information

Article

Quadratic Voting in Blockchain Governance

Nicola Dimitri

Department of Economics and Statistics, University of Siena, 53100 Siena, Italy; dimitri@unisi.it

Abstract: Governance in blockchain platforms is an increasingly important topic. A particular concern related to voting procedures is the formation of dominant positions, which may discourage participation of minorities. A main feature of standard majority voting is that individuals can indicate their preferences but cannot express the intensity of their preferences. This could sometimes be a drawback for minorities who may not have the opportunity to obtain their most desirable outcomes, even when such outcomes are particularly important for them. For this reason a voting method, which in recent years gained visibility, is quadratic voting (QV), which allows voters to manifest both their preferences and the associated intensity. In voting rounds, where in each round users express their preference over binary alternatives, what characterizes QV is that the sum of the squares of the votes allocated by individuals to each round has to be equal to the total number, budget, of available votes. That is, the *cost* associated with a number of votes is given by the square of that number, hence it increases quadratically. In the paper, we discuss QV in proof-of-stake-based blockchain platforms, where a user's monetary stake also represents the budget of votes available in a voting session. Considering the stake as given, the work focuses mostly on a game theoretic approach to determine the optimal allocation of votes across the rounds. We also investigate the possibility of the so-called *Sybil attacks* and discuss how simultaneous versus sequential staking can affect the voting outcomes with QV.

Keywords: quadratic voting; blockchain; proof of stake

Citation: Dimitri, N. Quadratic Voting in Blockchain Governance. *Information* **2022**, *13*, 305. https://doi.org/10.3390/info13060305

Academic Editor: Ge Yu

Received: 11 March 2022
Accepted: 13 June 2022
Published: 19 June 2022

1. Introduction

Governance models of blockchain platforms are becoming increasingly important, as they can meaningfully affect the platform attractiveness and the users' participation. For many blockchains, a main concern related to governance appears to be the possible emergence of dominant positions, that is of subjects who could keep under their control a large number of votes, possibly even the majority of votes, and therefore the platform evolution. Indeed, this may discourage users with small number of votes from participating in governance, perhaps inducing them to drop out of the platform. For this reason, a voting method, which in recent years has gained some attention for social decisions in general, hence also as a possible solution to the above problem in blockchain platforms, is quadratic voting (QV) [1–9] Its interest is additionally testified by an analogous quadratic criterion, which has recently been proposed for project co-funding [10]. In its most common application, represented by a voting session with a list of binary items to vote of the type A/B, QV allows participants to express both the *direction as well as the intensity* of one's preferences as it takes place, for example, with oral acclamation [1–5]. For this reason, unlike the standard 51% majority voting, QV sets up a framework where minority voters, that is those subjects with a limited number of votes, could still have chances to obtain the desirable outcomes for those issues which they care particularly about. Concern for. and protection of, such minorities would clearly make sense when a relatively small number of votes is not due to a user's lack of interest in the voted issues.

The main reason for this to take place is how available votes are considered in a QV session, where a session is composed of a sequence of voting rounds (items). More specifically, the number of votes available to a subject represents her *budget* of votes for the

session, which cannot be lower than the total cost of using the votes in the various rounds. For every round, such cost is assumed to be quadratic in the number of votes chosen for the item, and the total cost of the voting session cannot exceed the total number of available votes. Frequently, in the literature, the cost of voting is indeed expressed in monetary terms, rather than by a number of votes. However, in PoS-blockchain-based platforms, these two interpretations coincide, since the budget of votes is given by the monetary stake.

As an illustration of QV, assume an individual X has $n = 10$ votes available to participate in a voting session with two items under scrutiny. Suppose that in the first item, the decision is between A/B, and in the second item, it is between C/D, where B and D may simply be, respectively, *not A* and *not C*. Moreover, suppose also that X cares more about the first item than about the second item. Therefore, with QV, they could decide to use, for example, 3 votes when voting for the first item and 1 vote when voting for the second item, so that such distribution of votes will satisfy $3^2 + 1^2 = 10$. That is, 10 is the available budget of votes, while $3^2 = 9$ is the *cost* of using 3 votes in the first round and $1^2 = 1$ the cost of using one vote in the second round. Therefore, with QV, the marginal cost of the nth vote is $n^2 - (n-1)^2 = 2n - 1$, which is equal to twice as much the ordinal number of votes minus 1. Hence, for instance, the marginal cost of the first vote is $1^2 - 0^2 = 1$, while the marginal cost of the second vote is $2^2 - 1^2 = 3$ and so on. It follows that the most expensive vote for a user is the marginal (last) one.

Consider now another individual Y, with a total number of votes equal to $n = 4$, hence much less than X, with Y caring about the outcome of the second item only. Then, Y could decide to allocate 0 votes to the first item, basically avoiding voting, and 2 votes to the second item, so that her budget of votes is satisfied, $0^2 + 2^2 = 4$. Therefore, Y may have good chances of affecting the voting outcome of the second item in a way desirable for her. With only two individuals and only two items of the above example, if decisions within each round are taken according to the 51% majority criterion then, with QV, individual Y could guarantee for herself the most desirable voting outcome in the second round.

Instead, if the voting protocol were the standard 51% majority voting, where individuals use all of their votes in each round, then X will secure for herself the best outcome in both items, having 10 votes against 4. This, of course, does not mean that what is desirable for X is necessarily unwanted by Y. Indeed, their preferences may certainly be aligned, in which case the voting protocol would be irrelevant. However, since this is more of an exception than the rule, with QV the user with a lower budget of votes could have a higher chance to obtain the desirable outcome, at least for those items that they care particularly about.

The above numerical example identifies one important point. That is, the timing with which users communicate to the platform how many votes they intend to use in each round can be very important. For example, if voters need to reveal simultaneously, at the very beginning of the voting session, how many votes they want to allocate to each item, then the reasoning in the above example can make sense. However if instead X, for instance, before voting could be allowed to know the votes assignment across the two rounds decided by Y, then X could perhaps assign just 1 vote to the first item and 3 votes to the second, obtaining her most preferred outcome in both voting sessions. This point will be discussed in more detail later in the paper.

There could be protocols other than QV for *protecting* minority voters. Therefore, it is natural to ask which properties QV enjoys as compared to alternative voting criteria. One reason is certainly given by analytical simplicity and tractability of quadratic functions. Though attractive, this however would not be a strong enough motivation for choosing QV rather than, for example, cubic voting. [1,2] point out that, as a *vote pricing rule*, QV enjoys the main property of being *robustly optimal*. Broadly speaking, this means that whatever is the users' probability of winning a voting round in their model, QV ensures that the most desirable *social outcome* will receive the highest number of votes; alternatively, that the number of votes assigned by a user to an item is proportional to (a linear function of) the utility/value of the item.

