FinTech

MDPI

Article

The Economics of Consensus in Algorand

Nicola Dimitri

Department of Economics and Statistics, University of Siena, Piazza San Francesco 7, 53100 Siena, Italy; dimitri@unisi.it

Abstract: In the paper we investigate consensus formation, from an economic perspective, in a Proof-of-Stake (PoS) based platform inspired by the Algorand blockchain. In particular, we consider PoS in relation to governance, focusing on two main issues. First we discuss alternative sampling schemes, which can be adopted to select voting committees and to define the number of votes of committee members. The selection probability is proportional to one's stake and increases with it. Participation in governance allows users to affect the platform's decisions as well as to obtain a reward. Then, based on such preliminary analysis, we introduce a microeconomic model to investigate the *optimal* stake size for a generic user. In the model we conceptualize an *optimal* stake, for a user, as striking the balance between having Algos immediately available for transactions and setting aside currency units to increase the probability of becoming a committee member. Our main findings suggest that the optimal stake can be quite sensitive to the user's preferences and to the rules for selecting committees. We believe the findings may support policy decisions in PoS based platforms.

Keywords: proof of stake; consensus; algorand

check for updates

Citation: Dimitri, N. The Economics of Consensus in Algorand. *FinTech* **2022**, *1*, 164–179. https://doi.org/10.3390/fintech1020013

Academic Editor: Shyan-Ming Yuan

Received: 10 February 2022
Accepted: 12 May 2022
Published: 26 May 2022

1. Introduction

In the Algorand blockchain, platform blocks are confirmed/validated by *committees* of nodes/users, randomly selected by means of a *Proof of Stake* (PoS)-based mechanism, that is with a probability proportional to, and increasing in, the number of currency units *set aside* by a user from her monetary holdings [1–28]. More specifically, to introduce a new block in the blockchain, Algorand requires three steps: block proposal, block selection and block validation. Each of these three steps are performed by committees of users, randomly selected according to their set aside stake.

Additionally, the Algorand Foundation has recently introduced a model of Governance where decisions are taken by users, whose number of votes is defined by their monetary stakes. As of now any user staking just one Algo is allowed to vote, so no random drawing procedure is currently undertaken to form voting committees. However, unlike what happens with the three roles for block validation, governance participation is rewarded by Algorand. This is because voting participation is considered to be more costly, in terms of time and effort than block validation.

As said, a *stake* is the amount of the own money a user is willing to set aside, *freeze*, for a period of time to be allowed to validate a block and/or vote in governance issues. The stake fulfills two main goals for the platform. First, the temporary unavailability of the monetary *stake* represents an incentive to keep personal wealth within the platform. Secondly it may also be instrumental for blockchain platforms to mitigate/solve the "*nothing at stake*" problem that characterizes PoS. That is, unlike Proof of Work based platforms, such as Bitcoin, where eligibility to confirm blocks requires investing resources in a specific activity like "mining", PoS misbehavior such as double spending may have no cost for the relevant user. Hence, in this case the stake may be considered as a guarantee deposit and thereby *slashed* by the platform to punish such misbehavior.

Therefore, the healthy functioning of a PoS based blockchain such as Algorand is fundamental to induce the users to set up the stakes. Provided this is so, studying the

optimal stake for the users is very important for the nodes, as well as for the platform. Indeed, the stake size can meaningfully affect the dynamics of Algorand on many dimensions such as to prevent, for example, an individual/committee from being chosen too frequently or from nodes taking dishonest choices. The intuition suggests that for an appropriate, long lasting, functioning of the platform, the total size of the stakes in the community, should neither be too small but also not too large. Indeed, in the extreme case where no user sets aside any stake the chain could not even function, as no stake-based random drawing could take place. On the other hand, if each user sets aside his total monetary holdings as a stake, no transaction could take place in the community, which is inconsistent with the Algorand mission.

With the above considerations in mind, in the paper we investigate two main issues. First, as a preliminary step, we discuss the selection probability of users/committees when based on their stake, mostly focusing on the symmetric case, where all the users have the same stake as a main benchmark for the analysis. We consider alternative sampling schemes, with and without replacement, and argue that some of them may help, more than others, with the emergence of some dominant, prevailing, positions in block certification/governance participation. For the sake of generality, the analysis extends beyond the specificities of Algorand.

Based on the first part, we then conceptualize the optimal stake determination by a node. We do so by introducing a generic user's preferences in a dynamic microeconomic setting. This allows us to properly capture the fundamental trade-off faced by a user when deciding how much money to set aside as a stake. Indeed, on the one hand a smaller stake provides a larger amount of Algos available for the current user's transactions while, on the other hand, it means a lower probability of being selected for block validation/governance voting. The resolution to such a trade-off can only be modelled by considering the user preferences in a dynamic context. In the work we shall mostly focus on the analysis of the optimal stake as related to governance; to our knowledge this is the first contribution discussing in detail the issue within PoS blockchains.

The structure of the paper is as follows. In Section 2 we discuss the selection probability of single users and committees. In Section 3 we analyze the optimal stake determination considering a PoS selection-based procedure to vote on Algorand governance issues. Section 4 concludes the paper.

2. Committees and Voting

As above, both Algorand block validation and governance voting committees are based on PoS. When the members selection is random, a potential problem with PoS may be that nodes with a higher stake could be chosen too frequently, establishing forms of dominant positions in the platform. This is typically referred to as the *rich-get-richer* possible problem with PoS, which may also be an issue when member selection is not random. For this reason, we believe that a first important step in the analysis of users/committees selection is to gain insights on what may be the probabilities of being drawn according to PoS, as well as the implications of alternative sampling schemes.

A framework for the analysis could be founded on some simple, initial considerations. To further simplify, in what follows we shall interchangeably use the terms account/node/user. Suppose N is both the number and the set of nodes in Algorand at some point in time. Assume committees are formed by $C \leq N$ nodes, where C is both the number and the set of committee members selected by the platform. This is different from the procedure adopted by the Algorand Foundation for its governance, where for a user it is enough to stake 1 Algo to become a committee member. In that case, the committee size is not specified a priori and determined at each voting session by the number of users available to vote. In any case, adjusting the analysis to when C is endogenously defined by the users would not imply major changes.

Let $i = 1, 2, \ldots, N$, and $i \in N$, indicate the generic node, and $j = 1, 2, \ldots, C$ and $j \in C$ the generic committee member. For the sake of generality, at this stage we assume that

committees can refer to block validation as well as participation to governance activities; later we shall focus the discussion on governance only. Finally, we define a_i and $s_i \leq a_i$, respectively, the total amount of Algos in user $i's$ wallet and s_i her stake.

In what follows, within a *generalized sampling without replacement* scheme, we start considering three main random selection criteria to form committees.

(a) The first we call "*One-Node-One-Vote*" (ONOV). In ONOV, to be part of a committee, nodes are drawn with a probability which is proportional to their monetary stake. Once drawn, the user's Algos are removed from the sampling scheme and a node cannot be selected again. Therefore, in ONOV the Algos in the stake affect only the probability to be on a committee but not the number of votes a node has in the committee which, for each selected member, is just one. Of course, nothing prevents a_i and s_i to count *informally* within the committee; yet they do not formally matter when voting, since each node has a single vote.

