Equilibrium Staking Levels in a Proof-of-Stake Blockchain

Kose John[*] Thomas J. Rivera[†] Fahad Saleh[‡]

Abstract

We study the equilibrium level of staking in a Proof-of-Stake blockchain when investors have different trading horizons. We find that, contrary to conventional wisdom, staking levels do not always increase in block rewards. Rather, block rewards serve as an inflationary transfer from short-horizon cryptocurrency investors to long-horizon cryptocurrency investors. Thus, increasing block rewards reduces short-horizon cryptocurrency investment which, under certain conditions, reduces the overall transfer to long-horizon cryptocurrency investors and therefore reduces long-horizon investment as well. When this is the case, increasing block rewards decreases total cryptocurrency investment which leads to a reduction in the equilibrium value of staked cryptocurrency.

Keywords: Blockchain, Proof-of-Stake, Staking, Block Rewards

[*]New York University Stern School of Business. Email: kjohn@stern.nyu.edu
[†]McGill University. Email: thomas.rivera@mcgill.ca
[‡]Wake Forest University. Email: salehf@wfu.edu

1 Introduction

Achieving consensus in a Proof-of-Stake blockchain generally involves a process known as *staking*. A cryptocurrency unit is said to be staked if its holder forfeits the right to trade it for a pre-specified amount of time. Staking a cryptocurrency unit confers a monetary reward (in expectation) so that investors weigh the aforementioned constraint of not trading against the monetary reward to determine whether to stake their coins. In this paper, we provide an equilibrium analysis to examine the staking level of a Proof-of-Stake (PoS) blockchain where the staking level is defined as the market value of staked cryptocurrency units.

The PoS equilibrium staking level is of particular importance because it determines the security of a PoS blockchain. In particular, John et al. (2021) demonstrate that whether a malicious agent would find disrupting a PoS blockchain incentive compatible depends upon the PoS blockchain's staking level whereby the probability of disruption to transaction activity (e.g., denial of service or 51% attack) decreases with the staking level. It is commonly believed that a high staking level (and thus high security) is generated by high *block rewards* which are new cryptocurrency units that are issued and paid to investors as an incentive to stake their cryptocurrency. Nonetheless, this paper overturns that conventional wisdom, demonstrating that increasing block rewards does not necessarily increase the equilibrium staking level.

To understand why the staking level is not necessarily increasing in block rewards, it is important to recognize that block rewards represent inflationary transfers of welfare rather than increases in aggregate welfare. Consequently, an increase in block rewards increases pay-offs for some cryptocurrency investors but reduces pay-offs for other cryptocurrency investors. The increased pay-offs for the former group induces additional investment and staking from the former group, whereas the decreased pay-offs for the latter group induces reduced investment and staking from the latter group. In turn, the overall effect of block rewards upon staking levels is ambiguous.

Our formal analysis considers a discrete time infinite horizon model. At the beginning of each period, a unit measure of investors arrive, each with a unit endowment. Each investor may invest in the cryptocurrency or in an alternative investment which is modeled as an outside option with a pay-off drawn from an exogenous distribution. If an investor invests in the cryptocurrency, she optimally maintains her holding until she receives a random liquidity shock that forces her to sell her position and exit the model. Staking the cryptocurrency yields an investor positive block rewards in expectation so that staking is optimal provided that the investor does not need to trade. In turn, each cryptocurrency investor optimally stakes her holdings in each period until she receives a liquidity shock and exits the model.

A key aspect of our analysis is that we allow for heterogeneity among investors in terms of their trading horizons. More precisely, while all investors face a liquidity shock with some probability at the beginning of each period, investors vary in the probability that this liquidity shock realizes. In particular, some investors are *long-horizon* investors with a low probability of facing a liquidity shock and therefore longer expected trading horizons while other investors are *short-horizon* investors with a high probability of facing a liquidity shock and therefore shorter expected trading horizons.

Our first result, Proposition 4.1, is that non-zero block rewards imply that long-horizon investors receive pay-offs that exceed those from zero block rewards, whereas short-horizon investors receive pay-offs below those from zero block rewards. This result highlights that block rewards transfer welfare from short-horizon investors to long-horizon investors. Intuitively, this result arises because short-horizon investors trade more frequently than long-horizon investors and thus stake less frequently. In turn, long-horizon investors accrue a disproportionately large share of block rewards and thus their losses from the inflation implied by block rewards are more than offset by the gains from receiving most of those block rewards that generate the inflation. In contrast, short-horizon investors accrue a disproportionately small share of block rewards and thus their losses from the inflation implied by block rewards exceed the gains from the block rewards that they accrue.

Although block rewards benefit long-horizon investors relative to zero block rewards, the effect of block rewards upon long-horizon investor pay-offs is not monotonic. In particular, Proposition 4.3 establishes that block rewards increase long-horizon investor pay-offs for low levels of block rewards but decrease long-horizon investor pay-offs for high levels of block rewards. This result arises because long-horizon investor pay-offs depend not only on the level of block rewards but also on the share of cryptocurrency investment coming from short-horizon investors: when short-horizon cryptocurrency investment falls, so too does the inflationary transfer received by long-horizon investors. Further, increases in block rewards always decrease short-horizon investor pay-offs and therefore their cryptocurrency investment. We demonstrate that the effect of increasing block rewards upon short-horizon cryptocurrency investment is limited when block rewards are low, but this effect dominates when block rewards are sufficiently high. In turn, long-horizon investor pay-offs increase in block rewards when block rewards are low but decrease in block rewards when block rewards are high.

While the effect of block rewards upon long-horizon investor pay-offs is non-monotonic, increases in block rewards always decrease short-horizon investor pay-offs and therefore short-horizon investor cryptocurrency demand. This is due to the fact that increasing block rewards implies higher inflation, and, as discussed, short-horizon investors accrue a disproportionately small share of block rewards and therefore do not fully recoup the losses from inflation. In turn, short-horizon investor cryptocurrency demand decreases in block rewards because investors have access to alternative investment opportunities so that the decreased pay-offs cause short-horizon investors to shift investment away from the cryptocurrency to those alternative investments. We formalize these results via Proposition 4.5.

The aforementioned results lead to our main result, Proposition 4.6, which establishes that block rewards have a non-monotonic effect on equilibrium staking levels. More formally, Proposition 4.6 provides two main findings: Proposition 4.6.1 establishes that block rewards increase equilibrium staking levels when block rewards are low, whereas Proposition 4.6.2 demonstrates that block rewards decrease equilibrium staking levels when block rewards are high. In practical terms, our findings establish that while block rewards can initially raise equilibrium staking levels, they eventually become self-defeating in that they lower equilibrium staking levels when block rewards become sufficiently high. Importantly, we demonstrate that this latter effect can be so severe that for sufficiently high block rewards the equilibrium level of staking will be lower than that implied by even zero block rewards (Corollary 4.9).

Our main result arises because, as we demonstrate, equilibrium staking levels depend upon three endogenous quantities: short-horizon investor cryptocurrency demand, long-horizon investor cryptocurrency demand, and the average trading horizon of investors holding the cryptocurrency. The equilibrium staking level increases in all three of these quantities. With regard to the first two quantities, an increase in cryptocurrency demand by short-horizon or long-horizon investors implies an increase in the market value of the cryptocurrency and thus a higher equilibrium staking value. With regard to the third quantity, a longer trading horizon for a cryptocurrency investor implies an increase in demand for staking because a cryptocurrency investor optimally stakes her cryptocurrency holdings whenever she does not trade. Hence, less frequent trading implies more frequent staking and therefore the equilibrium staking value increases in the average trading horizon.

