A Game-Theoretic Analysis of Delegation Incentives in Blockchain Governance

Lyudmila Kovalchuk[1,2], Mariia Rodinko[1,3], and Roman Oliynykov[1,3]

[1] Input Output, Singapore
[2] National Technical University of Ukraine
"Igor Sikorsky Kyiv Polytechnic Institute", Kyiv, Ukraine
[3] V.N. Karazin Kharkiv National University, Kharkiv, Ukraine

Abstract. The paper presents a mathematical description of the vote delegation incentive process for funding proposals in a decentralized governance system using a blockchain-based voting. Two models of bribing a delegate by a proposer submitting proposals for funding are considered: "Rational Delegates" and "Emotional Delegates". In terms of parameters describing the voting process, a sufficient condition for a Nash equilibrium is found to be as follows: if both a proposer and a delegate do not intend to participate in bribery. Moreover, it is shown at what share of the briber's stake this condition is satisfied. The main practical result of the paper is the possibility to define what kind of an attacker (in terms of the bribing capability) we will be able to resist under certain parameters.

Keywords: Blockchain, Blockchain Governance, Decentralized Voting, Delegation Incentives, Vote Delegation, Bribery, Nash Equilibrium

1 Introduction

Development of an effective on-chain decentralized governance remains one of the most complicated issues in blockchain-based systems design. Some solutions are hybrid off-chain and on-chain systems (e.g., Dash [1]) while others are purely on-chain governance systems (e.g., Tezos [4], Ethereum Classic [12]). More information about blockchain governance can be found in [5, 11, 13]. The important part of cryptocurrency governance is a self-funding mechanism, often called a treasury system, providing a decentralized funding distribution among projects aimed at cryptocurrency development and growth. One of such funding systems, called Catalyst, is implemented in Cardano [3]. There is a special platform where users can submit their proposals on Cardano improvement [2]. The voting process is carried out on Cardano blockchain using the special voting protocol that provides privacy [17].

As we can see from the past Catalyst Funds (rounds of voting), there are a lot of proposals related to different topics: from development and audit to marketing and global adoption etc. Obviously, stakeholders cannot be experts in all proposals' topics of all Catalyst Funds; they do not have enough time and expertise to go through hundreds of proposals and vote for them. In this regard, the problem of constructing an effective delegation incentive scheme arises. Such a scheme should provide:

- high quality decision-making by professional delegates;
- increased stake participation (stakeholders spend less time and may spend less effort in Catalyst);
- higher level of security against treasury attacks (harder attacks to takeover Catalyst control in fully decentralized environment).

So, the proposed delegation incentive scheme aims to satisfy interests of all honest players, minimize risks arising from malicious behavior and provide growth of the overall cryptocurrency value.

Construction, description and security rationale of such a complex process as Catalyst voting [17] requires use of results from various fields of applied mathematics. Most of all it is related to various areas in cryptology, since many symmetric, asymmetric and hybrid cryptosystems, zero-knowledge proofs, secret sharing schemes etc. are used in the voting process.

One of the most important fields of mathematics employed to build the incentive system in Catalyst is game theory. So, the paper [6] describes a probabilistic approach to incentives distribution using a kind of lottery. Existence of a Nash equilibrium for this model is proved, moreover, the proof

is constructive, and various properties of this equilibrium are described.

Contributions. The obtained results are also in the field of game theory, but they are related only to analysis of the conditions under which a threat of voter bribery arises.

To analyze the threats related to bribery, we fulfilled the following tasks:

- the mathematical model that fully describes the process of receiving incentives by delegates was built;
- two models of bribing a delegate by a proposer were considered: "Rational Delegates" and "Emotional Delegates";
- all possible conditions of a Nash equilibrium existence for these models were analyzed;
- in terms of parameters describing the voting process, a sufficient condition was formulated and proved that a Nash equilibrium exists only if both a proposer and a delegate do not intend to participate in bribery;
- it was shown at what stake share owned by a briber the above condition is satisfied.

1.1 Related Work

The problem of voting on the blockchain was studied in many papers. One of the most fundamental works in this field is [10]. This paper looks into the blockchain application in electronic voting. It was shown that the blockchain technology can solve some of the issues of electronic election systems, but there are questions regarding privacy protection and scalability. Besides, this paper also contains a large and detailed overview of other papers.

Among other studies dealing with the blockchain-based voting we can list the following ones:

- [16] – on advantages of using blockchain for voting and additional opportunities related to the blockchain application;
- [14] – on principles for building an anonymous decentralized e-voting system using a ring signature mechanism and the blockchain technology to ensure anonymity, integrity and transparency;
- [7] – on distributed protocols that privately compute outcomes of a voting scheme revealing a limited amount of information.

However, it should be noted that the subjects of these papers do not include the issue of bribery.

The book [8] studies many aspects of voting including risks related to bribery using game theory (Chapter 7). Similar issues were discussed in more detail in [15], [9], and each of these papers contains its own specific mathematical model corresponding to a certain practical task. However, the results obtained in these papers and recommendations given cannot be used for blockchain-based voting because of the following reasons:

- absence of a "trusted third party";
- identification of a stakeholder offering a bribe is challenging due to blockchain anonymity;
- inability to punish a stakeholder who is bribing because their identity is potentially unknown.

The issues considered in this paper are very different from the above ones as they are related to a completely new model of Catalyst voting developed specially for Cardano. We take into account Catalyst delegate selection scheme, procedure of voting for proposals and stake distribution among voters. So, the results obtained are original and valuable.

2 Preliminaries

There are the following types of participants with specific goals (regarding honest players) in the system:

- *proposers* submit proposals and aim to receive funding for their projects;
- *stakeholders* (aka voters) can either vote for proposals by themselves or delegate this job to delegates (in order for stakeholder to take part in the voting process, their stake must be greater than a given threshold, that is necessary for protection from DoS attacks; the specific value of this threshold is not significant for further analysis); stakeholders are interested in competent decision-making regarding funding (that increases the overall cryptocurrency value and hence the value of their stakes) and rewarding for voting (delegation);

– *delegates* (aka representatives) are authorized to vote on behalf of stakeholders and are interested in competent decision-making regarding funding and rewarding for voting.
– *experts* evaluate proposals and give constructive feedback receiving appropriate rewards for doing this work.

