information

Tracked for Impact Factor

CITESCORE 4.2

Article

Liquid Proof-of-Stake in Tezos: An Economic Analysis

Nicola Dimitri

Special Issue
Models for Blockchain Systems: Analysis and Simulation

Edited by
Prof. Dr. Sabina Rossi, Prof. Dr. Andrea Marin and Prof. Dr. Marco Bernardo

MDPI

https://doi.org/10.3390/info13120556

information

MDPI

Article

Liquid Proof-of-Stake in Tezos: An Economic Analysis

Nicola Dimitri

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

Abstract: In this paper, we investigate some economic fundamentals related to the Tezos blockchain platform under the Emmy* consensus protocol. The protocol is based on a *liquid* version of Proof-of-Stake, in the sense that users can temporarily delegate some or all of their Tz units to full nodes. In addition to increasing the stake of the full node, and thus the probability of being selected as a block baker/endorser, such delegation induces the property of the *super-additivity* of users' selection probability of baking/endorsing a block. That is, with delegation, the selection probability may be larger than the sum of the selection probabilities without delegation. In this paper, we study how monetary holdings and stakes can evolve with time, also discussing the individual user and the market implications of delegation.

Keywords: Tezos; delegated proof-of-stake; optimal staking

check for updates

Citation: Dimitri, N. Liquid Proof-of-Stake in Tezos: An Economic Analysis. *Information* **2022**, *13*, 556. https://doi.org/10.3390/info13120556

Academic Editors: Sabina Rossi, Andrea Marin and Marco Bernardo

Received: 14 August 2022
Accepted: 15 November 2022
Published: 27 November 2022

Publisher's Note: MDPI stays neutral with regard to jurisdictional claims in published maps and institutional affiliations.

1. Introduction

Tezos is an open-source, peer-to-peer blockchain platform founded in 2018. Since its inception, Tezos has attracted much attention [1–10] for a variety of reasons, the main one of which is its consensus protocol. In this paper, we consider the protocol version called Emmy*, recently replaced by Tenderbake. Emmy* is based on Delegated Proof-of-Stake (PoS) [2], in which the stake is represented by the number of so-called *rolls*, where a roll corresponds to 8000 units of the Tezos currency, named Tz. Users owning/managing rolls are called *delegates*, who can be selected by the platform either to *bake* (propose) or to *endorse* (validate) new blocks or to do both. Baking/endorsing is rewarding for a user but can only be accomplished by depositing, for a certain number of validated blocks, a sum of Tz for security. In the case of double baking/endorsing, the security deposit will be slashed by the platform.

Those users who own less than 8000 Tz, or do not want to run a costly full node to bake/endorse blocks, may *delegate* their Tz units to a user operating a full node, who could then temporarily increase her/his number of rolls. Upon successful baking/endorsing, the rewards will be shared between the delegating and delegated nodes, typically according to a proportion based on their number of rolls. For this reason, delegation operates in a way that is *akin*, though not identical, to *mining pools* in Bitcoin. Indeed, the main difference is the following. While in Bitcoin, when miners join their computational power into mining pools, the total hashing power is basically the sum of the individual hashing powers, in Tezos with Emmy*, the *success* probability with delegation will typically be larger than the sum of the individual success probabilities without delegation. That is, since the probability of being selected for baking/endorsing blocks in Tezos is based on the number of rolls, joining individual stakes through delegation will typically induce a *super-additivity property* of the success probability. In fact, taking as given the total number of rolls for a user, the selection (success) probability is a *step function* of the stake, namely, a function that increases only for multiples of 8000 Tz.

This paper aims to investigate some main economic issues related to Tezos under the Emmy* version of the protocol. To our knowledge, this is the first such contribution. In particular, we are interested in discussing how the optimal number of rolls is determined

by the nodes, how baking/endorsing rewards can be shared with delegation, and whether the possibility of delegation would induce the emergence of a market for such services. The analysis will proceed gradually, with the paper being structured as follows. In Section 2, we discuss single-block baking priorities, while in Section 3, we discuss endorsement priorities, both without delegation. In Sections 4 and 5, we define a user's expected revenue for a single block and a cycle of blocks, respectively. In Section 6, we introduce a user's preferences to investigate her/his optimal stake, that is, her/his optimal number of rolls. Delegation is analysed in Section 7, where the *super-additivity property* of the selection probability of being a baker/endorser is identified. Section 8 presents some economic fundamentals of the market for delegation services, while Section 9 concludes the paper.

2. Baking Priorities for a Single Block with No Delegation

In this section, we consider the fundamental elements of how priorities for baking blocks are established without delegation.

Suppose $R > 1$ is the number of rolls in the community at some date, with one roll corresponding to 8000 Tz, and $0 \leq r \leq R$ is the number of rolls owned by a generic user. We assume that rolls represent the user's stake.

Rolls are randomly drawn according to a *sampling-with-replacement scheme* to establish the priority, $p = 0, \ldots, R$, with which users owning the rolls bake (propose) the next block. Therefore, the same roll can be drawn more than once. Priority $p = 0$ is the highest priority, $p = 1$ is the second highest, and so on. The user owning the roll with priority $p = 0$ has the right to bake the next block. If, for some reason, she/he declines, then the right to bake shifts to the roll with the second highest priority and so on. The probability that a generic user will be selected in a single draw is $\frac{r}{R}$, so $\frac{(R-r)}{R}$ is the probability of not being selected in a single draw. Therefore, the user with the highest number of rolls, i.e., the largest stake, has the highest probability of being selected, which, of course, is the main incentive introduced by Tezos to induce users' stakes.

The reward ρ_b depends on the priority of the baker (roll) and on the number of endorsements ($e = 0, 2, \ldots, 256$) received by the block. Double baking, as well as double endorsement, is punished by the platform.

The reward for baking ρ_b is defined as follows:

$$\rho_b = \begin{cases} e \times a\ Tz & if\ p = 0 \\ e \times b\ Tz & if\ p > 0 \end{cases} \tag{1}$$

where $a = 0.078125\ Tz$ and $b = 0.011719\ Tz$. Thus, the reward for baking a block is a linear function of the number of endorsements e received by the block, whose slope varies according to the roll's priority. From (1), it follows that the only difference is between the highest priority and any other priority. Since the number of selected endorsers is 256, the maximum reward for baking a block is 20 Tz.