In order to explain why staking levels are initially increasing in block rewards (Proposition 4.6.1), recall that when block rewards are low, an increase in block rewards decreases pay-offs for short-horizon investors and increases pay-offs for long-horizon investors. When this is the case, increasing block rewards causes short-horizon cryptocurrency investor demand to decrease and long-horizon cryptocurrency investor demand to increase. We then show that when both sets of investors have access to similar alternative investments and block rewards are sufficiently low, then these two demand effects roughly offset each other. Yet, the reduction in short-horizon investor cryptocurrency demand coupled with the increase in long-horizon investor cryptocurrency demand implies an increase in the average trading horizon. Thus, when block rewards are low the dominant effect of increasing block rewards is to increase the average trading horizon which leads to an increase in equilibrium staking levels.

In contrast, staking levels decrease in block rewards when they are sufficiently high (Proposition 4.6.2) because increasing block rewards eventually undermines investor demand for the cryptocurrency. In particular, as per Proposition 4.4, the reduction in short-horizon investor cryptocurrency demand eventually reduces long-horizon investor pay-offs — and therefore long-horizon cryptocurrency investor demand — when block rewards are increased beyond a certain threshold. Consequently, cryptocurrency demand from both short-horizon and long-horizon investors decrease in block rewards when they are sufficiently high, in which case we show that increases in block rewards beyond this threshold must reduce equilibrium staking levels.

We conclude by providing a benchmark result, Proposition 4.10, which establishes that the equilibrium staking level is entirely invariant to block rewards when all investors possess identical expected trading horizons. Intuitively, when investors have the same trading horizons, they stake for the same amount of time (in expectation) and therefore earn the same pay-offs. Moreover, since block rewards represent inflationary transfers rather than aggregate productivity gains, overall investor pay-offs neither increase nor decrease in block rewards so that individual investor pay-offs also neither increase nor decrease in block rewards. Finally, since investor pay-offs are invariant to block rewards, investor cryptocurrency demand and therefore the equilibrium staking level must also be invariant to block rewards.

Broadly speaking, our paper contributes to the literature on the economics of blockchain fundamentals. John et al. (2022) provide a survey of that literature. Prominent papers within that literature include Biais et al. (2019), Easley et al. (2019), Basu et al. (2021), Cong et al. (2021a), Hinzen et al. (2022), Huberman et al. (2021) and Pagnotta (2022). Our paper differs from the referenced papers in that they examine Proof-of-Work (PoW), whereas we examine PoS.

More narrowly, our paper contributes to the literature on economics of PoS blockchain fundamentals. Prominent papers in that literature include Benhaim et al. (2021), Fanti et al. (2019), John et al. (2021), Rosu and Saleh (2021) and Saleh (2021). Benhaim et al. (2021) provide a rigorous study of committee-based PoS protocols. Fanti et al. (2019) put forth a valuation framework for a PoS payment system. John et al. (2021) put forth an economic model of PoS that determines adoption endogenously while incorporating blockchain security. Rosu and Saleh (2021) examine wealth concentration for a PoS cryptocurrency. Saleh (2021) studies the Nothing-at-Stake problem and the Double-Spending problem in the context of a PoS blockchain. Our paper differs from the aforementioned papers in that we focus upon the effect of block rewards upon equilibrium staking levels.

Our paper also relates to the literature on decentralized finance. In particular, blockchains that allow for decentralized applications typically employ PoS (see Irresberger et al. 2021) because PoS provides a scaling advantage over PoW (see John et al. 2021). Cong et al. (2021b), Cong et al. (2022) and Mayer (2022) provide models of blockchain that allow for decentralized applications, whereas Capponi and Jia (2021), Lehar and Parlour (2021) and Park (2021) study a prominent type of decentralized finance application.

2 Model

We model an infinite horizon, discrete-time setting with periods called epochs as per a typical PoS protocol. Each epoch consists of slots, and each slot corresponds to one block being added to the blockchain. As is the case in standard PoS protocols, we assume that each slot is assigned to a single investor on the basis of a lottery over staked cryptocurrency units. All slots within an epoch are assigned at the beginning of an epoch and thus staking decisions must also be made at the beginning of each epoch. For simplicity we assume that there is one slot per epoch.

2.1 Investors

At the beginning of each epoch, a unit measure of investors arrive, each with a unit endowment. We refer to each individual investor arriving in Epoch t as Investor (i, t) with $i \in [0, 1]$ denoting the investor's unique identifier among all investors arriving in the epoch. Each investor may invest in the cryptocurrency or an alternative investment opportunity described below. If the investor invests in the cryptocurrency, she may stake her cryptocurrency units in any future epoch so long as she does not sell her holdings.

We assume that, after investing in the cryptocurrency, each investor eventually incurs a liquidity shock and must liquidate her holdings. In particular, we assume that Investor (i, t) faces a liquidity shock with probability $\theta_{(i,t)} \in (0, 1)$ at the beginning of each Epoch $s > t$. Conditional on receiving a liquidity shock at the beginning of Epoch s, Investor (i, t) must liquidate her entire holdings, after which she exits the model. At the beginning of each Epoch t, each Investor (i, t) learns the value of $\theta_{(i,t)} \in \{\theta_L, \theta_S\}$ with $0 < \theta_L \leqslant \theta_S < 1$ before deciding whether to invest in the cryptocurrency or not. We refer to investors with $\theta_{(i,t)} = \theta_S$ as *short-horizon* investors and investors with $\theta_{(i,t)} = \theta_L$ as *long-horizon* investors because the former have shorter expected trading horizons than the latter. We assume that each investor has an ex-ante probability $p_S := \mathbb{P}(\theta_{(i,t)} = \theta_S)$ of being a short-horizon investor and complementary probability $p_L := \mathbb{P}(\theta_{(i,t)} = \theta_L) = 1 - p_S$ of being a long-horizon investor. Letting $\overline{\tau}_S$ denote the expected trading horizon of the short-horizon investors and $\overline{\tau}_L$ the expected trading horizon of the long-horizon investors, we can see that the following condition holds:

$$\overline{\tau}_S = \frac{1}{\theta_S} \leqslant \frac{1}{\theta_L} = \overline{\tau}_L \tag{1}$$

We let $\tau_{(i,t)} \sim \text{Geom}(\theta_{(i,t)})$ denote the random trading horizon of Investor (i, t) (as opposed to the expected trading horizon $\overline{\tau}_L$ or $\overline{\tau}_H$) so that each investor (i, t) expects to hold the cryptocurrency from time t to time $t+\tau_{(i,t)}$. Then, the pay-off for Investor (i, t) from investing in the cryptocurrency at the beginning of Epoch t, $\Pi_{(i,t)}$, is given as follows:

$$\Pi_{(i,t)} = \mathbb{E}[P_{t+\tau_{(i,t)}} \cdot Q_{(i,t),t+\tau_{(i,t)}}] \tag{2}$$

where P_s denotes the price of the cryptocurrency in Epoch s, and $Q_{(i,t),s}$ denotes the cryptocurrency holding of Investor (i,t) at the beginning of Epoch s.[1] If Investor (i,t) invests in the cryptocurrency at the beginning of Epoch t, then it is never optimal for her to sell her holdings until she receives a liquidity shock (i.e., until Epoch $t+\tau_{(i,t)}$).

