Article | Received 16 October 2024; Accepted 25 December 2024; Published 9 January 2025
https://doi.org/10.55092/blockchain20250001

An enhanced DPoS consensus mechanism using quadratic voting in Web 3.0 ecosystem

Tianyu Lei[1], Qinnan Zhang[1]*, Wangjie Qiu[1,2]*, Hongwei Zheng[1,3], Shuyi Miao[1], Wanqing Jie[1], Jianming Zhu[4], Jin Dong[1,3] and Zhiming Zheng[1,2]

[1] Institute of Artificial Intelligence, Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing, Beihang University, Beijing, China
[2] Zhongguancun Laboratory, Beijing, China
[3] Beijing Academy of Blockchain and Edge Computing (BABEC), Beijing, China
[4] School of Information, Central University of Finance and Economics, Beijing, China

* Correspondence authors; E-mail: zhangqn@buaa.edu.cn; wangjieqiu@buaa.edu.cn.

Abstract: Consensus mechanisms are fundamental to maintaining consistency in distributed systems. With the advent of Web 3.0, blockchain has revealed limitations of traditional Delegated Proof of Stake (DPoS) consensus mechanisms. To address these issues, we propose a novel Quadratic Voting-based DPoS (Q-DPoS) consensus mechanism. Our approach integrates Quadratic Voting into DPoS to optimize voting power distribution, vote counting, and reward settlement processes, thereby incentivizing participation from users with lower stakes while reducing the concentration of influence. To prevent the system from reverting to a linear reward structure under Sybil Attacks, we introduce admission rules and vote similarity detection mechanisms to strengthen its robustness. Simulation results demonstrate that Q-DPoS significantly increases voter participation and alleviates stake centralization, thereby enhancing overall decentralization. Additionally, theoretical analysis grounded in game theory confirms that the proposed mechanism effectively diversifies voting preferences, contributing to a more balanced and resilient consensus mechanism suitable for Web 3.0 ecosystem.

Keywords: Web 3.0; decentralization; consensus; DPoS; quadratic voting; game theory.

1. Introduction

Web 3.0, the emerging paradigm of the internet that emphasizes decentralization, is garnering significant interest by empowering users with ownership and control over their data [1]. This new paradigm relies on blockchain technology to ensure decentralization, privacy, governance, and incentives. The blockchain acts as a chain-like data structure within a peer-to-peer network, functioning as a distributed database. Through consensus algorithms, it maintains information consistency and facilitates system coordination without centralized control [2].

Achieving the full potential of Web 3.0 necessitates the integration of compatible consensus mechanisms [3]. In light of network scalability, Delegated Proof-of-Stake (DPoS), originally proposed by Dan Larimer [4], emerges as a suitable governance consensus mechanism. DPoS enables stakeholders to vote for delegate representatives responsible for block production and validation, addressing issues such as resource waste and centralization observed in Proof of Work (PoW) systems. Additionally, DPoS alleviates the concentration of voting power seen in Proof of Stake (PoS) mechanism. Consequently, DPoS has been widely adopted in various projects, including EOSIO, TRON, Tezos, and Ark.

Decentralization is the cornerstone of Web 3.0, and for this vision to be realized, the consensus mechanism must ensure a sufficiently decentralized governance model. While Delegated Proof of Stake (DPoS) offers a more scalable alternative to traditional PoW or PoS, it faces several critical challenges in the context of Web 3.0: (i) *Low voter participation and incomplete vote allocation:* Research indicates that voter turnout in DPoS systems is often low, with a significant portion of votes left unallocated. This lack of engagement creates vulnerabilities for malicious actors to manipulate the system and potentially seize control of the platform [5]. (ii) *Centralization of voting power due to stake dependence:* DPoS mechanisms typically tie voting power directly to stake holdings, resulting in a disproportionate influence of high-stakes voters. This dynamic can lead to the formation of monopolistic alliances among major stakeholders, threatening the network's decentralization and integrity. (iii) *Lack of rotation among delegate committee members:* Delegate committee members often remain in power for extended periods due to infrequent rotations. This concentration of block production authority in the hands of a few delegates diminishes overall decentralization and risks creating centralized points of failure [6].

Given the above challenges, traditional DPoS mechanisms struggle to meet Web 3.0's demands for decentralized, participatory, and trustless systems. Attempts to enhance DPoS often introduce additional complexity but fail to address these fundamental issues effectively.This paper begins by modeling the reward settlement phase, refining the framework of coin-based voting governance, and formalizing the processes of voting power distribution, vote counting, and reward settlement. We then present a Quadratic Voting-based DPoS, referred to as Q-DPoS. Initially, Quadratic Voting [7] is employed to improve the voting distribution process, followed by the integration of admission rules and similarity detection mechanisms to establish a comprehensive Q-DPoS consensus mechanism. Simulation results demonstrate that our Q-DPoS enhances voter participation while more effectively addressing stake centralization issues compared to traditional linear reward schemes. Moreover, theoretical analysis indicates its ability to broaden the spectrum of voting preferences, further highlighting its efficacy.

The major contributions of this paper are summarized as follows:

- *Coin-based voting governance:* By adding a reward settlement phase, we extend the coin-based three-stage voting governance [5] to four stages. To the best of our knowledge, it is the first attempt to model the reward settlement phase.
- *A novel Q-DPoS consensus:* Initially, we introduce Quadratic Voting into DPoS and redesign the consensus process rules to enhance voter engagement and stakes decentralization. Subsequently, by incorporating admission rules and similarity detection into the designed process, we propose a comprehensive Q-DPoS mechanism.
- *Simulation and analysis:* Simulation results demonstrate the efficacy of our Q-DPoS in enhancing decentralization, whereas theoretical analysis grounded in game theory indicates its effectiveness in fostering greater diversity in voting preferences.

The remaining portions of this paper are summarized below. Section 2. provides a brief review of related literature. Section 3. elucidates the coin-based voting governance system; Section 4. outlines the proposed scheme in detail; Section 5. presents a simulation and analysis of our Q-DPoS scheme; and finally, Section 6. offers concluding remarks.

