Stakepool Pledge Influence in Stake Rewards Distribution

An ADA Link Paper
www.adalink.io

By Mahmoud Nimer
Twitter: @MahmoudNimer

Aug 18, 2022

Abstract

A breakdown of the current equation used to calculate the optimal rewards for a pool [1] is discussed. The main focus of the draft paper is to understand the parameter a_0 and study possible scenarios that lead to more rewards for single pools(1) against multiple pools(2) to further push decentralization of the network and reduce ADA amounts in centralized exchanges.

CIP-50 [2] has already discussed the shortcomings of the current reward equation in giving k and a_0 their supposed effect. Similar to CIP-50, this paper will first understand the current reward equation. Next, it shows off the deficiencies regarding fairness among stakepools. Then, a simple yet elegant modification is proposed. A different approach is taken compared to CIP-50.

The research in this paper is far from complete. Nonetheless, it discusses the basic pillars that cannot be ignored or compromised in a PoS ecosystem. More research and analysis will be carried out in the future.

Motivation

Ouroborus has been studied and tested rigorously in the past years. Cardano's proof of stake is, with no doubt, a very robust system and shines amongst other used protocols in the crypto industry. Nonetheless, many honest SPOs(3) are constantly fighting big players and hardly surviving the long term game.

The formula of optimal rewards for a pool [1] will be referred to as "The Reward Equation" hereafter in this paper. In it, the effect of a_0 will be studied and several suggestions to tip the scale toward SPOs against multi & exchange pools are made at the end of the paper.

(1): Pools whose operators do not own more than one stakepool.
(2): Pools whose operators own more than one pool, e.g. centralized exchanges.
(3): Single pool operators.

Centralized Exchanges (CEX) Staking Strategy

Many CEXs users keep their crypto inside their exchange accounts rather than withdraw them to native wallets. Reasons vary for this, there are two main viewpoints for it. First, the amount/value of the bought coins is not high to incentivize the user to go through the process of withdrawing the coins and holding them in a native wallet. Second, some users do not feel confident enough to be in charge of their assets, and feel safer by knowing they can go back to some sort of authority if they lose access to their account, which defeats the main purpose of cryptocurrency.

Regardless, CEXs make use of this phenomenon by carefully staking any asset that can be staked and maximize their profit from it. This does not mean real owners are getting their fair share of the staking rewards. In fact, most users do not get any rewards at all.

In a nutshell, CEXs own all the assets in their platform “not your keys not your crypto" and hence in the case of ADA they spin up stake pools and delegate all the ADA they have in the exchange. Counting on the assumption that most users do not ask for their staking rewards, CEXs can offer slightly higher APY% range than the normal staking yields to their users who want to stake their ADA on the platform. To make sure not everyone “delegates” they add fictitious constraints, namely, locking periods and an upper limit ADA amount that can be staked by a user.

To make sure their platform is as liquid as possible, a common factor for stake pools that are run by exchanges is a low pledge amount, i.e as low as 2 ADA! [3].

Stake Pool Pledge and Centralized Exchanges

A stake pool operator is asked to “pledge” an amount of ADA when they create the stake pool. The main purpose for “pledge” is to outcome Sybil Attacks [4]. But in a more general sense, It can be thought of as the operator’s way to show confidence in their willingness to maintain the pool running with highest possible performance. This amount should be kept pledged as long as the pool is operating, and hence, we can say it can be thought of as a locked amount.

The last point is crucial and can be used to distinguish single pools from centralized exchange pools. As discussed in the previous section, CEXs prefer to keep their pledge to a minimum. Up to this point in time, the effect of staked pledge is barely noticeable in the protocol.