(b) The second criterion we call "*One-Node-Multiple-Votes*" (ONMV), where a committee is composed as follows. As for ONOV, a node is selected to be a committee member with a probability proportional to s_i. Once selected, as well as for ONOV, the stake of a node is removed from the procedure. However, unlike ONOV, with ONMV once C nodes are selected. each node in the committee will have a number of votes equal to s_i. Therefore, with ONMV the size of the stake will play a major role also in establishing the relative weights in the voting sessions.

(c) The third criterion we call "*One Node Multiple Draws*" (ONMD). According to ONMD a node is drawn with a probability proportional to s_i. Once selected, one Algo is eliminated from its stake and the node could be drawn again. Unlike criteria (a) and (b), in principle with criterion (c), all of the committee members may coincide with the same node, which can be sequentially selected at all draws.

Below we discuss the main features of the three criteria, starting with ONOV. However, prior to doing so we need to introduce some further notation.

Suppose a_i, with $i = 1, \ldots, N$, is the number of Algos held by node i at some date and that, with no loss of generality, it is $a_1 \geq a_2 \geq \ldots \geq a_N$. In case of a uniform holdings of the currency it is $a_i = \frac{a}{N}$. Moreover, consider $B \subseteq N$ and define $a = \sum_{i=1}^{N} a_i$, $a_B = \sum_{j \in B} a_j$, $a_{-B} = a - a_B$. Analogously, let $s = \sum_{i=1}^{N} s_i$, $s_B = \sum_{j \in B} s_j$, $s_{-B} = s - s_B$.

2.1. One-Node One-Vote (ONOV)

According to ONOV, each member of the committee must be a different node, since once an account is selected all its Algos will be eliminated from the subsequent draws.

Therefore, the number, and the set, of possible committees is $S(N) = \begin{pmatrix} N \\ C \end{pmatrix} = \frac{N!}{C!(N-C)!}$

(i) *Uniform probability of a committee selection*

Start considering a benchmark situation, where the stake is the same for all nodes and given by,

$$s_i = a_i = \frac{a}{N},$$

for all $i = 1, \ldots, N$. That is, one's stake coincides with her monetary holdings and so the probability of being drawn is uniform, across the nodes, and equal to $\frac{1}{N}$. Notice that we are implicitly assuming that all nodes are willing to be selected as a committee member. This is not necessarily the case since, in principle, there could be nodes which are only interested in Algos for transactions, but not for block validation and/or governance participation.

In this case, since each committee has the same chance of being selected then any one of them will be drawn with the following probability

$$\frac{1}{S(N)} = \frac{1}{\begin{pmatrix} N \\ C \end{pmatrix}} = \frac{C!(N-C)!}{N!}$$

Consider now n repeated committee selections, where N and C are kept as constant. Moreover, assume that rounds of selections are stochastically independent of each other. If K is the variable representing the number of times the same committee is chosen in n independent rounds of selection, then the probability of choosing $0 \leq k \leq n$ times the same committee is binomial and given by

$$P(K=k) = \binom{n}{k} \left(\frac{1}{\binom{N}{C}}\right)^{k} \left(1 - \frac{1}{\binom{N}{C}}\right)^{n-k} = \left(\frac{1}{\binom{N}{C}}\right)^{n} \binom{n}{k} \left(\binom{N}{C} - 1\right)^{n-k}$$

It follows that $E(K) = \frac{n}{\binom{N}{C}}$, while $Var(K) = \frac{n}{\binom{N}{C}} \left(1 - \frac{1}{\binom{N}{C}}\right)$, which is maximized for $\binom{N}{C} = 2$. Should Algorand wish EK not to exceed an upper bound $u(n)$ then, for given N, n and C could be chosen appropriately in such a way that

$$EK < u(n) \tag{1}$$

Since, regardless of N being even or odd, the binomial coefficient $\binom{N}{C}$ is always maximized for $C = \frac{(N+1)}{2}$, then a necessary condition for (1) to be at all satisfied is

$$\frac{n}{\binom{N}{\frac{(N+1)}{2}}} < u(n) \tag{2}$$

In general, it will have to be $\frac{n}{u(n)} < \binom{N}{C}$, namely the number of possible committees should be sufficiently large. For example, if $u(n) = \frac{n}{2}$ then there will have to be at least 2 possible committees in the set of nodes.

Finally if K_i, with $i = 1, \ldots, \binom{N}{C}$ and $K_1 + K_2 + \ldots + K_{\binom{N}{C}} = n$, are random variables defining the number of times the ith committee is selected in n repeated draws, then

$$P\left(K_1 = k_1, \ldots, K_{\binom{N}{C}} = k_{\binom{N}{C}}\right) = \frac{n!}{k_1! \ldots k_{\binom{N}{C}}!} \left(\frac{1}{\binom{N}{C}}\right)^{k_1} \cdots \left(\frac{1}{\binom{N}{C}}\right)^{k_{\binom{N}{C}}} = \frac{n!}{k_1! \ldots k_{\binom{N}{C}}!} \left(\frac{1}{\binom{N}{C}}\right)^{n}$$

with $k_1 + \ldots + k_{\binom{N}{C}} = n$. That is, the probability that in n independent draws the *ith* committee, for all $i = 1, \ldots, \binom{N}{C}$, will be chosen exactly k_i times is multinomial.

(ii) *Uniform probability of a node selection*

Based on the above assumptions, with uniform stakes each single node has probability $\frac{C}{N}$ to be part of the selected committee. Therefore in n repeated, independent, draws the

probability for the node to be part of h, with $h = 1, \ldots, n$, committees is again binomial, and given by

$$\left(\begin{array}{c} n \\ h \end{array} \right) \left(\frac{C}{N}\right)^{h} \left(1 - \frac{C}{N}\right)^{n-h} \tag{3}$$

Therefore, in n independent repetitions the expected number of times, EH, a node will be selected as a committee member is $EH = \frac{nC}{N}$ while the variance will be given by $VH = \frac{nC}{N}\left(1 - \frac{C}{N}\right)$. If Algorand wishes this not to exceed an upper bound $b(n)$, then C could be chosen appropriately as follows

$$\frac{nC}{N} \leq b(n) \tag{4}$$

For instance, if $b(n) = \frac{n}{2}$ then

$$C \leq \frac{nN}{2n} = \frac{N}{2}$$

Consistently with one's intuition, it may be interesting to observe that $\frac{C}{N} > \frac{1}{\left(\begin{array}{c} N \\ C \end{array} \right)}$, that is, the probability for a node to be part of a committee is larger than the probability to draw a specific committee, which includes that node.

Also in this case, if H_i with $i = 1, \ldots, N$ and $H_1 + H_2 + \ldots + H_N = n$, are the random variables defining the number of times the *ith* user is drawn in n repeated draws, then

$$P(H_1 = h_1, \ \ldots, H_N = h_N\ ) = \frac{n!}{h_1! \ldots ! h_N!} \left(\frac{C}{N}\right)^{h_1} \cdots \left(\frac{C}{N}\right)^{h_N} = \frac{n!}{h_1! \ldots h_N!} \left(\frac{C}{N}\right)^{n}$$

with $h_1 + h_2 + \ldots + h_N = n$.