Considering a *sampling-with-replacement scheme* for the selection of baking priorities, the general expression for a user's probability of baking the next block $P(B)$ is given by

$$P(B) = \frac{r}{R} + \frac{(R-r)qr}{R^2} + \frac{[(R-r)q]^2 r}{R^3} + \ldots + \frac{[(R-r)q]^{(R-1)} r}{R^R} = \frac{r\left[1 - \left(\frac{(R-r)q}{R}\right)^R\right]}{[R(1-q) + rq]} \tag{2}$$

where $0 \leq q \leq 1$ is the probability that a user with higher priority will not bake, for whatever reason, the next block. Equation (2) assumes that users may not bake a block independently of each other. Admittedly, this may be a simplification, as well as assuming that q is the same for each user. However, as the first step in the analysis, we find this to be acceptable. It is worth noticing that as q tends to 0, $P(B)$ tends to $\frac{r}{R}$. That is, when delegates tend to bake blocks, then basically, the only possibility for a user to bake a block is to have the highest priority, $p = 0$. Likewise, as q tends to 1, $P(B)$ tends to $1 - \left(\frac{(R-r)}{R}\right)^R$. That is,

if users with higher priorities never bake a block, the probability that a generic user will bake the next block is maximised, and

$$P(B) \sim 1 - exp(-r)$$

as R becomes very large.

From an operational perspective, the value of q can be estimated from the data by observing the frequency with which users do not bake.

Some comments on the above expression are in order. First, observe that if, assuming users' symmetry, q is the probability with which *any* user declines to bake the next block, then (2) should become

$$P(B) = \frac{(1-q)r\left[1 - \left(\frac{(R-r)q}{R}\right)^R\right]}{[R(1-q) + rq]}$$

which is corrected by a multiplyng factor $(1-q)$, since the user behind Equation (2) may not bake with some probability. However, without much loss of generality, we decided to simplify the expression by assuming that q is the probability with which each user, *except for the generic one*, refuses to bake.

Additionally, notice that the only *exogenous* quantity in (2) is q, and it may be interesting to investigate how r should vary with q to keep $P(B)$ unaltered.

Clearly, for $r > 0, R > 1$, $P(B)$ is increasing in q, that is,

$$\frac{\partial P(B)}{\partial q} > 0$$

Moreover, $P(B) = 0$ for $r = 0$, and $P(B) = 1$ for $r = R$. However, how $P(B)$ would change with r is less immediate, since it depends on the behaviour of R as r varies. Indeed, when r changes, there could be two main scenarios. In the first scenario, the total number of rolls R remains unaltered, which implies that, as r changes, some other user's number of rolls also has to change. Alternatively, in the second scenario, R varies by the same amount of r.

(a) R is given and independent of r

In this case,

$$\frac{\partial P(B)}{\partial r} = \frac{\left[1 - \left(1 - \frac{r}{R}\right)^R\right]R(1-q) + r\left(1 - \frac{r}{R}\right)^{R-1}[R(1-q) + rq]}{[R(1-q) + rq]^2} > 0 \tag{3}$$

independently of the value of q.

(b) R is a function of r and $\frac{\partial R}{\partial r} = 1$

When R is positively related to r, then the first derivative of $P(B)$ with respect to r is given by

$$\frac{\partial P(B)}{\partial r} = \frac{\left[1 - \left(\left(1 - \frac{r}{R}\right)q\right)^R\right](R(1-q) + rq) - r\left[\left(1 - \frac{r}{R}\right)q\right]^R\left[\log\left(\left(1 - \frac{r}{R}\right)q\right) - 1\right][R(1-q) + rq]}{[R(1-q) + rq]^2} > 0 \tag{4}$$

which is again positive. Hence, unsurprisingly, also in this case $r = R$ would maximise the probability of baking the next block, regardless of the value of q.

Therefore, if $dP(B)$ is the total differential of $P(B)$, we have $dP(B) = \frac{\partial P(B)}{\partial q}dq + \frac{\partial P(B)}{\partial r}dr$. Posing $dP(B) = 0$, it follows that, consistent with intuition, it is $\frac{dr}{dq} < 0$; that is, as q increases, r decreases for $P(B)$ to remain constant.

3. Endorsement Priorities for a Single Block without Delegation

In addition to eligibility for baking blocks, a user in Tezos with Emmy* can be eligible for endorsing a block, again, as long as she/he has at least one roll. The reward ρ_e for a single-block endorsement is given by

$$\rho_e = \begin{cases} s \times a\ Tz & if\ p = 0 \\ s \times c\ Tz & if\ p > 0 \end{cases} \tag{5}$$

where $c = 0.052083\ Tz$, and $s = 0, 1, \ldots, 256$ is the number of endorsing slots of the user.

As in the case of baking, endorsers are drawn according to a *sampling-with-replacement scheme*, so, in a single draw, the probability that a user will be selected is again $\frac{r}{R}$. Therefore, since there are 256 slots available to assign an endorsement, the probability that a user will obtain s slots is binomial and given by $\binom{256}{s}\left(\frac{r}{R}\right)^s\left(1-\frac{r}{R}\right)^{256-s}$, with $s = 0, 1, \ldots, 256$.

Interestingly, notice that with priority $p > 0$, it is $b < c$; that is, the reward for a single endorsement is larger than the reward received for baking a block. Since b and c should be interpreted as *economic incentives* for baking and endorsing blocks, respectively, the above inequality means that Tezos decided to provide a stronger incentive for endorsing than for baking.

Finally, it is worth observing that although b and c share similarities, being per endorsement rewards, they also exhibit some differences, since b refers to endorsements *received* by a baker for proposing a block, while c refers to endorsements *assigned* by a user to a baked block. Hence, while b is an acknowledgement a user receives when *acting as a baker*, c is an acknowledgement that a user *assigns to a baker*.

In the Emmy* version of Tezos, a user can not only be a baker, as well as an endorser, but also endorse a block that she/he her-/himself baked. Indeed, with 256 endorsement slots, the potential conflict of interest is assumed to be diluted by the large number of endorsing slots, and the related probability is negligible. Indeed, as we shall see, bakers and endorsers may or may not overlap; likewise, a user may or may not appear as an endorser more than once for the same block.

