PQV: Fully Decentralized Sybil-Resistant Quadratic Voting with Probability

D3LAB[*]
d3lab.dao@gmail.com

Figure 1. D3LAB logo, 2022.

Abstract

DAO (Decentralized Autonomous Organization) has emerged as an innovative way of building community organizations in Web3. Current centralized organization can only reflect opinions of top managements, however in the new DAO based governance, many of stakeholders can participate in the decision making process based on smart contract.

Already DAO voting platforms like snapshot[9], Tally[10] are helping more people to build improved community. The key for building successful DAO is making a fair governance system, which makes many of community members make their voices and lead the group to the better direction.

Our Probabilistic Quadratic Voting (PQV) is going to enhance Web3 ecosystem by stabilizing voting environment and make decision making process fairer[6, 7].

Keywords: governance, quadratic voting, Sybil attack

1 Introduction

Voting system has evolved to coordinate communities in better way. Quadratic Voting[5] seemed to more fairly accept the opinion of the majority. However, Sybil attack vulnerability has revealed.

We suggests new Sybil-resistant quadratic voting system, named PQV, to mitigate Sybil attack. By adding probabilistic factor to the existing system, PQV made the Sybil attack situation less profitable for attackers. To the best of our knowledge, PQV is the first Sybil-resistant quadratic voting system without harming decentralization.

In addition, we releases **Governor C** smart contract as an open source, which is a fully decentralized Sybil-resistant quadratic voting system based on PQV and Chainlink VRF[1]. Web 3 pioneers who want to apply better governance system based on PQV can easily use this contract. As more people use PQV, the DAO ecosystem will become more mature.

PQV contributes to the DAO ecosystem by (1) providing healthier voting system through (2) releasing PQV contract, named **Governor C**, as an open source.

The next section describes the background of voting systems and explains deeply on what problem PQV wants to solve. Section 3 provides mathematical explanation on PQV, and finally, Section 4 introduce **Governor C** with its development guide.

2 Background

The key of building successful DAO is fair governance system, and improved voting system can support it. From one-person-one-vote (1P1V) to quadratic voting (QV), voting system has evolved to provide a better decision-making environment. PQV will create a new paradigm by making up for the shortcomings of existing methods.

2.1 One-Person-One-Vote

One-person-one-vote is the voting system that individuals should have equal power in voting. This has made current democracy and most of the votes follow this principle.

However, one-person-one-vote has a problem that people not interested or unrelated to the agenda also have the equal representation in voting. This can lead to another problem like *Tyranny of the majority*. Moreover, there is no way to

[*] 0x8Ac73BF28226fF63399A6E827790A0c9257051a0 on Ethereum

Table 1. Number and Cost of Each Voting Method

Method	Number of Votes	Cost of Votes
One-Person-One-Vote	1 (immutable)	1
One-Dollar-One-Vote	v	v
Quadratic Voting	v	v^2

express each individual's eagerness in the vote, as same voting power is given to everyone without taking into account the circumstances of each voter.

2.2 One-Dollar-One-Vote

To solve the problem of one-person-one-vote, one-dollar-one-vote appeared as an alternative. Individuals who pay more can have more decision making power. People with high willingness to influence voting result can buy as many votes as possible at the same price per vote. Now, voters deeply involved in the agenda can express their opinions strongly.

However, this principle also has a weakness that the society could be ruled by a few strong individuals with enough assets to support their opinions.

2.3 Quadratic Voting

Quadratic voting can solve the problems of existing methods. In this principle, voters should pay v^2 to make v votes. In one-dollar-one-vote, the cost of votes increased linearly. QV tried to refrain some individuals from exercising excessive influence by making the cost of voting increase exponentially.

To exercise 10 votes of voting power, people had to pay 10 under one-dollar-one-vote principle. But under QV, the cost increases rapidly and individuals should pay $10^2 = 100$. See Table 1 for further information.

In terms of voting methods, QV could be the mathematically optimal system, but it is exposed to risk called 'Sybil attack' that could undermine fairness of whole governance.

2.4 Sybil Attack

Sybil attack is type of network service attack in which an attacker gaining a large influencing power by creating multiple pseudonymous identities. The attacker can act as if there are multiple users. The vulnerability to Sybil attack depends on how easily new identity could be generated, which means Web3 ecosystem is strongly exposed to the danger of Sybil attack. In Web3, most of the accounts are in the form of anonymity and users can cheaply make new identities as many as they want.