Notations

– $\mathbf{V} = \{V_1, ..., V_m\}$, $m \in \mathbb{N}$ is a set of stakeholders (voters);
– $\mathbf{D} = \{D_1, ..., D_n\}$, $n \in \mathbb{N}$ is a set of delegates;
– $s_1, ..., s_m$, $s_i \in (0, 1)$ are corresponding stake shares of delegates (including a delegated stake);
– $s'_1, ..., s'_n$, $s'_j \in (0, 1)$ are corresponding stake shares of stakeholders;
– $e = const$, $e \in \mathbb{R}_+$ is an escrow that a delegate D_i makes during a registration;
– $\Theta \in \mathbb{R}_+$ is a total treasury fund for one round of voting;
– $\psi \in (0, 1)$ is a share of the treasury fund allocated for delegates' reward (e.g., $\psi = 0.02$);
– $R = \psi\Theta$ is a delegates' total reward;
– $\phi \in [0, 1]$ is a share of the treasury fund allocated for stakeholders' reward (e.g., $\phi = 0.12$);
– $R' = \phi\Theta$ is a stakeholders' total reward;
– $s_{total} \in \mathbb{R}_+$ is a total stake participating in the voting (registered stake);
– $A = \{A_0, A_1, A_2\}$ are shares of the escrow e_i that should be burnt if the delegate D_i has not submitted a ballot, for various delegation levels (e.g. $A = \{0.1, 0.2, 1.0\}$);
– $r_i = Rs_i$ is a total reward of the delegate D_i for honest activity, or if he is bribed but not detected;
– $r^v_j = R's'_j$ is a reward of the stakeholder V_j;
– $\alpha \in [0, 1]$ is a share of a delegates's reward allocated for short-term reward (e.g., $\alpha = 0.7$);
– $r^s_i = \alpha \cdot r_i$ is a short-term reward of the delegate D_i (paid immediately);
– $r^l_i = \begin{cases} r^l_i = (1-\alpha) \cdot r_i & \text{if Conditions 1 and 2 are satisfied} \\ 0 & \text{otherwise} \end{cases}$,
is a long-term reward of the delegate D_i (paid at the end of k rounds of voting);

  Condition 1: $s^{av}_i \geq \lambda \cdot s_{total}$, the delegate P_i is delegated with not less than some constant percent of stake on average during k rounds of voting (e.g., $\lambda = 0.02$)
  Condition 2: D_i participated at least in x rounds of voting out of k (e.g., $x = 6$, $k = 8$)
  If a delegate does not participate in any of k rounds of voting, then he will get neither short- nor long-term rewards for this round
– $r_i = r^s_i + r^l_i$;
– $e_i > 0$, efforts paid by D_i for one round of voting;
– p, probability to bribe D_i ($p = Pr(D_i$ *accepts a bribe*$)$ for randomly chosen D_i);
– q, probability that bribery of D_i will be detected;
– v, the average funding a proposer gets in k rounds of voting;
– $F \in \mathbb{R}_+$, profit that P gets from bribing;
– $C_i = cs_i$, for some $c > 0$, $C_i \in \mathbb{R}_+$, costs that P proposes to D_i as a bribe;
– $K_i = \kappa s_i$, for some $\kappa \geq 0$, risk cost/moral price if D_i accepts a bribe (with "–"); or interest for refusing (with "+") because D_i is proud of himself (if he is honest).

3 Delegation scheme

A delegation process consists of the following steps.

1. Stakeholders and delegates are registered on a blockchain:
   – each delegate D_i makes an escrow e on registration;
   – decision-making process is supported by experts using their separate platform (currently it is IdeaScale [2]).
2. Stakeholders and delegates vote on proposals:

- to be rewarded, a delegate D_i must vote (Yes/No) not less than on a fixed number of proposals and write a rationale for each voted proposal on a public resource with its address provided to stakeholders;
- to be rewarded, a stakeholder V_i must do one of the following:
  - vote (Yes/No) not less than on a fixed number of proposals;
  - delegate their voting power to a delegate who must vote not less than on a fixed number of proposals;
- the current treasury protocol allows parallel voting providing ballot privacy both for stakeholders and delegates.

3. Rewards are paid to stakeholders (r_j^v) and eligible delegates (r_i):
   - a *short-term* delegate's reward r_i^s is paid immediately after the voting;
   - a *long-term* delegate's reward r_i^l is accumulated and paid at the end of k funds (e.g., 2 years);
   - undistributed delegates' rewards are sent back to further funds.
4. If a delegate sends no ballot (covering necessary amount of proposals) or gets no delegation, he gets no reward and a fine (voting liveness protection):
   - no delegation at all: amount of A_0 of his escrow e is burnt;
   - having delegated less than δ (i.e., 1% of the total stake) tokens and no ballot: amount of A_1 of his escrow e is burnt;
   - having delegated at least δ tokens and no ballot: amount of A_2 delegate's escrow e (100%) is burnt.

3.1 Calculation of a delegate's total reward

To define the value of a bribe that may be interesting for some delegate D_i, we first should define the total reward of D_i that he will lose if the fact of bribery is detected. We assume the following.

- D_i loses at least short-term rewards for the nearest k rounds of voting and one long-term reward, assuming that the long-term reward is paid after every k rounds of voting.
- The value of money that D_i gets now is more valuable than the same value of money that will be received later, with some coefficient $t \in (0, 1)$. More precisely, if D_i gets a short-term reward r_i^s in every voting round, then the value in the nearest voting round is r_i^s, in the next voting round this value is tr_i^s, then $t^2 r_i^s$, $t^3 r_i^s$ etc., respectively.