(iii) *Non-Uniform probability of a committee selection*

In this paragraph we still assume $a_i = s_i$, however without imposing uniform, symmetric, money holdings. If, as previously discussed, the committee selection is ruled by a ONOV random draw based on PoS, then the committee C_1, formed by the following miners $C_1 = \{1, \ldots, C\}$, will be the most likely, while committee $C_{N-C} = \{(N - C + 1), \ldots, N\}$ the least likely. With asymmetric stakes the probability of selecting a given committee in this case will require much more involved computation.

To gain some insights on the computational involvement, consider, for example, $N = 3$ and $C = 2$. Then because of sequential drawing of nodes, without replacement, when selecting a committee, the probability p_{C_1} of choosing $C_1 = \{1, 2\}$ in a single draw is given by

$$p_{C_1} = \frac{a_1}{a} \frac{a_2}{a_{-\{1\}}} + \frac{a_2}{a} \frac{a_1}{a_{-\{2\}}} = \frac{a_1 a_2 \left(a_{-\{1\}} + a_{-\{2\}}\right)}{a a_{-\{1\}} a_{-\{2\}}} \tag{5}$$

Analogously, for $C_2 = \{1, 3\}$ and $C_3 = \{2, 3\}$ it is

$$p_{C_2} = \frac{a_1 a_3 \left(a_{-\{1\}} + a_{-\{3\}}\right)}{a a_{-\{1\}} a_{-\{3\}}} \ and \ p_{C_3} = \frac{a_2 a_3 \left(a_{-\{2\}} + a_{-\{3\}}\right)}{a a_{-\{2\}} a_{-\{3\}}} \tag{6}$$

Therefore, in n repeated, independent, drawings of a two-members committee, if K_i is the number of times that committee C_i, with $i = 1, 2, 3$, is drawn, with $K_1 + K_2 + K_3 = n$, then the joint probability $P(K_1 = k_1, \ K_2 = k_2; \ K_3 = k_3)$ is again Multinomial and given by

$$P(K_1 = k_1, \ K_2 = k_2; \ K_3 = k_3) = \frac{n!}{k_1! k_2! k_3!} {p_{C_1}}^{k_1} {p_{C_2}}^{k_2} {p_{C_3}}^{k_3} \text{ with } k_1 + k_2 + k_3 = n$$

with $EK_i = np_{C_i}$. Since $p_{C_1} > p_{C_2} > p_{C_3}$ it follows immediately that C_1 is the committee which, on average, is most frequently drawn.

Likewise, the probability that node $j = 1$ for example is included in a committee is

$$p_1 = p_{C_1} + p_{C_2} = \frac{a_1 a_2 \left(a_{-\{1\}} + a_{-\{2\}}\right)}{a a_{-\{1\}} a_{-\{2\}}} + \frac{a_1 a_3 \left(a_{-\{1\}} + a_{-\{3\}}\right)}{a a_{-\{1\}} a_{-\{3\}}} \tag{7}$$

while $p_2 = p_{C_1} + p_{C_3}$ and $p_3 = p_{C_2} + p_{C_3}$.

With different monetary holdings there are some interesting considerations to make when comparing the probability to select a node, with the probability of drawing a committee containing that node.

Consider the following numerical example. Suppose $a_1 = 10$, $a_2 = 5$, $a_3 = 1$. Then $p_{C_1} = 0.8049$, $p_{C_2} = 0.1458$ and $p_{C_3} = 0.0492$ which implies that committee C_1 will be selected in about 80% of the drawings, in almost 15% of the drawings committee C_2 is selected while committee C_3 appears in only 5% of the draws. Hence, in this case, the probability that node $j = 1$ will be a committee member is about 0.95, the probability that $j = 2$ is a committee member is around 0.85 while the probability that $j = 3$ is selected is about 0.20.

It is worth noticing that, for each committee, the above probabilities are lower than the share of the total Algos belonging to the same committee. Indeed, for C_1 the share of Algos over the total number of units would be given by $\frac{15}{16} = 0.93 > 0.8049$, for C_2 given by $\frac{11}{16} = 0.6875 > 0.1458$ while for C_3 it is $\frac{6}{16} = 0.375 > 0.0492$. As for single nodes instead we have that for $j = 1$ his share of Algos are $\frac{10}{16} = 0.625 < 0.95$, for $j = 2$ his share of Algos are $\frac{5}{16} = 0.3125 < 0.85$ while for $j = 3$ we have $\frac{1}{16} = 0.0625 < 0.20$. That is, for each user the share of Algos is higher than the probability to be selected in the committee.

We now ask the following question. Suppose nodes 1 and 2 agree to maximise the probability of being jointly drawn in the committee; what would be the optimal distribution of Algos between them? With the above distribution of Algos the probability $p_{C_1} = 0.8049$ seems already rather high, but could it be higher? The answer is yes, and the reason why can be seen by considering the following assignment of the total 15 Algos units jointly owned by nodes 1 and 2; $a_1 = 8$, $a_2 = 7$, $a_3 = 1$. That is, an allocation where the Algos belonging to the first two nodes are now more evenly distributed between them. In this case $p_{C_1} = 0.8263$, $p_{C_2} = 0.0958$ and $p_{C_3} = 0.0777$. That is, as compared to the initial allocation of Algos, now committee C_1 will increase its selection probability, as well as C_3 while C_2 will decrease its chance to be selected. However, now $p_1 = 0.9222 < 0.95$, $p_2 = 0.9041 > 0.85$ and $p_3 = 0.1736 < 0.20$, that is node 1 will decrease its probability to be drawn, as well as node 3, while node 2 will increase its selection probability.

The example suggests the existence of a trade-off taking place with ONOV: the more equally distributed are the Algos, across committee members, the larger the probability for that committee to be drawn. However, the larger the number of Algos owned by a node, the higher its probability to be drawn. Furthermore, the example also helps illustrating that alternative distributions of Algos, within a subset of users, can produce externalities also affecting the selection probability of nodes outside that subset.

To conclude, it is worth observing that ONOV would certainly provide a larger probability, to be selected in a committee, to nodes with higher stakes. However, once selected such advantage will disappear since each committee member will only have a single vote available when deciding.

2.2. One-Node Multiple-Votes (ONMV)

With ONMV the probability for a node/committee to be drawn is the same as in ONOV. However, the difference now stands in the fact that once drawn, each node, in the committee, will have a number of votes equal to the number of its own Algos. In case of symmetric stakes, in terms of voting power there will be no difference with respect to

ONOV. However, unlike ONOV, if stakes are asymmetric the distribution of votes within the committee will no longer be uniform.

2.3. One-Node Multiple-Draws (ONMD)

With ONMD a node can be drawn multiple times in the committee, and each separate draw is an additional committee member. Therefore, in principle a committee could also be formed by a single node, whose Algos are the only ones that were selected. Hence, in general, node i can be represented by a number of Algos, votes, $V_i = 0, 1, 2, \ldots, C$, which for this reason is a random variable. We begin the discussion considering again the case of uniform money holdings and stakes $a_i = s_i$, and so uniform initial probability to be selected for each node.