Pledge, Stake and a_0 Parameter

$a_0 \in [0, \infty)$ is by definition the parameter that determines the influence of pledge on pool rewards [1]. When it is zero, it means pledge is similar to normal delegation coming from other wallets. Following are some manipulations on the reward equation (1) to show the influence of a_0 more clearly.

$$f(s,\sigma) = \frac{R}{1+a_0} \cdot \left(\sigma' + s' \cdot a_0 \cdot \frac{\sigma' - s' \frac{z_0 - \sigma'}{z_0}}{z_0} \right) \quad (1)$$

Where:
- R are the total available rewards for the epoch (in ADA).
- $a_0 \in [0, \infty)$ is a parameter determining owner-stake influence on pool rewards.
- $z_0 = 1/k$ is the size of a saturated pool.
- k is the current optimal number of stake pools, as of today's date it is 500.
- $\sigma' = \min(\sigma, z_0)$, where σ is the relative stake of the pool.
- $s' = \min(s, z_0)$, where s is the relative stake of the pool owner(s) (the amount of ADA pledged during pool registration.

We will divide the equation into two main parts. One increases as a_0 decreases, grouped below as $(\ )_1$, while the other increases with increasing a_0 value, grouped below as $(\ )_2$.

$$f(s,\sigma) = \left(\frac{1}{1+a_0} \cdot R \cdot \sigma' \right)_1 + \left(\frac{a_0}{1+a_0} \cdot R \cdot s' \cdot \frac{\sigma' - s' \frac{z_0 - \sigma'}{z_0}}{z_0} \right)_2 \quad (2)$$

By substituting $\sigma' = s' + d' \quad (3)$; $d' = min(d, z_0)$ where d is the relative delegations coming from other wallets, $(\ )_2$ can be rearranged as follows,

$$\left(\frac{a_0}{1+a_0} \cdot R \cdot s' \cdot \frac{\sigma' - s' \frac{z_0 - \sigma'}{z_0}}{z_0} \right)_2 = \left(\frac{a_0}{1+a_0} \cdot R \cdot \frac{s'}{z_0} \left\{ \left[1 + \frac{s'}{z_0} \right] \cdot d' + \frac{s'}{z_0} s' \right\} \right)_2 \quad (4)$$

Substituting back $z_0 = 1/k$ in (4) we get,

$$\left(\frac{a_0}{1+a_0} \cdot R \cdot \frac{s'}{z_0} \left\{ \left[1 + \frac{s'}{z_0} \right] \cdot d' + \frac{s'}{z_0} s' \right\} \right)_2 = \frac{a_0}{1+a_0} \cdot R \cdot k \cdot s' \cdot \left([1 + k \cdot s'] d' + k \cdot s'^2 \right) \quad (5)$$

Finally, $()_2$ can be written as shown in (6),

$$(\ )_2 = \frac{a_0}{1+a_0} \cdot R \cdot \left[k \cdot s' \cdot (1 + k \cdot s') \cdot d' + (k \cdot s')^2 \cdot s' \right]_2 \quad (6)$$

$[\,]_2$ is analogous to σ' in $(\,)_1$ and can be thought of as the "resultant" or "felt" stake amount in $(\,)_2$. We will refer to this value, i.e. $[\,]_2$, as σ'_a and can be named as "the effective relative stake from the pledge".

Examining Previous Findings and Apply it to Current Network State

The general outcome of staking performance can be deduced from equations (2) and (6). In this section two scenarios are examined. First, is a comparison between two current pools, one is an SPO and the other is for an exchange. Different a_0 values are tested. Naturally, one would expect a_0 to tip the scales in favor toward players who value decentralization and willing to "share the cake", so to speak.

Case Study 1:

Inputs:

- Stakepool 1
  - Type: SPO
  - Name: SPO
  - Stake: 2M ADA ⇒ $\sigma' = 0.000060606$ where k=500 and T=33 billion
  - Pledge: 100k ADA ⇒ $s' = 00000303$
  - Delegation from others ⇒ $d' = 0.000057576$
- Stakepool 2
  - Type: Exchange
  - Name: CEX
  - Stake: 66M ADA ⇒ $\sigma' = 0.002$ where k=500 and T=33 billion
  - Pledge: 10 ADA ⇒ $s' = 0$
  - Delegation from others ⇒ $d' = 0.002$

At current state of the blockchain a_0 is at 0.3 and R around 13 million, substituting (6) into (1) the equation becomes as follows:

$$f(s,\sigma) = \left(\frac{1}{1+a_0} \,.\, R \,.\, \sigma'\right)_1 + \left(\frac{a_0}{1+a_0} \,.\, R \,.\, \left[k \,.\, s' \,.\, (1 + k \,.\, s') \,.\, d' + (k \,.\, s')^2 \,.\, s'\right]_2\right)_2 \quad (7)$$