Then the total reward, R_i, for the i-th delegate (D_i) for the whole "cycle" (k voting rounds or the number of rounds between long-term rewards) is:

$$R_i = r_i^s + tr_i^s + ... + t^{k-1} r_i^s + t^{k-1} r_i^l k = r_i^s \frac{1-t^k}{1-t} + t^{k-1} r_i^l k =$$

$$= \alpha R s_i \frac{1-t^k}{1-t} + t^{k-1}(1-\alpha) R s_i k = R s_i \left(\alpha \frac{1-t^k}{1-t} + k(1-\alpha) t^{k-1} \right). \quad (1)$$

The value of t may be taken, in particular, based on deposit interest. For example, if there are 3 months between funds, and the annual interest is 4%, then for every 3rd month the interest is 1%, so $t \approx 0.99$ or so. In this case, and if, for example, $k = 8$, we get the value of the total reward as

$$R_i = R s_i \left(\alpha \frac{1-0.99^8}{0.01} + 8 \cdot (1-\alpha) \cdot 0.99^7 \right) = R s_i \big(7.73\alpha + 7.46 \cdot (1-\alpha) \big) = R s_i (0.27\alpha + 7.46).$$

4 Bribery scenario in pure strategies

A bribery scenario in pure strategies can be modeled as an asymmetric sequential game among delegates and proposers. Each proposer may play two strategies:

- (B_1) – does not propose a bribe for voting in his interest;
- (B_2) – proposes a bribe for voting.

Each delegate may also play two strategies:

- (S_1) – refuses to take a bribe;

– (S_2) – is waiting for a bribe (after that he votes as a briber wants).

If a proposer plays (B_1), i.e., does not try to bribe a delegate D_i, then D_i gets a payoff R_i – a total reward (1) for participation in k sequential votings, taking into account the fact that different parts of the total reward are paid in different times. But in the case if the delegate was waiting for a bribe, i.e. plays (S_2), he also has some moral suffering κ_i that his expectations were not met. Then the payoff of D_i is:

$$u_i(B_1, S_1) = R_i - ke_i, \tag{2}$$

$$u_i(B_1, S_2) = R_i - ke_i - K_i, \tag{3}$$

where e_i are efforts paid by D_i for one voting.

We also assume that a proposer receives some fixed v that may be considered as the average funding he gets in k funds (we do not care about this value and may assume $v = 0$):

$$u_P(B_1, \cdot) = v. \tag{4}$$

If a proposer plays (B_2), a delegate may play two strategies, and his payoff is:

$$u_i(B_2, S_1) = R_i - ke_i + K_i; \tag{5}$$

$$u_i(B_2, S_2) = C_i + (1 - q)R_i - K_i, \tag{6}$$

where all notations were introduced in *Notations* (subsection 2.1).

The payoff of the proposer who plays (B_2) is:

$$u_P(B_2, S_1) = -K_i; \tag{7}$$

$$u_P(B_2, S_2) = F - K_i - C_i, \tag{8}$$

where $F = 0$ iff a stake ratio s_i that briber managed to bribe, is not sufficient to win voting.

The corresponding payoff matrices of the game are:

$$M_i = \begin{matrix} \\ (S_1) \\ (S_2) \end{matrix} \begin{matrix} \begin{matrix} (B_1) & (B_2) \end{matrix} \\ \begin{pmatrix} R_i - ke_i & R_i - ke_i + K_i \\ R_i - ke_i - K_i & C_i + (1 - q)R_i - K_i \end{pmatrix} \end{matrix} \tag{9}$$

payoff for delegate D_i; and

$$M_P = \begin{matrix} \\ (B_1) \\ (B_2) \end{matrix} \begin{matrix} \begin{matrix} (S_1) & (S_2) \end{matrix} \\ \begin{pmatrix} v & v \\ -K_i & F - K_i - C_i \end{pmatrix} \end{matrix} \tag{10}$$

payoff for proposer.

Note that for case of rational players, we assume $\kappa = 0$, hence $K_i = 0$. From (9) and (10) we get the following trivial Proposition.

Proposition 1 (Nash equilibrium in pure strategies). *The conditions for a Nash equilibrium in pure strategies are the following.*

1. *The point (B_1, S_1) is always a Nash equilibrium.*
2. *The point (B_2, S_2) is a Nash equilibrium iff* $\begin{cases} F - K_i - C_i > v; \\ C_i + (1 - q)R_i - K_i > R_i - ke_i + K_i. \end{cases}$
3. *The point (B_1, S_2) is a Nash equilibrium iff* $\begin{cases} K_i = 0; \\ F - C_i < v. \end{cases}$
4. *The point (B_2, S_1) is a Nash equilibrium iff* $\begin{cases} K_i = v = 0; \\ qR_i \geq C_i + ke_i - 2K_i. \end{cases}$

Note that the described voting system is vulnerable to bribery only in the case when (B_2, S_2) is a Nash equilibrium, because in three other points no bribery occurs. Using Proposition 1 and (1), we can formulate the following Corollary.

Corollary 1. *The necessary condition to have a Nash equilibrium (in pure strategies) in the point* (B_2, S_2) *is:*

$$F > v + K_i + C_i > v + K_i + (R_i - ke_i + K_i - (1-q)R_i + K_i) =$$
$$= v + s_i\left(3\kappa + qR\left(\alpha\frac{1-t^k}{1-t} + k(1-\alpha)t^{k-1}\right) - ke_i\right)$$

or

$$s_i < \frac{F + ke_i - v}{3\kappa + qR\left(\alpha\frac{1-t^k}{1-t} + k(1-\alpha)t^{k-1}\right)}.$$

In other words, the necessary condition for a Nash equilibrium in (B_2, S_2) is that the stake that a briber needs to buy to win the voting is not larger than the right part of the equality.

For example, if $F = \$1,000,000$; $k = 8$; $\alpha = 0.15$; $v = \$50,000$; $\kappa = 0$; $e_i = \$2250$; $q = 0.96$; $t = 0.99$; $R = \$360,000$ we get:

$$s_i < \frac{\$1,000,000 + 8 \cdot \$2250 - \$50,000}{0.96 \cdot \$360,000 \cdot \left(0.15 \cdot \frac{1-0.99^8}{0.01} + 8 \cdot 0.85 \cdot 0.99^7\right)} \iff s_i < 0.374.$$

Note 1. According to (7) and (8), to get some profit from bribery, a proposer should bribe some amount of stake, say not less than s, to win voting. As in our model, a bribe is proportional to the amount of stake bribed, the optimal case for him is to bribe delegates $D_{i1}, ..., D_{ik}$ such that:

$$(i_1, ..., i_k) = \arg\min_{j_1,...,j_l}\left\{\sum_{t=1}^{l} s_{j_t} \geq s\right\}.$$

5 Bribery scenario in mixed strategies

We consider two models for two different types of players behavior: rational players and emotional players. Rational players are interested only in increasing their profit or income and do not pay attention to how moral or how honest their actions are. Emotional players may also try to increase their income in some malicious way, but they feel shame if they do this. And vise versa: they may be proud of themselves if they find strength to resist some profitable proposition that may increase their income. In the model with emotional players, we consider that both sides of the game, the delegate and the proposer, are emotional. And so called "moral price" for them is proportional (with some coefficient κ) to the delegated stake ratio that corresponds to the delegate that briber (proposer) is trying to bribe.