In this work, we investigate QV as applied to the governance of PoS-based blockchain platforms, by assuming that a user's *stake* represents her budget of votes in a voting session. Taking such budget as given, the paper first considers some alternative definitions of the success probability in single voting rounds, to provide closed forms for the optimal number of votes to be allocated to the relevant items under voting. The analysis is game theoretic, and the optimal number of votes is characterized as a Nash Equilibrium of the game. To the best of our knowledge, no such contribution exists in the literature. We then extend the analysis to a general formulation of the success probability. Additionally, we also investigate one of the main concerns in blockchain voting procedures. That is, when users are anonymous, they may decide to split their monetary holdings, hence their stakes, into several accounts to increase their chances of successful voting. This is well known in the literature as the *Sybil attack* [11,12], indeed characterized by users taking multiple identities. Moreover, we discuss if and how the voting timing can affect the outcome of the elections. The paper is structured as follows. In Section 2, we introduce the model fundamentals and provide a symmetric Nash Equilibrium characterization of the optimal number of votes in each round. In Section 3, we discuss whether or not QV may represent an incentive for users to engage in Sybil attacks, while Section 4 considers the implication of simultaneous versus sequential votes selection in the various rounds. In Section 5, we consider a more detailed description of the users' preferences, while Section 6 concludes the paper.

2. The Framework

In this initial section, we introduce a framework to investigate the optimal number of votes with QV in proof-of-stake-based blockchains.

We begin assuming that C is the number of committee members in a voting session and $s_1, s_2, \ldots, s_C$ their stakes, typically defined by a number of currency units. Henceforth, s_i, with $i = 1, \ldots, C$, will be considered as already chosen by the users and a given in the analysis.

We assume a voting session takes place over a time interval, and it is defined by a sequence of voting rounds, one for each item under consideration. Each vote is binary, that is, it has two alternatives: A or B, where A/B could also simply mean disapproval of B/A.

Let R be the total number of voting rounds, which we also refer to as issues/items to be voted in the same session, and suppose $v_{ir} > 0$, with $i = 1, \ldots, C$ and $r = 1, \ldots, R$, is the *(reserve) value* assigned by user i to round r.

That is, we define v_{ir} to be the maximum number of currency units that member i is willing to pay for the most desirable alternative A_r/B_r, in the rth voting session. To simplify, without losing much in generality, we also assume that for each user, the least desirable of the two options under voting has 0 value. Therefore, v_{ir} represents the maximum utility that user i can obtain when voting for issue r.

Hence, if s_i is the stake of the generic ith user, with QV, the total number of votes available in the R rounds of a voting session is equal to

$$s_i = {s_{i1}}^2 + {s_{i2}}^2 + {s_{i3}}^2 + \ldots + {s_{iR}}^2$$

where $0 \leq s_{ir} \leq s_i$ is the number of currency units, i.e., votes, allocated to round r.

For example, suppose $s_i = 15$, $R = 4$. Then, $s_{i1} = 1$, $s_{i2} = 1$, $s_{i3} = 2$, $s_{i4} = 3$ is the number of votes adopted by the user, and therefore, ${s_{i1}}^2 = 1$, ${s_{i2}}^2 = 1$, ${s_{i3}}^2 = 4$, ${s_{i4}}^2 = 9$ is agent $i's$ distribution of the total votes over the four issues under voting. In what follows, to simplify the exposition, without much loss of generality, we shall also consider the possibility of fractional, non-integer votes.

The quantity ${s_{ir}}^2$ is also interpreted as the *cost* of using s_{ir} votes in round r while s_i as the budget of votes available for the entire voting session.

Therefore, at a general level, *for given* s_i, the optimal s_{ir} could be defined as the solution to the following problem

$$max_{s_{ir}}\ EU_i(s_{ir}\ ) = \sum_{r=1}^{R} v_{ir} P_{ir}(s_{ir}, s_{-ir}) such\ that\ \sum_{r=1}^{R} {s_{ir}}^2 = s_i$$

where $P_{ir}(s_{ir}, s_{-ir})$ is user $i's$ probability of obtaining value v_{ir} and s_{-ir} the profile of stakes chosen by the committee members other than user i in round r. More specifically, if $\sigma_r = (s_{1r}, s_{2r}, \ldots, s_{ir}, \ldots s_{Cr})$ is the profile of stakes in round r, then $s_{-ir} = \sigma_r - \{s_{ir}\}$.

It seems reasonable to assume $P_{ir}\ (s_{ir}, s_{-ir})$ to be increasing with respect to s_{ir}, while its behaviour with respect to s_{-ir} may vary according to whether or not the other committee members would vote as agent i.

The optimal choice of s_{ir} can depend upon several elements. In particular, it could depend on whether the chosen s_{ir} is communicated sequentially by the users to the platform, round by round, or "simultaneously" at the very beginning of the session for all $r = 1, \ldots, R$. Moreover, in general, s_{ir} would be chosen within a game theoretic context with strategic interaction and would therefore also depend upon s_{-ir}.

In what follows, we begin the analysis considering a very simple case, where users choose s_{ir} independently of each other, "simultaneously", in a game with *complete information* over the other users' values. More specifically, s_{ir} will be selected by users at the beginning of the session and independently communicated to the platform.

2.1. A Benchmark Framework with Simultaneous Selection of s_{ir}

In this paragraph, we assume that users vote independently of each other and know each other's value. This is clearly a strong assumption, which nevertheless may become more realistic when voters are not strangers to each other. To gain some initial insights, as a very first step in the analysis, we introduce the following expression for the success probability:

$$P_{ir}\ (s_{ir}, s_{-ir}) = \frac{s_{ir}}{S_r}\ for\ all\ i = 1, \ldots, C$$

where $S_r = \sum_{j=1}^{C} s_{jr}$ is the total number of votes in the committee used in round r, and $\frac{s_{ir}}{S_r}$ is the probability that i will obtain the value v_{ir} in the rth voting round. The above definition captures the idea that the committee members vote independently of each other and that they consider the *worst case*, where the success probability decreases with the number of members' votes other than i.

Admittedly, assuming $P_{ir}\ (s_{ir}, s_{-ir}) = \frac{s_{ir}}{S_r}$ may be a simplification of what occurs in reality, since other users may cast the same vote as the ith member. However, as an initial approximation, we find the probability definition to be acceptable. A more detailed discussion on users' preferences is deferred until Section 5.

It follows that the above problem becomes

$$max_{s_{ir}}\ EU_i\ (s_{ir}\ ) = \sum_{r=1}^{R} v_{ir} \frac{s_{ir}}{S_r} such\ that\ \sum_{r=1}^{R} {s_{ir}}^2 = s_i \tag{1}$$

Problem (1), in terms of the associated Lagrange function, can be formulated as follows:

$$max_{s_{ir}}\ L_i\ (s_{ir}, \lambda_i) = \sum_{r=1}^{R} v_{ir} \frac{s_{ir}}{S_r} - \lambda_i \Big(\sum_{r=1}^{R} {s_{ir}}^2 - s_i \Big) \tag{2}$$

With no major loss of generality, treating s_{ir} as a continuous variable for convenience and considering the first-order condition with respect to s_{ir}, derived from expression (2), we obtain

$$v_{ir} \frac{S_r - s_{ir}}{{S_r}^2} = 2\lambda_i s_{ir} \tag{3}$$

where $\lambda_i > 0$ is the Lagrange multiplier associated with constraint $\sum_{r=1}^{R} {s_{ir}}^2 = s_i$.

Before proceeding, it is worth noticing that, unlike what occurs in [1,2] in expression (3), the chosen stake s_{ir} is not a linear but rather a non-linear function of v_{ir}. This is due to our assumption of the success probability $\frac{s_{ir}}{S_r}$, which is indeed introducing the non-linearity in expression (3). Below, in Section 2.5.1, we shall discuss a case with a linear relation between s_{ir} and v_{ir}.