Baking and Endorsing Joint Probability for a Single Block

The selection procedure for baking is independent of the selection procedure for endorsing. Hence, given the previous considerations, the joint probability of being selected with priority $p = 0, 1, \ldots, R$ for baking a block and of being assigned $s = 0, 1, \ldots, 256$ slots for endorsements is

$$P(p,\ s) = \frac{[(R-r)q]^p r}{R^{(p+1)}}\binom{256}{s}\left(\frac{r}{R}\right)^s\left(1-\frac{r}{R}\right)^{256-s}$$

4. Expected Revenue for a Single Block

The analysis conducted so far allows us to define and compute the user's expected revenue $E\rho(r)$ related to the baking priority as well as to the number of endorsements. Before doing so notice that, from (2), it follows that the probability of the highest level of priority for baking in a single draw, $p = 0$, is $\frac{r}{R}$, while the probability of any other priority, $p > 0$, is

$$P(B) - \frac{r}{R} = \frac{(R-r)qr}{R}\frac{\left[1-\left(\frac{(R-r)q}{R}\right)^{R-1}\right]}{[R(1-q)+rq]}$$

Therefore, a user's expected revenue related to a single block, obtained from both baking and endorsing activities, is given by the following expression:

$$\begin{aligned} E\rho(r) = \sum_{e=0}^{256} e \left[a\frac{r}{R} + b\frac{(R-r)qr}{R} \frac{\left[1-\left(\frac{(R-r)q}{R}\right)^{R-1}\right]}{[R(1-q)+rq]} \right] \pi(e) \\ + \sum_{s=0}^{256} s[a(1-q)+cq] \binom{256}{s} \left(\frac{r}{R}\right)^{s} \left(1-\frac{r}{R}\right)^{256-s} \end{aligned} \tag{6}$$

which is equal to

$$E\rho(r) = \left[a\frac{r}{R} + b\frac{(R-r)qr}{R} \frac{\left[1-\left(\frac{(R-r)q}{R}\right)^{R-1}\right]}{[R(1-q)+rq]} \right] \sum_{e=0}^{256} e\, \pi(e) + [a(1-q)+cq]256\left(\frac{r}{R}\right) \tag{7}$$

where $\pi(e)$ is the probability that the next block will receive e endorsements.

The closed form of (7) requires the explicit expression of $\pi(e)$, which, in turn, is likely to depend upon the baking priority. From an operational point of view, $\pi(e)$ can be estimated from the data by replacing $\pi(e)$ with the observed frequencies for each number of endorsements, $e = 0, 1, \ldots, 256$. Moreover, notice that $[a(1-q)+cq]256\left(\frac{r}{R}\right)$ is a user's expected reward when acting as an endorser under the simplifying assumption that the user will endorse the block with all of his/her slots. Indeed, more realistically, the model should contemplate the possibility that a block will not be endorsed because of unacceptable transactions, etc. However, as a first approximation, we deem our assumption to be acceptable, and, in any case, the value obtained can always be considered as an upper bound to the user's revenues when all of his/her endorsement slots have been used.

Finally, we also observe that, from an analytical perspective, $\pi(e)$ should be written more appropriately as $\pi(e) = \pi(e, p)$, where, for a given p, we assume that $\pi(e, p)$ increases with e. Moreover, we should also assume that for a given e, the probability $\pi(e, p)$ decreases with p. That is, the larger the block priority, that is the smaller the p, the larger the probability of obtaining a high number of endorsements.

Defining the expected number of endorsements received by a baked block as $E(e) = \sum_{e=0}^{256} e\, \pi(e)$, $E\rho(r)$ can finally be written as

$$E\rho(r) = \left[a\frac{r}{R} + b\frac{(R-r)qr}{R} \frac{\left[1-\left(\frac{(R-r)q}{R}\right)^{R-1}\right]}{[R(1-q)+rq]} \right] E(e) + [a(1-q)+cq]256\left(\frac{r}{R}\right) \tag{8}$$

Consistent with intuition, as r gets close to R, Equation (8) tends to take its largest possible value, namely, $E\rho(r = R) = [aE(e) + (a(1-q)+cq)256]$, while as r becomes close to 0, $E\rho(r = 0) = 0$.

5. Expected Revenue for a Cycle of Blocks

In the Tezos Emmy* protocol, a cycle of blocks given by a sequence of $\Gamma = 8192$ blocks, validated in about 2 days, 20 h and 10 min, is the relevant operating unit over which the lists of baking priorities and endorsement slots are established. Therefore, considering r, R and q as being fixed over a single cycle, the user's expected revenue from a cycle is given by $E\rho(r)\Gamma$, which is just Γ times the single block's expected revenue.

Indeed, Equation (1) suggests that, for each block, the reward from baking is driven by a two-outcome Bernoulli variable related to the value of the priority, $p = 0$ or $p > 0$. As a consequence, the expected revenue over the cycle is simply the sum, over the number of blocks in a cycle, of the expected revenue for a single block.

Because of the sampling-with-replacement scheme, this is the case regardless of whether or not the list of R priorities for each block is made block by block or if a long list

of $R(8192)$ drawings is composed, where after every sequence of R draws, the priorities of a new block are established. Indeed, for every R draws, concerning the priorities of a block, another list of R priorities will follow for the next block and so on.

6. Optimal Stake and Number of Rolls in a Cycle

Based on the previous analysis, in this section, we start modelling how a user may optimally determine her/his stake and number of rolls for baking and endorsing. To proceed gradually, we shall assume that every node is a full node, deferring the discussion on delegation until later.

To investigate the issue, we first introduce what we believe to be a fundamental economic trade-off characterizing users of Proof-of-Stake (PoS)-based blockchains. On the one hand, the stake increases the probability of being selected as a baker/endorser and thus obtaining future rewards in Tz units. On the other hand, staking prevents the immediate usage of one's currency units and the possibility of implementing monetary transactions, which may be beneficial for the user. For this reason, staking may produce a disutility to the user.

To simplify the exposition, with no major loss of generality, unless otherwise indicated in what follows, we assume the stake to coincide with the number of rolls, which, moreover, will be treated as a continuous variable. Additionally, to simplify, we still omit a budget constraint for the users.