In this chapter we first prove some general statements for two-player game that later we use to obtain results for these two models.

For simplicity, we define elements of the matrices M_i and M_P as:

$$M_i = \begin{pmatrix} d_{11} & d_{12} \\ d_{21} & d_{22} \end{pmatrix};\ M_P = \begin{pmatrix} b_{11} & b_{12} \\ b_{21} & b_{22} \end{pmatrix}. \tag{11}$$

For describing a Nash equilibrium in mixed strategies, we need two auxiliary lemmas.

Lemma 1. *Let* $a, b \in \mathbb{R}$, $a + b \neq 0$. *Define* $p = \frac{a}{a+b}$. *Then* $p \in [0,1] \iff \begin{cases} a + b \neq 0; \\ \left[\begin{array}{l} ab \geq 0; \\ ab \leq 0. \end{array}\right. \end{cases}$

Proof. Let us consider four cases for a and b.

Case 1: $a \geq 0$, $b \geq 0$, $a + b \neq 0$.

In this case $0 \leq a \leq a + b$ holds that is equivalent to $0 \leq p \leq 1$.

Case 2: $a \leq 0$, $b \leq 0$, $a + b \neq 0$.

Define $a = -a_1$, $b = -b_1$. Then $p = \frac{-a_1}{-a_1-b_1} = \frac{a_1}{a_1+b_1}$, when $a_1 \geq 0$, $b_1 \geq 0$, $a_1 + b_1 \neq 0$ and, according to Case 1, we get $0 \leq p \leq 1$.

Case 3: $a > 0$, $b \leq 0$, $a + b \neq 0$.

In this case $a + b < a$ and $p < 0$ (if $a + b < 0$) or $p > 1$ (if $a + b > 0$).

Case 4: $a < 0$, $b \geq 0$, $a + b \neq 0$.

In this case $p < 0$ if $b + a > 0$ (or $b > -a$), or $p = \frac{-a}{-(b+a)} = \frac{-a}{-a-b} > 1$ if $b < -a$.

In what follows, we will consider mixed strategies $\mu_1 = (p_1, 1-p_1)$ for the Delegate and $\mu_2 = (p_2, 1-p_2)$ for the Briber. For simplicity, we say "point (p_1, p_2)" instead of "point (μ_1, μ_2)".

Lemma 2. *Let payoff matrices M_i and M_P be as in (11). Then:*

1. *For any p_1, p_2 a point (p_1, p_2) is a Nash equilibrium iff*

$$\begin{cases} d_{21} = d_{11}; \\ d_{12} = d_{22}; \\ b_{21} - b_{22} - b_{11} + b_{12} = 0; \\ b_{12} = b_{22}. \end{cases} \tag{12}$$

2. *A point $\left(p_1, \frac{d_{12}-d_{22}}{d_{21}-d_{11}-d_{22}+d_{12}}\right)$ is a Nash equilibrium for any $p_1 \in [0,1]$ iff*

$$\begin{cases} b_{12} = b_{22}; \\ b_{21} = b_{11}; \\ d_{21} - d_{11} - d_{22} + d_{12} \neq 0; \\ \left[\begin{cases} d_{12} - d_{22} \geq 0; \\ d_{21} - d_{11} \geq 0; \end{cases} \right. \\ \left. \begin{cases} d_{12} - d_{22} \leq 0; \\ d_{21} - d_{11} \leq 0. \end{cases} \right. \end{cases} \tag{13}$$

3. *A point $\left(\frac{b_{12}-b_{22}}{b_{21}-b_{22}-b_{11}+b_{12}}, p_2\right)$ is a Nash equilibrium for any $p_2 \in [0,1]$ iff*

$$\begin{cases} d_{12} = d_{22}; \\ d_{21} = d_{11}; \\ b_{21} - b_{11} - b_{22} + b_{12} \neq 0; \\ \left[\begin{cases} b_{12} - b_{22} \geq 0; \\ b_{21} - b_{11} \geq 0; \end{cases} \right. \\ \left. \begin{cases} b_{12} - b_{22} \leq 0; \\ b_{21} - b_{11} \leq 0. \end{cases} \right. \end{cases} \tag{14}$$

4. *A point $\left(\frac{b_{12}-b_{22}}{b_{21}-b_{22}-b_{11}+b_{12}}, \frac{d_{12}-d_{22}}{d_{21}-d_{22}-d_{11}+d_{12}}\right)$ is a Nash equilibrium iff*

$$\begin{cases} b_{21} - b_{11} - b_{22} + b_{12} \neq 0; \\ \left[\begin{cases} b_{12} - b_{22} \geq 0; \\ b_{21} - b_{11} \geq 0; \end{cases} \right. \\ \left. \begin{cases} b_{12} - b_{22} \leq 0; \\ b_{21} - b_{11} \leq 0. \end{cases} \right. \\ d_{21} = d_{11}; \\ \left[\begin{cases} d_{12} - d_{22} \geq 0; \\ d_{21} - d_{11} \geq 0; \end{cases} \right. \\ \left. \begin{cases} d_{12} - d_{22} \leq 0; \\ d_{21} - d_{11} \leq 0. \end{cases} \right. \end{cases} \tag{15}$$

There are no other Nash equilibria in mixed strategies.