Expression (3) clarifies that a user's optimal stake level also depends on the other committee members' profile of stakes s_{-ir}, which implies that the selection of the optimal s_{ir} across agents could be modeled as a game. Indeed, expression (3) provides the *best reply correspondence* of each user, which explicitly depends on the other users' number of votes.

Below, we state the first result, which represents a benchmark for the rest of the analysis.

Proposition 1. *Suppose $v_{ir} = v_r$ and $s_i = s$, for all $i = 1, \ldots, C$ and all $r = 1, \ldots, R$. Then, there exists a unique symmetric pure strategy Nash Equilibrium of the game with complete information, $s_{ir} = s_r$, given by*

$$s_r = \sqrt{s\frac{v_r}{V}} \tag{4}$$

where $V = \sum_{r=1}^{R} v_r$ is each user's total value in the voting session.

Proof. Immediate. Since $v_{ir} = v_r$ and $s_i = s$, it is $\lambda_i = \lambda$ for all $i = 1, \ldots, C$. Hence, it follows that expression (3) can be re-written as

$$v_r \frac{(C-1)s_r}{C^2 {s_r}^2} = 2\lambda s_r \tag{5}$$

and therefore

$${s_r}^2 = v_r \frac{(C-1)}{2\lambda C^2} \tag{6}$$

Thus, summing up both sides of expression (6) with respect to r, we obtain

$$2\lambda = \frac{V(C-1)}{sC^2} \tag{7}$$

Finally, replacing 2λ obtained from expression (7), into expression (5), the result follows. □

Expression (4) captures some main intuitions of a symmetric equilibrium, in that the optimal number of votes assigned to an item is proportional to its importance $\frac{v_r}{V}$, representing such share of the total stake s. Since expression (4) is the same for all committee members, then the probability that an issue is voted according to the preferences of a user is $\frac{1}{C}$, while user's expected utility given by $EU_i\ (s_{ir}\ ) = \frac{V}{C}$. Finally, notice also that s_r is an increasing and concave function with respect to v_r, a shape due to both the probability assumption $P_{ir}\ (s_{ir}, s_{-ir}) = \frac{s_{ir}}{S_r}$ and to QV.

If Proposition 1 presents an explicit result, for our specific assumption of the success probability, it is also true that it is a benchmark, a limit case, since it is unlikely for reality to be so nicely symmetric. Yet, as we discuss below, computing explicit solutions of s_{ir} under asymmetric values and stakes can be rather cumbersome. However, before doing so, in what follows, we explore the first simple extension of QV.

2.2. An "Alternative" Quadratic Voting (AQV)

It would be interesting to discuss how this benchmark model would compare with some of its possible extensions. As the very first generalization of the QV protocol, we consider the following alternative modality of quadratic voting, which we name AQV:

$$s_i = (s_{i1} + s_{i2} + \ldots + s_{iR})^2 \tag{8}$$

That is, now, the budget of votes is no longer given by the sum of squares of s_{ir} but rather by the squares of the sum of s_{ir}. That is, the squaring and summation operations are permuted. Therefore, problem (2) would now become

$$max_{s_{ir}}\ L_i\ (s_{ir}, \lambda_i) = \sum_{r=1}^{R} v_{ir}\frac{s_{ir}}{S_r} - \lambda_i\left(\ \left(\sum_{r=1}^{R} s_{ir}\right)^2 - s_i\ \right) \tag{9}$$

Solving problem (9) leads to the following result.

Proposition 2. *Suppose $v_{ir} = v_r$ and $s_i = s$, for all $i = 1, \ldots, C$ and all $r = 1, \ldots, R$. Then, there exists a unique symmetric pure strategy Nash Equilibrium of the game $s_{ir} = s_r$ given by*

$$s_r = \frac{\sqrt{sv_r}}{V^{sr}} \tag{10}$$

where $V^{sr} = \sum_{r=1}^{R} \sqrt{v_r}$ is the users' sum of the values' square roots in the voting rounds.

Proof. In a symmetric equilibrium where $s_{ir} = s_r$, the first-order condition in expression (3) now becomes

$$v_r \frac{(C-1)s_r}{C^2 {s_r}^2} = 2\lambda C s_r \tag{11}$$

Again, since $v_{ir} = v_r$ and $s_i = s$ is $\lambda_i = \lambda$ for all $i = 1, \ldots, C$, following the same procedure as in Proposition 1, we obtain

$$2\lambda = (V^{sr})^2 \frac{(C-1)}{sC^3} \tag{12}$$

and the replacement of expression (12) by expression (11) proves the result. □

It is worth noticing that, since $V^{sr} > \sqrt{V}$, then s_r in expression (4) is larger than s_r in expression (10).

2.3. Extending Quadratic Voting to "Any Power" Voting

An additional, somewhat natural extension to the above model can be obtained by generalizing quadratic voting to any *ath* power voting, with $a = 1, 2, 3, \ldots$. More specifically, expression (2) now becomes

$$L_i\left(s_{ir}, \lambda_i\right) = \sum_{r=1}^{R} v_{ir} \frac{s_{ir}}{S_r} - \lambda_i \Big(\sum_{r=1}^{R} {s_{ir}}^a - s_i \Big) \tag{13}$$

The following Corollary generalizes Proposition 1.

Corollary 1. *Suppose that all is as in Proposition 1, except that now, it is $\sum_{r=1}^{R} {s_{ir}}^a = s_i$ with $a = 1, 2, 3, \ldots$ Then, there exists a unique symmetric pure strategy Nash Equilibrium of the game $s_{ir} = s_r(a)$ given by*

$$s_r(a) = \sqrt[a]{s\frac{v_r}{V}} \tag{14}$$

Proof. Since the first order condition is now

$$v_r \frac{(C-1)s_r}{C^2 {s_r}^2} = a\lambda s_r^{a-1}$$

following a procedure analogous to that of Proposition 1, we obtain expression (14). □

Expression (14) immediately shows that $s_r(a+1) > s_r(a)$ for $0 < s\frac{v_r}{V} < 1$, while $s_r(a+1) < s_r(a)$ for $1 < s\frac{v_r}{V}$ and $s_r(a+1) = s_r(a)$ for $1 = s\frac{v_r}{V}$. Therefore, if $0 < s\frac{v_r}{V} < 1$ for all $\frac{v_r}{V}$, then increasing the power of the voting protocol increases the number of votes at stake for the issue under voting. Likewise, if $1 < s\frac{v_r}{V}$, increasing the power of the voting protocol decreases the number of votes at stake for the issue under voting. Finally, as a varies, there will be no changes in the votes if $s\frac{v_r}{V} = 1$.

2.4. An Asymmetric Model with Simultaneous Choice

We now discuss how much more involved the optimal determination of s_{ir} becomes with asymmetric users, that is when values and stakes may differ across committee members. As we shall see, values and stakes can interact in a complex way in the expression of s_{ir}.