(i) *Uniform probability of a node-committee selection*

Since, in this case, $a_i = \frac{a}{N}$ then, assuming $\frac{(N-1)a}{N} > C$, it follows that the probability that agent i will have a number of votes V_i equal to $v = 0, 1, 2, \ldots, Min\left(\frac{a}{N}, C\right)$ is, exactly (or approximately), Hypergeometric and given by

$$P(V_i = v) = \frac{\begin{pmatrix} \frac{a}{N} \\ v \end{pmatrix}\begin{pmatrix} \frac{(N-1)a}{N} \\ C - v \end{pmatrix}}{\begin{pmatrix} a \\ C \end{pmatrix}} \tag{8}$$

Consistently with the intuition, the expected number of votes is given by $EV_i = \frac{C}{N}$, that is coinciding with the probability for a user to be part of a committee in ONOV. Instead, in this case, the probability that a user is part of a committee, namely that she has at least one vote in the committee, is

$$P(V_i > 0) = 1 - \frac{\begin{pmatrix} \frac{(N-1)a}{N} \\ C \end{pmatrix}}{\begin{pmatrix} a \\ C \end{pmatrix}} \tag{9}$$

Likewise, the probability that a particular committee will be drawn can be expressed, again exactly or approximately, by the Multivariate Hypergeometric distribution. More precisely, consider, for example, the probability that $V_i = v_i$, for all $i = 1, 2, , \ldots, N$. Then

$$P(V_1 = v_1, \ldots, V_N = v_N) = \frac{\prod_{i=1}^{N}\begin{pmatrix} \frac{a}{N} \\ v_i \end{pmatrix}}{\begin{pmatrix} a \\ C \end{pmatrix}} \; with \; \sum_{i=1}^{N} v_i = C \tag{10}$$

(ii) *Non-Uniform probability of a node/committee selection*

The above expression could be immediately extended to the case of asymmetric stakes

$$(V_1 = v_1, \ldots, V_N = v_N) = \frac{\prod_{i=1}^{N}\begin{pmatrix} a_i \\ v_i \end{pmatrix}}{\begin{pmatrix} a \\ C \end{pmatrix}} \; with \; \sum_{i=1}^{N} v_i = C \tag{11}$$

and the expected number of votes $E(V_i) = C\left(\frac{a_i}{a}\right)$ showing that the share of Algos held by node i is what drives its average number of votes.

2.4. Sampling with Replacement

We conclude this section by discussing a committee selection made by using a *sampling with replacement scheme*. In this case, ONOV, ONMV and ONMD collapse to the same single selection criterion. Indeed, with symmetric stakes, now the probability that a node will have v available votes in the committee, with $v = 0, 1, \ldots, C$, is binomial and given by

$$\left(\begin{array}{c} C \\ v \end{array} \right) (\frac{1}{N})^{v} (\frac{N-1}{N})^{C-v}$$

and the expected number of nodes given by $EV = \frac{C}{N}$, as in ONMD.

3. Governance Reward and Staking

In the previous sections we anticipated that a main decision for Algorand users is how much money should be *set aside*, as the own *stake*, for block validation and governance participation. In this Section we discuss the *optimal stake* determination for a node related to governance, as founded on the trade-off between participation to governance voting sessions and the temporary *set-aside* of Algos to obtain the right and benefits to such participation. Adopting an ONMV sampling principle, the *stake* will be used to determine the probability with which a node is drawn to become a committee member, and/or the number of his available votes, in a voting session concerning Algorand governance. So, as already mentioned, the larger the stake the higher the probability to be drawn as a voter, however the smaller the amount of money available for transactions. That is, the stake works as a temporary impediment to the use of a portion of one's Algos. Though the governance analysis will be currently related to the Algorand Foundation, its insights may turn out to be useful also for Algorand Inc. and other PoS based blockchain platforms.

Let a_i again be the Algos held by node i, and likewise define its *stake* for the next voting session as the amount s_i, such that $s_i \leq a_i$. Assume ONMV and suppose $m = 1, 2, \ldots, M$, is the generic *binary* item in the agenda of the next voting session, with M being the number, as well as the set, of items in the agenda.

For each node $i = 1, 2, \ldots, N$ the approval and rejection, of an item implies different levels of utility defined as follows

$$\left\{ \begin{array}{ll} u_{mi} & if\ m\ is\ approved \\ u_{-mi} & if\ m\ \ is\ not\ approved \end{array} \right. \tag{12}$$

In principle, u_{mi} and u_{-mi} could stand in any order; that is, a larger utility level could come either from approval as well as from disapproval of an item.

In a general setting, when choosing the stake s_i, the node will face *two types of uncertainties*. First, if it will be selected to be a committee member and then if, once selected, for each item to be voted either $Max(u_{mi}, u_{-mi})$ or $Min(u_{mi}, u_{-mi})$ would be realised.

Furthermore, suppose $s = (s_i, s_i, \ldots, s_N) = (s_i, s_{-i})$ is the vector of the stakes chosen by the nodes, where $s_{-i} = s - \{s_i\}$. Then, conditional to having been selected as a committee member, we can define $\pi_i(s_i, s_{-i})$ to be the probability with which node i obtains $Max(u_{mi}, u_{-mi})$, and $1 - \pi_i(s_i, s_{-i})$, the probability with which i obtains $Min(u_{mi}, u_{-mi})$. Its expression clarifies that in general $\pi_i(s_i, s_{-i})$ depends on s_i as well as on s_{-i}, with the former being chosen by i, while the latter chosen by nodes other than i.

Therefore, the utility level $u_i(m)$ associated to the voting outcome is a Bernoulli random variable, defined as

$$u_i(m) = \left\{ \begin{array}{ll} Max(u_{mi}, u_{-mi}) & with\ probability\ \ \pi_i(s_i, s_{-i}) \\ Min(u_{mi}, u_{-mi}) & with\ probability\ \ 1 - \pi_i(s_i, s_{-i}) \end{array} \right. \tag{13}$$

In what follows we assume that $Max(u_{mi}, u_{-mi}) > Min(u_{mi}, u_{-mi})$ for at least one m. Later, in Section 3.1.3, we'll discuss the implications of $Max(u_{mi}, u_{-mi}) = Min(u_{mi}, u_{-mi})$ for all m.

Hence, for each item m, it is possible to define the expected utility of the node in the voting session as

$$Eu_i(m) = \pi_i(s_i, s_{-i})Max(u_{mi}, u_{-mi}) + (1 - \pi_i(s_i, s_{-i}))Min(u_{mi}, u_{-mi}) \tag{14}$$

Finally, suppose T is the time length during which the monetary stake s_i is unavailable to node i. Thus, consider (14) and assume for the *time being* that the selection to become a committee member is based on (symmetric) money holdings and that all the users are willing to be drawn for governance participation. Hence each user is selected with probability $\frac{C}{N}$. To investigate the optimal *stake* for node i we can introduce a simple, though sufficiently general, definition for its preferences as follows.

$$U_i(s_i) = \begin{cases} W_i(a_i - Ts_i + r) + \sum_{m=1}^{M} Eu_i(m) & \textit{with probability } \frac{C}{N} \\ W_i(a_i + r) & \textit{with probability } 1 - \frac{C}{N} \end{cases} \tag{15}$$

In (15) $r \geq 0$ stands for the reward in Algos paid by Algorand for participation to governance voting sessions, and more broadly we assume that r is paid to all users simply for their willingness to be selected, even if they are not selected, and independently of their stakes. Alternative models may consider a per-unit-of-the-stake reward, such as rs_i, and/or no reward if the user is not selected.