2. Related work

2.1. Improvements to the voting and incentive processes

Reputation-Based Approaches: Numerous studies aim to enhance the security and efficiency of the DPoS mechanism through the refinement of its voting protocols. Chen *et al.* [8] proposed a reputation-based voting model that improves the DPoS consensus mechanism by increasing node incentives and operational efficiency, applying this model to a network opinion collaborative governance framework. Sun *et al.* [9] integrated stake voting with trust values to create evaluation criteria that reduce the risks of collusion attacks, similar reputation-based approaches have been explored by Song *et al.* [10] and Hu *et al.* [11]. Furthermore, Bing *et al.* [12] developed a weighted voting mechanism based on k-shell-calculated credit values to improve delegate selection, thus improving node incentives and system fairness. Wang *et al.* [13] introduced block producer weights to more accurately assess producer contributions.

Game-Theoretic Perspectives: Other research efforts have focused on improving DPoS from a game-theoretic perspective. Zhang *et al.* [14] established a voting incentive mechanism aimed at encouraging token holders' participation in consensus processes. Wei *et al.* [15] proposed a game-theoretic reward and punishment mechanism to boost node voting enthusiasm. Tong *et al.* [16] proposed the Ta-DPoS consensus algorithm, which introduces a reputation model and a reputation reward and punishment mechanism based on dynamic games to enhance the reliability and fairness of nodes while strengthening the supervision of node behavior.

Mathematical and Novel Approaches: A subset of studies is dedicated to enhancing the decentralization of the DPoS mechanism. Mišić *et al.* [17] introduced the concept of virtual risk to guide delegate elections. Xu *et al.* [18] incorporated approval, disapproval, and abstention votes into the DPoS mechanism, utilizing fuzzy sets to address tie votes among delegates. Liu *et al.* [19] proposed a decentralization method that employs adjacency voting and average fuzziness based on fuzzy values. Luo *et al.* [20] integrated an improved a ring-based coordinator election algorithm into the DPoS consensus to uphold system fairness. Liu *et al.* [21] utilized the K-means algorithm for candidate node pre-selection, thereby enhancing DPoS decentralization and reducing the likelihood of malicious node selection. Li *et al.* [22] proposed the HL-DPoS consensus algorithm, which leverages verifiable random functions for node sharding, introduces a longest chain verification mechanism to mitigate long-range attacks, and enhances security by reducing centralization and malicious behaviors in witness node selection.

2.2. Improvements to the entire mechanism

Moreover, some research has focused on redesigning the entire DPoS mechanism to enhance efficiency and fault tolerance. Yang *et al.* [23] introduced a proof-of-work competition for the formation of DPoS agent candidates and proposed a degradation mechanism for the swift replacement of malicious nodes. Wang *et al.* [24] designed block generation and validation tasks to be executed by nodes using enhanced proof-of-probability and delegated proof-of-stake consensus algorithms. Bachani *et al.* [25] developed a dual-layer DPoS consensus model to achieve high throughput and scalability. Hu *et al.* [26] proposed a consensus mechanism called High-Quality Delegated Proof of Stake (HQ-DPoS), which integrates an improved Practical Byzantine Fault Tolerance (PBFT) algorithm into DPoS block validation to significantly enhance its security.

Despite these individual efforts to improve DPoS, these approaches often exhibit complex logic and tend to fall short of addressing the simultaneous challenges of low decentralization and low voter engagement. Unlike previous methods, our work focuses on two critical aspects: (i) simultaneously mitigating the centralization of stake distribution and enhancing voter participation, (ii) achieving these improvements without relying on cryptographic complexities or introducing significant overhead to the system. By redesigning the governance and consensus processes with a practical, lightweight approach, our method provides a feasible pathway to a more decentralized and participatory DPoS mechanism.

3. Coin-based voting governance in Web 3.0

In this section, we introduce a coin-based voting governance model [27], which comprises the staking/unstaking phase, voting power distribution, the formation of a proxy committee to govern the community, and the reward settlement. The reward settlement phase includes two typical approaches: rewarding only block producers and distributing rewards linearly to voters based on the number of valid votes they cast. The linear reward scheme, in particular, serves as a baseline for comparison in this study, highlighting the effectiveness of our proposed enhancements. Let $V = \{v_1, v_2, ..., v_m\}$ denote the set of voters; $C = \{c_1, c_2, ..., c_n\}$ the set of candidates; and $W = \{w_1, w_2, ..., w_k\}$ the set of proxy committees. Each stage will now be elaborated in detail:

Table 1. Summary of notations.

notations	meanings
V	The set of voters
m	The number of voters
C	The set of candidates
n	The number of candidates
W	The set of proxy committees
k	The number of proxy committees
$Coin$	The staked coin sets of voters
P	The voting power sets of voters
P_i	The voting power of voter v_i
p_{ij}	The voting power from voter v_i to candidate c_j
$S(S^{-1})$	The (inverse) conversion rules of coins to voting power
λ	The conversion rate of coins(stake) to voting power
F_i	The set of preferred candidates by voter v_i
$Votes$	The total votes received by candidates
$Votes_j$	The total votes received by candidate c_j
W'	The set of successful block producers in proxy committee
R	The fixed reward for each successful block
$Reward$	The set of rewards
α	The proportion of rewards allocated to block producers
Rp_j	Rewards for successful block producers
Rv_i	Rewards for voter v_i

3.1. Staking/Unstaking phase

In the coin staking phase, the input consists of the staked coin set $Coin$ corresponding to the stakes, and the output comprises the voting power set P. Here, $Coin = \{coin_1, coin_2, ..., coin_m\}$ represents the quantities of coins staked by m voters, while $P = \{P_1, P_2, ..., P_m\}$ denotes the transformed voting power of the m voters. The conversion process is defined by $P_i = S(coin_i, \lambda)$, where λ denotes the conversion rate of coins to voting power, and S describes the rules of conversion from coins to voting power. Once staked, coins cannot be withdrawn for a certain period.

After the staking period, voters can convert their voting power back to coins. The conversion rule is expressed as $coin_i = S^{-1}(P_i, \lambda)$, where S^{-1} denotes the rule for converting voting power back to coins. Through staking and unstaking, dynamic changes in the voting power of voters are realized.