Sybil attack can happen very easily in QV. By creating multiple anonymous accounts, several voters with bad intentions can gain disproportionately large influence. QV suppressed the concentration of power by increasing cost of voting sharply. But, user can split their account and pay linearly like one dollar one vote. That is, user pays same amount of money per vote only.

If someone wants to buy 10 votes with one account, he should pay 10^2. However, after making 3 more accounts (total 4 accounts) and spend 25 from each, the person can exercise more voting power ($4 \times \sqrt{25} = 20 > \sqrt{100} = 10$) without additional costs. If 99 more accounts (total 100 accounts) and spend 1 from each, it's the same as one dollar one vote.

2.5 Mitigation Sybil Attack

To mitigate QV, multiple account generation from one person should be prevented, but it is quite difficult to detect and block those actions on blockchain.

Gitcoin[3], which funds Web3 projects based on Quadratic Funding (based on QV) also recognized the danger of Sybil attack. Gitcoin chose to increase cost of attack by making identity verification complicated. By making attackers to put lots of effort into verifying their identities, it minimized the motive to attack. However, it does not fundamentally prevent the Sybil attack. There is a centralization problem in which identity verification is processed outside the blockchain.

The solution beyond relying on third-parties to centrally verify ID is needed. The most reasonable solution is making attackers' Sybil attack very inefficient, so they can voluntarily refrain from attacking. We made voters voluntarily avoid choosing Sybil attack by suggesting new voting method, PQV.

3 Probabilistic Quadratic Voting

Sybil attack is advantageous in QV because the more votes are divided, the more profitable it is. We suggests PQV which applies a probabilistic model so dividing votes always results in a loss.

Assume that the total number of votes (among all users) are 100, and a user submitted 10 votes. There is a 10% ($\frac{10}{100}$) of chance that his opinion will be reflected, or a 90% ($1 - \frac{10}{100}$) chance that it will not. The expected value of voting in this condition is $\sqrt{10} \times 0.1 \approx 0.3162$. However if the user split the 10 votes in two, the expected value lowered to $2 \times \sqrt{5} \times 0.05 \approx 0.2246$. This means doing Sybil attack is less beneficial.

3.1 Sybil Resistancy on PQV

PQV can prove its quality as a new voting system by mathematically proving its Sybil resistancy without (less) harming the result of existing QV.

Assume that total number of votes is N and the number of votes a user has is x. The expected value of votes when x votes are honestly voted at once from one account can be expressed as Equation 1.

$$E_L = \frac{x}{N}\sqrt{x} \tag{1}$$

Table 2. Comparison Between QV and PQV

Method	Reflected Votes	Sybil Attack	Sybil Resistancy
QV	$\sqrt{x}$	$\sqrt{kx}$	X
PQV	$\sqrt{x}$ or 0, E_L	E_R	O

Equation 2 is expected value of votes in a situation when x votes are divided into k to do Sybil attack. p is the number of groups reflected in the vote out of k.

$$E_R = \sum_{p=0}^{k} \binom{k}{p} \left(\frac{x/k}{N}\right)^{p} \left(1 - \frac{x/k}{N}\right)^{k-p} p\sqrt{\frac{x}{k}} \tag{2}$$

In order for a Sybil attack to always less beneficial than an honest vote, the condition of Equation 3 needs to be satisfied. This condition is always satisfied because x, N are not 0 and k is always bigger than 2 to do Sybil attack.

$$E_L > E_R \text{ when } \frac{kN}{x} \neq 0 \vee k > 1 \tag{3}$$

PQV makes it always a loss to do Sybil attack by applying probabilistic element on quadratic voting. Splitting voting power makes the expected value of voting power lower that executing 1 voting power. Therefore, rational users who want to maximize their voting influence will honestly exercise their votes at once by using one account. This means PQV can prevent Sybil attacks. See Table 2 in short.

4 Simulation

The quality of voting result should be maintained while making QV Sybil resistant. Therefore, the result of PQV and QV should be similar. We conducted a simulation experiment to prove similarities between QV and PQV. In the simulation we compared the voting results of three traditional voting methods (one-person-one-vote, one-dollar-one-vote, QV) and PQV.

The result of simulation showed that QV and PQV have high similarities. For the more detailed information about simulation, please visit the Github[8] for implementation details.

4.1 Environment

In order to reflect the real political situation well, the votes were randomly distributed according to Pareto distribution. Applying Pareto distribution can represent the real-world gap between rich and poor.