Proof. In our notations,

$$u_i(p_1, p_2) = d_{11}p_1p_2 + d_{12}p_1(1-p_2) + d_{21}(1-p_1)p_2 + d_{22}(1-p_1)(1-p_2).$$

Then, from equality

$$u_i(0, p_2) = u_i(1, p_2)$$

we get

$$(d_{21} - d_{11} - d_{22} + d_{12})p_2 = d_{12} - d_{22}. \tag{16}$$

Case 1: $\begin{cases} d_{12} \neq d_{22}; \\ d_{21} - d_{11} - d_{22} + d_{12} = 0. \end{cases}$
In this case (16) has no solutions.
Case 2: $\begin{cases} d_{12} = d_{22}; \\ d_{21} - d_{11} - d_{22} + d_{12} = 0 \end{cases}$ or $\begin{cases} d_{12} = d_{22}; \\ d_{21} = d_{11}. \end{cases}$
In this case any $p_2 \in [0, 1]$ is a solution of (16).
Case 3: $d_{21} - d_{11} - d_{22} + d_{12} \neq 0$.
In this case (13) has only one solution

$$p_2 = \frac{d_{12} - d_{22}}{d_{21} - d_{11} - d_{22} + d_{12}}.$$

From condition $p_2 \in [0, 1]$ and using Lemma 1, we get additional restrictions:

$$\begin{cases} \begin{bmatrix} d_{12} - d_{22} \geq 0; \\ d_{21} - d_{11} \geq 0; \end{bmatrix} \\ \begin{bmatrix} d_{12} - d_{22} \leq 0; \\ d_{21} - d_{11} \leq 0. \end{bmatrix} \end{cases}$$

Applying the same considerations to the equality

$$u_B(p_1, 0) = u_B(p_1, 1),$$

we complete the proof.

5.1 Model 1: Rational Players

In this subsection the first model with rational players is considered.

Proposition 2. *For Model 1 (with rational players) the conditions for a Nash equilibrium in mixed strategies are:*

– *a Nash equilibrium in the point* (p_1, p_2) *for arbitrary* $p_1, p_2 \in [0, 1]$ *iff*

$$\begin{cases} qR_i = F - ke_i; \\ F = C_i. \end{cases} \tag{17}$$

– *a Nash equilibrium in the point* $(p_1, 1)$ *for arbitrary* $p_1 \in [0, 1]$ *iff*

$$\begin{cases} qR_i \neq C_i + ke_i; \\ v = 0; \\ F = C_i. \end{cases} \tag{18}$$

– *a Nash equilibrium in the point* $(1, p_2)$ *for arbitrary* $p_1 \in [0, 1]$ *iff*

$$\begin{cases} qR_i = C_i + ke_i; \\ v = 0; \\ F < C_i. \end{cases} \tag{19}$$

– *a Nash equilibrium in the point* $(\frac{F-C_i-v}{F-C_i}, p_2)$ *for arbitrary* $p_2 \in [0,1]$ *iff*

$$\begin{cases} qR_i = C_i + ke_i; \\ 0 < v \le F - C_i; \\ F > C_i. \end{cases} \tag{20}$$

– *a Nash equilibrium in the point* $(1,1)$ *iff*

$$\begin{cases} qR_i \ne C_i + ke_i; \\ v = 0; \\ F < C_i. \end{cases} \tag{21}$$

– *a Nash equilibrium in the point* $(\frac{F-C_i-v}{F-C_i}, 1)$ *iff*

$$\begin{cases} qR_i \ne C_i + ke_i; \\ 0 < v \le F - C_i. \end{cases} \tag{22}$$

There are no others Nash equilibria in mixed strategies.

Proof. For Model 1 we can rewrite (12) as

$$\begin{cases} R_i - ke_i - (R_i - ke_i) - (C_i + (1-q)R_i + (R_i - ke_i) = 0; \\ R_i - ke_i = C_i + (1-q)R_i; \\ v - (F - C_i) - v + 0 = 0; \\ v = F - C_i \end{cases}$$

that is equivalent to $\begin{cases} R_i - ke_i = C_i + (1-q)R_i; \\ F = C_i \end{cases}$ or $\begin{cases} qR_i = C_i + ke_i; \\ F = C_i. \end{cases}$

Next, (13) can be rewritten as

$$\begin{cases} v = F - C_i; \\ 0 - (F - C_i) - v + v = 0; \\ (R_i - ke_i) - (R_i - ke_i) - (C_i + (1-q)R_i) + (R_i - ke_i) \ne 0; \\ \left[\begin{cases} R_i - ke_i \ge C_i - (1-q)R_i; \\ R_i - ke_i \ge R_i - ke_i; \end{cases} \right. \\ \left. \begin{cases} R_i - ke_i \le C_i - (1-q)R_i; \\ R_i - ke_i \le R_i - ke_i \end{cases} \right. \end{cases}$$

that is equivalent to $\begin{cases} F = C_i; \\ v = 0; \\ qR_i \ne C_i + ke_i. \end{cases}$

Note that in this case $p_2 = 1$ because of $d_{21} = d_{11}$, so we have a Nash equilibrium as $(p_1, 1)$ for arbitrary $p_1 \in [0,1]$.

Then, the condition (14) can be rewritten as

$$\begin{cases} R_i - ke_i = C_i + (1-q)R_i; \\ R_i - ke_i = R_i - ke_i; \\ 0 - (F - C_i) - v + v = 0; \\ \left[\begin{cases} v - (F - C_i) \ge 0; \\ 0 - v \ge 0; \end{cases} \right. \\ \left. \begin{cases} v - (F - C_i) \le 0; \\ 0 - v \le 0 \end{cases} \right. \end{cases}$$

or

$$\begin{cases} qR_i = C_i + ke_i; \\ F \neq C_i; \\ \left[\begin{cases} v \geq F - C_i; \\ v \leq 0; \end{cases} \right. & \leftrightarrow \begin{cases} v = 0; \\ F - C_i < 0 \end{cases} \\ \left[\begin{cases} v \leq F - C_i; \\ v \geq 0. \end{cases} \right. & \leftrightarrow 0 \leq v \leq F - C_i \end{cases} \iff$$

$$\begin{cases} qR_i = C_i + ke_i; \\ \left[\begin{cases} F - C_i > 0; \\ 0 \leq v \leq F - C_i; \end{cases} \right. \\ \quad \begin{cases} F - C_i < 0; \\ v = 0 \end{cases} \end{cases} \iff \begin{cases} qR_i = C_i + ke_i; \\ \left[\begin{cases} F > C_i; \\ 0 \leq v \leq F - C_i; \end{cases} \right. \\ \quad \begin{cases} F < C_i; \\ v = 0. \end{cases} \end{cases}$$

In this case

$$p_1 = \frac{b_{12} - b_{22}}{b_{21} - b_{22} - b_{11} + b_{12}} = \frac{v - (F - C_i)}{v - (F - C_i) + 0 - v} = \frac{F - C_i - v}{F - C_i} = \begin{cases} 1 & \text{if } v = 0; \\ \frac{F - C_i - v}{F - C_i} & \text{if } 0 \leq v \leq F - C_i \end{cases}$$

and $p_2 \in [0, 1]$.