Indeed, admittedly, Equation (15) may be considered as a benchmark case. However, besides its possible interest per se, if rewards are given to all those nodes which are available to participate in block certification/governance activities, even if not selected, probabilistic asymmetries may tend to disappear. The following simple example briefly illustrates why this is so. Consider two nodes, $i = 1$ and $i = 2$ and suppose $a_1 > a_2$, so that the ratio between the two nodes' selection probability is $\frac{a_1/a}{a_2/a} = \frac{a_1}{a_2}$. Now assume that both nodes are willing to participate in governance activities and receive r currency units as a reward.

The ratio between the selection probabilities would now become $\frac{a_1+r}{a_2+r} < \frac{a_1}{a_2}$, which is then reduced as compared to what it was before the reward assignment. Hence, rewarding all available nodes, even if not selected, could be a policy measure adopted by Algorand to mitigate asymmetries in money holdings.

Unwillingness to participate in governance implies $U_i(s_i) = W_i(a_i)$, namely the utility would be given by the availability of the total money holdings. As well as with the utility for being available to vote but unselected, $U_i(s_i) = W_i(a_i + r)$, assuming $U_i(s_i) = W_i(a_i)$ is also a simplification since a user may obtain some benefits from the voting sessions, even if she does not participate. Yet, this will not meaningfully affect the analysis. Finally, in (15) the term $-Ts_i$ is modelling the disutility due to the temporary unavailability of the stake; later we shall also consider alternative ways to formalize such disutility.

Additionally, $a_i + r \geq Ts_i$, which captures the idea that the larger T the smaller should be the stake s_i for the constraint to be satisfied.

Equation (15) clarifies that, before the random selection of committee members, the utility level of a node is a random variable. Indeed in case the node is not selected as committee member, which takes place with probability $1 - \frac{C}{N}$, the amount of money planned to be the *stake* would not be *set aside* and remain available to the node. Instead, if the node is selected as committee member, with probability $\frac{C}{N}$, then the *stake* will be set aside and used in the voting sessions. Finally, we suppose the function $W_i(x)$ to be increasing and concave in the (monetary) argument x. Therefore, conditional to being willing to participate in Algorand governance, the node expected utility, as a function of the stake, is given by

$$EU_i(s_i) = \left(1 - \frac{C}{N}\right) W_i(a_i + r) + \left(\frac{C}{N}\right) [W_i(a_i - Ts_i + r) + \sum_{m=1}^{M} Eu_i(m)] \tag{16}$$

Assuming differentiability of the relevant functions, to maximise (16) with respect to s_i we take its first derivative to obtain the following expression

$$\frac{dU_i(s_i)}{ds_i} = \left(\frac{C}{N}\right)[-T\frac{dW_i(a_i - Ts_i + r)}{ds_i} + \sum_{m=1}^{M} \frac{dEu_i(m)}{ds_i}] \tag{17}$$

Equation (17) may be hard to analyze unless we introduce some additional assumptions. To do so, in what follows we set $Max(u_{mi}, u_{-mi}) = 1$ and $Min(u_{mi}, u_{-mi}) = 0$. Hence,

$$\sum_{m=1}^{M} Eu_i(m) = M\pi_i(s_i, s_{-i}) \tag{18}$$

To grant consistency in the unit of measurement, we shall interpret $M\pi_i(s_i, s_{-i})$ as the monetary equivalent of the user's utility induced by the voting session.

Finally, since users hold the same quantity of Algos, $a_i = \frac{a}{N}$ and committee members are drawn according to the Algos held in their wallet (rather than to the stake) following the ONMV criterion, then, based on the above assumptions, $\pi_i(s_i, s_{-i})$ can take the following, particularly simple, form

$$\pi_i(s_i, s_{-i}) = (\frac{s_i}{S_C}) \tag{19}$$

where $S_C = \sum_{j=1}^{C} s_j$ is the total stake of all committee members. That is, in such a simplified framework, we suppose that nodes are completely uncertain as to whether or not they will be able to approve the items, in the agenda, and as a reasonable approximation they consider the probability of approval proportional to their own stakes and equal to $(\frac{s_i}{S_C})$. Later we shall also explicitly introduce the possibility of alliances in voting.

3.1. A Symmetric Nash Equilibrium of the "Stake Game" with Identical, Risk Neutral, Agents

To obtain a close expression of the stake, now assume identical preferences across nodes, and risk neutrality, that is

$$W_i(a_i - Ts_i + r) = a_i - Ts_i + r \ \ with \ \frac{(a_i + r)}{T} \ \ \geq s_i$$

Equalising to 0 Equation (17), we obtain

$$\frac{dEU_i(s_i)}{ds_i} = \left(\frac{C}{N}\right)[-T + (\frac{S_C - s_i}{S_C^2})M] = 0 \tag{20}$$

The above condition shows that one's stake depends on the other users' stakes. For this reason, users interact strategically giving rise to what we call the *Stake Game*. We can therefore formulate the following first result.

Proposition 1. *The unique symmetric Nash Equilibrium s_*, of the Stake Game with risk neutral users is*

$$s_* = Min\left(\frac{M(C-1)}{TC^2}, \ \frac{a}{N}, \frac{\frac{a}{N} + r}{T}\right) \tag{21}$$

Proof of Proposition 1. *Immediate. Indeed, because of symmetry it is $s_i = s_*$ and therefore $S_C = Cs_*$, which replaced into (20) provides $s_* = Min(\frac{M(C-1)}{TC^2}, \frac{a}{N}, \frac{\frac{a}{N}+r}{T})$.* □

Despite its simplicity, Equation (21) provides some interesting early insights on the optimal stake level for the nodes. First observe that the equilibrium s_* may be independent of N. Indeed, intuitively this is because selection to become a committee member in this case does not depend on the stake, but only on the Algos held in the wallet, which is the same for all users. For identical, risk neutral, users the optimal stake may also not depend on r, but only on the utility gains expected to obtain in the governance process. This is due

to the linearity of the utility function and to the reward being stake independent. It is also easy to realise that, because of this, any reward lower than r for unselected, but willing to participate, users will leave s_* unaltered.

Then notice also that s_* may increase in M while decreasing in the size of the committee, for $C > 1$, and in the time horizon T during which the monetary stake cannot be used by nodes. In the extreme case of $C = 1$, then $s_* = 0$, which is its global minimum. Instead, for $C > 1$ the minimum value of s_*, as a function of C, would be reached for $C = N$ and equal to $Min\left(\frac{M(N-1)}{TN^2},\ \frac{a}{N}, \frac{\frac{a}{N}+r}{T}\right)$. Finally, it is easy to see that s_* obtains its maximum at $C = 2$, and equal to $Min\left(\frac{M}{4T},\ \frac{a}{N}, \frac{\frac{a}{N}+r}{T}\right)$.

It follows that, in such symmetric equilibrium, the total community stake is

$$S_N = Ns_* = \min\left(\frac{NM(C-1)}{TC^2}, a, \frac{a+Nr}{T}\right) \tag{22}$$

which is increasing with N, unless $S_N = a$, and decreasing with $C > 1$. However, only part of (22) will be effectively set aside in the platform, the one related to the committee members, that is

$$S_C = Cs_* = \min\left(\frac{M(C-1)}{TC}, \frac{Ca}{N}, \frac{C\left(\frac{a}{N}+r\right)}{T}\right)$$

which unlike (22) is increasing, rather than decreasing, with C.