Subsititunig values of SPO and CEX pools we get:

$$f_{spo}(s,\sigma) = (0.000046620R)_1 + (0.00000002R)_2$$
$$f_{spo}(s,\sigma) = (606.060606\,ADA)_1 + (0.262125\,ADA)_2$$
$$f_{spo}(s,\sigma) = 606.322731\,ADA$$

$$f_{CEX}(s,\sigma) = (0.001538462R)_1 + (0R)_2$$

$$f_{CEX}(s, \sigma) = (20000\ ADA)_1 + (0.00091\ ADA)_2$$
$$f_{CEX}(s, \sigma) = 20000.00091\ ADA$$

Changing a_0 to 1 while keeping everything else as is, the outcome becomes as follows:

$$f_{spo}(s, \sigma) = (0.000030303R)_1 + (0.000000044R)_2$$
$$f_{spo}(s, \sigma) = (393.939394\ ADA)_1 + (0.567938\ ADA)_2$$
$$f_{spo}(s, \sigma) = 394.507332\ ADA$$

$$f_{CEX}(s, \sigma) = (0.001R)_1 + (0R)_2$$
$$f_{CEX}(s, \sigma) = (13000\ ADA)_1 + (0.00197\ ADA)_2$$
$$f_{CEX}(s, \sigma) = 13000.00197\ ADA$$

Case Study 2:

Inputs:

- Stakepool 1
  - Type: SPO
  - Name: SPO
  - Stake: 2M ADA $\Rightarrow \sigma' = 0.000060606$ where k=500 and T=33 billion
  - Pledge: 100k ADA $\Rightarrow s' = 00000303$
  - Delegation from others $\Rightarrow d' = 0.000057576$
- Stakepool 2
  - Type: Exchange
  - Name: CEX
  - Stake: 66M ADA $\Rightarrow \sigma' = 0.002$ where k=500 and T=33 billion
  - Pledge: 10 ADA $\Rightarrow s' = 0$
  - Delegation from others $\Rightarrow d' = 0.002$

In this case, we change a_0 to a high value compared to the current 0.3 and set it to 1000:

$$f_{spo}(s, \sigma) = (0.000000061R)_1 + (0.000000087R)_2$$
$$f_{spo}(s, \sigma) = (0.787092\ ADA)_1 + (1.134742\ ADA)_2$$
$$f_{spo}(s, \sigma) = 1.921834\ ADA$$

$$f_{CEX}(s, \sigma) = (0.000001998R)_1 + (0R)_2$$
$$f_{CEX}(s, \sigma) = (25.974026\ ADA)_1 + (0.003935\ ADA)_2$$
$$f_{CEX}(s, \sigma) = 25.977961\ ADA$$

Remarks

The effect of a_0 is not as one would expect. While is does reduce $(\ )_1$ effect on the overall stake rewards, it does not increase $(\ )_2$ term in same rate (mathematically this is due to the raised powers on s'). Even at high a_0 values, the amount of "depreciation" felt in $(\ )_1$ is orders of magnitude larger than the increased influence of $(\ )_2$. Therefore, pledge influence is merely present at low to medium a_0 values. Mathematically, it would make sense to pledge as little as possible, i.e. 2 ADA, and put the rest of the other stake as delegation, which is the approach currently adopted by exchanges.

In the next section a modification on the "reward equation (1)" is suggested to further incentivise decentralization.

Suggestion

The general concept of comparing the stake of one pool to the overall available stake in the network is the core concept that guarantees the security of the network. This concept can be reused in handling pledge amounts. Namely, the pledge of a stake pool gets compared to the overall pledged amount in the network.

With this in mind, a new variable called $\hat{s}$ is defined. $\hat{s}$ is the relative live stake of the pool owner(s) (the current amount of ADA in the live pledge) compared to the total pledged ADA of all operating stake pools P. In other words, the relative stake in $(\ )_2$ is no longer compared to T (current total ADA in circulation) anymore, but rather to the total pledged ADA of all operating stake pools, call it P.

