive Knowledge and Collective Intelligence on Web and Social Media, Proceedings of the Second EAI International Conference, PerSOM, Hyderabad, India, 24–25 November 2023*; Castillo, O., Sudhakar Babu, T., Aluvalu, R., Eds.; Springer Nature: Cham, Switzerland, 2024; pp. 203–219.

33. Pavlyshyn, I.; Petrenko, A.; Opryshko, B.; Oliinyk, B.; Kavun, S. Social Media Impact on the 'Cosmos' Blockchain Ecosystem: State and Prospect. *Data Sci. J.* **2024**, *23*, 8. [CrossRef]
34. Kim, M.S.; Chung, J.Y. Sustainable Growth and Token Economy Design: The Case of Steemit. *Sustainability* **2019**, *11*, 167. [CrossRef]
35. Guidi, B.; Michienzi, A.; Ricci, L. A Graph-Based Socioeconomic Analysis of Steemit. *IEEE Trans. Comput. Soc. Syst.* **2021**, *8*, 365–376. [CrossRef]
36. Tang, H.; Ni, J.; Zhang, Y. Identification and Evolutionary Analysis of User Collusion Behavior in Blockchain Online Social Media. *IEEE Trans. Comput. Soc. Syst.* **2024**, *11*, 522–530. [CrossRef]
37. Guidi, B.; Michienzi, A.; Ricci, L. Assessment of Wealth Distribution in Blockchain Online Social Media. *IEEE Trans. Comput. Soc. Syst.* **2024**, *11*, 671–682. [CrossRef]
38. Song, H.; Zhu, N.; Xue, R.; He, J.; Zhang, K.; Wang, J. Proof-of-Contribution Consensus Mechanism for Blockchain and Its Application in Intellectual Property Protection. *Inf. Process Manag.* **2021**, *58*, 102507. [CrossRef]
39. Hisseine, M.A.; Chen, D.; Yang, X. The Application of Blockchain in Social Media: A Systematic Literature Review. *Appl. Sci.* **2022**, *12*, 6567. [CrossRef]
40. Fu, X.; Wang, H.; Shi, P.; Mi, H. PoPF: A Consensus Algorithm for JCLedger. In Proceedings of the 12th IEEE International Symposium on Service-Oriented System Engineering, SOSE and 9th International Workshop on Joint Cloud Computing, JCC, Bamberg, Germany, 26–29 March 2018.
41. Prodan, R.; Saurabh, N.; Zhao, Z.; Orton-Johnson, K.; Chakravorty, A.; Karadimce, A.; Ulisses, A. ARTICONF: Towards a Smart Social Media Ecosystem in a Blockchain Federated Environment. In *Euro-Par 2019: Parallel Processing Workshops, Proceedings of the 25th International European Conference on Parallel and Distributed Computing, EuroPar, Göttingen, Germany, 26–30 August 2019*; Springer: Cham, Switzerland, 2020; Volume 11997 LNCS.
42. Li, X.; Wang, X.; Kong, T.; Zheng, J.; Luo, M. From Bitcoin to Solana—Innovating Blockchain Towards Enterprise Applications. In *Blockchain–ICBC 2021, Proceedings of the 4th International Conference, Held as Part of the Services Conference Federation, SCF 2021, Virtual Event, 10–14 December 2021*; Springer: Cham, Switzerland, 2022; Volume 12991 LNCS.
43. Koh, J.; Kim, Y.-G.; Butler, B.; Bock, G.-W. Encouraging Participation in Virtual Communities. *Commun. ACM* **2007**, *50*, 69–73. [CrossRef]
44. Guan, T.; Wang, L.; Jin, J.; Song, X. Knowledge Contribution Behavior in Online Q&A Communities: An Empirical Investigation. *Comput. Hum. Behav.* **2018**, *81*, 137–147. [CrossRef]
45. Castro, M.; Liskov, B. Practical Byzantine Fault Tolerance and Proactive Recovery. *ACM Trans. Comput. Syst.* **2002**, *20*, 398–461. [CrossRef]
46. Li, W.; Feng, C.; Zhang, L.; Xu, H.; Cao, B.; Imran, M.A. A Scalable Multi-Layer PBFT Consensus for Blockchain. *IEEE Trans. Parallel Distrib. Syst.* **2021**, *32*, 1146–1160. [CrossRef]
47. Gilad, Y.; Hemo, R.; Micali, S.; Vlachos, G.; Zeldovich, N. Algorand: Scaling Byzantine Agreements for Cryptocurrencies. In Proceedings of the 26th Symposium on Operating Systems Principles, Shanghai, China, 28 October 2017.