An initial, very simple step to embody such trade-off into a preference specification for generic user i, with $i = 1, 2, \ldots, N$, where N is the number of platform users, is to introduce the user's utility function $U_i(r_i)$, which we define below in Equation (9), where r_i is the number of rolls chosen by agent i. Hence $R = \sum_{i=}^{N} r_i$, and we assume that user i, for all $i = 1, 2, \ldots, N$ at the beginning of each cycle, solves the following problem:

$$max_{r_i} U_i(r_i) = max_{r_i} \left[\delta_i E\rho(r_i)\Gamma - {\delta_i}^{-5} C(r_i) - f \right] \tag{9}$$

where $0 \leq \delta_i \leq 1$ is user i's discount factor related to one cycle of blocks, which quantifies her/his intertemporal preferences. Moreover, $C(r_i)$ is the per *single-cycle* user's cost due to security deposits, expressed as a function of r_i, and $f \geq 0$ is the cost of running a full node as a baker/endorser, which we assume to be constant and independent of r_i. A few comments are in order.

The first term $\delta_i E\rho(r_i)\Gamma$ of (9) formalises the present value, before a cycle starts, of the utility-enhancing side in the above trade-off. The prospect of obtaining a reward in a cycle indeed represents an attractive incentive for a user to set up a stake and become a baker/endorser.

The second term, $-{\delta_i}^{-5} C(r_i)$, is a simple representation of the compounded disutility due to keeping r_i rolls as a stake, which is hence unused for five cycles, as specified in Emmy*. Note that such disutility increases with the time duration of the security deposit, and this is why the exponent of the discount factor is negative. In particular, we interpret $C(r_i)$ as the single-cycle cost for the user induced by a stake of r_i rolls.

Since 640 Tz and 2.5 Tz are the security deposits for each block baked and each endorsement assigned to a block, respectively, the simplest expression for $C(r_i)$ can be given by:

$$C(r_i) = 640 \sum_{b=0}^{8192} bP(B)^b (1 - P(B))^{8192-b} + 2.5 \sum_{s=0}^{2097152} sP(B)^s (1 - P(B))^{8192-s} \tag{10}$$

Therefore,

$$C(r_i) = (640)(8192)P(B) + (2.5)(2097152)P(B) = 10485760P(B) = wP(B) \tag{11}$$

where $w = 10485760$ is a constant, and $P(B)$, defined as in (2), is a function of r_i. Indeed, to emphasise this, we write $P(B, r_i)$. It follows that (9) can now be rewritten as

$$U_i(r_i) = \delta_i E\rho(r_i)\Gamma - {\delta_i}^{-5} wP(B, r_i) - f \tag{12}$$

Based on (12), we can proceed to user $i's$ determination of the optimal r_i in a game-theoretic framework. The reason that a setup based on strategic interaction can be suitable for modelling the optimal stake decision is due to the presence of Proof-of-Stake (PoS). Indeed, as we previously discussed, the probability of being drawn for baking/endorsing blocks typically depends on the ratio between one's rolls and the total number of rolls $\frac{r_i}{R}$. Hence, the optimal number of rolls chosen by a user may also depend on the number of rolls chosen by the other users.

The Staking Game

In this section, we consider the strategic interaction among agents and derive user $i's$ best reply correspondence $r_i(r_{-i})$, where r_{-i} is the profile of rolls chosen by $i's$ opponents. Following the above analysis and assuming, for simplicity, $q = 0$, Equation (12) becomes

$$U_i(r_i) = {\delta_i}^{-5}[{\delta_i}^{6}\Gamma a(E(e) + 256) - w]\left(\frac{r_i}{R}\right) - f \tag{13}$$

For any $0 \leq E(e) \leq 256$ and $0 \leq \delta_i \leq 1$, the following benchmark result holds:

Proposition 1. *If all users have preferences as in (13), then there is a unique Nash Equilibrium of the game in strictly dominating strategies, given by*

$$r_i(r_{-i}) = 0 \ (14) \ i = 1, \ldots, N$$

Proof. It is easy to verify since $U_i(r_i)$ is a negatively sloped function with respect to r_i. Indeed, recalling that $R = \sum_{i=}^{N} r_i$ and $\frac{\partial R}{\partial r_i} = 1$, differentiating (13) with respect to r_i leads to

$$\frac{dU_i(r_i)}{dr_i} = {\delta_i}^{-5}[{\delta_i}^{6}\Gamma a(E(e) + 256) - w]\frac{(R - r_i)}{R^2}$$

and because $[{\delta_i}^{6}\Gamma a(E(e) + 256) - w] < 0$, the result follows. □

Therefore, if all users' preferences are represented by (12), with $q = 0$, the chain will not even start since none of them will stake any rolls. The main reason for this is due to the specification of preferences in (13), which are linear in $\frac{r_i}{R}$, as well as to the definition of the cost.

However, it is easy to verify that if the cost is defined by $C(r_i) = cw\left(\frac{r_i}{R}\right)$, with $0 < c < 1$, then the Nash Equilibrium number rolls will, in general, differ from zero.

The above finding is interesting, as a reference, and suggests that not all utility functions can be linear in $\frac{r_i}{R}$ for the chain to develop. A simple way to introduce alternative preferences is to consider the following modification of (12):

$$U_i(r_i) = \delta_i E\rho(r_i)\Gamma - \frac{{\delta_i}^{-5} w(P(B, r_i))^2}{2} - f \tag{14}$$

that is, with convex (quadratic) costs, where we still consider $q = 0$, $R = \sum_{i=}^{N} r_i$ and $\frac{\partial R}{\partial r_i} = 1$.

Since user $i's$ best reply maximises (14), the first step towards finding it is to differentiate (14) with respect to r_i to obtain

$$\frac{dU_i(r_i)}{dr_i} = \delta_i \Gamma\left(\frac{dE\rho(r_i)}{dr_i}\right) - w{\delta_i}^{-5} P(B, r_i)\left(\frac{dP(B, r_i)}{dr_i}\right) \tag{15}$$

Based on the above considerations, the first-order condition associated with Equation (15) becomes

$$\delta_i \Gamma a \left(\frac{R - r_i}{R^2} \right) (E(e) + 256) = w {\delta_i}^{-5} \left(\frac{r_i}{R} \right) \left(\frac{R - r_i}{R^2} \right) \tag{16}$$

Therefore, assuming the optimal stake solves (16), we obtain the following result:

Proposition 2. *Suppose useri has preferences as in (14). Then, her/his best reply* $r_i(r_{-i})$ *satisfies*

$$\frac{r_i(r_{-i})}{R} = \frac{\Gamma a {\delta_i}^6 (E(e) + 256)}{w} \tag{17}$$

Proof. Immediate. Rearranging (16) leads to (17). □

Some comments are in order. First, notice that (17) is a proper probability expression since $0 \leq \frac{r_i}{R} \leq 1$. Moreover, it is interesting to observe that the ratio $\frac{r_i}{R}$ in (17) increases in both δ_i and $E(e)$. That is, the more patient the user, the higher the expected number of endorsements for baked blocks, and the larger the proportion $\frac{r_i}{R}$. Furthermore, it is easy to determine that the maximum value that Equation (17) can take when $\Gamma(e) = 256$ and $\delta_i = 1$ is around 3%, which means that if all users of the platform have preferences as in (14), then the money supply will be widely spread across them.