3.2. Voting power distribution

In this phase, given the sets of voters and candidates (V, C) along with the voting power set P of voters, the output is the set of proxies W, where $W \subseteq C$ and $|W| = k$, indicating that the proxy committee is selected from the top k candidates with the highest number of votes [28].

In the cumulative voting scheme, each voter v_i distributes his voting power P_i. Let $F_i \subseteq C$ represent the set of preferred candidates by voter v_i, $c_j \in F_i$ denotes that voter v_i votes for candidate c_j, and p_{ij} represents the voting power allocated from voter v_i to candidate c_j. The distribution of voting power satisfies $P_i = \{p_{ij} | c_j \in F_i, \sum_j p_{ij} \leq P_i\}$. When a voter exhausts all their votes, the distribution rule is expressed as:

$$P_i = \sum_{c_j \in F_i} p_{ij} \tag{1}$$

For each candidate c_j, the voting power received from all voters is aggregated, and the vote counting rule is expressed as:

$$Votes_j = \sum_{v_i \in V} |\{c_j\} \cap F_i| \cdot p_{ij} \tag{2}$$

where $|\{c_j\} \cap F_i|$ equals 1 if $c_j \in F_i$ and 0 otherwise, indicating whether voter v_i votes for candidate c_j. Through the aforementioned vote-counting rule, the candidate set C obtains the received votes set $Votes = \{Votes_j | c_j \in C\}$, based on which candidates are then ranked, and the top k candidates are selected to form the proxy committee.

3.3. Undertake governance responsibilities

After the establishment of the proxy committee, the selected k proxies assume governance roles within the community. Proposals are deemed effective only upon receiving approval from at least $\frac{2}{3}k+1$ of the proxies.

3.4. Reward settlement

3.4.1. Reward scheme for successful block producers

Following the conclusion of consensus, the reward settlement phase commences. In the original DPoS consensus, only block producers who successfully produce blocks are eligible for rewards. The input set $\{W', R\}$ is provided, where $W' \subseteq W$ denotes the set of successful block producers in the proxy committee, and R represents the fixed reward for each successful block. The output comprises the reward set *Reward*, where $Reward = \{Reward_j | c_j \in W'\}$, with each $Reward_j$ equal to R.

3.4.2. Linear reward scheme with voter incentives

The linear reward scheme is a method of reward distribution adopted by some DPoS platforms, such as TRON. In the scheme, The input set $\{W', P, R, \alpha\}$ is provided, yielding the reward set *Reward*. Here, α determines the proportion of rewards allocated to block producers, with $(1-\alpha)$ designated for voter incentives. For successful block producers, their rewards are calculated as $Rp_j = \alpha \cdot R$. For voters who support these block producers, their total potential voting rewards amount to $(1-\alpha) \cdot R$. Voters, represented by v_i, share the voting rewards based on their proportional voting contribution to the respective block producer. The total voting reward for voter v_i is calculated as:

$$Rv_i = \sum_{c_j \in W'} \frac{(1-\alpha)R \cdot |\{c_j\} \cap F_i| \cdot p_{ij}}{\sum_{v_i \in V} |\{c_j\} \cap F_i| \cdot p_{ij}} \tag{3}$$

The output reward set encompasses both voter incentives and rewards for successful block producers, expressed as $Reward = \{Rv_i, Rp_j | c_j \in W', v_i \in V\}$.

4. Proposed scheme

To enhance the decentralization of the DPoS system, increase voter participation, and alleviate disparities in stake distribution, we propose the Q-DPoS scheme. The entire workflow unfolds as Figure 1: Ordinary users transition into voters following the successful completion of the admission rules. Upon staking their stake(coin) and acquiring voting power, voters distribute their voting power and participate in voting elections for candidates. After eliminating similar votes from unchecked votes, the system proceeds to the vote-counting phase. With the vote-counting rule, members of the proxy committee are elected. Subsequently, they engage in block-producing consensus operations. Following the conclusion of the consensus, rewards are allocated to voters and successfully block-producing proxies based on relevant