To do so, we consider the simplest case in which $i = 1,\ 2$ and $r = 1,\ 2$, still assuming

$$P_{ir}\ (s_{ir}, s_{-ir}) = \frac{s_{ir}}{S_r}$$

It follows immediately that the first-order condition (3) for, respectively, $s_{11}, s_{12}, s_{21}, s_{22}$ becomes

$$(i)\ v_{11}\frac{s_{21}}{{S_1}^2} = 2\lambda_1 s_{11}; (ii)\ v_{12}\frac{s_{22}}{{S_2}^2} = 2\lambda_1 s_{12};\ (iii)\ v_{21}\frac{s_{11}}{{S_1}^2} = 2\lambda_2 s_{21};\ (iv)\ v_{22}\frac{s_{12}}{{S_2}^2} = 2\lambda_2 s_{22}$$

Dividing the left-hand side and right-hand side of (i) by (ii), we obtain

$$\frac{v_{11}s_{21}{S_2}^2}{v_{12}s_{22}{S_1}^2} = \frac{s_{11}}{s_{12}} \tag{15}$$

Likewise, dividing (iii) by (iv), we obtain

$$\frac{v_{21}s_{11}{S_2}^2}{v_{22}s_{12}{S_1}^2} = \frac{s_{21}}{s_{22}} \tag{16}$$

Replacing expression (15) into expression (16) leads to

$$\frac{{S_2}^2}{{S_1}^2} = \sqrt{\frac{v_{12}v_{22}}{v_{11}v_{21}}} \tag{17}$$

Expression (17) clarifies that the proportion between the total number of votes dedicated to the first and second item depends exclusively upon the users' values. In particular, if $\frac{v_{12}v_{22}}{v_{11}v_{21}} = 1$, then the total amount of votes will be the same in each of the two items. This is so, for example, if $\frac{v_{12}=10}{v_{11}=1} = 10$ and $\frac{v_{22}=10}{v_{21}=100} = \frac{1}{10}$ that is, if the values' ratio for a user is the inverse of the values' ratio for the other user. In the example, user $i = 1$ values item $r = 1$ ten times more than item $r = 2$, while user $i = 2$ values item $i = 2$ ten times more than item $r = 1$. The condition could also be interpreted by observing that the product of values for the second item must equal the product of value for the first item. Likewise, if $\frac{v_{12}v_{22}}{v_{11}v_{21}} > 1$, then the second item will attract more votes than the first, and, conversely, if $\frac{v_{12}v_{22}}{v_{11}v_{21}} < 1$, the second item will attract fewer votes than the first item.

Moreover, replacing expression (17) into expression (15), we derive the following expression:

$$\frac{s_{21}}{s_{22}} = \frac{s_{11}}{s_{12}}\sqrt{\frac{v_{12}v_{21}}{v_{22}v_{11}}}$$

hence

$$\frac{{s_{21}}^2}{{s_{22}}^2} = \frac{{s_{21}}^2}{s_2 - {s_{21}}^2} = \frac{{s_{11}}^2}{s_1 - {s_{11}}^2}\alpha = \frac{{s_{11}}^2}{{s_{12}}^2}\alpha \tag{18}$$

where $\alpha = \left(\frac{v_{12}v_{21}}{v_{22}v_{11}}\right)$. Therefore,

$${s_{11}}^2 = \left(\frac{{s_{21}}^2 s_1}{(s_2 - {s_{21}}^2)\alpha + {s_{21}}^2}\right) = \left(\frac{{s_{21}}^2 s_1}{(s_2\alpha + (1-\alpha){s_{21}}^2}\right) \tag{19}$$

Expression (19) provides some interesting information on the relationship between s_{11} and s_{21}. First, notice that α can be any positive number, hence not necessarily less than one.

It follows that $(s_2\alpha + (1-\alpha){s_{21}}^2)$ is not necessarily a convex combination between, an average of, s_2 and s_{21}. In any case, it will always be non-negative.

Then, observe that expression (19) is a decreasing function of α; in particular, ${s_{11}}^2$ tends to s_1 as α goes to zero, and ${s_{11}}^2$ goes to zero as α tends to infinity. For given v_{21} and $v_{22,}$ this is consistent with the intuition, since α goes to zero when v_{12}/v_{11} goes to zero, which means that the outcome of the first round of voting is by far the most important item for agent 1. Analogous considerations hold for when α goes to infinity.

Additionally, it is also interesting to point out that, for given v_{11} and v_{12}, the stake ${s_{11}}^2$ would tend to s_1 when v_{21} is very large as compared to v_{22}, that is, when user 2 assigns a high value to the outcome of the first voting round. All this implies that agent 1 will set a high s_{11} as long as one of the two players assigns a high value to the first item, as compared to the other user.

Moreover, ${s_{11}}^2$ is an increasing concave function of ${s_{21}}^2$, which is equal to ${s_{11}}^2 = 0$ for ${s_{21}}^2 = 0$, reaching its maximum value of ${s_{11}}^2 = s_1$ at ${s_{21}}^2 = s_2$.

Furthermore, notice that in the specific case of $\alpha = 1$, then ${s_{11}}^2 = \frac{{s_{21}}^2 s_1}{s_2}$, which implies that $s_{11} > s_{21}$ if $s_1 > s_2$. More generally, based on expression (19), it follows that ${s_{21}}^2 > {s_{11}}^2$ holds if

$$ {s_{21}}^2 > \left(\frac{{s_{21}}^2 s_1}{(s_2 - {s_{21}}^2)\alpha + {s_{21}}^2} \right) $$

that is, if

$$ (1-\alpha){s_{21}}^2 > s_1 - s_2\alpha \tag{20} $$

To see if and when the inequality in expression (20) can be satisfied, we discuss four possibilities:

(i) $\alpha > 1$ and $s_1 - s_2\alpha > 0$, then expression (20) is never satisfied;
(ii) $\alpha > 1$ and $s_1 - s_2\alpha < 0$, then expression (20) can be satisfied;
(iii) $\alpha < 1$ and $s_1 - s_2\alpha > 0$, then expression (20) can be satisfied;
(iv) $\alpha < 1$ and $s_1 - s_2\alpha < 0$, then expression (20) is always satisfied.

Points (i)–(iv) suggest how the relative size of s_{11} and s_{21} is related to both the users' values and their budget of votes. For example, according to (i), ${s_{21}}^2 \geq {s_{11}}^2$ takes place when s_2 is sufficiently smaller than s_1 and item $r = 2$ is relatively more important for user $i = 1$ than for user $i = 2$. Analogous considerations hold for the other three points.