Furthermore, observe that the only element in (17) that differs across users is δ_i. Therefore, users with a larger discount factor (more patient) will have more rolls than users with a lower δ_i (less patient).

Finally, it is important to point out that (17) does not determine a unique value for r_i but rather the proportion $\frac{r_i}{R}$. This means that if all users have preferences as described by (14), the level of R will not be uniquely determined, and moreover, summing both sides of (17) with respect to i, the following equalities will be satisfied.

$$1 = (\sum_{i=1}^{N} {\delta_i}^6) \frac{\Gamma a (E(e) + 256)}{w} \; ; \; \frac{r_i}{R} = \frac{\delta_i}{(\sum_{j=1}^{N} {\delta_j}^6)} \tag{18}$$

That is, in our simplified model, a user's proportion of rolls is fully determined by the proportion of individuals' discount rates.

7. Delegated Proof-of-Stake for a Cycle of Blocks

As previously said, one of the distinguishing features of Tezos is that, rather than running a full node to bake/endorse blocks, generic user j may decide to delegate all or some of her/his Tz units to another baking node, say i, who would also bake/endorse on $j's$ behalf. Delegation typically has the following main features:

(i) The costs f of running a full node are paid by the delegated node only, if the delegating node is not a full node.
(ii) The probability of baking/endorsing exhibits a *super-additivity property*. That is, with delegation, the joint selection probability is at least as large as the sum of the selection probabilities without delegation.
(iii) The rewards obtained by the delegated node are shared with the delegating user proportionally to the number of their rolls.

Based on the above three points, it is natural to ask whether there is a benefit for a user to run a full node. Indeed, the delegating user pays no operating cost for running a full node and, moreover, may enjoy the advantage of obtaining some reward, even if it does not even have a single roll to stake individually. Intuition certainly suggests that there must be benefits in operating a full node because, alternatively, a scenario where nobody wants to run a full node may be envisaged, and the platform would not even operate.

To gain some insights on the above point, below, we discuss some simple cases. Consider the following example with two users i and j, whose money holdings and stakes are equal to m_i, m_j and s_i, s_j, respectively. Moreover, assume that i runs a full node, while j does not.

(1) Suppose $m_i = 7999\ Tz$ and $m_j = 500\ Tz$. Therefore, neither user i nor user j can bake a single roll since none of them individually has at least 8000 Tz. However, if j delegates i of at least 1 Tz, then, jointly, the two nodes can reach at least 8000 Tz and potentially bake/endorse blocks, which separately they could not. Given this initial *symmetric* situation, where neither of them can bake individually, the observed block/endorsing joint reward $\rho(r = 1)$, which is a random variable, is likely to be shared *exclusively* according to the monetary sum at stake. Indeed, this may prevent one user from free riding on the other user, trying to convince him/her to stake as much money as possible. If s_i is the stake of user i and s_j is the stake of user j, then the share

$$\frac{s_i}{s_i + s_j}$$

of the reward, jointly obtained by the two users, will go to user i, while the rest goes to user j.

Hence, for this particular example, assuming $q = 0$, the joint success probability is given by

$$P_{ij}(B) = \frac{Int[(s_i + s_j)/8000]}{R} = \frac{1}{R}$$

where $Int[(s_i + s_j)/8000]$ stands for the integer number of $[(s_i + s_j)/8000]$, while the sum of the individual success probabilities with no delegation would be 0. Though very simple, the example immediately shows how delegation may induce *super-additivity* on such probabilities. That is, the joint success probability $P_{ij}(B) = \frac{1}{R}$ is larger than the sum of the individual success probabilities, which is $P_i(B) = 0 = P_j(B)$. Finally, notice that a similar argument could hold even if j were a full node; this is also true for the following considerations.

(2) Suppose now that $m_i = 15999\ Tz$ and $m_j = 500\ Tz$. In this case, the situation is slightly different, as compared to the previous point, since user i can stake one roll for baking/endorsing blocks, while user j alone still cannot. If j delegates at least 1 Tz to i, then j can participate in the baking activity, which otherwise would be impossible. User i, even without the support of user j, in this case, can be selected with a success probability given by

$$P_i(B) = \frac{1}{R}$$

However, if user j delegates at least 1 Tz, then the success probability will increase to

$$P_{ij}(B) = \frac{2}{R}$$

Since the increase in the success probability will affect the reward, in this case, an agreement on how to share the joint revenues may be a more involved decision. A reasonable way to take into account that, with delegation, the expected revenue will increase could be the following. If $E\rho(r = 1) < \rho(r = 2)$, then the amount $E\rho(r = 1)$ could go completely to user i, since even with no delegation, she/he could have been selected to bake/endorse blocks.

Then, the difference between the observed joint reward with two rolls $\rho(r = 2)$ and the expected revenue with one roll $\rho(r = 2) - E\rho(r = 1)$ can be divided according to the following criterion. The share

$$\frac{(s_i - 8000)}{(s_i - 8000) + s_j}$$

may be assigned to user i, while the rest is assigned to user j. That is, revenues will be distributed according to the additional stake contribution of the users with respect to what they could obtain individually. Clearly, the application of this criterion presupposes an agreement on the value of $E\rho(r=1)$. In our model, considering (8) and assuming, for simplicity, $q=0$, we obtain

$$E\rho(r=1) = \left(\frac{a}{R}\right)E(e) + 256\left(\frac{a}{R}\right) = \left(\frac{a}{R}\right)[E(e)+256] \tag{19}$$

which is easily computable by observing R and estimating $E(e)$ from the data.