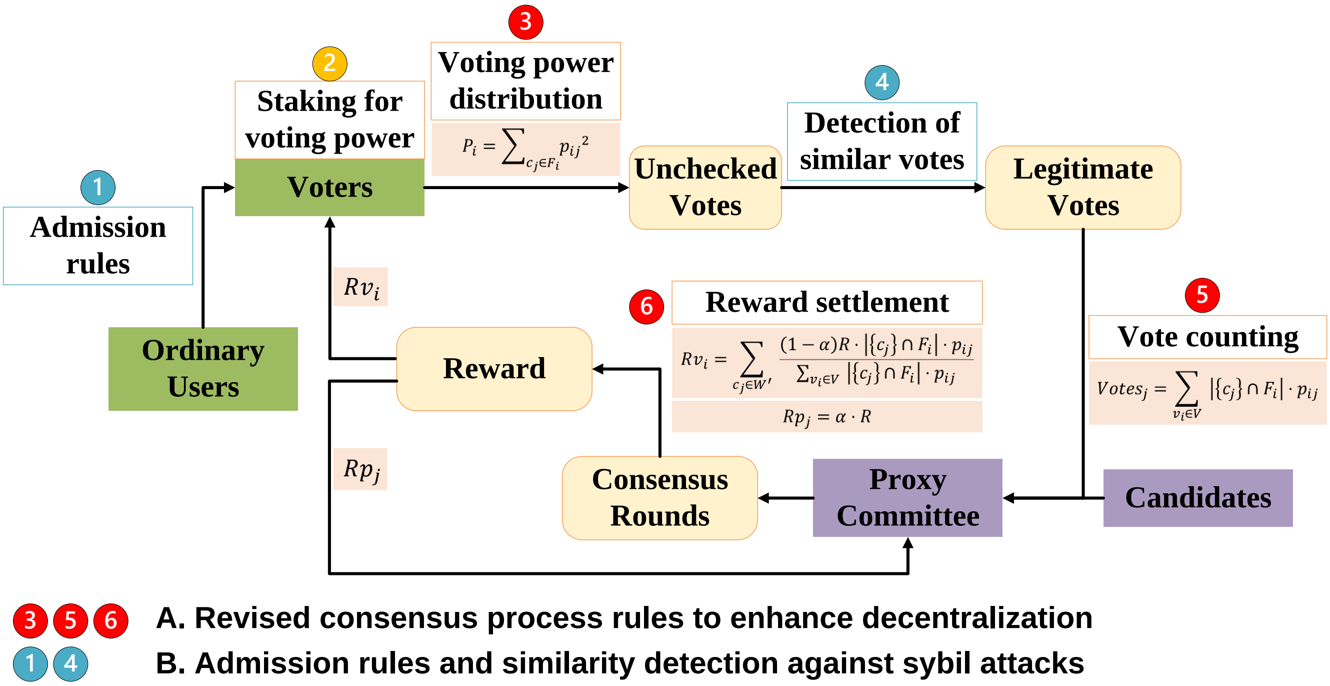

Figure 1. The Workflow of Q-DPoS (Steps 2, 3, 5, and 6 represent the original workflow of DPoS in Web 3.0. We have revised rules 3, 5, and 6. Additionally, to prevent Sybil Attacks from disrupting the rules, steps 1 and 4 have been introduced to form the complete Q-DPoS scheme.).

criteria.

In the above steps, the distribution of voting power, vote counting, and reward settlement represent revised consensus process rules to enhance decentralization, which is depicted in Section 4.1., however, stability are susceptible to Sybil Attacks. Therefore, we introduce admission rules and similar vote detection to refine the process above, which is discussed in Section 4.2. By integrating these steps, the comprehensive design of the Q-DPoS scheme is accomplished.

4.1. Revised consensus process rules to enhance decentralization

Given the challenges of stake concentration and insufficient voter engagement in conventional DPoS, This section will first analyze the issues present in the linear reward scheme. Subsequently, it will propose enhancements aimed at resolving these issues.

4.1.1. Issues within linear reward mechanism

In the preceding section, equations (1), (2), and (3) respectively provided formalized descriptions of the voting power distribution, candidate tally, and linear reward settlement for voters. However, under this linear reward scheme, there is a tendency for wealth disparities within the community to widen during the process of voting rewards allocation.

Given the visibility of candidates' historical block production success rates, two strategies emerge during the voting process. Stability strategy: Voters opt for candidates with consistently high success rates in block production, aiming for stable returns. Risky strategy: Voters support candidates with slightly lower success rates, anticipating potentially higher but volatile returns if elected.

In the stability strategy, rewards per vote remain low due to vote concentration on one block producer. Rewards are proportional to votes cast for a successful producer, favoring high-stakes voters. Conversely, the risky strategy offers higher rewards per vote but carries risks of candidate failure. High-stakes voters may pursue stable returns through the Stability Strategy while investing smaller stakes in speculative candidates. However, low-stakes voters risk no returns if their candidates fail. Both strategies disadvantage low-stakes voters, discouraging their active participation and potentially leading to the rise of plutocracy as high-stakes voters gain more influence.

4.1.2. Improvements in vote counting and reward settlement

This section will cover multiple aspects. It will discuss the modification of the reward rule, the modification of the vote-counting rule, and the redefinition of the rules with Quadratic Voting.

Within Equation (3), the direct linear relationship between voter reward weight and voting power proportion may exacerbate wealth accumulation among high stakeholders. To address this issue, we first attempt to modify the voter reward rule as follows:

$$Rv_i = \sum_{c_j \in W'} \frac{(1-\alpha)R \cdot |c_j \cap F_i| \cdot f(p_{ij})}{\sum_{v_i \in V} |c_j \cap F_i| \cdot f(p_{ij})} \tag{4}$$

where $f(p_{ij})$ represents the weight conversion formula from voting power to reward calculation. Our objective is to adhere to the principle of rewarding high-stakes voters more generously while increasing the proportion of low-stakes voters in the reward distribution. (i.e., the proportion of rewards for low-stakes voters should be higher than that in the linear scheme).

Theorem 1 *The condition that $f(p_{ij})$ is a concave function is a sufficient condition for the aforementioned objective.*

Proof of Theorem 1: Due to the absence of voting power leading to no reward settlement, the reward being positive, and the principle of rewarding high-stakeholders more generously, the function $f(p_{ij})$ must satisfy $f(0) = 0$, $f(x) \geq 0$, and $\frac{f(x_2)-f(x_1)}{x_2-x_1} \geq 0$. $f(p_{ij})$ being concave means it satisfies, for any $0 < \theta < 1$, $f(\theta x_2 + (1-\theta)x_1) \geq \theta f(x_2) + (1-\theta)f(x_1)$. In the linear reward scheme, with p_{1j} and p_{2j} representing the voting powers of two voters who respectively allocate their voting powers p_{1j} and p_{2j} to the same successful block producer c_j, and satisfying $p_{1j} \leq p_{2j}$, according to Equation (3), the ratio of rewards that the two voters respectively receive is $p_{1j} : p_{2j}$. Meanwhile, under Equation (4), the ratio of rewards they respectively receive is $f(p_{1j}) : f(p_{2j})$. To prove that $f(p_{ij})$ is a concave function, demonstrating that low-stakes voters have a higher proportion of benefits compared to the linear scheme, it suffices to establish that under $f(0) = 0$, $f(x) \geq 0$, $0 < \theta < 1$, and $f(\theta x_2 + (1-\theta)x_1) \geq \theta f(x_2) + (1-\theta)f(x_1)$, if $p_{1j} \leq p_{2j}$, then $f(p_{1j}) : f(p_{2j}) \geq p_{1j} : p_{2j}$.