At last, the condition (15) for Model 1 can be rewritten as

$$\begin{cases} 0 - (F - C_i) - v + v \neq 0; \\ \left[\begin{cases} v - (F - C_i) \geq 0; \\ 0 - v \geq 0; \end{cases} \right. \\ \left[\begin{cases} v - (F - C_i) \leq 0; \\ 0 - v \leq 0; \end{cases} \right. \\ R_i - ke_i - (R_i - ke_i) - (C_i + (1 - q)R_i) + R_i - ke_i \neq 0; \\ \left[\begin{cases} R_i - ke_i - (C_i + (1 - q)R_i) \geq 0; \\ R_i - ke_i - (R_i - ke_i) \geq 0; \end{cases} \right. \\ \left[\begin{cases} R_i - ke_i - (C_i + (1 - q)R_i) \leq 0; \\ R_i - ke_i - (R_i - ke_i) \leq 0 \end{cases} \right. \end{cases} \iff$$

$$\begin{cases} F - C_i \neq 0; \\ \left[\begin{cases} v \geq F - C_i; \\ v \leq 0; \end{cases} \right. \\ \left[\begin{cases} v \leq F - C_i; \\ v \geq 0; \end{cases} \right. \\ qR_i \neq C_i + ke_i; \\ \left[\begin{cases} qR_i \geq C_i + ke_i; \\ qR_i \leq C_i + ke_i \end{cases} \right. \end{cases} \iff \begin{cases} F - C_i \neq 0; \\ qR_i \neq C_i + ke_i; \\ \left[\begin{cases} F - C_i > 0; \\ 0 \leq v \leq F - C_i; \end{cases} \right. \\ \quad \begin{cases} F - C_i < 0; \\ v = 0 \end{cases} \end{cases} \iff \begin{cases} F \neq C_i; \\ qR_i \neq C_i + ke_i; \\ \left[\begin{cases} F > C_i; \\ 0 \leq v \leq F - C_i; \end{cases} \right. \\ \quad \begin{cases} F < C_i; \\ v = 0. \end{cases} \end{cases}$$

In this case

$$p_1 = \begin{cases} 1 & \text{if } v = 0; \\ \frac{F - C_i - v}{F - C_i} & \text{if } 0 \leq v \leq F - C_i \end{cases}$$

and $p_2 = 1$ as $d_{21} = d_{11}$.

5.2 Model 2: Emotional Players

For Model 2 (with emotional players) we can formulate the following proposition.

Proposition 3. *There exists only one Nash equilibrium in the mixed strategies for Model 2 iff:*

$$\begin{cases} 0 \le v \le F - C_i - K_i; \\ (1-q)R_i \ne K_i - C_i - ke_i; \\ qR_i \le C_i + ke_i - 2K_i. \end{cases} \tag{23}$$

Under the condition (23) the point (p_1, p_2) is a Nash equilibrium, where

$$p_1 = 1 - \frac{K_i + v}{F - C_i};\ p_2 = 1 - \frac{K_i}{C_i + ke_i - K_i - qR_i}.$$

Proof. 1. For this Model we can rewrite the first equality in (12) as

$$(R_i - ke_i - K_i) - (R_i - ke_i) = 0,$$

that does not hold because in this Model $K_i \ne 0$.
Then there are no conditions for a Nash equilibrium in (p_1, p_2) for arbitrary $p_1, p_2 \in [0, 1]$.

2. Next, in conditions (13) the second equality can be rewritten as

$$-K_i = v,$$

that does not hold as $v \ge 0$, $K_i > 0$.

3. The second condition in (14) can be rewritten as

$$R_i - ke_i - K_i = R_i - ke_i + K_i,$$

that does not hold as $K_i > 0$.

4. The condition (15) can be rewritten as

$$\begin{cases} -K_i - (F - C_i - K_i) - v + v \ne 0; \\ \left[\begin{cases} v - (F - C_i - K_i) \ge 0; \\ -K_i - v \ge 0; \end{cases} \right. \\ \left[\begin{cases} v - (F - C_i - K_i) \le 0; \\ -K_i - v \le 0; \end{cases} \right. \\ (R_i - ke_i - K_i) - (R_i - ke_i) - (C_i + (1-q)R_i - K_i) + (R_i - ke_i + K_i) \ne 0; \\ \left[\begin{cases} (R_i - ke_i + K_i) - (C_i + (1-q)R_i - K_i) \ge 0; \\ (R_i - ke_i - K_i) - (R_i - ke_i) \ge 0; \end{cases} \right. \\ \left[\begin{cases} (R_i - ke_i + K_i) - (C_i + (1-q)R_i - K_i) \le 0; \\ (R_i - ke_i - K_i) - (R_i - ke_i) \le 0 \end{cases} \right. \end{cases}$$

that is equivalent to

$$\begin{cases} F \ne C_i; \\ v \le F - C_i - K_i; \\ -C_i - (1-q)R_i + K_i - ke_i \ne 0; \\ R_i - ke_i + K_i \le C_i + (1-q)R_i - K_i \end{cases}$$

or

$$\begin{cases} F \ne C_i; \\ v \le F - C_i - K_i; \\ (1-q)R_i \ne K_i - C_i - ke_i; \\ qR_i \le C_i + ke_i - 2K_i = -K_i - (K_i - C_i - ke_i) \end{cases}$$

or

$$\begin{cases} v \le F - C_i - K_i; \\ (1-q)R_i \ne K_i - C_i - ke_i; \\ qR_i \le C_i + ke_i - 2K_i. \end{cases}$$

In this case

$$p_1 = \frac{v - (F - C_i - K_i)}{v - (F - C_i - K_i) - K_i - v} = \frac{F - C_i - K_i - v}{F - C_i} = 1 - \frac{K_i + v}{F - C_i};$$

$$p_2 = \frac{(R_i - ke_i + K_i) - C_i - (1-q)R_i + K_i}{(R_i - ke_i + K_i) - (1-q)R_i + K_i + R_i - ke_i - K_i - R_i + ke_i} = \frac{2K_i - C_i - ke_i + qR_i}{K_i - C_i - ke_i + qR_i} =$$

$$= 1 - \frac{K_i}{C_i + ke_i - K_i - qR_i}.$$

5.3 Sufficient conditions for a Nash equilibrium in terms of a delegated stake ratio

Here we formulate the condition for a Nash equilibrium in terms of a stake ratio that a proposer needs to buy to be guaranteed to win the voting. First, we formulate some general sufficient conditions based on results from 2.4, 2.5.1 and 2.5.2.