Finally, if $E\rho(r=1) \geq \rho(r=2)$, then we can imagine more than one possibility. Either the entire observed revenue $\rho(r=2)$ goes to user i, or, alternatively for example, $\rho(r=2)$ is shared according to the above formula used to distribute $\rho(r=2) - E\rho(r=1)$, or some other arrangement.

Therefore, if $E\rho(r=1) < \rho(r=2)$, the expected revenue of user i with delegation $E_d\rho(r=2)$ will be given by

$$E_d\rho(r=2) = E\rho(r=1) + \frac{(s_i-8000)}{(s_i-8000)+s_j}[\rho(r=2) - E\rho(r=1)] = \frac{(s_i-8000)}{(s_i-8000)+s_j}\rho(r=2) + \frac{s_j}{(s_i-8000)+s_j}E\rho(r=1) \tag{20}$$

that is, a convex combination, an average, of $\rho(r=2)$ and $E\rho(r=1)$, with weights given by $\frac{(s_i-8000)}{(s_i-8000)+s_j}$ and $\frac{s_j}{(s_i-8000)+s_j}$, respectively. In Paragraph (7.1), we discuss a similarity of (20) with some notable axiomatic bargaining solutions. Expression (20) is certainly larger than $E\rho(r=1)$, the expected revenue with no delegation. However, though an unlikely event, the possibility of $\rho(r=1) > E_d\rho(r=2)$ cannot be excluded if, with just one roll, user i was particularly lucky in being selected for several blocks and relatively unlucky with two rolls.

Finally, obviously, with delegation, user j would also, in general, be better off than with no delegation.

(c) Suppose now that $m_i = 23999\ Tz$ and $m_j = 1500\ Tz$; that is, both users can be selected separately for baking with two rolls and one roll, respectively. Moreover, in this case, if user j delegates user i with $1\ Tz$, then two users, jointly, will obtain four rolls. Again, also in this case, delegation induces super-additivity in the success probabilities

$$P_{ij}(B) = 4 > 2 + 1 = 3 = P_i(B) + P_j(B)$$

and additional gains for both agents. However, as in the previous point, it is important to discuss how the revenues can be shared in this case. Following a reasoning analogous to the previous point, we can imagine that if

$$E\rho_i(r=2) + E\rho_j(r=1) < \rho_{ij}(r=4) \tag{21}$$

then they may agree on granting a reward of $E\rho_i(r=2)$ to user i and a reward equal to $E\rho_j(r=1)$ to user j. Additionally, user i will obtain the share

$$\frac{(s_i - 16000)}{(s_i - 16000) + (s_j - 8000)} \tag{22}$$

of the reward $\rho_{ij}(r=4) - \left[E\rho_i(r=2) + E\rho_j(r=1)\right]$, while the remaining share of it will go to user j. However, (21) may not necessarily be satisfied, and the following can take place:

$$E\rho_i(r=1) < \rho_{ij}(r=4) < E\rho_i(r=2) \tag{23}$$

Hence, if (22) is the case, what could be a criterion for sharing $\rho_{ij}(r=4)$? User i could claim that since the observed reward $\rho_{ij}(r=4)$ is not enough to cover the expected reward $E\rho_i(r=2)$ that she/he could obtain with no delegation, then she/he should receive the

entire reward $\rho_{ij}(r = 4)$. However, user j may claim that with no delegation, on average, she/he might have obtained $E\rho_j(r = 1)$ and thus disagree with user $i's$ claim.

In such circumstances, the observed $\rho_{ij}(r = 4)$ could perhaps be divided between the two users, assigning the share

$$\frac{E\rho_i(r = 2)}{E\rho_j(r = 1) + E\rho_i(r = 2)}$$

to user i and the remaining share to user j. Alternatively, user i could obtain the share as in (22) or, perhaps, simply the share

$$\frac{s_i}{s_i + s_j}$$

Analogous reasoning could apply for

$$\rho_{ij}(r = 4) < E\rho_j(r = 1) \tag{24}$$

In the above example, we assume that user i, the one running a full node, receives no specific benefit for running such a node. That is, rewards are shared with reference only to some *relative stake* criterion, with no concern for the fact that without user i, user j may not enjoy additional benefits.

One possibility to account for this may be to introduce a multiplying factor, $\alpha > 1$, as an additional weight to the stake of user i. For example, (22) could now become

$$\frac{\alpha(s_i - 16000)}{\alpha(s_i - 16000) + (s_j - 8000)} \tag{25}$$

and analogously, we would obtain, for example,

$$\frac{\alpha s_i}{\alpha s_i + s_j}$$

An additional possibility may be to introduce a weight, in this case, $\beta < 1$, such as in (26) below:

$$\left(\frac{(s_i - 16000)}{(s_i - 16000) + (s_j - 8000)}\right)^{\beta} \tag{26}$$

A simple way to fix those two coefficients could be to define them, for instance, as

$$\beta = \frac{1}{\alpha} \text{ and } \alpha = \frac{(s_i - 16000) + (s_j - 8000)}{(s_i - 16000)}$$

which would also be a possibility for the coefficients to account for the relative stakes.

Nash and Kalai–Smorodinsky Non-Cooperative Bargaining Solutions

Another approach to consider when discussing how users may share the rewards obtained with delegation is given by two main axiomatic bargaining models in economics. These are the Nash solution and the Kalai–Smorodinsky (KS) solution, where the *status quo* is given by the users' expected reward obtained without delegation. To see what such solutions suggest, we start by taking the first example of the previous paragraph. In this case, the status quo is zero for both users, since neither of them can bake without delegation. Hence, if $\rho_{ij}(r = 1)$ is the revenue obtained with delegation, which implies just one roll for the two of them, the Nash Bargaining solution can be obtained by solving the following problem:

$$max_{\rho_i}[\rho_{ij}(r = 1) - \rho_i]\rho_i \tag{27}$$

and similarly for ρ_j, where ρ_i, ρ_j with $\rho_i + \rho_j = \rho_{ij}(r = 1)$ are the shares of the observed revenue $\rho_{ij}(r = 1)$ going to users i and j. It immediately follows that (27) is solved by

$\rho_i = \frac{\rho_{ij}(r=1)}{2} = \rho_j$, which would also coincide with the KS solution. Indeed, differentiating $[\rho_{ij}(r=1) - \rho_i]\rho_i$ with respect to ρ_i leads to $\rho_{ij}(r=1) - 2\rho_i$, which, equalised to 0, provides the result. This solution, however, by its very definition, does not take into consideration the different stakes between the two users.