2.5. The General Model of QV

After having gained some early insights into the optimal number of votes, we can now go back to the general formulation of the problem. For a generic success probability $P_{ir}(s_{ir}, s_{-ir})$, the optimal allocation of votes with QV can be obtained considering the initial setting of the problem:

$$ max_{s_{ir}}\ EU_i\ (s_{ir}\ ) = \sum_{r=1}^{R} v_{ir} P_{ir}\ (s_{ir}, s_{-ir}) such\ that\ \sum_{r=1}^{R} {s_{ir}}^2 = s_i \tag{21} $$

Assuming that $\frac{\partial P_{ir}}{\partial s_{ir}} > 0$ and $\frac{\partial^2 P_{ir}}{\partial {s_{ir}}^2} < 0$, we find that the optimal s_{ir} solves the following first-order condition:

$$ v_{ir} \frac{\partial P_{ir}}{\partial s_{ir}} = 2\lambda_i s_{ir} \tag{22} $$

Squaring both sides and summing them up over the rounds, we obtain

$$ 2\lambda_i = \sqrt{\frac{\sum_{k=1}^{R} \left(v_{ik} \frac{\partial P_{ik}}{\partial s_{ik}} \right)^2}{s_i}} \tag{23} $$

and therefore

$$s_{ir} = (v_{ir}\frac{\partial P_{ir}}{\partial s_{ir}})\sqrt{\frac{s_i}{\sum_{k=1}^{R}(v_{ik}\frac{\partial P_{ik}}{\partial s_{ik}})^2}} \tag{24}$$

which, without introducing specific assumptions on the shape of $P_{ir}\ (s_{ir}, s_{-ir})$, could not be explicitly determined. Yet, it can be immediately observed that $s_{ir} > s_{ir'}$, with $r \neq r'$ if and only if $(v_{ir}\frac{\partial P_{ir}}{\partial s_{ir}}) > (v_{ir'}\frac{\partial P_{ir'}}{\partial s_{ir'}})$, that is, if, for user i, the marginal expected value of issue r is larger than the marginal expected value of issue r'.

If, based on the above considerations, a comparison across votes of the same committee member is immediate and relatively easy to interpret, it is more difficult to compare the number of votes across different users for the same issue.

In some special cases, however, such comparison can be performed with no major problems. Suppose, for example, that the only quantity differing between members i and j is their total stake, that is, $s_i \neq s_j$. In this case, it follows immediately that $s_{ir} > s_{jr}$ if and only if $s_i > s_j$. However, even if the members' values would differ then, for example, $s_i > s_j$ does not necessarily imply $s_{ir} > s_{jr}$ for all r. Indeed, suppose $s_i > s_j$, $\sum_{k=1}^{R}(v_{ik}\frac{\partial P_{ik}}{\partial s_{ik}})^2 = \sum_{k=1}^{R}(v_{jk}\frac{\partial P_{jk}}{\partial s_{jk}})^2$ but that $(v_{jr}\frac{\partial P_{jr}}{\partial s_{jr}})$ is sufficiently larger than $(v_{ir}\frac{\partial P_{ir}}{\partial s_{ir}})$; then, it may be $s_{ir} < s_{jr}$.

To summarize, when the committee members vote independently of each other, differences in the number of votes allocated to the various rounds depend on three main quantities: the member's value of the item under voting, the perceived probability of obtaining that value and the total stake of a committee member.

2.5.1. A Linear Success Probability

An additional interesting form of the *subjectively perceived* success probability is $P_{ir}\ (s_{ir}, s_{-ir}) = ps_{ir}$, with $0 \leq s_{ir} \leq s_i$ and $0 \leq p \leq \frac{1}{s_{ir}}$ being a non-negative constant. We also assume that the value of p is the same for all users. Unlike what it may appear at first, this is not a strong assumption since, as we shall see, the level of p plays no role in the optimal s_{ir}. Notice that, being a subjectively perceived probability, *we do not require* that

$$\sum_{i=1}^{C} P_{ir}\ (s_{ir}, s_{-ir}) = \sum_{i=1}^{C} ps_{ir} = 1$$

In this case, $\frac{\partial P_{jr}}{\partial s_{jr}} = p$, which is constant, which is what [1,2] basically considered. Notice that, with such specification, the success probability does not depend upon the stake of the other committee members, that is, it embodies no strategic interaction.

Under this assumption, expression (22) would become

$$v_{ir}p = 2\lambda_i s_{ir} \tag{25}$$

Following the same procedure as above, we are able to find

$$s_{ir} = v_{ir}\sqrt{\frac{s_i}{V_i^{sq}}} \tag{26}$$

where $V_i^{sq} = \sum_{r=1}^{R} {v_{ir}}^2$. Interestingly, expression (26) is independent of the constant p, which means that the result is the same for the whole class of linear success probabilities $P_{ir}\ (s_{ir}, s_{-ir}) = ps_{ir}$, with any p in its relevant domain. In this sense, the solution can be considered *robust* with respect to the specification of p.

Finally, it is interesting to observe that in expression (26), a *truth revealing* stake, namely $s_{ir} = v_{ir}$, would take place if $s_i = V_i^{sq}$, that is, when, for agent i, the budget of votes coincides with the sum of squares of their values over the R issues under voting. Analogously, in expression (14) with $a = 1$, we would have $s_{ir} = v_{ir}$ if $s = V$, namely, if the budget of votes coincides with the sum of their values.

3. Sybil Attacks

As we anticipated, one of the main concerns of blockchain platforms is represented by the possibility of Sybil Attacks (SA). These take place when a user splits her own currency holdings across more than one account to increase the chance of obtaining the most desirable outcome. In this Section, we discuss if and to what extent *QV could be prone* to SA.

To do so, we consider again the previous model, where C is the number of committee members in a voting session and $s_1, s_2, \ldots, s_C$ their stakes. The simplest framework to gain some insights on the implications of SA is to assume that s_1 and s_2 refer to the same user $i = 1 = 2$, while the others, as before, act independently. To further simplify, henceforth we shall refer to user $i = 1$ to also mean $i = 2$. Assuming $P_{ir}\ (s_{ir}, s_{-ir}) = ps_{ir}$ it follows that for $i = 1$, expression (21) becomes

$$max_{s_{1r}, s_{2r},} EU_1(s_{1r}\ , s_{2r}\ ) = \sum_{r=1}^{R} v_{1r} p(s_{1r} + s_{2r}) such\ that\ \sum_{r=1}^{R} {s_{1r}}^2 + \sum_{r=1}^{R} {s_{2r}}^2 = s_1 \quad (27)$$

The first-order condition with respect to s_{1r} is given as in expression (25) by

$$v_{1r} p = 2\lambda_1 s_{1r} \quad (28)$$

and, likewise, the first-order condition with respect to s_{2r} is given by

$$v_{1r} p = 2\lambda_1 s_{2r} \quad (29)$$

which implies that $s_{1r} = s_{2r}$. For $i > 2$, the problem is as in expression (21), given by

$$max_{s_{ir},} EU_1\ (s_{ir}\ ) = \sum_{r=1}^{R} v_{ir} ps_{ir} such\ that\ \sum_{r=1}^{R} {s_{ir}}^2 = s_i$$

and the related first-order condition is also defined as in expression (25) by

$$v_{ir} p = 2\lambda_i s_{ir} \quad (30)$$

Therefore, the main difference between the pair of conditions (28) and (29) with (30) rests in the QV voting constraint in expression (30) versus the QV constraint in expression (27). Moreover, it should also be noticed that in this case, the number of different individuals is now equal to $C - 1$, although the number of committee members is still equal to C. The Proposition below contains the main result of this section.

Proposition 3. *Assume $P_{ir}(s_{ir}, s_{-ir}) = ps_{ir}$. Then, if user $i = 1$ and user $i = 2$ are the same individual, while the others are all different individuals, then the pure strategy Nash Equilibrium for each committee member $i = 1, 2, \ldots, C$, in each round $r = 1, 2, \ldots, R$, is given by*

$$s_{ir} = v_{ir} \sqrt{\frac{s_i}{2V_i^{sq}}}\ for\ i = 1, 2 \quad (31)$$

$$s_{ir} = v_{ir} \sqrt{\frac{s_i}{V_i^{sq}}}\ for\ i > 2 \quad (32)$$

where $V_i^{sq} = \sum_{r=1}^{R} {v_{ir}}^2$ is user i's total value in the voting session.