$(\ )_1$ and $(\ )_2$ will be modified in (2) and redefined as follows:

$$f\left(\hat{s}, \sigma\right) = \left(\frac{1}{1+a_0} \,.\, R \,.\, \sigma'\right)_1 + \left(\frac{a_0}{1+a_0} \,.\, R \,.\, \hat{s}'\right)_2 \qquad (8)$$

Where:

- $\hat{s}' = min\left(\hat{s}, z_0\right)$ is the pledge saturation of stakepools.
- $\hat{s} = \frac{Pledged\ ADA\ in\ the\ pool}{P}$ where P is the total pledged ADA in the network. For reference, as of August 1st, 2022, it is 2.129 billion ADA.

Notice that in the most efficient ADA distribution in the network the sum of all $f\left(\hat{s}, \sigma\right)$'s will be equal to R. Which is a crucial upper bound limit that also exists in (1). Additionally, $\hat{s}'$ has a saturation value of z_0 which implies that live pledge value gets saturated when it is at $z_0 \,.\, P$, analogous to stake saturation at $z_0 \,.\, T$.

Now, the a_0 presence will be a lot more present in reward calculations. In (8) stake pool operators are incentivised to increase their live pledge as their pool increases to maximize profit, yet not doing so, will still not punish the pool compared to the current state of the blockchain. In other words, $(\,)_1$ term is the same in both (1) and (8).

Previously, (1) reduced $()_1$ as a_0 increased at a faster rate than increasing $()_2$. Therefore, regardless of the pledge amount, currently, any stakepool would see a reduction in rewards as a_0 increases (Check case studies in previous section). What (8) proposes is to balance the reduction in $()_1$ by increasing $()_2$ at a similar rate. Hence, any stakepool with relatively large pledge, compared to the average pledge amount in the network, would benefit from increasing a_0. This is a vital key point to punish CEX pools, since their pledge to total stake ratio is as low as it can be.

The tipping point of which a stakepool starts seeing more total rewards when a_0 increases can be derived from (8) as follows:

$$f\left(\hat{s}, \sigma\right) = \left(\frac{1}{1+a_0} \,.\, R \,.\, \sigma'\right)_1 + \left(\frac{a_0}{1+a_0} \,.\, R \,.\, \hat{s}'\right)_2 = R \,.\, \left(\frac{1}{1+a_0} \,.\, \sigma' + \frac{a_0}{1+a_0} \,.\, \hat{s}'\right) \quad (9)$$

Considering a non saturated case, σ' can be substituted as:

$$min\left(\sigma, z_0\right) = \sigma = \frac{\Sigma}{T} = \frac{S+D}{T} \quad (10)$$

Where Σ is the staked amount in ADA, S is the pledged amount in ADA and D is the delegated amount in ADA from other wallets. Introducing φ as the ratio of $\frac{S}{\Sigma}$, (10) can be written as

$$\frac{S+D}{T} = \frac{S}{\varphi T} \quad (11)$$

Similarly,

$$\hat{s}' = min\left(\hat{s}, \Phi . z_0\right) = \hat{s} = \frac{S}{P} \quad (12)$$

Using (11) & (12) in (9),

$$R \,.\, \left(\frac{1}{1+a_0} \,.\, \sigma' + \frac{a_0}{1+a_0} \,.\, \hat{s}'\right) = R . \left(\frac{1}{1+a_0} \,.\, \frac{S}{\varphi T} + \frac{a_0}{1+a_0} \,.\, \frac{S}{P}\right) = R \,.\, \left(\frac{P \,.\, S + a_0 \,.\, S \,.\, \varphi \,.\, T}{\left(1+a_0\right) \,.\, P \,.\, \varphi \,.\, T}\right)_3 \quad (13)$$