Now, take the second example, assuming $E\rho_i(r=1) < \rho_{ij}(r=2)$. The status quo for user i in this case is $E\rho_i(r=1)$, while for user j, it is again zero. Following a similar procedure to that above, the Nash Bargaining solution can solve the problem below:

$$max_{\rho_j}[\rho_{ij}(r=2) - \rho_j - E\rho_i(r=1)]\rho_j \tag{28}$$

where $\rho_i + \rho_j = \rho(r=2)$, from which we find that the solutions are given by

$$\rho_i = \frac{\rho_{ij}(r=2) + E\rho_i(r=1)}{2} \text{ and } \rho_j = \frac{\rho_{ij}(r=2) - E\rho_i(r=1)}{2}$$

which, also in this case, coincide with the KS solutions. As mentioned above, it is easy to observe the similarity between (28) and (20), except that the former assigns a uniform weight to $E\rho_i(r=1)$ and $\rho_{ij}(r=2)$, while the latter assigns a weight proportional to the users' stakes.

To summarise, in the above discussion we considered just some possibilities to determine revenue shares and possible weights to account for the asymmetry in running a full node, but other criteria could certainly be considered.

8. Delegation Service Market

As a follow-up to the previous section, we now briefly discuss what a market for delegation services may look like. In what follows, we only provide a sketch of it. Indeed, such a competitive market may emerge quite naturally when non-full nodes are asking for delegation services, which a plurality of full nodes is willing to offer them to the other nodes. Although, in principle, they could receive delegated funds from any node, it is likely that most delegations would come from non-full nodes.

The very existence of a market and its configuration is crucially related to why and how delegating nodes may choose from among available full nodes. This is what we discuss below.

There may be several features making a full node attractive for delegation and consequently successful in the market. However, we believe that the following two features would play a major role in succeeding as delegation service providers.

The first is, broadly speaking, their *trustworthiness*, associated by any node j to generic full node i. We assume it to be sufficiently well represented as a numerical indicator by some increasing function $\tau_j(d_i)$ associated by generic node j to full node i, which depends on the total amount of delegated funds d_i received by node i. Of course, this may raise a few questions including, for example, how to define $\tau_j(d_i)$ for the first cycle the node to which it is providing delegation services. One solution could be to assume that the initial reputation is an average of the existing nodes' reputations or, alternatively, some other combination of them. A good reputation is certainly an attractive element, as much as a bad reputation may be a repulsive one, for those nodes that have decided to delegate their funds.

The second, as in the previous section, is the type of share agreements (fees) that full node i is paying to the delegating nodes in the case of positive rewards. More explicitly, suppose d_{ij} is the funds of node j delegated to node i; therefore, $d_i = \sum_{j=1}^{N} d_{ij}$. In general, we can assume that $f_{ij} = f_i(d_{ij})$, where $0 \leq f_{ij} \leq 1$ is the share of node $i's$ revenue ρ_i, paid as a fee by node i to node j, as a function f_i of the delegated funds. How the sharing rules are chosen by full nodes requires some detailed analysis based on mechanism design, which will not be discussed here. Additionally, we also assume that $\sum_{j=1}^{N} f_{ij}\rho_i \leq \rho_i$. In principle, the f_i function could take a variety of different forms, which would then represent an

element of competition across alternative full nodes to attract delegated funds. A possible form of the share function f_i could be the following:

$$f_i(d_{ij}) = \begin{cases} \alpha_i + g_i(d_{ij}) \; if \; d_{ij} > 0 \\ 0 \qquad\qquad\quad if \; d_{ij} = 0 \end{cases} with \; 0 \leq \alpha_i \leq 1 \tag{29}$$

which is additive, with a fixed and a variable component $g_i(d_{ij})$. The simplest example of (29) would be the constant (flat) function $f_i(d_{ij}) = \alpha_i$ for all $d_{ij} > 0$. A slightly more detailed version of (29) could be linear, that is, $f_i(d_{ij}) = \alpha_i + \beta_i d_{ij}$ for all $d_{ij} > 0$ and with $\beta_i > 0$.

However, once $\alpha_i + g_i(d_{ij})$ is announced by the node, there is no guarantee that $\alpha_i + g_i(d_{ij}) \leq 1$ for all d_{ij}. Therefore, in general, an operational version of (29) may be as follows:

$$f_i(d_{ij}) = \begin{cases} min(\sigma_i, \alpha_i + g_i(d_{ij})) \; if \; d_{ij} > 0 \\ 0 \qquad\qquad\qquad\quad if \; d_{ij} = 0 \end{cases} \tag{30}$$

where $\sigma_i \leq 1$ is the maximum revenue share paid by the delegated node to the delegating ones. For example, suppose $\sigma_i = 0.8$. Finally, $\alpha_i = 0.4$ and $g_i(d_{ij})) = (d_{ij})^2$: therefore, if $d_{ij} > 0$ then

$$f_i(d_{ij}) = \begin{cases} \alpha_i + g_i(d_{ij}) = 0.4 + (d_{ij})^2 \; if \; d_{ij} \leq \sqrt[2]{0.4} = 0.6324 \\ \sigma_i = 0.8 \qquad\qquad\qquad\qquad\qquad\quad if \; d_{ij} > 0.6324 \end{cases}$$

Notice that for $\alpha_i = 0$ and $g_i(d_{ij}) = \sigma_i\left(\frac{d_{ij}}{d_i}\right)$, definition (30) becomes akin to the sharing rules discussed in the previous section.