Proof. Squaring both sides of expression (28) and (29) and summing up their left-hand sides and right-hand sides, we obtain

$$\sum_{r=1}^{R} (v_{1r} p)^2 + \sum_{r=1}^{R} (v_{2r} p)^2 = 2\sum_{r=1}^{R} (v_{1r} p)^2 = 2p^2 V_1^{sq} = (2\lambda_1)^2 [\sum_{r=1}^{R} (s_{1r})^2 + \sum_{r=1}^{R} (s_{2r})^2] = (2\lambda_1)^2 s_1 \quad (33)$$

from which expression (31) is obtained. By a similar reasoning, expression (32) too follows immediately. □

According to the above result, the success probability of user $i = 1$ will now be

$$P_{ir}\ (s_{ir}, s_{-ir}) = p(v_{1r}\sqrt{\frac{2s_1}{V_1^{sq}}}) \tag{34}$$

which is larger than the success probability

$$P_{ir}(s_{ir}, s_{-ir}) = p(v_{1r}\sqrt{\frac{s_1}{V_1^{sq}}})$$

which is obtained when $i = 1$ would not split their money holdings in two wallets, suggesting that with QV a Sybil Attack may be profitable. Though within the limits of the model assumptions, the above conclusion may provide some interesting early indications on the possibility of Sybil attacks with QV.

4. Simultaneous versus Sequential Staking

Until now we assumed that users choose, at the beginning of a voting session, both the total number of votes for the entire session as well as the number of votes for each round. More explicitly, at the start of the session, user i announces s_i as well as s_{ir}, for each round $r = 1, \ldots, R$, to which she commits throughout the whole voting session. We also assumed that users choose simultaneously, that is, they communicate to the blockchain platform their choice independently of each other, without having observed how many votes the other users had allocated to the various rounds.

In this section, we analyze some alternative scenarios with sequential staking to discuss whether and how the disclosure of some information could affect the users' strategy.

In what follows, we consider two cases:

(1) at some round, when (at least one) user chooses the number of votes to allocate for that item, they are able to observe the number of votes chosen by the other users *for that round*.
(2) at some round, users are able to observe the votes chosen by the other users *in previous rounds* and possibly change their plans made at the beginning of the voting session.

(1) We start with the simplest case already mentioned in the Introduction. Suppose there are two users $i = 1, 2$ and two voting rounds $r = 1, 2$. Moreover, assume $v_{11} = 10$, $v_{12} = 5$, $v_{21} = 5$, $v_{21} = 10$, $s_1 = 13$ $s_2 = 9$. That is, the two users have opposite preferences and, furthermore, $i = 1$ has a larger budget of votes than $i = 2$. Finally, though we consider the possibility of fractional votes, assume that the outcome of a voting round is valid if at least one user casts one vote in it.

Take user $i = 1$. If when choosing s_{11} and s_{12} she does not know s_{21}, s_{22}, then, with QV, a reasonable allocation of votes for her may be $s_{11} = 3, s_{12} = 2$, since $3^2 + 2^2 = 13$, which is slightly higher in the first round, since she cares more about its outcome. Likewise, since user $i = 2$ cares more about the second item, she may decide to cast all of her votes on it, and so $s_{21} = 0, s_{22} = 3$, since $0^2 + 3^2 = 9$. As a result, user $i = 1$ will have the majority in the first round, while user $i = 2$ in the second round. Therefore, even though $i = 2$ has a lower overall stake as compared to $i = 1$, she could still guarantee for herself the outcome of the second voting round, i.e., the most desirable for her. So, overall, in the two rounds, both users would secure a value between 10 and 15 units. Indeed, in the first round, $i = 1$, having the majority of votes, would certainly obtain a value of 10 and possibly an additional value of 5 in the second round, if their preferences are aligned with those of user $i = 2$. An analogous reasoning holds for user $i = 2$. In any case, the example shows that the weaker user $i = 2$ could be certain to obtain a value of at least 10. That is, with QV, she could still obtain a sufficiently high value by focusing her votes on the second round.

However, suppose that now $i = 1$ knows that $i = 2$ has chosen $s_{21} = 0$; then $i = 1$ could choose, for example $s_{11} = 1$ and $s_{12} = \sqrt{13 - 1^2} \sim 3.46$, which is larger than

$s_{22} = \sqrt{9} = 3$, so that $i = 1$ would win both voting rounds and would guarantee for herself the maximum possible value of 15.

To summarize, even with QV, the sequential staking of the kind discussed in this point can meaningfully affect the outcome of the voting rounds, typically favoring the user with an informational advantage.

(2) In this second case, we consider the following situation. As above, we still assume that users announce at the beginning of a voting session the total number of votes they intend to have as a stake s_i. However, we now suppose that s_{ir} is announced simultaneously before each round, rather than at the very beginning of the voting session for all rounds, discussing what difference this would make as compared to the model in Section 1.

From a conceptual perspective, the main difference with simultaneous announcement at the beginning of the session is given by the following elements. First, except for the first round, after each voting round, the user can observe the outcome of the previous rounds, that is, which of the two alternatives to be chosen prevailed, which, in principle, may provide useful information on how to choose in the following rounds. Moreover, each user could also observe how many votes have been allocated by the other committee members to the previous rounds.

There may be multiple ways of taking account of the above observations to try answering the question, depending upon the user's goal function. To gain some insights, we study the case of *any power* $a = 1, 2, 3 \ldots$voting, $i = 1, \ldots, C$ and $r = 1, \ldots, R$. Moreover, we still assume

$$P_{ir}\left(s_{ir}, s_{-ir}\right) = \frac{s_{ir}}{S_r}$$

symmetric agents, as in Proposition 1, and consider the following reasoning.

At the first voting round $r = 1$, user i solves expression (13) to obtain expression (14), which, for convenience, we report below:

$$s_r\left(a\right) = \sqrt[a]{s\frac{v_r}{V}} \tag{35}$$

Expression (14) would provide a solution for $s_1\left(a\right)$ as well as an indication, though *not a commitment*, for the values of $s_r\left(a\right)$ with $r > 1$. Hence, assume $s_1\left(a\right) = \sqrt[a]{s\frac{v_1}{V}}$ is adopted in the first round but then, upon reaching the second round, the user evaluates whether she's still willing to choose $s_2\left(a\right) = \sqrt[a]{s\frac{v_2}{V}}$, as computed by expression (14), or a different number of votes. Suppose that such an alternative number of votes would now be calculated by solving the following problem, which updates expression (13) after the first round:

$$max_{s_{ir}} EU_i(s_{ir}) = \sum_{r=2}^{R} v_{ir}\frac{s_{ir}}{S_r} such\ that\ \sum_{r=2}^{R} {s_{ir}}^a = s_i - s_1(a)^a = s_i - s_i\frac{v_1}{V} = s - s\frac{v_1}{V} \tag{36}$$

That is, if $s_{-1r}\left(a\right)$ stands for the solution to expression (36), then following the same procedure as in expression (14), we obtain

$$s_{-1r}(a) = \sqrt[a]{s_{-1}\frac{v_r}{V_{-1}}} \tag{37}$$

where $s_{-1} = s - s\frac{v_1}{V}$ and $V_{-1} = V - v_1$. Therefore, still considering a symmetric equilibrium, it is

$$s_{-12}(a) = s_{-1}\frac{v_2}{V_{-1}} = \left(s - s\frac{v_1}{V}\right)\frac{v_2}{V_{-1}} = \frac{sV_{-1}}{V}\frac{v_2}{V_{-1}} = s\frac{v_2}{V} \tag{38}$$

which implies that $s_2(a) = s_{-12}(a)$. That is if the user, after the first round, re-calculates the number of votes to choose in the second round and finds, as in expression (36), the same solution, we say that the user is *dynamically consistent* at the second round. That is, the

number of votes that, in the first round, the user planned to choose for the second round, she will indeed find it convenient to choose upon reaching the second round.