Alternative Investments: We assume that Investor (i,t) has access to an alternative investment with gross return $\sigma_{(i,t)} \sim G$ where $G \in \mathcal{C}^{\infty}$ is strictly increasing and supported on $[\underline{\sigma}, \overline{\sigma}]$ with $0 < \underline{\sigma} < 1 < \overline{\sigma} < \infty$. Consequently, Investor (i,t) invests in the cryptocurrency in Epoch t if and only if her pay-off from that investment weakly exceeds the pay-off from her alternative investment opportunity. More formally, letting A_t denote the set of investors who arrive in Epoch t and invest in the cryptocurrency, then

$$(i,t) \in A_t \Longleftrightarrow \Pi_{(i,t)} \geqslant \sigma_{(i,t)} \tag{3}$$

2.2 Block Rewards

We normalize the level of the cryptocurrency supply at the beginning of Epoch zero to $M_0 = 1$. We further allow for an arbitrary cryptocurrency growth rate, $\rho > 0$. Then, letting M_t denote the cryptocurrency supply at the beginning of Epoch t, the cryptocurrency supply is governed by the equation:

$$M_{t+1} = M_t \cdot e^{\rho} \tag{4}$$

Consequently, the block reward over Epoch t, B_t, is given by:

$$B_t = M_{t+1} - M_t = M_t \cdot (e^{\rho} - 1) \tag{5}$$

Block rewards are allocated to users chosen to update the next block in the blockchain. The PoS protocol selects a staked cryptocurrency unit uniformly at random and allocates the right to update the next block to the owner of that unit. Therefore, conditional on staking, the evolution of cryptocurrency holdings for any Investor (i,t) who invests in the cryptocurrency is given as follows:[2]

[1]All prices are denominated in the investor's endowment good.

[2]For exposition, we consider a limiting case by which each epoch consists of infinitely many blocks. Moreover, we assume that block rewards are evenly distributed across slots within an epoch.

$$Q_{(i,t),s+1} = Q_{(i,t),s} + \gamma_{(i,t),s} \times B_t \tag{6}$$

for all s such that $t < s < t + \tau_{(i,t)}$ and where $\gamma_{(i,t),s} \in [0, 1]$ denotes the probability that Investor (i, t) is selected to add a block in any particular slot during Epoch t, and therefore earn the block rewards B_t. In turn, $\gamma_{(i,t),s}$ is determined as follows:

$$\gamma_{(i,t),s} = \frac{Q_{(i,t),s}}{S_s} \tag{7}$$

where S_s denotes the overall number of staked cryptocurrency units at the beginning of Epoch s. We discuss how S_s is determined in the following Section 2.3.

2.3 Equilibrium Staking Levels

Once an investor owns the cryptocurrency, staking until liquidation is a dominant strategy so that all holders of the cryptocurrency who are not trading within an epoch stake their cryptocurrency. Moreover, it is not optimal for an investor to sell her cryptocurrency holding prior to a forced liquidation if it was optimal for her to invest in the cryptocurrency initially. As a consequence, the equilibrium staking level at the beginning of Epoch t, S_t, is given by the aggregate holdings of investors who previously purchased the cryptocurrency but have yet to liquidate. In particular,

$$S_t = \sum_{z:z<t} \int_{i:(i,z)\in A_{z,t}} Q_{(i,z),t}\ d\mu_z(i) \tag{8}$$

where $\mu_z(i)$ denotes the uniform measure over investors arriving in Epoch z, and $A_{z,t} \subseteq A_z$ denotes the investors arriving in Epoch z who invested in the cryptocurrency but have not been forced into liquidation by time t. Explicitly, $A_{z,t}$ is defined as follows for $z < t$:

$$A_{z,t} := A_z \bigcap \{(i, z) : z + \tau_{(i,z)} > t\} \tag{9}$$

In turn, the overall demand for the cryptocurrency at the beginning of Epoch t is the sum of the total amount of staked cryptocurrency and the demand from investors arriving in Epoch t and purchasing the cryptocurrency. Then, the market clearing condition for the cryptocurrency is given as follows:

$$M_t = S_t + \int\limits_{i:(i,t):A_{t,t}} \frac{1}{P_t} \, d\mu_t(i) \tag{10}$$

where the left-hand side pertains to the cryptocurrency supply and the right-hand side pertains to cryptocurrency demand. Note that the demand for each investor arriving in Epoch t who invests in the cryptocurrency is given by $\frac{1}{P_t}$ because each investor possesses a unit endowment and partial investment is not optimal.

Note that S_t and M_t are measured in cryptocurrency units rather than economic value. As such, to ease our subsequent discussion, we define the market value analogs of each as follows:

$$\mathcal{S}_t := P_t \cdot S_t, \qquad \mathcal{M}_t := P_t \cdot M_t \tag{11}$$

3 Model Solution

We solve for an equilibrium characterized by a stationary equilibrium staking level, $\mathcal{S}$, and a stationary equilibrium cryptocurrency market value, $\mathcal{M}$. More formally, we solve for an equilibrium characterized by the following conditions:

$$\mathcal{S}_t = \mathcal{S} \text{ for all } t, \qquad \mathcal{M}_t = \mathcal{M} \text{ for all } t \tag{12}$$

Note that in any stationary equilibrium if Investor (i, t) with alternative investment opportunity $\sigma_{(i,t)}$ is indifferent between investing in the cryptocurrency and the alternative investment opportunity then any Investor (i', t') with $\theta_{(i,t)} = \theta_{(i',t')}$ would invest in the cryptocurrency if and only if $\sigma_{(i',t')} \leqslant \sigma_{(i,t)}$. As a consequence, our equilibrium is also characterized by stationary cut-offs $\sigma_S^\star$ and $\sigma_L^\star$ such that Investor (i, t) of type θ_j invests in the cryptocurrency if and only if $\sigma_{(i,t)} \leqslant \sigma_j^\star$ for each $j \in \{S, L\}$. Therefore, the set of investors that invest in the cryptocurrency in Epoch t is given by

$$A_t = \{(i,t) : \theta_{(i,t)} = \theta_S, \sigma_{(i,t)} \leqslant \sigma_S^\star\} \bigcup \{(i,t) : \theta_{(i,t)} = \theta_L, \sigma_{(i,t)} \leqslant \sigma_L^\star\} \tag{13}$$

Our next proposition provides the solution for the stationary equilibrium:

Proposition 3.1. ***Equilibrium Solution***

Let $\overline{\tau}$ denote the average trading horizon for investors purchasing the cryptocurrency given explicitly as:

$$\overline{\tau} = \pi_S \cdot \overline{\tau}_S + \pi_L \cdot \overline{\tau}_L$$

where π_S and π_L denote the endogenous share of demand from short-horizon and long-horizon investors respectively arriving in any epoch, and $\overline{\tau}_S$ and $\overline{\tau}_L$ denote the expected trading horizons of each respective type θ_S and θ_L given explicitly in (1). Further, note that π_S and π_L are given explicitly as follows:

$$\pi_S = \frac{p_S \cdot G(\sigma_S^\star)}{p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star)}, \qquad \pi_L = \frac{p_L \cdot G(\sigma_L^\star)}{p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star)}$$

The steady state equilibrium is characterized as follows:

$$\mathcal{M} = \overline{\tau} \cdot (p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star))$$

$$\mathcal{S} = (\overline{\tau} - 1) \cdot (p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star))$$

Further, $\sigma_S^\star$ and $\sigma_L^\star$ are defined as the solutions to the following simultaneous equations:

$$\Pi_S = \frac{(\overline{\tau} - 1) \cdot \theta_S \cdot e^{-\rho}}{(1 - \theta_S) \cdot e^{-\rho} + (\theta_S \cdot \overline{\tau} - 1)} = \sigma_S, \qquad \Pi_L = \frac{(\overline{\tau} - 1) \cdot \theta_L \cdot e^{-\rho}}{(1 - \theta_L) \cdot e^{-\rho} + (\theta_L \cdot \overline{\tau} - 1)} = \sigma_L \tag{14}$$

Proof. See Appendix Section A.1. □

4 Results

Our primary focus is on understanding the relationship between block rewards and equilibrium staking levels. To understand that relationship, we first provide some preliminary results in Section 4.1. We then utilize our preliminary results to establish our main results in Section 4.2. Our main finding, Proposition 4.6, is that equilibrium staking levels are non-monotonic in block rewards whereby staking levels increase in block rewards when block rewards are low but decrease in block rewards when block rewards are sufficiently high. In what follows, we will assume that the cryptocurrency growth rate (which determines block rewards) satisfies $\rho < \overline{\rho}$ whereby $\overline{\rho}$ is the upper bound that ensures a positive level of equilibrium investment by both short horizon and long horizon investors whenever $\rho < \overline{\rho}$.[3]

4.1 Preliminary Results

We begin by presenting a result which establishes that block rewards constitute a transfer of wealth from short-horizon investors to long-horizon investors.