Finally, in case $s_* = \frac{M(C-1)}{TC^2}$ then the *indirect* (maximum) expected utility function of the node is given by

$$\mathrm{E}U_i(s_i = s_*) = \frac{a}{N} + r + \left(\frac{C}{N}\right)\left[-\frac{M(C-1)}{C^2} + \frac{M}{C}\right] = \frac{a}{N} + r + \frac{M}{NC} \tag{23}$$

which decreases with N and C, increases with a, M, r and is independent of T.

As a final point, notice that (23) confirms that in the model willingness to participate in governance activities is always preferable to non-participation, since the expected utility will be larger than $U_i(s_i) = \frac{a}{N}$. This may also be due to the fact that, in (16), the only *costs* faced by users for participation in governance voting sessions is given by the unavailability of the monetary stake for a period of time. With additional, specific, participation costs for keeping the node always operating etc., the above preference for the willingness to participate in governance activities may be reversed.

The previous analysis can be extended in several directions, which we begin doing in the next paragraph.

3.1.1. Exponential Time Discounting

We start extending the model by considering alternative ways to introduce the time-period during which the stake must be unspent for. More specifically, suppose that now

$$W_i\left(a_i - \delta^{-T}s_i + r\right) = a_i - \delta^{-T}s_i + r \text{ with } a_i + r \geq \delta^{-T}s_i \tag{24}$$

where $0 < \delta < 1$ is the user's discount factor, and so with $\delta^{-T} > 1$, representing the user's intertemporal preference. In this case

$$s_* = Min\left(\frac{\delta^T M(C-1)}{C^2}, \frac{a}{N}, \delta^T\left(\frac{a}{N} + r\right)\right) \tag{25}$$

which, as compared to (21), explicitly embodies the importance assigned by the user to the future. Indeed, while s_* still decreases with T it increases with δ. That is, the more patient the user, the larger the *stake*. This is because the node is more willing to wait and *set-aside* the available money for a period of time in order to participate in a governance voting session, which it considers as important.

3.1.2. Stake-Proportional Committee Selection Probability

Until now, in the analysis, we assumed the probability for being selected as a committee member to depend on the Algos owned in the users' wallets, and not on their own stake. We then assumed Algos in the community to be uniformly held by nodes, so that with ONMV the probability to select a single account was $\frac{C}{N}$.

In what follows, somewhat more realistically, we suppose that also the selection probability depends on the stake, to investigate how this may affect the optimal s_* in a symmetric Nash Equilibrium of the stake game. In this case, following (iii) of Section 2.1, to gain some useful insights we simplify the computation assuming $N = 3$ and $C = 2$. Therefore, the probability for node 1 to be selected as committee member is now

$$p_1(s_1, s_{-1}) = p_{C_1} + p_{C_2} = \frac{s_1 s_2 \left(s_{-\{1\}} + s_{-\{2\}}\right)}{S_N s_{-\{1\}} s_{-\{2\}}} + \frac{s_1 s_3 \left(s_{-\{1\}} + s_{-\{3\}}\right)}{S_N s_{-\{1\}} s_{-\{3\}}} = (\frac{s_1}{S_N})(1 + \frac{s_2}{s_{-\{2\}}} + \frac{s_3}{s_{-\{3\}}}) \quad (26)$$

where $S_N = s_1 + s_2 + s_3$ and $s_{-\{i\}} = S_N - s_i$. The definition of $p_2(s_2, s_{-2})$ and $p_3(s_3, s_{-3})$ is analogous to (26).

Therefore, still considering $i = 1$ and risk neutrality, now it is clear that

$$EU_1(s_1) = \frac{a}{N} + r + p_1(s_1, s_{-1})[-Ts_1 + \pi_1(s_1, s_{-1})M]$$

Hence

$$\frac{dU_1(s_1)}{ds_1} = \frac{dp_1(s_1)}{ds_1}[-Ts_1 + \pi_1(s_1, s_{-1})M] + p_1(s_1, s_{-1})\left[-T + \frac{d\pi_1(s_1)}{ds_1}M\right] \quad (27)$$

where

$$\frac{dp_1(s_1)}{ds_1} = \left(\frac{s_{-\{1\}}}{S_N^2}\right)\left(1 + \frac{s_2}{s_{-\{2\}}} + \frac{s_3}{s_{-\{3\}}}\right) - \left(\frac{s_1}{S_N}\right)\left(\frac{s_2}{s_{-\{2\}}^2} + \frac{s_3}{s_{-\{3\}}^2}\right) \quad (28)$$

and again

$$\frac{d\pi_1(s_1)}{ds_1} = \left(\frac{S_C - s_1}{S_C^2}\right) \quad (29)$$

According to (21) the optimal stake with $N = 3,\ C = 2$ would be

$$s_* = Min\left(\frac{M(C-1)}{TC^2}, \frac{a}{N}, \frac{\frac{a}{N} + r}{T}\right) = Min\left(\frac{M}{4T}, \frac{a}{3}, \frac{\frac{a}{3} + r}{T}\right) \quad (30)$$

Instead, replacing (28) and (29) in (27), the first order condition associated to (27) provides a maximum, under symmetry $s_1 = s_2 = s_3 = s_*$ we obtain

$$s_* = Min\left(\frac{4M}{11T}, \frac{a}{3}, \frac{\frac{a}{3} + r}{T}\right) \quad (31)$$

thus larger, when less than $\frac{a}{3}$, with respect to $\frac{M}{4T}$. The intuition is immediate; if also the selection for becoming a committee member is based on the *stake*, rather than on the overall amount of Algos held in the wallet, then nodes have an incentive to augment their *stake* in order to increase the joint likelihood of being selected, as committee member, and succeed in the voting session.

3.1.3. Equal utility in voting

Before replacing risk neutral with risk averse users, in Section 3.2, we briefly discuss the case in which $Max(u_{mi}, u_{-mi}) = Min(u_{mi}, u_{-mi})$ for all $m = 1, 2, \ldots, M$, namely when

the user is completely indifferent about the outcomes of each item under consideration in the voting session. In this circumstance, (15) could simplify to

$$U_i(s_i) = \begin{cases} W_i(a_i - Ts_i + r) & \text{with probability } \frac{C}{N} \\ W_i(a_i + r) & \text{with probability } 1 - \frac{C}{N} \end{cases}$$

because the user would obtain the same benefits, whether or not she's a committee member. It is easy to see that for a such user it would be optimal to set $s_i = \varepsilon > 0$, with ε small enough, but such that

$$-T\varepsilon + r > 0$$

and

$$EU_i(s_i = \varepsilon) = \frac{W_i(a_i - T\varepsilon + r)C}{N} + W_i(a_i + r)\left(1 - \frac{C}{N}\right) > W_i(a_i)$$

Indeed, if the above two inequalities hold, a positive stake is optimal and the chain initialised. The finding suggests that users must perceive voting to be important for them, in order to find it profitable, setting aside stakes of meaningful size.