Following a similar reasoning, it can be immediately observed that, upon reaching any voting round $r > 1$, the user will have no incentive to change the number of votes that she planned to use at any round $r - j$, with $j = 1, \ldots, r - 2$.

To summarize, under the assumptions of the model, the simultaneous versus sequential choice of the voting stake will make no difference for the user who, for this reason, we define to be *dynamically consistent*.

5. A More Detailed Specification of the Users' Preferences

In Section 1, we introduced the main fundamentals of the model, assuming that in each round of a voting session users would obtain a positive value if the outcome of the round was the most desirable one, or a zero value otherwise. Admittedly, this might be considered too simplified a representation of the committee members' preferences, since we did not make it explicit which of the alternatives under voting was preferred by the individuals. Indeed, specifying the alternative that the users prefer may improve our understanding of their behavior when individuals vote under QV.

The following simple example illustrates the point. Consider a session with three voting rounds $r = 1, 2, 3$ and three committee members $i = 1, 2, 3$. For each round r, there is a binary choice to make, which we indicate with A_r / B_r. Finally, by v_{irA} we define the value of user i in round r with preference for alternative A_r and analogously for alternative B_r. As before, we assume that if $v_{irA} > 0$, then $v_{irB} = 0$, and if $v_{irB} > 0$, then $v_{irA} = 0$ for all users and all rounds. The table below contains a complete description of the users' preferences over the items under voting.

Some comments are in order. Table 1 suggests that over the whole voting session, user $i = 2$ is the one with the largest value, equal to 35. The total value per user provides an indication on how important the voting session is for them. The "A_r / B_r round value" row provides the total value, for the two alternatives in each round. For example, in round $r = 1$, alternative A_1 has a value of 18, while B_1, a value of 20, which also implies that round 1 exhibits the highest total value of 38. The total value per round provides an indication of the overall importance for the voters of the round under consideration. Moreover, the "Number of users" row summarizes how many users prefer each alternative.

Table 1. Users' values with three voting rounds.

		Rounds			**Total Value**
		1	**2**	**3**	
Users	**1**	$v_{11A} = 10$	$v_{12B} = 15$	$v_{13A} = 2$	$V_1 = 27$
	2	$v_{21B} = 20$	$v_{22A} = 10$	$v_{23B} = 5$	$V_2 = 35$
	3	$v_{31A} = 8$	$v_{32A} = 8$	$v_{33A} = 4$	$V_3 = 20$
A_r / B_r **round value**		$A_1 = 18,\ B_1 = 20$	$A_2 = 18\ B_2 = 15$	$A_3 = 6,\ B_3 = 5$	
Total round value		38	33	11	82
Number of users		$A_1 = 2,\ B_1 = 1$	$A_2 = 2,\ B_2 = 1$	$A_3 = 2,\ B_3 = 1$	

Additionally, the most important item under voting for user $i = 1$ is $r = 2$, while for user $i = 2$, it is $r = 1$ and for $i = 3$, it is both $r = 1$ and $r = 2$. Finally, the maximum total value that could be obtained in the entire session by the three voters is equal to 44 out of 82, a little more than a half the overall value of the voting session.

Based on the description of Table 1, we observe that, from the point of view of the whole "committee", because of the wide dispersion of preferences and values, regardless of the outcome of the voting rounds, there will be some meaningful "social waste", in the sense that a value of at least $82 - 44 = 38$, namely 46% of the total value, could not be obtained by anyone in the session.

Given the above preferences, the outcome of each single round of voting will depend on each user's stake s_i, which is likely to be positively correlated with the total value V_i. Indeed, assume $s_i = V_i$; in what follows, we discuss what would occur with standard majority voting versus QV.

(i) *Standard majority voting*. It follows that if they vote independently of each other in the first round, alternative A_1 prevails with 47 votes against 35. In the second round, alternative A_2 prevails with 55 votes against 2. In the third round, A_3 prevails again with 47 votes against 35. Globally, the value achieved in the session is equal to 42, almost the maximum possible one.

However, there are two points to note here. First, user $i = 2$, despite having the highest global stake of 32 for the entire voting session, will be able to obtain only a total value of 10, namely just 28% of their value in the whole voting session. Secondly, user $i = 3$ will obtain 100% of their value, even though their global stake is the lowest and equal to 20. Table 2 below summarizes all of this.

Table 2. Users' values obtained with standard majority voting.

		Rounds			% Value
		1	**2**	**3**	
Value obtained by the users	**1**	10	0	2	$12/27 = 0.44$
	2	0	10	0	$10/35 = 0.28$
	3	8	8	4	$20/20 = 1$

Majority voting is feared to penalize minorities because in case somebody has more than 51% of the votes, they can always guarantee for themselves the best possible outcome, which sometimes may not coincide with the best possible outcome of minority voters. However, the above example shows that this may not always be the case, since the user with the largest overall value is the one penalized.

Indeed, if the outcome contained in Table 2 is perceived as unfair/inefficient, we now discuss whether the "any power voting" criterion can somehow improve the situation.

(ii) "*Any power" voting*. Suppose now that users have a budget of votes s_i, as in Section 2.3, and expression (13), must satisfy constraint $\sum_{r=1}^{R} {s_{ir}}^a = s_i$ where $a = 1, 2, \ldots$. In this case, alternative scenarios can take place, depending upon how users would allocate their votes across the rounds.

Start considering $a = 1$ and, since $s_i = V_i$, suppose that somewhat naturally, $s_{ir} = v_{ir}$. In this case, it is easy to check that now user $i = 1$ will obtain an even lower value than with majority voting, equal to 2; user $i = 2$ would now increase her total value to 30, while user $i = 3$ would reduce her total value to 12. If this outcome certainly improves user $i = 2's$ situation, it further decreases user $i = 1's$ total value as well as user $i = 3's$ overall value. Though the unit power $a = 1$ seems to be re-balancing the situation for users 2 and 3, making it more consistent with their overall values, it further deteriorates the situation of $i = 1$. However, as hinted at, the distribution of votes may differ from $s_{ir} = v_{ir}$. For example, if player $i = 1$ chooses $s_{12} = 27 = s_1$ with the other two players still choosing $s_{ir} = v_{ir}$, a different scenario would be obtained. Now $i = 1$ could guarantee for themselves a value of 15, while $i = 2$ would obtain an overall value of 20 and $i = 3$ a total value of equal to 4. With $a = 2$, that is QV, again several scenarios can take place depending upon the stakes chosen over the three rounds by the users. For example, if users *naturally* select $s_{ir} = \sqrt{v_{ir}}$, then it can be immediately noticed that nothing would change with respect to standard majority in terms of voting outcomes. So, if majority voting is perceived as somewhat biased in this case, QV, with the above allocation of votes, would not fix the issue. However, with an alternative distribution of votes, outcomes may change, as it occurred with the unit power $a = 1$.