Proposition 4.1. ***Block Rewards Create Redistribution***

Let $\Pi^\star_S(\rho)$ and $\Pi^\star_L(\rho)$ denote the equilibrium pay-offs for short and long horizon investor's respectively as a function of the cryptocurrency growth rate, ρ. Then,

1. *Without Block Rewards, All Investors Earn Identical Pay-Offs*

   $\Pi^\star_S(0) = \Pi^\star_L(0)$

2. *Block Rewards Reduce Short-Horizon Investor Pay-offs Relative to No Rewards*

   For any $\rho > 0$: $\Pi^\star_S(\rho) < \Pi^\star_S(0)$.

3. *Block Rewards Increase Long-Horizon Investor Pay-offs Relative to No Rewards*

   For any $\rho > 0$: $\Pi^\star_L(\rho) > \Pi^\star_L(0)$

Proof. See Appendix Section A.2. □

Proposition 4.1 establishes that all investors earn identical pay-offs in the absence of block rewards (Proposition 4.1.1) but that pay-offs for short-horizon investors and long-horizon investors diverge in the presence of block rewards. More explicitly, when block rewards are positive (i.e., $\rho > 0$), short-horizon investor pay-offs decrease when compared to the case of zero block rewards (Proposition 4.1.2), whereas long-horizon investor pay-offs increase (Proposition 4.1.3).

We interpret Proposition 4.1 as demonstrating that block rewards transfer welfare from short-horizon investors to long-horizon investors because long-horizon investors accrue a disproportionately large share of block rewards, and the value of block rewards arises from the inflationary

[3]The case in which only one set of investors invest in the cryptocurrency is subsumed by Proposition 4.11.

losses they impose upon all cryptcurrency investors. More precisely, since block rewards are new units of cryptcurrencies, their value arises from diluting the value of existing cryptocurrency holdings, thereby imposing an inflationary loss on all cryptocurrency investors. Nonetheless, in a PoS blockchain, block rewards are distributed back to cryptocurrency investors. Consequently, investors who receive a disproportionately large share of block rewards gain from block rewards at the expense of investors who accrue a disproportionately small share of block rewards. Long-horizon investors accrue a disproportionately large share of block rewards, whereas short-horizon investors accrue a disproportionately small share of block rewards, hence our interpretation that block rewards serve as a transfer of welfare from short-horizon investors to long-horizon investors. We clarify this last point regarding block rewards accruing disproportionately to long-horizon investors with the following result:

Proposition 4.2. ***Block Rewards Accrue Disproportionately to Long-Horizon Investors***
Let $\eta^{\star}_{(i,t),s}$ denote the equilibirum share of cryptocurrency units held by Investor (i,t) at the beginning of Epoch $s > t$. More explicitly:

$$\eta^{\star}_{(i,t),s} = \frac{Q^{\star}_{(i,t),s}}{M^{\star}_{s}}$$

Additionally, for any investor who invests in the cryptocurrency (i.e., $(i,t) \in A_t$), we define $\nu^{\star}_{(i,t)}$ as the expected proportion by which her share increases from her purchase to her sale in the steady state equilibrium:

$$\nu^{\star}_{(i,t)} = \frac{\mathbb{E}[\eta^{\star}_{(i,t),t+\tau_{(i,t)}}]}{\eta^{\star}_{(i,t),t}}$$

The following results hold:

1. *Short-Horizon Investor Shares Decrease*

   If $\rho > 0$ and $\theta_{(i,t)} = \theta_S$ then $\nu^{\star}_{(i,t)} < 1$.

2. *Long-Horizon Investor Shares Increase*

   If $\rho > 0$ and $\theta_{(i,t)} = \theta_L$ then $\nu^{\star}_{(i,t)} > 1$.

Proof. See Appendix Section A.3. □

Proposition 4.2 demonstrates that the expected share of cryptocurrency units increases for long-horizon investors but decreases for short-horizon investors. This result arises because short-horizon investors trade more frequently than long-horizon investors and thus stake less frequently. Therefore, given that more block rewards are accrued by investors that stake longer, long-horizon investors acrue a disproportionately large share of block rewards relative to short-horizon investors. In turn, the cryptocurrency share for short-horizon investors decreases, whereas the cryptocurrency share for long-horizon investors increases.

While long-horizon investors earn higher pay-offs in the presence of block rewards as compared to the absence of block rewards (Proposition 4.1.3), our next result formalizes that long-horizon investors do not benefit monotonically from increases in block rewards.

Proposition 4.3. ***Non-Monotonic Block Reward Effect On Long-Horizon Investor Pay-Offs***
Let $\Pi_L^\star(\rho)$ denote the equilibrium pay-offs for a long-horizon investor as a function of the cryptocurrency growth rate, ρ. Then, the following results hold:

1. *Long-Horizon Investor Pay-Offs Increase For Low Block Reward Levels*
   There exists a $\underline{\rho}_L > 0$ such that for all $\rho \in [0, \underline{\rho}_L] : \frac{d\Pi_L^\star}{d\rho} > 0$.

2. *Long-Horizon Investor Pay-Offs Decrease For High Block Reward Levels*
   There exists a $\overline{\rho}_L > 0$ such that for all $\rho \in [\overline{\rho}_L, \overline{\rho}) : \frac{d\Pi_L^\star}{d\rho} < 0$.

Proof. See Appendix Section A.4. □

Proposition 4.3 establishes that block rewards have a non-monotonic monotonic effect upon long-horizon investor pay-offs. More explicitly, block rewards initially increase long-horizon investor pay-offs (i.e., $\frac{d\Pi_L^\star}{d\rho} \geqslant 0$ for low values of ρ) but eventually decrease long-horizon investor pay-offs (i.e., $\frac{d\Pi_L^\star}{d\rho} \leqslant 0$ for high values of ρ). To help illustrate the intuition for this result, we offer the following supplementary proposition:

Proposition 4.4. ***Reformulating Long-Horizon Investor Pay-Offs***
Let $\Pi_L^\star(\rho)$ denote the equilibrium pay-offs for a long-horizon investor as a function of the cryptocurrency growth rate, ρ. $\Pi_L^\star(\rho)$ is given explicitly as follows:

$$\Pi_L^\star(\rho) = \tilde{\Pi}_L^\star(\rho, \pi_S^\star(\rho)) := \frac{(\pi_S^\star(\rho) \cdot (\overline{\tau}_S - \overline{\tau}_L) + \overline{\tau}_L - 1) \cdot \theta_L \cdot e^{-\rho}}{(1-\theta_L) \cdot e^{-\rho} + (\theta_L \cdot \pi_S^\star(\rho) \cdot (\overline{\tau}_S - \overline{\tau}_L) + \theta_L \cdot \overline{\tau}_L - 1)}$$

where long-horizon investor pay-offs depend on block rewards not only directly but also through the equilibrium share of short-horizon investors, $\pi_S^\star(\rho)$. In turn, we can decompose the direct effect of block rewards upon long-horizon investor pay-offs (i.e., $\frac{\partial \tilde{\Pi}_L^\star}{\partial \rho}$) from the indirect effect of block rewards upon long-horizon investor pay-offs through the share of short-horizon investors (i.e., $\frac{\partial \tilde{\Pi}_L^\star}{\partial \pi_S} \cdot \frac{d\pi_S^\star}{d\rho}$):

$$\frac{d\Pi_L^\star}{d\rho} = \frac{\partial \tilde{\Pi}_L^\star}{\partial \rho} + \frac{\partial \tilde{\Pi}_L^\star}{\partial \pi_S} \cdot \frac{d\pi_S^\star}{d\rho}$$

The following results hold:

1. *Holding Short-Horizon Share Constant, Long-Horizon Pay-Offs Increase with Block Rewards*

   For all $\rho < \overline{\rho}$: $\frac{\partial \tilde{\Pi}_L^\star}{\partial \rho} > 0$.