$$f(\theta x_2 + (1-\theta)x_1) \geq \theta f(x_2) + (1-\theta)f(x_1)$$
$$f(x_1 + \theta(x_2 - x_1)) \geq \theta(f(x_2) - f(x_1)) + f(x_1)$$
$$f(x_1 + \theta(x_2 - x_1)) - f(x_1) \geq \theta(f(x_2) - f(x_1))$$
$$\frac{f(x_1 + \theta(x_2 - x_1)) - f(x_1)}{\theta} \geq f(x_2) - f(x_1)$$

let $x_2 > x_1$, divide both sides by $x_2 - x_1$:

$$\frac{f(x_1 + \theta(x_2 - x_1)) - f(x_1)}{\theta(x_2 - x_1)} \geq \frac{f(x_2) - f(x_1)}{x_2 - x_1}$$

let $p_{2j} = x_2$, $x_1 = 0$, $p_{1j} = x_1 + \theta(x_2 - x_1) = \theta(x_2 - x_1)$:

$$\frac{f(p_{1j}) - f(0)}{p_{1j}} \geq \frac{f(p_{2j}) - f(0)}{p_{2j}}$$
$$\frac{f(p_{1j})}{f(p_{2j})} \geq \frac{p_{1j}}{p_{2j}}$$

For computational convenience, we adopt the concave function $f(p_{ij}) = \sqrt{p_{ij}}$. Consequently, the reward calculation rule is modified as follows:

$$Rv_i = \sum_{c_j \in W'} \frac{(1-\alpha)R \cdot |\{c_j\} \cap F_i| \cdot \sqrt{p_{ij}}}{\sum_{v_i \in V} |\{c_j\} \cap F_i| \cdot \sqrt{p_{ij}}} \tag{5}$$

We've revised the reward rule for low-stakes voters. While higher-powered votes still yield greater rewards, the rate of reward weight growth is slower compared to the original linear reward scheme. This helps bridge the gap in voting rewards between high and low-stakes voters, encouraging more active participation from low-stakes voters.

However, relying solely on reward incentives may lack power incentives from the voter's perspective. In the election of the proxy committee, the vote counting process (Equation 2) still follows a linear votes-based approach, heavily influenced by high-stakeholders, diminishing the impact of low-stakes voters despite their numbers. This could dampen the enthusiasm of low-stakes voters to participate in system governance.

To strengthen the voice of low-stakes voters and promote their active participation, we further modify the vote counting method in (2) as follows:

$$Votes_j = \sum_{v_i \in V} |\{c_j\} \cap F_i| \cdot \sqrt{p_{ij}} \tag{6}$$

The reward settlement remains as per Equation (5). At this point, both from the perspective of reward settlement and voting influence, the system demonstrates friendliness toward low-stakes voters. Consequently, the overall process becomes:

$$\begin{cases} P_i = \sum_{c_j \in F_i} p_{ij} \\ Votes_j = \sum_{v_i \in V} |\{c_j\} \cap F_i| \cdot \sqrt{p_{ij}} \\ Rv_i = \sum_{c_j \in W'} \frac{(1-\alpha)R \cdot |\{c_j\} \cap F_i| \cdot \sqrt{p_{ij}}}{\sum_{v_i \in V} |\{c_j\} \cap F_i| \cdot \sqrt{p_{ij}}} \end{cases} \tag{7}$$

For ease of tallying, we perform variable substitutions in Equation (7), rewriting it as:

$$\begin{cases} P_i = \sum_{c_j \in F_i} {p_{ij}}^2 \\ Votes_j = \sum_{v_i \in V} |\{c_j\} \cap F_i| \cdot p_{ij} \\ Rv_i = \sum_{c_j \in W'} \frac{(1-\alpha)R \cdot |\{c_j\} \cap F_i| \cdot p_{ij}}{\sum_{v_i \in V} |\{c_j\} \cap F_i| \cdot p_{ij}} \end{cases} \tag{8}$$

It appears that we have merely introduced Quadratic Voting into the process of voting power distribution, yet its effect aligns with the enhancement of both the vote counting and reward rules as outlined in Equation (7). In both vote counting and rewarding, the process relatively increases the voting power and reward of the low-stakes, thereby enhancing their participation in system governance.

4.2. Admission rules and similarity detection against Sybil Attacks

Algorithm 1 Clustering Detection for Voting Behaviors [6]

Input: The set of voters V, voting records of voters $Records$, selected threshold θ
Output: A set of voter clusters with similar voting behaviors $Cluster$

```
visited = ∅
Cluster = ∅
for voter v_i in V − visited do
    add v_i to visited
    C_i = {V_i}
    N_θ = {v ∈ V | v ≠ v_i and Similarity(R(v), R(v_i)) ≤ θ}
    for voter v_j in N_θ do
        N'_θ = N_θ
        if v_j not in visited then
            add v_j to visited
            add v_j to C_i
            for voter v_k ∈ N'_θ do
                add v_k to N_θ
            end for
        end if
    end for
    if len(C_i)! = 1 then
        add C_i to Cluster
    end if
end for
```

The revised rules in the preceding section are designed to incentivize low-stakes voters' participation by increasing their power and reward. However, the implementation of these rules varies depending on the type of blockchain system. In permissioned chains, where voter identities and accounts are generally verified and controlled, the risk of certain attacks, such as account proliferation, is mitigated by design. In contrast, permissionless chains, such as public blockchains, are inherently open and decentralized, making them more susceptible to Sybil Attacks [29, 30].

Without any safeguards in place, high-stakes voters on a permissionless chain could exploit their original high stakes by creating multiple low-stakes accounts, thereby compromising or invalidating the rules designed in this paper. Under extreme conditions, when a high-stakes voter allocates all their voting power P_i to a single candidate, the candidate receives actual votes equal to $\sqrt{P_i}$ according to the Quadratic Voting rule. However, suppose the voter creates $|P_i|$ accounts, each with a stake of 1, voting for the same candidate. In that case, each account's voting power of 1 translates into actual votes of 1, resulting in the candidate receiving $|P_i| \cdot 1 = P_i$ actual votes. Consequently, this strategy undermines the Quadratic Voting rule by converting it into a conventional linear reward scheme.

As a result, the advantage of incentivizing low-stakes voters to increase their participation is lost. Similarly, when high-stakes voters have multiple candidates in their voting intention set F_i, a comparable effect can be achieved by creating multiple accounts. This method of exploiting system vulnerabilities by creating multiple accounts is referred to as Sybil Attacks.

To address these vulnerabilities, particularly in permissionless chains, two defensive measures are proposed: admission rules for voters and similarity vote detection. These measures are designed to safeguard the integrity of the voting process without introducing significant operational overhead, ensuring that the incentivization mechanisms remain effective across different blockchain environments.