Proposition 4. *Let condition*

$$\begin{cases} qR_i > C_i + ke_i - 2K_i; \\ F < C_i \end{cases} \tag{24}$$

hold. Then:

1. *if $K_i = 0$ then:*
   - *(B_1, S_1) is a Nash equilibrium;*
   - *(B_2, S_2) is not a Nash equilibrium;*
   - *there are no Nash equilibria in mixed strategies;*
2. *if $K_i \ne 0$ then the only Nash equilibrium in both pure and mixed strategies is (B_1, S_1).*

Proof. 1. Let $K_i = 0$. From Proposition 1 it is easy to see that (B_1, S_1) is a Nash equilibrium and (B_2, S_2) is not due to the condition $F < C_i$ from (24) that contradicts the first condition $F - K_i - C_i > v > 0$ from p.2 of Proposition 1. Next, this condition also contradicts (17), (18), (20) and (22) in Proposition 2.
The condition $qR_i > c_i + ke_i - 2K_i$ from (24) contradicts (19) in Proposition 2. And note that the condition (24) entails the fulfillment of the condition (21) in Proposition 2 that means (B_1, S_1) is a Nash equilibrium.

2. Let $K_i \ne 0$. Then from Proposition 1 we again see that (B_1, S_1) is a Nash equilibrium, and there are no other Nash equilibria in pure strategies.
From Proposition 3 we also see that there are no Nash equilibria in mixed strategies, because the first inequality in (24) contradicts the third inequality in (23).

In our notations we may rewrite (24) as

$$\begin{cases} s_i > \frac{ke_i}{qR(\alpha \cdot \frac{1-t^k}{1-t} + k(1-\alpha)t^{k-1}) - c + 2\kappa}; \\ s_i > \frac{F}{c} \end{cases}$$

or

$$s_i > \max\left\{ \frac{ke_i}{qR(\alpha \cdot \frac{1-t^k}{1-t} + k(1-\alpha)t^{k-1}) - c + 2\kappa}, \frac{F}{c} \right\}. \tag{25}$$

In other words, the condition (25) is sufficient to have a Nash equilibrium only in (B_1, S_1) and not to have it in (B_2, S_2) and in the mixed strategies.

6 Numerical results

Using the formula from Corollary 1, we calculated the values of the maximum stake share that bribery can buy to have a Nash equilibrium in (B_2, S_2) for the following parameters:

- the total treasury fund for one voting round $\Theta = \$8,000,000$;
- the profit that a proposer gets from bribing $F = \$1,000,000$;
- the number of voting rounds in one cycle: $k = 5, ..., 10$ for Fig. 1 and $k \in [4; 35]$ for Fig. 2;
- the share of short-term reward $\alpha = 0.15$;
- the proposer's average profit in the case of no bribery $v = \$50,000$;
- the moral price $\kappa = 0$;
- the effort spent for voting on all proposals in one voting round, i.e. one Catalyst Fund, $e_i = \$2250$;
- the probability of bribery detection $q = 0.96$;
- the value of a delegate's reward $t = 0.99$;
- the total reward for delegates per one voting round: $R \in [\$136,000; \$1,600,000]$ for Fig. 1 and $R = \$360,000$ for Fig. 2.

The obtained results are summarized in Figures 1-2.

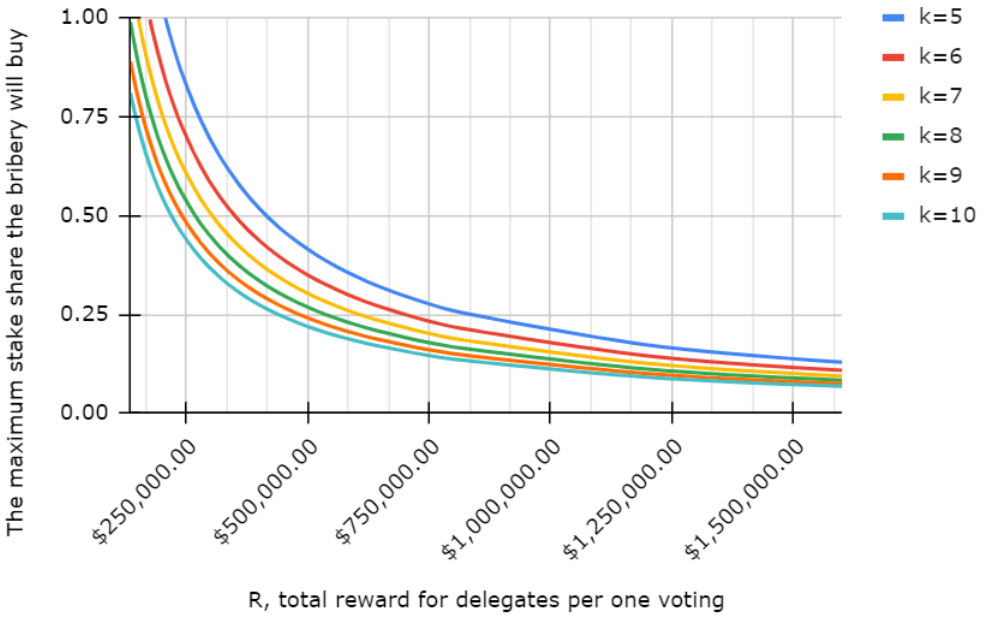


Fig. 1. Dependency of the maximum stake share that bribery can buy to have a Nash equilibrium in (B_2, S_2) on R, the total reward for delegates per voting round (for different k)

Let us look at the Fig. 1 and the curve for $k = 8$ (the green one). For $R = \$440,000$, a Nash equilibrium in the point (B_2, S_2) will exist only if the delegates' stake share that a briber needs to buy to win voting is not larger than 0.3057. That means spending the amount of $R = \$440,000$ for the total delegates' reward, we will provide protection of the delegation scheme against a bribery involving buying more than 30% of delegates' stake.