2. *Long-Horizon Pay-Offs Increase In the Share of Short-Horizon Investors*

   For all $\rho < \overline{\rho}$: $\frac{\partial \tilde{\Pi}_L^\star}{\partial \pi_S} > 0$.

3. *Share of Short-Horizon Investors Decrease in Block Rewards when they are Sufficiently High and Low.*

   There exists $\underline{\rho}_L$ and $\overline{\rho}_L$ such that $\frac{d\pi_S^\star}{d\rho} < 0$ when $\rho \in [0, \underline{\rho}_L) \bigcup (\overline{\rho}_L, \overline{\rho}]$.

These results clarify the ambiguity in the overall effect (i.e., $\frac{d\Pi_L^\star}{d\rho}$ has an ambiguous sign) as arising because the direct effect is positive (i.e., $\frac{\partial \tilde{\Pi}_L^\star}{\partial \rho} \geqslant 0$) but the indirect effect is negative when ρ is sufficiently high or low (i.e., $\frac{\partial \tilde{\Pi}_L^\star}{\partial \pi_S} \cdot \frac{d\pi_S^\star}{d\rho} \leqslant 0$).

Proof. See Appendix Section A.5 □

Proposition 4.4 demonstrates that block rewards have both a direct and indirect effect upon long-horizon investor pay-offs and that these effects compete so that the overall effect of block rewards upon long-horizon investor pay-offs depends upon which effect dominates. More explicitly, long-horizon investor pay-offs, $\Pi_L^\star$, depend on block rewards, ρ, not only directly but also through the endogenous share of cryptocurrency investors who have short-horizons, $\pi_S^\star(\rho)$. Proposition 4.4 establishes that the direct effect of block rewards upon long-horizon investor pay-offs is always positive but that the indirect effect of block rewards upon long-horizon investor pay-offs, through the share of short-horizon cryptocurrency investors, is negative when ρ is either sufficiently small or sufficiently large. We then show that the direct effect dominates for low levels of block rewards so that long-horizon investor pay-offs increase in block rewards when block rewards are low (Proposition 4.3.1). In contrast, the indirect effect dominates for high levels of block rewards so that long-horizon investor pay-offs decrease in block rewards when block rewards are high (Proposition 4.3.2).

To understand the underlying channel for Proposition 4.4, recall that block rewards constitute a transfer from short-horizon investors to long-horizon investors. Holding the share of short-horizon cryptocurrency investors fixed, long-horizon investor pay-offs monotonically increase in block rewards (Proposition 4.4.1) because higher block rewards imply a larger transfer from each short-horizon cryptocurrency investor. Nonetheless, the short-horizon cryptocurrency investor share is not fixed; rather, short-horizon investors anticipate that larger block rewards imply a larger transfer from themselves to long-horizon investors when they invest in cryptocurrencies. As a consequence, short-horizon investors optimally respond to increases in block rewards by reallocating towards their alternative investments. In turn, the share of short-horizon cryptocurrency investors declines as block rewards increase (Proposition 4.4.3) and this reduced share of short-horizon cryptocurrency investors implies fewer short-horizon investors transferring wealth to long-horizon investors (Proposition 4.4.2).

In contrast to long-horizon investor pay-offs, short-horizon investor pay-offs are monotonic in block rewards. In particular, increases in block rewards always decrease short-horizon investor pay-offs. Our next result formalizes that point:

Proposition 4.5. ***Short-Horizon Investor Pay-Offs***

Let $\Pi_S^\star(\rho)$ denote the equilibrium pay-offs for a short-horizon investor as a function of the cryptocurrency growth rate, ρ. Then, the following result holds:

$$\text{For all } \rho \geqslant 0 : \frac{d\Pi_S^\star}{d\rho} < 0$$

Proof. See Appendix Section A.6. □

4.2 Main Results

Our main result demonstrates that increasing block rewards have a non-monotonic effect upon the equilibrium staking level:

Proposition 4.6. ***Non-Monotonic Block Reward Effect on the Equilibrium Staking Level***

The following results hold:

1. *Staking Levels Are Increasing in Block Rewards When They Are Low*

   There exists a $\underline{\rho}_{\mathcal{S}} > 0$ *such that for all* $\rho \in [0, \underline{\rho}_{\mathcal{S}}] : \frac{d\mathcal{S}}{d\rho} > 0$.

2. *Staking Levels Are Decreasing in Block Rewards When They Are High*

   There exists a $\overline{\rho}_{\mathcal{S}} < \overline{\rho}$ *such that for all* $\rho \in (\overline{\rho}_{\mathcal{S}}, \overline{\rho}] : \frac{d\mathcal{S}}{d\rho} < 0$.

Proof. See Appendix Section A.7. □

Crucially, while block rewards increase the staking level when block rewards are low (Proposition 4.6.1), this effect is not monotonic. Rather, for a sufficiently high level of block rewards, increases in block rewards decrease the staking level (Proposition 4.6.2).

Proposition 4.6 arises because the equilibrium staking level depends upon three equilibrium quantities: new short-horizon investor cryptocurrency demand, new long-horizon investor cryptocurrency demand, and the average cryptocurrency investor trading horizon. Explicitly, via Proposition 3.1, the equilibrium staking level can be decomposed as follows:

$$\mathcal{S} = \mathcal{S}(\overline{\tau}, \mathcal{D}_S, \mathcal{D}_L) = (\overline{\tau} - 1) \cdot (\mathcal{D}_S + \mathcal{D}_L) \tag{15}$$

where $\overline{\tau}$ denotes the average trading horizon of cryptocurrency investors while $\mathcal{D}_S := p_S \cdot G(\sigma_S^\star)$ and $\mathcal{D}_L := p_L \cdot G(\sigma_L^\star)$ denote the equilibrium cryptocurrency demand of newly arriving short-horizon and newly arriving long-horizon investors respectively. Note that the equilibrium staking level, $\mathcal{S}$, increases in each of the three quantities (i.e., $\frac{\partial \mathcal{S}}{\partial \overline{\tau}} > 0$, $\frac{\partial \mathcal{S}}{\partial \mathcal{D}_S} > 0$, $\frac{\partial \mathcal{S}}{\partial \mathcal{D}_L} > 0$).

In order to understand Proposition 4.6.1, which establishes that the staking level increases for low levels of block rewards, recall that increasing block rewards increases long-horizon investor pay-offs when block rewards are low (Proposition 4.3) and always decreases short-horizon investor pay-offs (Proposition 4.5). Thus, when block rewards are low, increasing block rewards increases long-horizon investor cryptocurrency demand (i.e., $\frac{d\mathcal{D}_L}{d\rho} > 0$ for low ρ) but decreases short-horizon cryptocurrency investor demand (i.e., $\frac{d\mathcal{D}_S}{d\rho} < 0$ for low ρ). We show how these two demand effects roughly offset each other in terms of overall demand (i.e., $|\frac{d[\mathcal{D}_L+\mathcal{D}_s]}{d\rho}|$ is small for low ρ) but also lead to an increase in the average trading horizon (i.e., $\frac{d\overline{\tau}}{d\rho} > 0$ for low ρ) since long-horizon investors effectively replace short-horizon investors. Then, since an increase in the average trading horizon increases the staking level (i.e., $\frac{\partial \mathcal{S}}{\partial \overline{\tau}} > 0$), and the demand effects roughly offset each other when ρ is low, an increase in block rewards consequently increases the equilibrium staking level when block rewards are low as per Proposition 4.6.1. We formalize the referenced intuition with the following supplementary result:

Proposition 4.7. ***The Staking Level Increases In Rewards When Rewards Are Low***
Let $\overline{\tau}(\rho)$ denote the equilibrium average trading horizon for cryptocurrency investors as a function of the cryptocurrency growth rate, ρ. Further, let $\mathcal{D}_S(\rho)$ and $\mathcal{D}_L(\rho)$ denote the equilibrium cryptocurrency demand coming from new short-horizon and long-horizon investors respectively. Finally, let $\mathcal{S}(\overline{\tau}, \mathcal{D}_S, \mathcal{D}_L)$ denote the equilibrium staking level as a function of the equilibrium average trading horizon and new cryptocurrency demand from short-horizon and long-horizon investors as given by (15)*. Then, the following results hold:*

1. *Block Rewards Have a Negligible Effect on Demand When They Are Low*

   For all $\varepsilon > 0$ there exists $\underline{\rho}_{\varepsilon} > 0$ such that $\frac{d}{d\rho}[\mathcal{D}_S + \mathcal{D}_L] < \varepsilon$ for all $\rho \leqslant \underline{\rho}_{\varepsilon}$.

2. *Block Rewards Increase the Average Trading Horizon*

   There exists $\underline{\rho}_{\overline{\tau}} > 0$ such that for all $\rho < \underline{\rho}_{\overline{\tau}} : \frac{d\overline{\tau}}{d\rho} > 0$.

Proof. See Appendix Section A.8. □

While the effect of increasing block rewards upon overall cryptocurrency demand is small for low levels of block rewards (Proposition 4.7.1), this is not true for higher levels of block rewards. Crucially, Proposition 4.6.2, which establishes that increasing block rewards decreases the staking level when block rewards are high (i.e., $\frac{d\mathcal{S}}{d\rho} < 0$ for $\rho \geqslant \overline{\rho}_{\mathcal{S}}$), arises precisely because increasing block rewards decreases overall cryptocurrency investor demand when block rewards are high. Recall that increasing block rewards decreases long-horizon investor pay-offs when block rewards are high (Proposition 4.3), whereas increasing block rewards decreases short-horizon investor pay-offs at all levels of block rewards (Proposition 4.5). In turn, when block rewards are high, increasing block rewards unambiguously decreases investor demand (i.e., $\frac{d[\mathcal{D}_S+\mathcal{D}_L]}{d\rho} < 0$ for large ρ), and this effect dominates any effect through the average trading horizon. Then, since the equilibrium staking value increases in cryptocurrency investor demand (i.e., $\frac{\partial \mathcal{S}}{\partial \mathcal{D}_S} > 0$ and $\frac{\partial \mathcal{S}}{\partial \mathcal{D}_L} > 0$), the overall effect of increasing block rewards is that equilibrium staking value decreases when block rewards are sufficiently high as per Proposition 4.6.2. The following supplementary result formalizes the referenced intuition:

Proposition 4.8. ***The Staking Level Decreases In Rewards When Rewards Are High***
Let $\overline{\tau}(\rho)$ denote the equilibrium average trading horizon for cryptocurrency investors as a function of the cryptocurrency growth rate, ρ. Further, let $\mathcal{D}_S(\rho)$ and $\mathcal{D}_L(\rho)$ denote the equilibrium cryptocurrency demand coming from new short-horizon and long-horizon investors respectively. Finally, let $\mathcal{S}(\overline{\tau}, \mathcal{D}_S, \mathcal{D}_L)$ denote the equilibrium staking level as a function of the equilibrium average trading horizon and new cryptocurrency demand from short-horizon and long-horizon investors as given by (15). Then, the following results hold:

1. *Rewards Reduce Cryptocurrency Demand When Rewards Are High*
   There exists a $\overline{\rho}_{\mathcal{D}} < \overline{\rho}$ such that $\frac{d}{d\rho}[\mathcal{D}_S + \mathcal{D}_L] \leqslant 0$ for all $\rho \in [\overline{\rho}_{\mathcal{D}}, \overline{\rho}]$.

2. *The Demand Effect Dominates The Trading Horizon Effect When Rewards Are High*
   There exists a $\overline{\rho}_{\mathcal{S}} < \overline{\rho}$ such that $\frac{\partial \mathcal{S}}{\partial \mathcal{D}_S} \cdot \frac{d\mathcal{D}_S}{d\rho} + \frac{\partial \mathcal{S}}{\partial \mathcal{D}_L} \cdot \frac{d\mathcal{D}_L}{d\rho} \leqslant \frac{\partial \mathcal{S}}{\partial \overline{\tau}} \cdot \frac{d\overline{\tau}}{d\rho}$ for all $\rho \in [\overline{\rho}_{\mathcal{S}}, \overline{\rho}]$.

Proof. See Appendix Section A.9. □

Figure 1 demonstrates our main findings by plotting the equilibrium staking level $\mathcal{S}(\rho)$ as a function of ρ when the return from the alternative investment $\sigma_{(i,t)}$ is uniformly distributed over $[.9, 1.9]$. As can be seen, the equilibrium payoff and therefore equilibrium cut-off of the short-horizon investor is strictly decreasing in block rewards (ρ). Further, the equilibrium payoff of the long-horizon investor is first increasing in block rewards and then eventually decreasing in block rewards. This means that the equilibrium staking level is increasing in block rewards when they are small so that the effect of the increased time horizon $\frac{d\overline{\tau}}{d\rho}$ outweighs the demand effect $\frac{d[\mathcal{D}_L+\mathcal{D}_S]}{d\rho}$. Then, as the level of block rewards passes a threshold, the demand effect overtakes the time horizon effect in which case staking levels start decreasing in block rewards.

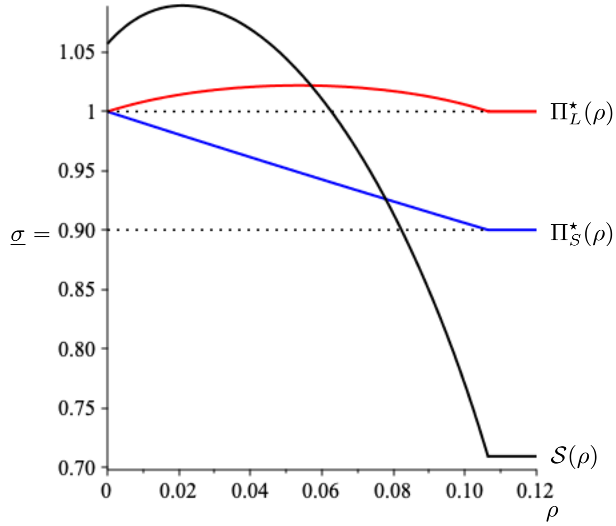

Figure 1: Plot of equilibrium staking level $\mathcal{S}(\rho)$ (scaled by $\frac{1}{7}$) and equilibrium payoffs $\Pi^{\star}_{S}(\rho)$, and $\Pi^{\star}_{L}(\rho)$ when $G = Uniform[.9, 1.9]$, $\theta_H = .9$, $\theta_L = .1$, and $p_S = p_L = \frac{1}{2}$.