- Voting participants have random preferences for the candidates they should select.
- The amount of votes distributed to participants is randomly distributed according to a Pareto distribution like Figure 2.

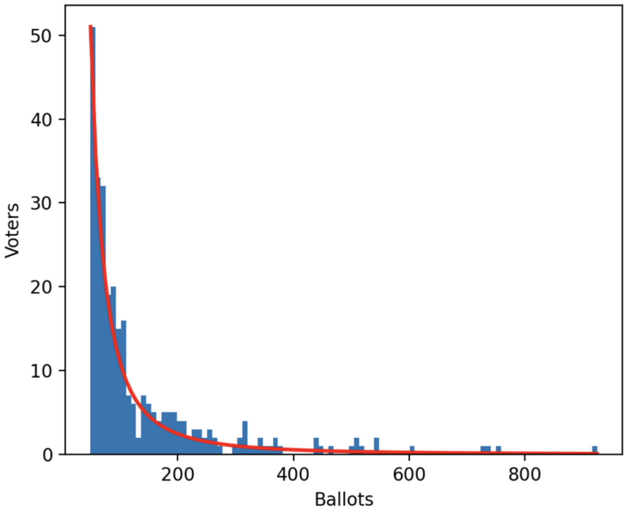

Figure 2. Voting power distribution following Pareto.

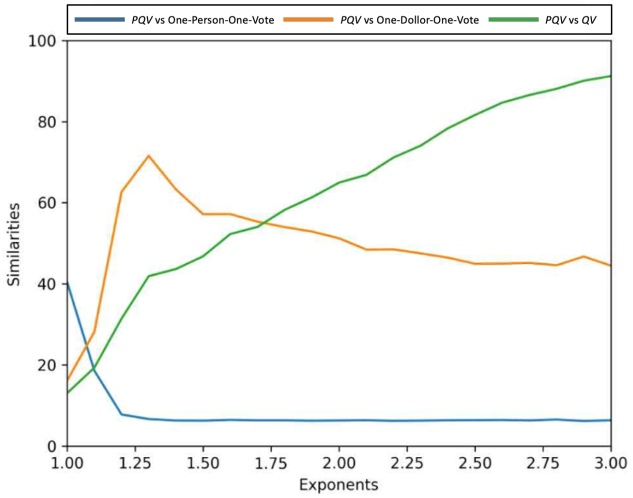

Figure 3. Similarities among voting methods as PQV's probability changes.

If the same candidate is elected under the same conditions, it is assumed that the two voting methods are similar.

We conducted the simulation in 2 stages. (1) Change of similarity according to change of PQV probabilistic element. (2) Changes in similarity according to changes in the number of participants and candidates.

4.2 Similarity according to a Hyperparameter

The experimental parameters are as follows:

- Probabilistic element is x^e/N
- Increase e from 1 to 3 in scale of 0.5
- Fixed variable: the number of participants = 300
- Fixed variable: the number of candidates = 16

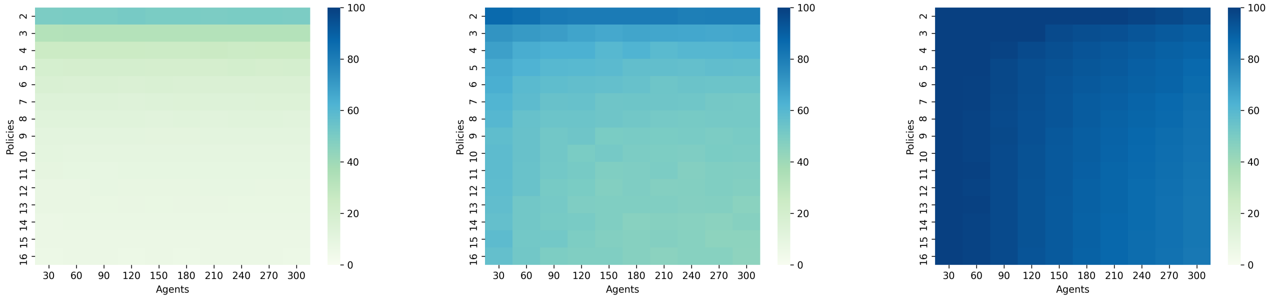

Figure 4. Similarities between PQV and the others.

Figure 3 shows the similarities between couple of different voting systems. PQV and QV tend to become more similar as the probability of a vote e being selected increases. This is because QV is equal to PQV with 100% adoption probability. However, PQV and one-person-one-vote shows low similarity. The similarity converges to 6.25(1/16)%. PQV and one-dollar-one-vote shows 50% of similarity.