3.2. A Symmetric Nash Equilibrium with Identical, Risk Averse, Agents

Assume now that nodes are all risk averse, with the same preferences given by

$$W_i(a_i - Ts_i + r) = log(a_i - Ts_i + r) \tag{32}$$

Logarithmic utility functions are interesting, and frequently used in economics, because when a user owns say x Algos, the marginal, incremental, monetary equivalent of the utility of an additional small amount of Algos is $\frac{1}{x}$, which may appear reasonable in various circumstances. In this case, if nodes hold the same amount of Algos and the selection to become a committee member depends again on the Algos held, the analogue of (20) becomes

$$\frac{dU_i(s_i)}{ds_i} = -\frac{T}{(\frac{a}{N} - Ts_i + r)} + \frac{C}{N}(\frac{S_C - s_i}{S_C^2})M = 0 \tag{33}$$

From (33) the next result follows

Proposition 2. *The unique symmetric Nash Equilibrium of the Stake Game with logarithmic utility function, is*

$$s_i = s_* = Min\left(\frac{(\frac{a}{N} + r)M(C-1)}{T(NC + M(C-1))}, \frac{a}{N}\right) \tag{34}$$

Proof of Proposition 2. *Indeed, again because of symmetry it is* $s_i = s_*$ *and* $S_C = Cs_*$*, which replaced into (33) provide* $s_* = Min\left(\frac{(\frac{a}{N}+r)M(C-1)}{T(NC+M(C-1))}, \frac{a}{N}\right)$*, proving the result.* □

As compared to Proposition 1, the finding in Proposition 2 exhibits some differences. Due to risk aversion, when $s_* = \frac{(\frac{a}{N}+r)M(C-1)}{T(NC+M(C-1))}$ the optimal stake level may be positively related to the reward r and the amount of Algos $\frac{a}{N}$ held in the wallet, which instead played no role in the analogous expression with risk neutrality. Moreover, as M becomes large, (34) does not grow indefinitely like in (30), rather it converges to $\frac{(\frac{a}{N}+r)}{T}$. Finally, in general, whether the expression in (30) is larger than (34) will depend on the size of the parameters.

3.3. The Optimal Stake with Risk Neutrality and Alliances

In this paragraph we further extend the model discussing how stakes, in a symmetric Nash Equilibrium with risk neutral users, may change when a node is allied with other nodes, where an alliance implies that the relevant nodes cast the same vote for the same issue under voting.

Suppose again that nodes hold the same amount of Algos $\frac{a}{N}$ and the probability to be selected as a committee member does not depend on the stake but on the number of Algos held by a node. Assume nodes $i = 1$ and $i = 2$ are allied while the others are not.

It follows that the success probability (19) in the voting session is in turn a random variable whose value depends on whether both $i = 1$ and $i = 2$ are drawn, alternatively, only one of them is selected or else none of them becomes a committee member. Consider, for example, node $i = 1$, observing that for $i = 2$ the reasoning would be analogous. In order to fully describe $\pi_1(s_1, s_{-1})$, in this case we first need to compute the probabilities of the possible drawing of the two users which, under the ONMV selection criterion, are given by the following expressions:

$$Probability \ = \begin{cases} \frac{C(C-1)}{N(N-1)} & to\ draw\ both\ i=1\ and\ i=2 \\ \frac{C(N-C)}{N(N-1)} & to\ draw\ i=1\ but\ not\ i=2 \\ \frac{C(N-C)}{N(N-1)} & to\ draw\ i=2\ but\ not\ i=1 \\ 1-\frac{C(2N-C-1)}{N(N-1)} & to\ draw\ neither\ i=1\ nor\ i=2 \end{cases} \tag{35}$$

Based on (35), and assuming that users 1 and 2 will cast the same votes, we can now define the success probability, for each item under voting, in the previous circumstances as

$$\pi_1(s_1, s_{-1}) = \begin{cases} \left(\frac{s_1}{S_C}\right) & with\ probability\ \frac{C(N-C)}{N(N-1)} \\ \left(\frac{s_2}{S_C}\right) & with\ probability\ \frac{C(N-C)}{N(N-1)} \\ \left(\frac{s_1+s_2}{S_C}\right) & with\ probability\ \frac{C(C-1)}{N(N-1)} \end{cases} \tag{36}$$

According to (36), we can also define the utility of user 1, as a random variable, in the following way

$$U_1(s_1) = \begin{cases} W_1(a_1 + r) & with\ probability\ 1-\frac{C(2N-C-1)}{N(N-1)} \\ W_1(a_1 + r) + M\left(\frac{s_2}{S_C}\right) & with\ probability\ \frac{C(N-C)}{N(N-1)} \\ W_1(a_1 - Ts_1 + r) + M\left(\frac{s_1}{S_C}\right) & with\ probability\ \frac{C(N-C)}{N(N-1)} \\ W_1(a_1 - Ts_1 + r) + M\left(\frac{s_1+s_2}{S_C}\right) & with\ probability\ \frac{C(C-1)}{N(N-1)} \end{cases} \tag{37}$$

and therefore

$$EU_1(s_1) = \left(1 - \frac{C}{N}\right) W_1(a_1 + r) + \left(\frac{C}{N}\right)[W_1(a_1 - Ts_1 + r) + M\left(\frac{s_1 + s_2}{S_C}\right)] \tag{38}$$

Interestingly, (38) coincides with (16) except for s_2 appearing in its last term.

Suppose again W_1 to be linear. Then taking the first order condition, related to (38), with respect to s_1, we obtain

$$\frac{dEU_1(s_1)}{ds_1} = \left(\frac{C}{N}\right)[-T + (\frac{S_C - (s_1 + s_2)}{S_C^2})M] = 0 \tag{39}$$

Assuming symmetry, that is $s_1 = s_2 = s^*$ and $s_i = s^{**}$ for all $i = 3, \ldots, C$ from (39), then $S_C = 2s^* + (C-2)s^{**}$ and it follows that

$$s^{**} = \frac{(C-2)M}{(C-1)^2 T} \tag{40}$$

and

$$s^* = \frac{(C-2)M}{2(C-1)^2 T} \tag{41}$$

Equations (40) and (41) seem to suggest that with alliances, individual stakes may decrease, for both the allied nodes and the remaining ones, as compared to when there are no alliances. Indeed, in our model the allied users, that is 1 and 2, split between them the stake of those users acting independently, since they behave *as if* they were a single user. The intuition for this is immediate; an alliance reduces the number of competing voters in the committee which in turn reduces the needed stake.

Admittedly, the assumptions driving the results simplify reality; nonetheless, the findings may provide some interesting suggestions for policy decisions. For instance, following (40) and (41), if larger stakes are preferable to smaller ones, for Algorand, then the platform should try to keep users as independent as possible when voting.

4. Conclusions

In the paper we have discussed two main issues related to consensus formation inspired by the Algorand platform: the selection of committees voting for governance and the users' optimal stake. To our knowledge, this is the first contribution referring to Algorand which investigates these issues from an economic perspective. Admittedly the model, together with its extensions, has limitations. Yet we believe the findings may provide some interesting early insights for policy making in PoS-based blockchains, such as Algorand. First, the users' monetary stakes are very sensitive to their dynamic preferences. Broadly speaking, the more patient are the users the larger the stake and, conversely, if they are impatient. Additionally, the stake seems to be negatively related to the time span during which it is unavailable to users. Therefore, if the platform is interested in users setting aside meaningful stakes, it should keep such time horizon sufficiently short and/or, if possible, induce sufficiently patient users to join the community. Additionally, the mechanism to select voting committees may also affect the stake. In the paper we focused on the one-node-multiple-votes (ONMV) criterion, however hinting at how alternative criteria might have different consequences on the stake size. Moreover, the users' risk attitude can also play an important role in defining the stake size. In particular, we argued how with risk aversion the numerosity of nodes in the population, as well as the number of committee members, may play a different role in the optimal stake as compared to risk neutral preferences. Such difference emerges also in the role of the benefits associated to the voting outcomes. Finally, the model also suggests that alliances, between committee members, may decrease the individual stakes since they basically reduce the number of independent voters.