Of particular note, at $\rho = \overline{\rho}$, the equilibrium staking level is strictly less than the staking levels with zero block rewards (i.e. $\rho = 0$) so that a strictly positive block reward level can generate a lower equilibrium staking level than no block rewards. We generalize this point with the following result:

Corollary 4.9. *There exists a threshold $\bar{\rho}_0 < \bar{\rho}$ such that the equilibrium staking level with block rewards ρ is less than the equilibrium staking level with zero block rewards whenever $\rho > \bar{\rho}_0$. Formally: $\mathcal{S}(\rho) < \mathcal{S}(0)$ for all $\rho > \bar{\rho}_0$.*

Proof. See Appendix Section A.10. □

We conclude by examining a benchmark setting in which all investors possess identical expected trading horizons (i.e., $\theta_L = \theta_S$). In this setting, we establish the generic failure of the conventional wisdom that block rewards increase equilibrium staking levels by showing that the equilibrium staking level is entirely invariant to the level of block rewards:

Proposition 4.10. ***Staking Level Is Invariant to Rewards With Ex-Ante Identical Investors***
Assume that $\theta_L = \theta_S$ so that all investors possess identical expected trading horizons. Then, the following result holds:

$$\frac{d\mathcal{S}}{d\rho} = 0$$

In particular, the equilibrium staking level is entirely invariant to the level of block rewards.

Proof. See Appendix Section A.11. □

Proposition 4.10 arises because, as discussed, block rewards constitute a transfer from short-horizon investors to long-horizon investors; in turn, when all investors have identical expected trading horizons, then there are no net transfers (in expectation). To clarify this point, we offer the following supplementary result:

Proposition 4.11. ***Investor Pay-Offs With Ex-Ante Identical Investors***

Assume that $\theta_L = \theta_S$ so that all investors possess identical expected trading horizons. Then, for all $\rho \geqslant 0$ and any Investor (i, t), the following result holds:

$$\Pi^{\star}_{(i,t)} = 1$$

Hence, all investor pay-offs are identically one and therefore all investor pay-offs are invariant to the level of block rewards (i.e., $\frac{d\Pi^{\star}_{(i,t)}}{d\rho} = 0$).

Proof. See Appendix Section A.11. □

Proposition 4.11 formalizes our assertion that there are no expected transfers of wealth when all investors possess identical expected trading horizons. This is done by establishing that when investors have identical expected trading horizons then all investors receive pay-offs equivalent to their initial endowments which we normalized to unity: each investor stakes the cryptocurrency just long enough (in expectation) to recoup the same amount of block rewards that they pay in inflation. Note that this result of no net transfers applies for any level of block rewards so that investor pay-offs are invariant to block rewards as a corollary (i.e., $\frac{d\Pi_{(i,t)}}{d\rho} = 0$). Then, since investor pay-offs are invariant to block rewards, so too is investor cryptocurrency demand. In turn, per (15), the equilibrium staking level is also invariant to block rewards which yields us the result of Proposition 4.10.

5 Conclusion

This paper examines the effect of block rewards upon equilibrium staking levels. Contrary to conventional wisdom, we find that block rewards do not increase equilibrium staking levels in general. Our results have important implications for PoS blockchain security.

References

Basu, S., D. Easley, M. O'Hara, and E. Sirer. 2021. StableFees: A Predictable Fee Market for Cryptocurrencies. *Working Paper* .

Benhaim, A., B. H. Falk, and G. Tsoukalas. 2021. Scaling Blockchains: Can Elected Committees Help? *Working Paper* .

Biais, B., C. Bisière, M. Bouvard, and C. Casamatta. 2019. The Blockchain Folk Theorem. *Review of Financial Studies* 32(5):1662–1715.

Capponi, A., and R. Jia. 2021. The Adoption of Blockchain-based Decentralized Exchanges. *Columbia University Working Paper* .

Cong, L. W., Z. He, and J. Li. 2021a. Decentralized Mining in Centralized Pools. *Review of Financial Studies* 34(3):1191–1235.

Cong, L. W., Y. Li, and N. Wang. 2021b. Tokenomics: Dynamic Adoption and Valuation. *Review of Financial Studies* 34(3):1105–1155.

Cong, L. W., Y. Li, and N. Wang. 2022. Token-based platform finance. *Journal of Financial Economics* 144:972–991. URL https://www.sciencedirect.com/science/article/pii/S0304405X21004414.

Easley, D., M. O'Hara, and S. Basu. 2019. From Mining to Markets: The Evolution of Bitcoin Transaction Fees. *Journal of Financial Economics* 134(1):91–109.

Fanti, G., L. Kogan, and P. Viswanath. 2019. Economics of Proof-of-Stake Payment Systems. *Working Paper* .

Hinzen, F. J., K. John, and F. Saleh. 2022. Bitcoin's limited adoption problem. *Journal of Financial Economics* 144:347–369. URL https://www.sciencedirect.com/science/article/pii/S0304405X22000198.

Huberman, G., J. D. Leshno, and C. Moallemi. 2021. Monopoly without a Monopolist: An Economic Analysis of the Bitcoin Payment System. *The Review of Economic Studies* URL https://doi.org/10.1093/restud/rdab014.

Irresberger, F., K. John, P. Mueller, and F. Saleh. 2021. The Public Blockchain Ecosystem: An Empirical Analysis. *NYU Stern Working Paper* .

John, K., M. O'Hara, and F. Saleh. 2022. Bitcoin and Beyond. *Annual Review of Financial Economics* 14.

John, K., T. Rivera, and F. Saleh. 2021. Economic Implications of Scaling Blockchains: Why the Consensus Protocol Matters. *NYU Stern Working Paper* .

Lehar, A., and C. Parlour. 2021. Decentralized Exchanges. *Working Paper* .

Mayer, S. 2022. Token-Based Platforms and Speculators. *Working Paper* .

Pagnotta, E. 2022. Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security. *Review of Financial Studies* 35(2):866–907.

Park, A. 2021. The Conceptual Flaws of Constant Product Automated Market Making. *University of Toronto Working Paper* .

Rosu, I., and F. Saleh. 2021. Evolution of Shares in a Proof-of-Stake Cryptocurrency. *Management Science* 67(2):661–672.

Saleh, F. 2021. Blockchain Without Waste: Proof-of-Stake. *Review of Financial Studies* 34(3):1156–1190.

Appendices

A Proofs

A.1 Proof of Proposition 3.1

Proof. First, denote by $\mathcal{M}_S$ and $\mathcal{M}_L$ the steady state market values of short and long horizon holdings, respectively. Then, given that $\mathcal{M}_S$ and $\mathcal{M}_L$ are time independent in the steady state, this implies that

$$\mathcal{M}_j = (1-\theta_j) \cdot \mathcal{M}_j + p_j \cdot G(\sigma_j^\star)$$

for each $j \in \{S, L\}$ or equivalently

$$\mathcal{M}_j = \frac{p_j \cdot G(\sigma_j^\star)}{\theta_j} = \overline{\tau}_j \cdot p_j \cdot G(\sigma_j^\star)$$

for each $j \in \{S, L\}$. Next, noting that $\mathcal{M}_S + \mathcal{M}_L = \mathcal{M}$, we rearrange to obtain

$$\mathcal{M} = (\frac{\overline{\tau}_S \cdot p_S \cdot G(\sigma_S^\star)}{p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star)} + \frac{\overline{\tau}_L \cdot p_L \cdot G(\sigma_L^\star)}{p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star)}) \cdot (p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star))$$

and therefore after substituting for π_S, π_L, and finally $\overline{\tau}$ we obtain $\mathcal{M} = \overline{\tau} \cdot (p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star))$.

In order to derive $\mathcal{S}$, we multiply (10) by P_t to obtain

$$\mathcal{M} = \mathcal{S} + p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star)$$

and therefore after rearranging we obtain $\mathcal{S} = (\overline{\tau} - 1) \cdot (p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star))$.