4.3 Similarity according to the number of Participants and Candidates

The details about experiment are as follows:

- Fixed variable: probability element is x^2/N ($e = 2$, If the value e is too small, there is a possibility that too many votes may not be reflected)
- Max number of the participants = 300
- Max number of the candidates = 16

Figure 4 shows the similarities between PQV and the other one through heatmap visualization. PQV and one-person-one-vote do not show similarities in most circumstances. The similarity between PQV and one-dollar-one-vote do not exceed 60%. However, PQV and QV show 80% or more similarity in most environments.

5 Governor C

Governor C is the *Solidity* implementation of PQV, fully decentralized Sybil resistant quadratic voting system, based on Chainlink VRF. We are going to release it as open source[4].

5.1 Chainlink VRF

To implement the probability factor of PQV without compromising decentralized manner, we use Chainlink-VRF[1]. The contract receives random number every time user cast a vote and this will make contract more decentralized and cost-efficient.

5.2 Compound Governance Standard

Governor C allows the deployment on-chain voting system using PQV, with respect to Compound's Governor Alpha & Bravo interface[2]. Therefore current DAOs using compound module based on Governor Bravo can easily apply our new solution which is developed under the same standard.

6 Discussions

6.1 PQV on Multi-chain

In this paper, we only treated cases of voting on a single blockchain. To let more users to experience new governance system on various blockchains, PQV should be supported on multi-chain environment.

By using Chainlink CCIP(Cross-Chain Interoperability Protocol) solution, users on various blockchain networks can participate in one vote at the same time. For example, if one of the DAO community using both Polygon and Ethereum, CCIP solution can easily support PQV to run on this scenario.

The easiest way to implement Multi-chain PQV is for all users to bridge their voting tokens to one chain and vote together there. However, users who do not want to use the bridge can vote on their own chain and then collect the total number of votes (N) from all chains through Chainlink CCIP. After the aggregation, we can calculate how each vote will be reflected among the whole chains.

6.2 Gas Optimization

By expanding the above discussion, we can reduce the gas cost required for PQV calculation. Voting on polygon and using the results on Ethereum for instance.

7 Conclusion

This paper introduced a new voting method PQV which imitates the result of QV without worry about Sybil attack. Through simulations, we shows that PQV emulates QV with high similarities in various environments.

The Web3 services can take fairness at voting in a fully decentralized manner using PQV. A **Governor C** smart contract, the open source based on PQV and Chainlink VRF, enables faster implementation for them.

Acknowledgments

We would like to express our gratitude to Chainlink and its community for their continuous interest and supports.

References

[1] Chainlink VRF 2022. *Chainlink VRF.* Retrieved Apr 28, 2022 from https://docs.chain.link/docs/chainlink-vrf

[2] Compound 2022. *Compound Governor Bravo.* Retrieved Apr 28, 2022 from https://compound.finance/docs/governance#governor-bravo

[3] Gitcoin 2022. *Gitcoin.* Retrieved Apr 28, 2022 from https://gitcoin.co

[4] Governor-C 2022. *Governor C: Fully Decentralized Sybil-Resistant Quadratic Voting System.* Retrieved Apr 28, 2022 from https://github.com/D3LAB-DAO/Governor-C

[5] Steven P Lalley and E Glen Weyl. 2018. Quadratic voting: How mechanism design can radicalize democracy. In *AEA Papers and Proceedings*, Vol. 108. 33–37.

[6] Junmo Lee, Sanghyeon Park, and Soo-Mook Moon. 2020. Secure Voting System with Sybil Attack Resistance using Probabilistic Quadratic Voting and Trusted Execution Environment. *Proceedings of the Korean Information Science Society Conference* (2020), 804–806.

[7] Junmo Lee, Sanghyeon Park, and Soo-Mook Moon. 2021. Secure Voting System with Sybil Attack Resistance using Probabilistic Quadratic Voting and Trusted Execution Environments. *KIISE Transactions on Computing Practices* 27, 8 (2021), 382–387.

[8] PQV-simulator 2022. *Probabilistic Quadratic Voting Simulator.* Retrieved Apr 28, 2022 from https://github.com/D3LAB-DAO/PQV-simulator

[9] Snapshot 2022. *Snapshot.* Retrieved Apr 28, 2022 from https://snapshot.org

[10] Tally 2022. *Tally.* Retrieved Apr 28, 2022 from https://www.tally.xyz