Defining $(\,)_3$ as a function of φ and taking first derivative for finding the global minima

$$g\left(a_0\right) = \left(\frac{P\,.\,S + a_0\,.\,S\,.\,\varphi\,.\,T}{\left(1 + a_0\right).\,P\,.\,\varphi\,.\,T}\right)_3$$

$$\frac{d}{da_0}\,g\left(a_0\right) = \frac{S\,.\,\varphi\,.\,T\,.\left(1 + a_0\right).\,P\,.\,\varphi\,.\,T - P\,.\,\varphi\,.\,T\,.\left(P\,.\,S + a_0\,.\,S\,.\,\varphi\,.\,T\right)}{\left(\left(1 + a_0\right).\,P\,.\,\varphi\,.\,T\right)^2} = 0$$

Which gives,

$$S\,.\,\varphi\,.\,T\,.\left(1 + a_0\right) - \left(P\,.\,S + a_0\,.\,S\,.\,\varphi\,.\,T\right) = 0$$
$$S\,.\,\varphi\,.\,T - P\,.\,S = 0$$
$$\varphi\,.\,T - P = 0 \Rightarrow \varphi = \frac{P}{T}$$

Final result shows that a stake pool will see a proportional relation between a_0 and its rewards when the pledged amount is higher than $\frac{P}{T}$. At the current state of the network this value is 6%.

What is most interesting in (8) is that to maximize the performance of a stakepool, its live pledge should increase as its total stake does. This shows that the bigger the pool, the bigger the pledge should be. CEX pools configuration, i.e. high stake with low pledge, will become the least efficient to extract rewards.

Equation (8) rewards honest/serious players in the game. Replacing (1) with (8) while keeping a_0 will not result in any reduction of rewards to any pool. On the other hand, rewards would increase for pools who have higher pledge.

Second point is increasing a_0 using (8). As seen in the last derivation, stakepools who have their pledge less than 6% of their total stake would feel a negative net effect on rewards as a_0 increases. However, this decrease is again proportional to how little pledge there is in the pool, and hence CEX and multiple pool operators would suffer the most.

As a comparison to the case study in the previous section, the same cases will be compared using equation (8).

Case Study 1:

Inputs:

- Stakepool 1
  - Type: SPO
  - Name: SPO
  - Stake: 2M ADA $\Rightarrow \sigma' = 0.000060606$ where k=500 and T=33 billion
  - Pledge: 100k ADA $\Rightarrow s' = 0.000046968$ where P=2.13 billion

- Stakepool 2
    - Type: Exchange
    - Name: CEX
    - Stake: 66M ADA ⇒ $\sigma' = 0.002$ where k=500 and T=33 billion
    - Pledge: 10 ADA ⇒ $s' = 0$

At current state a_0 is at 0.3 and R around 13 million, substituting into (8):

$$f\left(\hat{s}, \sigma\right) = \left(\frac{1}{1+a_0} \,.\, R \,.\, \sigma'\right)_1 + \left(\frac{a_0}{1+a_0} \,.\, R \,.\, \hat{s}'\right)_2$$

Subsititunig values of SPO and CEX pools we get:

$$f_{spo}(s, \sigma) = (0.00004662R)_1 + (0.000010839R)_2$$
$$f_{spo}(s, \sigma) = (606.060606\ ADA)_1 + (140.904649\ ADA)_2$$
$$f_{spo}(s, \sigma) = 746.965255\ ADA$$

$$f_{CEX}(s, \sigma) = (0.001538462R)_1 + (0R)_2$$
$$f_{CEX}(s, \sigma) = (20000\ ADA)_1 + (0.01409\ ADA)_2$$
$$f_{CEX}(s, \sigma) = 20000.01409\ ADA$$

Changing a_0 to 1 while keeping everything else as is, the outcome becomes as follows:

$$f_{spo}(s, \sigma) = (0.000030303R)_1 + (0.000023484R)_2$$
$$f_{spo}(s, \sigma) = (393.939394\ ADA)_1 + (305.293405\ ADA)_2$$
$$f_{spo}(s, \sigma) = 699.232799\ ADA$$

$$f_{CEX}(s, \sigma) = (0.001R)_1 + (0R)_2$$
$$f_{CEX}(s, \sigma) = (13000\ ADA)_1 + (0.030529\ ADA)_2$$
$$f_{CEX}(s, \sigma) = 13000.030529\ ADA$$