At a high level, each delegating node must make two major decisions: which node(s) to delegate its funds to and the delegated amount of Tz. Therefore, if $B_j(\tau_j(d_i),\ f_i(d_{ij}))$ denotes node $j's$ benefit function provided by the level of trustworthiness, and the proposed sharing rule of node i, and $c_j(d_{ij})$ denotes the cost for node j of delegating d_{ij} to node i, then node j would identify the optimal pair $(i, d_{ij},)$ by solving the problem:

$$max_{i,\ d_{ij}} U_j(\tau_j(d_i),\ f_i(d_{ij})) = B_j(\tau_j(d_i),\ f_i(d_{ij})) - c_j(d_{ij}) \tag{31}$$

For example, suppose $\tau_j(d_i) = d_i$, $f_i(d_{ij}) = 0.4 + d_{ij}$, $B_j(\tau_j(d_i)d_i,\ f_i(d_{ij})) = B_j(\tau_j(d_i),\ f_i(d_{ij})) = \tau_j(d_i) * f_i(d_{ij}) = d_i(0.4 + d_{ij})$ and $c_j(d_{ij}) = \lambda(d_{ij})^2$, with $\lambda \geq 0$, so that (31) becomes

$$max_{i,\ d_{ij}} U_j(\tau_j(d_i),\ f_i(d_{ij})) = d_i(0.4 + d_{ij}) - \lambda(d_{ij})^2 \tag{32}$$

Defining $d_{-ij} = d_i - d_{ij}$ and assuming, again, that m_j is the amount of money in $j's$ wallet, by differentiating (32) with respect to d_{ij}, we obtain

$$0.4 + d_{-ij} + 2(1 - \lambda)d_{ij}$$

and thus, the best d_{ij} is given by

$$d_{ij} = \begin{cases} m_j \qquad\qquad\qquad\quad if \; \lambda \leq 1 \\ min\left(\frac{(0.4 + d_{-ij})}{2(\lambda - 1)},\ m_j\right) \; if \; \lambda > 1 \end{cases} \tag{33}$$

Equation (33) provides the best choice if node j delegates node i. Hence, to find the overall optimal d_{ij}, node j will have to choose the full node that provides the highest utility.

Therefore, to summarise, depending upon the sharing rules proposed by full nodes, their reputation and the delegating nodes' preferences, full nodes will be chosen, and the market for their services will emerge in the network. Finally, notice that since the optimal choice of d_{ij} depends on d_i, that is, on the amount of funds delegated to node i by all

the nodes other than j, the value of the selected d_{ij} may represent a Pure Strategy Nash Equilibrium of the model.

9. Conclusions

In this paper, we present what, to our knowledge, is the first economic analysis of the Tezos liquid (with delegation) Proof-of-Stake model under the Emmy* consensus protocol. Although recently replaced by the Tenderbake consensus protocol, the model may still provide some helpful indications to the platform and its users, also for the new protocol. The main findings of the paper are the following. To some extent, unsurprisingly, the users' preferences, as well as the incentive schemes introduced by Tezos to induce users to participate in platform activities, are going to play a major role in the dynamics of the monetary stakes. This is likely to remain true also with Tenderbake. Additionally, as a less expected finding, in Emmy* the delegation of one's funds to other nodes induces what we identified to be a super-additivity property of the success probability. That is, with delegation, the probability that a full node will be selected as a baker/endorser is typically larger than the sum of the individual success probabilities. Intuitively, this is because such a probability depends upon multiples of 8000 Tz (one roll), which means that the success probabilities turn out to be a step function of the number of rolls. Finally, the possibility of delegation is likely to develop a market of full nodes of different reputations, providing such services under different economic conditions. We only outlined how the market could emerge and operate, and more work is needed to fill in a number of missing elements in the analysis. We conclude by observing that despite its simplicity and limitations, we believe this paper may offer some interesting insights on the economics of Tezos with Emmy* and possibly also with the Tenderbake consensus protocol.

Funding: This research was funded by the Tezos Foundation.

Acknowledgments: I would like to thank the Editor and the Referees for their constructive comments. I would also like to thank the Tezos Foundation for its financial support and constructive discussion on this paper. I'm grateful to the participants of a Nomadic Labs seminar, of a preliminary version of this paper, for their very useful comments.

Conflicts of Interest: The author declares no conflict of interest.

References

1. Allombert, V.; Bourgoin, M.; Tesson, J. Introduction to the Tezos Blockchain. In Proceedings of the 2019 International Conference on High Performance Computing & Simulation (HPCS), Dublin, Ireland, 15–19 July 2019; IEEE: Piscataway, NJ, USA, 2019; pp. 1–10.
2. Bamakan, S.; Motavali, A.; Bondarti, A. A Survey of Blockchain Consensus Algorithms Performance Evaluation criteria. *Exp. Syst. Appl.* **2020**, *154*, 113385.
3. Bernardo, B.; Cauderlier, R.; Hu, Z.; Pesin, B.; Tesson, J. Mi-Cho-Coq, a framework for certifying Tezos smart contracts. In *International Symposium on Formal Methods*; Springer: Cham, Switzerland, 2019; pp. 368–379.
4. Conchon, S. Some Insights on Open Problems in Blockchains: Explorative Tracks for Tezos (Invited Talk). In Proceedings of the 5th International Symposium on Foundations and Applications of Blockchain 2022 (FAB 2022), Berkeley, CA, USA, 3 June 2022; Schloss Dagstuhl-Leibniz-Zentrum für Informatik: Wadern, Germany, 2022.
5. Fernandes, M.; Alexandre, L.A. Robotchain: Using tezos technology for robot event management. *Ledger* **2019**, *3*, 32–41. [CrossRef]
6. Goodman, L.M. Tezos: A Self-Amending Crypto-Ledger Position Paper; 2014. Available online: https://tezos.com/position-paper.pdf (accessed on 1 November 2022).
7. Neuder, M.; Moroz, D.J.; Rao, R.; Parkes, D.C. Selfish behavior in the tezos proof-of-stake protocol. *arXiv* **2019**, arXiv:1912.02954. [CrossRef]
8. Neuder, M.; Moroz, D.J.; Rao, R.; Parkes, D.C. Defending against malicious reorgs in Tezos Proof-of-Stake. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, New York, NY, USA, 21–23 October 2020; pp. 46–58.
9. Nishida, Y.; Saito, H.; Chen, R.; Kawata, A.; Furuse, J.; Suenaga, K.; Igarashi, A. Helmholtz: A Verifier for Tezos Smart Contracts Based on Refinement Types. *New Gener. Comput.* **2022**, *40*, 507–540. [CrossRef]
10. Sguerra, L.M.; Jouvelot, P.; Arias, E.J.G.; Memmi, G.; Coelho, F. Blockchain Performance Benchmarking: A VCG Auction Smart Contract Use Case for Ethereum and Tezos (Short Paper). In Proceedings of the FAB 2021—Fourth International Symposium on Foundations and Applications of Blockchain, online, 7 May 2021.