Finally, it is worth pointing out that some more general versions of the paper, to consider users with different money holdings, alternative users' preferences and selection mechanisms, can be simulated. This can be done by extending the assumptions in the model and computing the stakes evolution.

Funding: This research was funded by the Algorand Foundation.

Institutional Review Board Statement: Not applicable.

Informed Consent Statement: Not applicable.

Data Availability Statement: Not applicable.

Acknowledgments: I would like to the thank the Algorand Foundation for having funded this research project.

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

References

1. Bentov, I.; Lee, C.; Mizrahi, A.; Rosenfeld, M. Proof of activity: Extending Bitcoin's proof of work via proof of stake. *ACM Sigmetrics* **2014**, *42*, 34–37. [CrossRef]
2. Bentov, I.; Gabizon, A.; Mizrahi, A. Cryptocurrencies without proof of work. *arXiv* **2017**, arXiv:1406.5694v9 [cs.GT].
3. BitFury Group, Proof of Stake versus Proof of Work. *White Paper*. 2015. Available online: https://bitfury.com/content/downloads/pos-vs-pow-1.0.2.pdf (accessed on 9 February 2022).
4. Buterin, V.; Griffith, V. Casper the friendly finality gadget. *arXiv* **2019**, arXiv:1701.09437v4 [cs.CR].

5. Brown-Cohen, J.; Narayanan, A.; Psomas, C.-A.; Weinberg, S. Formal barriers to longest-chain proof-of-stake protocols. *arXiv* **2018**, arXiv:1809.06528v1 [cs.GT].
6. Chen, J.; Micali, S. Algorand. *Theor. Comput. Sci.* **2019**, *177*, 155–183. [CrossRef]
7. Deirmentzoglou, E.; Papakyriakopoulos, G.; Patsakis, C. A survey on long-range attacks for proof of stake protocols. *IEEE Access* **2019**, *7*, 28712–28725. [CrossRef]
8. Dimitri, N. Monetary dynamics with proof-of-stake. *Front. Blockchain* **2021**, *4*, 443966. [CrossRef]
9. Fan, L.; Zhou, H. A scalable proof-of-stake blockchain in the open setting. *Cryptol. Eprint Arch. Rep.* **2017**, *2017*, 656.
10. Fanti, G.; Kogan, L.; Oh, S.; Ruan, K.; Viswanath, P.; Wang, G. Compounding of wealth in proof-of-stake cryptocurrencies. In *Financial Cryptography*; LNCS; Goldberg, I., Moore, T., Eds.; Springer: Berlin/Heidelberg, Germany, 2019; Volume 11598, pp. 42–61.
11. Ferdous, S.; Chowdury, M.; Hoque, M.; Colman, A. Blockchain consensus algorithms: A Survey. *arXiv* **2020**, arXiv:2001.07091v2 [cs.GT].
12. Fooladgar, M.; Manshaei, M.; Jadliwala, M.; Rahman, M. On incentive compatible role-based reward distribution in algorand. In Proceedings of the 50th Annual IEEE/IFIP International Conference on Dependable Systems and Networks (DSN), Valencia, Spain, 29 June–2 July 2020.
13. Gilad, Y.; Hemo, R.; Micali, S.; Vlachos, G.; Zeldovich, N. Algorand: Scaling byzantine agreements for cryptocurrencies. In Proceedings of the the 26th Symposium on Operating Systems Principles (SOSP'17), Shanghai, China, 28 October 2017.
14. Halaburda, H.; Sarvary, M. *Beyond Bitcoin*; Palgrave McMillan: London, UK, 2016.
15. Houy, N. It will cost you nothing to 'kill' a proof-of-stake crypto-currency. *Econ. Bull.* **2014**, *34*, 1038–1044.
16. Kiayias, A.; Russell, A.; David, B.; Oliynykov, R. Ouroboros: A provably secure proof-of-stake blockchain protocol. In Proceedings of the Annual International Cryptology Conference, Santa Barbara, CA, USA, 20–24 August 2017; pp. 357–388.
17. King, S.; Nadal, S. PPCoin: Peer-to-Peer Cryptocurrency with Proof-of-Stake. Available online: https://decred.org/research/king2012.pdf (accessed on 9 February 2022).
18. Leshno, J.; Strack, P. Bitcoin: An Axiomatic Approach and an Impossibility Theorem. *Am. Econ. Rev. Insights* **2020**, *2*, 269–286. [CrossRef]
19. Narayanan, A.; Bonneau, J.; Felten, E.; Miller, A.; Goldfeder, S. *Bitcoin and Cryptocurrency Technologies*; Princeton University Press: Princeton, NJ, USA, 2016.
20. Nguyen, C.; Hoang, D.; Nguyen, D.; Niyato, D.; Nguyen, H.; Dutkiewicz, E. Proof-of-Stake consensus mechanisms for future blockchain networks: Fundamentals, applications and opportunities. *IEEE Access* **2019**, *7*, 85727–85745. [CrossRef]
21. Nijsse, J.; Litchfield, A. A taxonomy of blockchain consensus methods. *Cryptography* **2020**, *4*, 32. [CrossRef]
22. Rijsberger, D.; Szalachowki, P.; Ke, J.; Li, Z.; Zhou, J. LaKSA: A probabilistic proof-of-stake protocol. *arXiv* **2021**, arXiv:2006.01427v2 [cs.CR].
23. Rosu, I.; Saleh, F. Evolution of shares in a proof of stake cryptocurrency. *Manag. Sci.* **2021**, *67*, 661–672. [CrossRef]
24. Saleh, F. Blockchain without waste: Proof of stake. *Rev. Financ. Stud.* **2021**, *34*, 1156–1190. [CrossRef]
25. Vasin, P. Blackcoin's Proof of Stake Protocol v2. *White Paper*. 2014. Available online: https://blackcoin.org/blackcoin-pos-protocol-v2-whitepaper.pdf (accessed on 9 February 2022).
26. Wang, W.; Hoang, D.; Xiong, Z.; Niyato, D.; Wang, P.; Hu, P.; Wen, Y. A Survey on consensus mechanisms and mining management in blockchain networks. *IEEE Access* **2019**, *7*, 22328–22369. [CrossRef]
27. Wang, Y.; Yang, G.; Bracciali, A.; Leung, H.; Tian, H.; Ke, L.; Xu, X. Incentive compatible and anti-compounding of wealth in proof-of-stake. *Inf. Sci.* **2020**, *530*, 85–94. [CrossRef]
28. Xiao, Y.; Zhang, N.; Lou, W.; Hou, Y. A survey of distributed consensus protocols for blockchain networks. *IEEE Commun. Surv. Tutor.* **2020**, *22*, 1432–1465. [CrossRef]