The admission rules serve as a preliminary account screening step before voting occurs. Setting the threshold for becoming a voter, increases the cost for high-stake users to create multiple accounts. Similar vote detection, on the other hand, is a post-voting detection step. Initially, it partitions users' historical voting records by time. Subsequently, within each time partition, it employs the similarity algorithm proposed in the article [6] to detect voters engaging in similar voting behaviors. Finally, based on the detection results, the current voting outcomes are purged. Together, these two steps convert unchecked votes into legitimate ones, combined with rule designs from the preceding section, forming the Q-DPoS.

5. Simulation and analysis

To explore the impacts of the Q-DPoS consensus mechanism, we undertook simulations comparing our proposed scheme with a linear reward system. We aimed to analyze the fluctuations in stake distribution and the involvement of lower-stakes voters in the voting process.

5.1. Theoretical analysis of single-round rewards

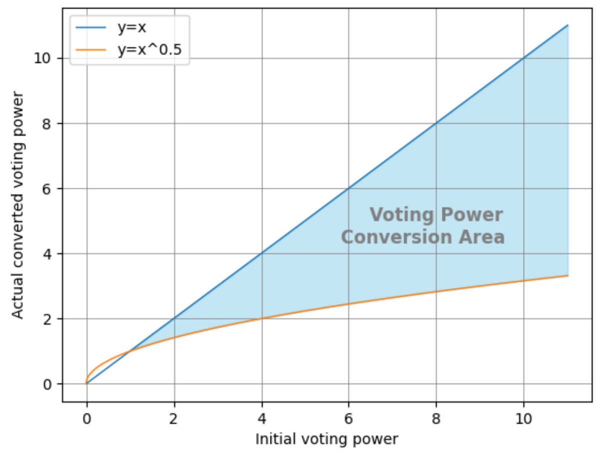

Figure 2. Voting power conversion.

We analyze Single-round reward variation from two perspectives. From the perspective of individual voters, the voting power-to-real votes conversion rate is dynamic in the improved scheme. When voter distributes his voting power to one candidate ($|F_i| = 1$), according to the Quadratic Voting conversion rule,it transforms to true votes $\sqrt{P_i}$, with a conversion rate of $\frac{1}{\sqrt{P_i}}$. When distributes to $|P_i|$ candidates, it transforms to $|P_i| \cdot 1 = P_i$, with a conversion rate of 1. Under a certain initial stake(coin), the larger the voter's preference set F_i, the higher the conversion rate. The converted voting power is tied to rewards, incentivizing rational voters to expand their preference set F_i as extensively as possible. Consequently, the conversion rate will fall within an intermediate range as depicted in Figure 2. Expanding the preference set F_i enhances system variability and may even alter the current state of overly fixed committee members. Additionally, in cases of bribery, voters tend to allocate all their voting power P_i to the bribing party. In our scheme, due to the low conversion rate when $|F_i| = 1$, the bribing party would need to pay more for the same votes, and voters would exercise greater caution towards bribery. From the perspective of different voters with initial stake(coin) ratios of $b : 1$, when their preference sets F_i consist of only one candidate, who then succeeds in the election and block production. In a linear reward scheme following $y = x$, the voting power ratios and reward distribution ratios of the voters remain as $b : 1$. In the improved voting scheme following $y = \sqrt{x}$, their voting power ratios and reward distributions are $\sqrt{b} : 1$. More often, since $|F_i| \neq 1$, the voting power ratios and reward distribution ratios will lie between $b : 1$ and $\sqrt{b} : 1$. When the preference set is certain, the voting power conversion rate of low-stakes voters tends to be higher than that of high-stakes, and flexible strategies can be exerted to increase both power and rewards.

5.2. Simulation of stakes and enthusiasm variation

To study the evolution of stake and engagement of different stakeholders under various schemes, we conducted multi-round iterative simulations with both the linear scheme and the proposed scheme.

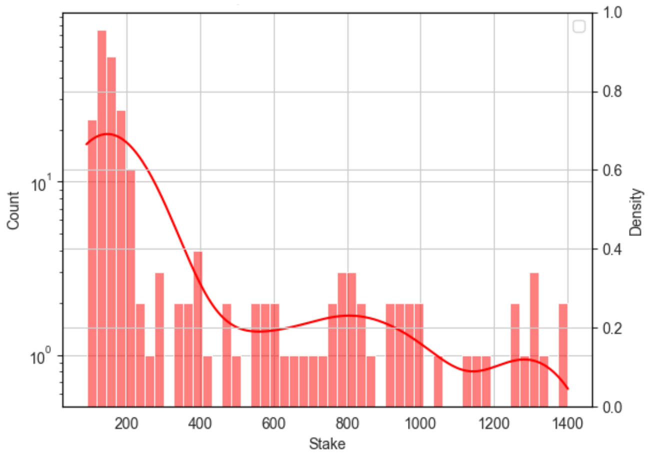

Figure 3. Stakes distribution in quadratic reward mechanism after 150 rounds.

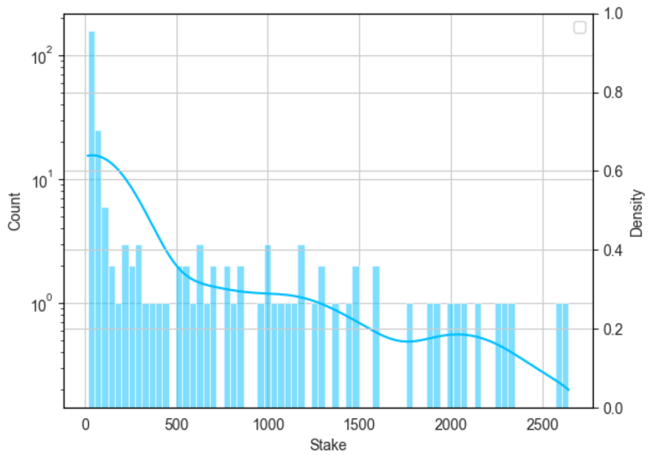

Figure 4. stakes distribution in linear reward mechanism after 150 rounds.