7 Conclusions

In this paper we present the mathematical model that fully describes the vote delegation incentive process for decentralized governance system for funding distribution that uses a blockchain-based voting. Two models of bribing a delegate by a proposer submitting proposals for funding are considered: "Rational Delegates" and "Emotional Delegates".

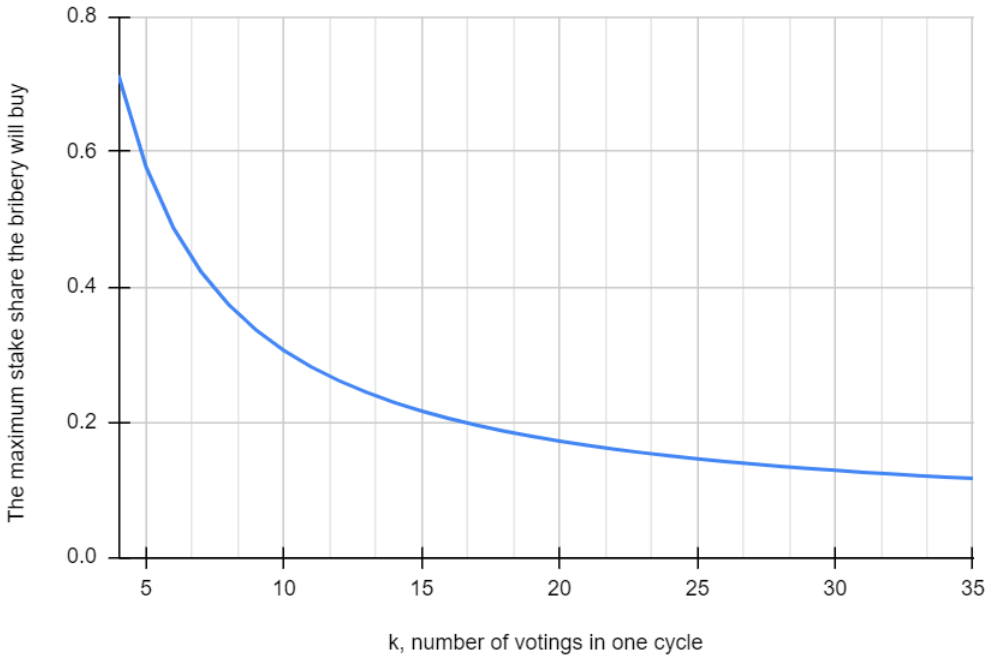


Fig. 2. Dependency of the maximum stake share that bribery can buy to have a Nash equilibrium in (B_2, S_2) on k, the number of voting rounds in one cycle

In terms of parameters describing the voting process, it is stipulated that the sufficient condition that a Nash equilibrium exists only if both a proposer and a delegate do not intend to participate in bribery, and it is shown at what stake share owned by a briber this condition is satisfied. The main practical result of the paper is the possibility to define what kind of an attacker (in terms of the bribing capability) we will be able to resist under certain parameters.

Acknowledgements

We gratefully thank Philip Lazos for fruitful discussions.

Bibliography

[1] Understanding dash governance, 2021. URL https://docs.dash.org/en/stable/governance/understanding.html.

[2] Create, fund and deliver the future of cardano, 2022. URL https://cardano.ideascale.com/.

[3] Fund your project with catalyst, 2022. URL https://developers.cardano.org/docs/governance/project-catalyst.

[4] V. Allombert, M. Bourgoin, and J. Tesson. Introduction to the tezos blockchain. In *2019 International Conference on High Performance Computing & Simulation (HPCS)*, pages 1–10. IEEE, 2019.

[5] H. O. Balogun. *Towards Sustainable Blockchains: Cryptocurrency Treasury and General Decision-Making Systems With Provably Secure Delegable Blockchain-Based Voting*. Lancaster University (United Kingdom), 2021.

[6] G. Birmpas, L. Kovalchuk, P. Lazos, and R. Oliynykov. Parallel contests for crowdsourcing reviews: Existence and quality of equilibria. *arXiv preprint arXiv:2202.04064*, 2022.

[7] F. Brandt and T. Sandholm. Decentralized voting with unconditional privacy. In *Proceedings of the fourth international joint conference on Autonomous agents and multiagent systems*, pages 357–364, 2005.

[8] F. Brandt, V. Conitzer, U. Endriss, J. Lang, and A. D. Procaccia. *Handbook of computational social choice*. Cambridge University Press, 2016.

[9] E. Dal Bó, P. Dal Bó, and R. Di Tella. "plata o plomo?": bribe and punishment in a theory of political influence. *American Political science review*, 100(1):41–53, 2006.

[10] U. Jafar, M. J. A. Aziz, and Z. Shukur. Blockchain for electronic voting system — review and open research challenges. *Sensors*, 21(17), 2021. ISSN 1424-8220. URL https://www.mdpi.com/1424-8220/21/17/5874.

[11] S. Jairam, J. Gordijn, I. da Silva Torres, F. Kaya, and M. Makkes. A decentralized fair governance model for permissionless blockchain systems. In *Proceedings of the International Workshop on Value Modelling and Business Ontologies*, pages 4–5, 2021.

[12] D. Kaidalov, L. Kovalchuk, A. Nastenko, M. Rodinko, O. Shevtsov, and R. Oliynykov. Ethereum classic treasury system proposal. *IOHK RESEARCH REPORT*, 2017.

[13] A. Kiayias and P. Lazos. Sok: Blockchain governance. *arXiv preprint arXiv:2201.07188*, 2022.

[14] O. Kurbatov, P. Kravchenko, O. Shapoval, N. Poluyanenko, M. Malchyk, A. Sakun, and V. Kovtun. Anonymous decentralized e-voting system. In *CMiGIN*, pages 12–22, 2019.

[15] S. Lianju and P. Luyan. Game theory analysis of the bribery behavior. *International Journal of Business and Social Science*, 2(8), 2011.

[16] J. Liebkind. How blockchain technology can prevent voter fraud, Dec. 2020. URL https://www.investopedia.com/news/how-blockchain-technology-can-prevent-voter-fraud/.

[17] B. Zhang, R. Oliynykov, and H. Balogun. A treasury system for cryptocurrencies: Enabling better collaborative intelligence. *Cryptology ePrint Archive*, 2018.