Case Study 2:

Inputs:

- Stakepool 1
    - Type: SPO
    - Name: SPO
    - Stake: 2M ADA ⇒ $\sigma' = 0.000060606$ where k=500 and T=33 billion
    - Pledge: 100k ADA ⇒ $s' = 0.000046968$ where P=2.13 billion

- Stakepool 2
    - Type: Exchange
    - Name: CEX
    - Stake: 66M ADA $\Rightarrow \sigma' = 0.002$ where k=500 and T=33 billion
    - Pledge: 10 ADA $\Rightarrow s' = 0$

In this case, we change a_0 to a high value compared to the current 0.3 and set it to 1000:

$$f_{spo}(s, \sigma) = (0.000000061R)_1 + (0.000046921R)_2$$
$$f_{spo}(s, \sigma) = (0.787092\ ADA)_1 + (609.976834\ ADA)_2$$
$$f_{spo}(s, \sigma) = 610.763926\ ADA$$

$$f_{CEX}(s, \sigma) = (0.000001998R)_1 + (0R)_2$$
$$f_{CEX}(s, \sigma) = (25.974026\ ADA)_1 + (0.060998\ ADA)_2$$
$$f_{CEX}(s, \sigma) = 26.035024\ ADA$$

Remarks:

Equation (8) gives a better influence for pledge and a_0 parameter compared to (1) while still conserving main objectives. Namely, the upper bound of total rewards in an epoch, and the prevention of Sybil attacks.

One could argue (8) is more fair toward parties and give an edge to those willing to show confidence by increasing their pledge amount.

It should be noted that (8) can be modified to make the “tipping point” of 6% lower so SPOs can start benefiting from a_0 with less pledge value. More on this point will be investigated in future studies.

Table 1: Comparison between the result of case studies 1 & 2 with equation (1) and (8)

a_0	Current Reward Equation(1)		Proposed Reward Equation(1)	
0.3	Stakepool	Reward/Epoch	Stakepool	Reward/Epoch
	SPO(2)	606 ADA	SPO(2)	747 ADA
	CEX(3)	20,000 ADA	CEX(3)	20,000 ADA
1	Stakepool	Reward/Epoch	Stakepool	Reward/Epoch
	SPO(2)	395 ADA	SPO(2)	699 ADA
	CEX(3)	13,000 ADA	CEX(3)	13,000 ADA
1000	Stakepool	Reward/Epoch	Stakepool	Reward/Epoch
	SPO(2)	2 ADA	SPO(2)	611 ADA
	CEX(3)	26 ADA	CEX(3)	26 ADA

(1): T = 33 billion, k = 500, R = 13 million, P = 2.1 billion.
(2): Total Stake = 2 million ADA of which 100k ADA is pledged.
(3): Total Stake = 66 million ADA of which 10 ADA is pledged.

Conclusion

This draft paper shed light on a_0 and the influence of pledge amount on reward calculations. It proposed a modification on the reward equation to punish stakepool that most resemble CEX pools. It makes sense from the fairness point of view to reward pools with high pledge relative to their total stake. It shows that big pools do not necessarily have the biggest influence if their pledge does not compare to their stake. Additionally, the proposed equation naturally introduces a saturation limit "$z_0 \cdot P$" after which the pledge will not have any additional influence. Last point is important to incentivize SPOs to get delegations from other wallets, since it wont give any advantage to pledge all the stake, and therefore, delegations from user wallets are still strongly incentivized as well.

References

[1] Philipp Kant, et al., April 11, 2019, “Engineering Design Specification for Delegation and Incentives in Cardano–Shelley” (https://hydra.iohk.io/build/790053/download/1/delegation_design_spec.pdf)

[2] Michael Liesenfelt, April 5, 2022, “CIP-50: Shelleys Voltaire decentralization update” (https://github.com/cardano-foundation/CIPs/pull/242)

[3] Binance Steak Pools Group Data: (https://adapools.org/groups/binance-20)

[4] Lars Brünjes, October 29, 2018, “Preventing Sybil attacks” (https://iohk.io/en/blog/posts/2018/10/29/preventing-sybil-attacks/)