Finally, as noticed earlier, if the power a becomes large, then $\sqrt[a]{v_{ir}}$ would tend to 1, and the voting outcome in each round is be determined by how many users will have a

positive value for one alternative versus the other alternative. According to Table 1, the value distribution based on the voting outcomes would again be as in Table 2, that is, as with majority voting.

To summarize, in the example contained in Table 1, user $i = 3$, the one with a lower number of votes, appears to be able to obtain very satisfactory outcomes, both with majority voting as well as with QV. That is, QV does not seem to operate in a special way to "protect" her. A possible intuition for this might be the following. In the three voting rounds, user $i = 3$ is never alone to prefer one of the two alternatives and, moreover, the other user with the same preference has a sufficiently large number of votes. When this occurs, QV would perhaps not be needed for protecting the minorities, since they can obtain their most desirable outcome being supported by other voters. However, when minorities cannot enjoy additional support from other voters, then QV can help them grant for themselves at least some desirable outcome.

To see this, consider the following simple variation of Table 1.

In Table 3 below, user $i = 3$ is still the weak one, as in Table 1 and, moreover, numerically, she is always a minority in the three rounds, as well as in terms of the total value per round. Furthermore, she cares particularly about the third item, which is not the most desirable for the other two voters.

Table 3. Alternative users' values with three voting rounds.

		Rounds			**Total Value**
		1	**2**	**3**	
Users	**1**	$v_{11B} = 10$	$v_{12B} = 13$	$v_{13B} = 4$	$V_1 = 27$
	2	$v_{21B} = 20$	$v_{22B} = 10$	$v_{23B} = 5$	$V_2 = 35$
	3	$v_{31A} = 6$	$v_{32A} = 6$	$v_{33A} = 8$	$V_3 = 20$
A_r/B_r **round value**		$A_1 = 6\ B_1 = 30$	$A_2 = 6\ B_2 = 23$	$A_3 = 8,\ B_3 = 9$	
Total round value		36	29	17	82
Number of users		$A_1 = 1,\ B_1 = 2$	$A_2 = 1,\ B_2 = 2$	$A_3 = 1,\ B_3 = 2$	

Assuming again $s_i = V_i$, in Table 3, user $i = 3$ is certainly a minority and, moreover, in each voting round, she is the only one to prefer her own alternative. Majority voting will certainly prevent her from obtaining any of the desirable results. With unit power $a = 1$ and $s_{ir} = v_{ir}$, again, user $i = 3$ will not be able to improve her situation. However, if users $i = 1$ and $i = 2$ again choose $s_{ir} = v_{ir}$ but, for example, $s_{33} > 9$, then $i = 3$ will be able to guarantee for herself the most desirable outcome in the third round and a total value of 8. Likewise, with QV and $s_{ir} = \sqrt[2]{v_{ir}}$ for $i = 1, 2$ by posing $s_{33} = \sqrt[2]{20}$, then $i = 3$ would be able to secure a total value of 8 in the third round.

6. Conclusions

In the paper, we investigated some issues related to quadratic voting as applied to a sequence of rounds with binary alternatives within the context of a proof-of-stake-based blockchain platform. In particular, considering as given the monetary stake chosen by the voting committee members, which also represents the number of votes available for an entire voting session, we analyzed how users can optimally choose their stakes/votes in the rounds composing the session. In a game with complete information on the users' values, we were able to fully characterize a symmetric pure strategy Nash equilibrium of the game. Though interesting mostly as a benchmark, the model findings provide some interesting insights on the more realistic case of asymmetric users. As for policy making of the platform, the analysis suggests that, typically, the number of votes allocated by a user to a round of a voting session is positively related to the importance assigned to that round in relation to the importance of the entire voting session. Moreover, the number of votes in a round increases with one's stake. Based on our analysis, this finding appears to be

true both in symmetric but also asymmetric cases, that is, where users may assign different values to the outcomes of the voting rounds and when their stakes differ.

We also analyzed some extensions of the basic framework, considering alternatives to QV, as well as discussing the possibility of Sybil attacks and the importance of timing when users choose and communicate the allocations of votes to the platform at each round.

Finally, with reference to numerical examples, we argued that quadratic voting in principle does not seem to guarantee that users with a low number of votes will be able to obtain their most desirable outcome approved in a voting round. Indeed, we saw how the structure of preferences and the size of the stakes of all users may also affect the voting result.

Funding: The project was funded by the Algorand Foundation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: No data has been used.

Acknowledgments: I would like to thank the Algorand Foundation for funding this project.

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

References

1. Aggarwal, S.; Kumar, N. Attacks on Blockchain. In *The Blockchain Technology for Secure and Smart Applications across Industry Verticals*; Aggarwal, S., Kumar, N., Raj, P., Eds.; Academic Press: Cambridge, MA, USA, 2021; pp. 399–410.
2. Buterin, V.; Hitzig, Z.; Weyl, G. A flexible design for funding public goods. *Manag. Sci.* **2019**, *65*, 5171–5187. [CrossRef]
3. Chen, Y.; Chen, H.; Zhang, Y.; Han, M.; Siddula, M.; Cai, Z. A survey on blockchain systems: Attacks, defenses, and privacy preservation. *High Confid. Comput.* **2022**, *2*, 100048. [CrossRef]
4. Cheng, T.; Wenting, L.T.; Chou, Y.; Karahalios, K.; Sundaram, H. "I can show what I really like.": Eliciting preferences via quadratic voting. *Proc. ACM Hum. Comput. Interact.* **2021**, *5*, 182. [CrossRef]
5. Goodman, J.; Porter, P. Will quadratic voting produce optimal public policy? *Public Choice* **2021**, *186*, 141–148. [CrossRef]
6. Lalley, S.; Weyl, G. Quadratic Voting, Manuscript¸2014. Available online: https://www.aeaweb.org/conference/2015/retrieve.php?pdfid=3009&tk=BHDG8H2E (accessed on 10 March 2022).
7. Lalley, S.; Weyl, G. Quadratic voting: How mechanism design can radicalize democracy. *Am. Econ. Assoc. Pap. Proc.* **2018**, *108*, 33–37. [CrossRef]
8. Posner, E.; Weyl, G. Quadratic voting as efficient corporate governance. *Univ. Chic. Law Rev.* **2014**, *81*, 251–272.
9. Posner, E.; Weyl, G. Voting squared: Quadratic voting in democratic politics. *Vanderbilt Law Rev.* **2015**, *68*, 441–500.
10. Posner, E.; Weyl, G. *Radical Markets Uprooting Capitalism and Democracy for a Just Society*; Princeton University Press: Princeton, NJ, USA, 2018.
11. Weyl, G. The Robustness of Quadratic Voting. *Public Choice* **2017**, *172*, 75–107. [CrossRef]
12. Wright, D. Quadratic voting and blockchain governance. *UMKC Law Rev.* **2019**, *88*, 475.