Assuming a constant voting cost for voters, we set up 100 voters with initial stakes following a power-law distribution $y \sim x^{-1.98}$. After multiple voting rounds, the stakes distribution between the two schemes is shown in Figure 3 and 4. The scope of stakes distribution and the number gap between different stakeholders are effectively reduced.

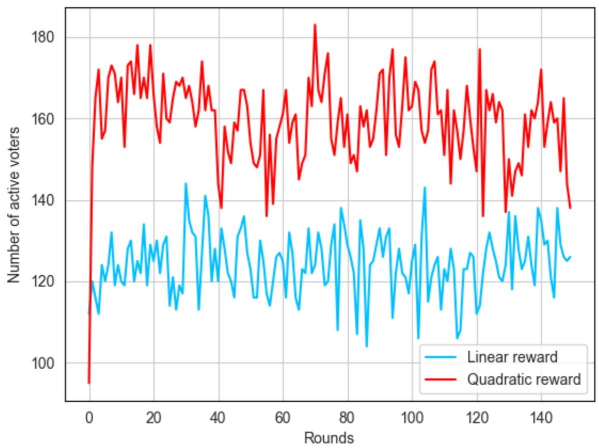

Figure 5. The variation of active voters.

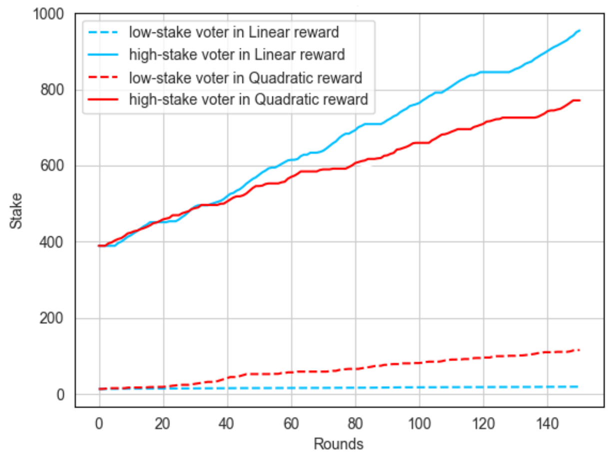

Figure 6. The stake variation of high-low stake voters.

Additionally, the graphical representation in Figure 5 delineates the contrast in the number of engaged voters between the two schemes, there is a stronger inclination for voters' participation. Also, We tracked the perspective of high and low-stakes voters, and the changes in their stakes are shown in the figures 6 for both scenarios. The stake gap between different voters is increasing in the linear scheme, while our scheme can alleviate it.

5.3. Theoretical analysis on game theory

In reality, the probability of successful block generation varies among candidates and the vote preference is dynamic. Voting strategies of different voters constitute a game process. In the early stages of the system, due to limited knowledge about the successful block generation probabilities of different candidates, a potential optimal strategy is to vote for as many candidates as possible. As the system evolves and understanding of candidates' block generation success rates improves, voters will weigh the balance between voting for candidates with high block generation success rates and voting for as many candidates as possible. In the later stages of system evolution, since the reward for the same successful block remains constant, voters will, on one hand, continue to vote for candidates with high winning and block generation rates, and on the other hand, vote for candidates close to winning positions to obtain a higher ratio of successful block rewards. This choice of strategy may lead to changes in the composition of the electoral committee, thereby increasing the decentralization of the system to a certain extent.

6. Conclusion

To adapt to the high decentralization of Web 3.0 and boost user participation, this paper proposes a novel consensus scheme, named Q-DPoS. Firstly, Quadratic Voting is introduced into the DPoS consensus mechanism. Subsequently, a vote similarity detection step is integrated, thereby creating a comprehensive Q-DPoS. Simulation results show that Q-DPoS effectively mitigates stake concentration, stimulates voter engagement, and promotes decentralization. While this approach offers novel perspectives on Web 3.0, subjective and rational factors were not taken into account in the simulation results, and the evolutionary trajectory of voter behavior remains exploratory. Subsequent research endeavors could center on achieving a more comprehensive understanding of the strategies employed and the systemic evolution involved.

Acknowledgment

This work was supported in part by the Beijing Advanced Innovation Center for Future Blockchain and Privacy Computing Postdoctoral Innovation Foundation; in part by National Key R&D Program of China under Grant 2022ZD0116800; in part by National Key R&D Program of China under Grant 2021YFB2700303; in part by Program of National Natural Science Foundation of China under Grant 62141605; in part by Beijing Natural Science Foundation under Grant Z230001; in part by the National Natural Science Foundation of China under Grant 62372493; in part by the China Postdoctoral Fellowship Fund 373500; in part by the Beihang Dare to Take Action Plan KG16336101.

Conflicts of interests

The authors declared that they have no conflicts of interests.

Authors'contribution

Conceptualization, L.T.Y.; Methodology, Formal analysis, Software, L.T.Y., Z.Q.N.; Visualization, Investigation, L.T.Y.; Data curation, Software, L.T.Y.; Writing-Original draft preparation, L.T.Y., Z.Q.N., Q.W.J.; Writing-Reviewing and Editing, L.T.Y., Z.Q.N., Q.W.J.; Supervision, Z.Q.N., Q.W.J.; All authors have read and agreed to the published version of the manuscript.

References

[1] Zheng J, Lee DKC. Understanding the Evolution of the Internet: Web 1.0 to Web3. 0, Web3 and Web 3. *Handb. Digit. Curr.* 2024, 553–581.

[2] Belotti M, Božić N, Pujolle G, Secci S. A vademecum on blockchain technologies: When, which, and how. *IEEE Commun. Surv. Tutor.* 2019, 21(4):3796–3838.

[3] Guan C, Ding D, Guo J. Web3. 0: A review and research agenda. In *2022 RIVF international conference on computing and communication technologies (RIVF)*, Ho Chi Minh City, Vietnam, 20–22 December, 2022 pp. 653–658.

[4] Schuh F, Larimer D. Bitshares 2.0: general overview. *Available: http://docs. bitshares.*

org/downloads/bitshares-general. pdf (accessed: June-2017) .
[5] Li C, Palanisamy B, Xu R, Duan L, Liu J, *et al.* How hard is takeover in dpos blockchains? understanding the security of coin-based voting governance. In *Proceedings of the 2023 ACM SIGSAC Conference on Computer and Communications Security*, Copenhagen, Denmark, 26-30 November, 2023 pp. 150–164.
[6] Liu J, Zheng W, Lu D, Wu J, Zheng Z. Understanding the decentralization of DPoS: Perspectives from data-driven analysis on EOSIO. *arXiv* 2022, 2201.06187.
[7] Dimitri N. Quadratic voting in blockchain governance. *Information* 2022, 13(6):305.
[8] Chen Y, Liu F. Improvement of DPoS Consensus Mechanism in Collaborative Governance of Network Public Opinion. In *2021 4th International Conference on Advanced Electronic Materials, Computers and Software Engineering (AEMCSE)*, Changsha, China, 26–28 March, 2021 .
[9] Sun Y, Yan B, Yao Y, Yu J. DT-DPoS: A Delegated Proof of Stake Consensus Algorithm with Dynamic Trust. *Proc. Comput. Sci.* 2021, 187:371–376.
[10] Song M, Li C, Ye J, Gong X, Luo Y. Efficient consensus algorithm based on improved DPoS in UAV-assisted mobile edge computing. *Comput. Commun.* 2023, 86–99.
[11] Hu Q, Yan B, Han Y, Yu J. An Improved Delegated Proof of Stake Consensus Algorithm. *Proc. Comput. Sci.* 2021, 341–346.
[12] Bing W, Hui-ling L, Li P. Optimized DPoS consensus strategy: Credit-weighted comprehensive election. *Ain Shams Eng. J.* 2023, 101874.
[13] Wang Q, Xu M, Li X, Qian H. Revisiting the Fairness and Randomness of Delegated Proof of Stake Consensus Algorithm. In *2020 IEEE Intl Conf on Parallel Distributed Processing with Applications, Big Data Cloud Computing, Sustainable Computing Communications, Social Computing Networking (ISPA/BDCloud/SocialCom/SustainCom)*, Exeter, United Kingdom, 17–19 December, 2020 .
[14] Zhang K, Qiu Z, Chen T, Lin J, Lian Y, *et al.* Research and improvement of blockchain DPoS consensus mechanism. *Int. Conf. Comput. Eng. Netw.* 2022, 1284–1292.
[15] Wei Y, Liang L, Zhou B, Feng X. A Modified Blockchain DPoS Consensus Algorithm Based on Anomaly Detection and Reward-Punishment. In *2021 13th International Conference on Communication Software and Networks (ICCSN)*, Chongqing China, 04–07 June, 2021 pp. 283–288.
[16] Tong S, Li J, Fu W. Improvement of DPos Consensus Algorithm Based on Reputation Authorization. In *2023 China Automation Congress (CAC)*, Chongqing, China, 17–19 November, 2023 pp. 2733–2738.
[17] Mišić J, Mišić VB, Chang X. Toward Decentralization in DPoS Systems: Election, Voting, and Leader Selection Using Virtual Stake. *IEEE Trans. Netw. Serv. Manag.* 2024, 21(2):1777–1790.
[18] Xu G, Liu Y, Khan PW. Improvement of the DPoS Consensus Mechanism in Blockchain Based on Vague Sets. *IEEE Trans. Ind. Inf.* 2020, 16(6):4252–4259.
[19] Liu Y, Xu G. Fixed degree of decentralization DPoS consensus mechanism in blockchain based on adjacency vote and the average fuzziness of vague value. *Comput. Netw.* 2021, 108432.
[20] Luo Y, Chen Y, Chen Q, Liang Q. A New Election Algorithm for DPos Consensus Mechanism in Blockchain. In *2018 7th International Conference on Digital Home (ICDH)*, Guilin, China, 30 November - 01 December 2018 .
[21] Liu W, Li Y, Wang X, Peng Y, She W, *et al.* A donation tracing blockchain model using improved DPoS consensus algorithm. *Peer-to-Peer Netw. Appl.* 2021, 14:2789–2800.
[22] Li Y, Xia C, Li C, Zhao Y, Chen C, *et al.* HL-DPoS: An enhanced anti-long-range attack DPoS algorithm. *Comput. Netw.* 2024, 249:110473.
[23] Yang F, Zhou W, Wu Q, Long R, Xiong NN, *et al.* Delegated Proof of Stake With Downgrade: A Secure and Efficient Blockchain Consensus Algorithm With Downgrade Mechanism. *IEEE Access* 2019, 7:118541–118555.
[24] Wang B, Li Z, Li H. Hybrid Consensus Algorithm Based on Modified Proof-of-Probability and

DPoS. *Futur. Internet* 2020, 12(8):122.

[25] Bachani V, Bhattacharjya A. Preferential Delegated Proof of Stake (PDPoS)—Modified DPoS with Two Layers towards Scalability and Higher TPS. *Symmetry* 2022, 15(1):4.

[26] Hu Q, Chen W, Chen Y. HQDPoS: DPoS-based hybrid consensus mechanism. In *Proceedings of 2021 Chinese Intelligent Systems Conference: Volume II*, Fuzhou, China, 16–17 October, 2022 pp. 716–724.

[27] Li C, Xu R, Duan L. Characterizing Coin-Based Voting Governance in DPoS Blockchains. In *Proceedings of the International AAAI Conference on Web and Social Media*, New York, USA,3–6 June, 2024 pp. 1148–1152.

[28] Li C, Xu R, Duan L. Liquid Democracy in DPoS Blockchains. In *Proceedings of the 5th ACM International Symposium on Blockchain and Secure Critical Infrastructure*, New York, NY, USA, 2023 pp. 25–33.

[29] Platt M, McBurney P. Sybil in the Haystack: A Comprehensive Review of Blockchain Consensus Mechanisms in Search of Strong Sybil Attack Resistance. *Algorithms* 2023, 16(1).

[30] Platt M, Platt D, McBurney P. Sybil attack vulnerability trilemma. *Int. J. Parallel Emerg. Distrib. Syst.* 2024, 39(4):446–460.