The equilibrium levels $\sigma_S^\star$ and $\sigma_L^\star$ are determined by the simultaneous equations $\Pi_S = \sigma_S$ and $\Pi_L = \sigma_L$. Thus, to prove the final result of this proposition we must derive Π_S and Π_L. In order to do so, denote by $\psi_{(i,t),s}$ the log-return from Investor (i, t) for staking in period $s > t$ so that

$$\psi_{(i,t),s} = log(\frac{P_{s+1}Q_{(i,t),s+1}}{P_s Q_{(i,t),s}})$$

Furthermore, using Equation (6) to substitute for $Q_{(i,t),s+1}$ we can see that

$$\psi_{(i,t),s} = log(\frac{P_{s+1}Q_{(i,t),s+1}}{P_s Q_{(i,t),s}}) = log(\frac{P_{s+1}}{P_s Q_{(i,t),s}}[Q_{(i,t),s} + \frac{Q_{(i,t),s}}{S_s} B_s]) = log(\frac{P_{s+1}}{P_s}[1 + \frac{B_s}{S_s}])$$

Further, using the fact that $B_s = M_{s+1} - M_s = M_s(e^\rho - 1)$ then

$$\psi_{(i,t),s} = log(\frac{P_{s+1}}{P_s} + \frac{P_{s+1}}{P_s}\frac{M_s}{S_s}(e^\rho - 1))$$

Finally, by our definition of stationary equilibrium we know that $P_s M_s = \mathcal{M}$ for all s and therefore

$$\frac{P_{s+1}}{P_s} = \frac{P_{s+1}M_{s+1}}{P_s M_s} \cdot \frac{M_s}{M_{s+1}} = \frac{\mathcal{M}}{\mathcal{M}} \cdot \frac{M_s}{M_{s+1}} = e^{-\rho}$$

while

$$\frac{M_s}{S_s} = \frac{P_s M_s}{P_s S_s} = \frac{\mathcal{M}}{\mathcal{S}} = \frac{\bar{\tau} \cdot (p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star))}{(\bar{\tau}-1) \cdot (p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star))} = \frac{\bar{\tau}}{\bar{\tau}-1}$$

Hence,

$$\psi_{(i,t),s} = log(e^{-\rho} + e^{-\rho}\frac{\bar{\tau}}{\bar{\tau}-1}(e^{\rho}-1)) = log(e^{-\rho} + (1-e^{-\rho}) \cdot \frac{\bar{\tau}}{\bar{\tau}-1})$$

Therefore, we have shown that the steady state log-return from staking in period $s > t$ for investor (i,t) is constant and equal to $\psi = log(e^{-\rho} + (1-e^{-\rho}) \cdot \frac{\bar{\tau}}{\bar{\tau}-1})$. Hence, the return from staking in period $s > t$ for Investor (i,t) is

$$e^{\psi} = e^{-\rho} + (1-e^{-\rho}) \cdot \frac{\bar{\tau}}{\bar{\tau}-1}$$

Now, to derive the profits Π_S and Π_L respectively, we first note that given Investor (i,t) cannot stake in their first period of holding then $Q_{(i,t),t+1} = Q_{(i,t),t}$. Therefore, using the fact that $P_t Q_{(i,t),t} = 1$ then

$$P_{t+1}Q_{(i,t),t+1} = \frac{P_{t+1}}{P_t}P_t Q_{(i,t),t+1} = \frac{P_{t+1}}{P_t}P_t Q_{(i,t),t} = \frac{P_{t+1}}{P_t}$$

Hence,

$$\Pi_j = \mathbb{E}[P_{t+1}Q_{(i,t),t+1} \cdot e^{\psi(\tau_{i,t}-1)}] = \mathbb{E}[\frac{P_{t+1}}{P_t} \cdot e^{\psi(\tau_{i,t}-1)}] = e^{-\rho}\sum_{z=0}^{+\infty} e^{\psi \cdot z}(1-\theta_j)^z \theta_j$$

Note that this sum is finite whenever $(1-\theta_j)e^{\psi} < 1$. Whenever this condition holds, then $\Pi_j = \frac{\theta_j e^{-\rho}}{1-(1-\theta_j)e^{\psi}}$ which after substituting for e^{ψ} and rearranging yields the expressions for Π_S and Π_L. □

A.2 Proof of Proposition 4.1

Proof. First, note that using the expressions for $\Pi_S(\rho)$ and $\Pi_L(\rho)$ from Proposition 3.1, it can be seen by inspection that $\Pi_S(0) = \Pi_L(0) = 1$ for all levels of σ_S and σ_L. Therefore, in equilibrium $\Pi_S^\star(0) = 1 = \Pi_L^\star(0)$.

Next note that, $\Pi_L(\rho) > \Pi_L(0) = 1$ if and only if (after rearranging)

$$(\overline{\tau} \cdot \theta_L - 1) \cdot e^{-\rho} > (\overline{\tau} \cdot \theta_L - 1)$$

and therefore whenever there is a positive mass of short horizon users that invest ($\sigma_S^\star > \underline{\sigma}$), which we assume when imposing $\rho < \bar{\rho}$, then the average expected trading horizon of investors $\overline{\tau} < \frac{1}{\theta_L}$ and therefore $\overline{\tau} \cdot \theta_L - 1 < 0$ so that this inequality always holds. Therefore, $\Pi_L(\rho) > \Pi_L(0)$ for all σ_L and all $\sigma_S > \underline{\sigma}$ and hence in any equilibrium with positive adoption by both types $\Pi_L^\star(\rho) > \Pi_L^\star(0)$

Similarly, note that $\Pi_S(\rho) < \Pi_S(0) = 1$ if and only if

$$(\overline{\tau} - 1) \cdot \theta_S \cdot e^{-\rho} < (1 - \theta_S) \cdot e^{-\rho} + \theta_S \cdot \overline{\tau} - 1$$

which after rearranging implies

$$(\overline{\tau} \cdot \theta_S - 1) \cdot e^{-\rho} < (\overline{\tau} \cdot \theta_S - 1)$$

which holds when $\overline{\tau} \cdot \theta_S > 1$. Finally, we note that $\overline{\tau} > \frac{1}{\theta_S}$ whenever there is a positive level of adoption for the L-types (i.e. $\sigma_L^\star > \underline{\sigma}$) as in that case there is a positive measure of L-type users so the average expected trading horizon of investors that invest in the cryptocurrency must be larger than the shortest expected trading horizon $\frac{1}{\theta_S}$. Hence, given that we have shown that $\Pi_L^\star(\rho) > 1$ when there is a positive level of adoption for both types, then this must imply that $\sigma_L^\star > 1 > \underline{\sigma}$. Therefore, it must be the case that $\Pi_S(\rho) < \Pi_S(0)$ for all thresholds σ_S and σ_L when $\rho < \bar{\rho}$ and therefore $\Pi_S^\star(\rho) < \Pi_S^\star(0)$. $\square$

A.3 Proof of Proposition 4.2

Proof. Note that in the steady state

$$\nu_{(i,t)} = \frac{\mathbb{E}[\eta_{(i,t),t+\tau_{(i,t)}}]}{\eta_{(i,t),t}} = \mathbb{E}[\frac{Q_{(i,t),t+\tau_{(i,t)}}}{Q_{(i,t),t}} \cdot \frac{M_t}{M_{t+\tau_{(i,t)}}}] = \mathbb{E}[\frac{Q_{(i,t),t+\tau_{(i,t)}}}{Q_{(i,t),t}} \cdot \frac{P_{t+\tau_{(i,t)}}}{P_t}] = \mathbb{E}[Q_{(i,t),t+\tau_{(i,t)}} \cdot P_{t+\tau_{(i,t)}}]$$

This last term is equal to Π_S if $\theta_{(i,t)} = \theta_S$ and Π_L if $\theta_{(i,t)} = \theta_L$. Finally, note that we have shown in the proof of Proposition 4.1 that $\Pi_S(\rho) < \Pi_S(0) = 1 = \Pi_L(0) < \Pi_L(\rho)$ for all $\rho \in (0, \overline{\rho})$. $\square$

A.4 Proof of Proposition 4.3

Proof. In order to prove this result we will focus on the change to adoption cutoffs $\sigma_S^\star$ and $\sigma_L^\star$ as a function of ρ which in any equilibrium satisfying (14) display the identical behavior as Π_S and Π_L. We will invoke the implicit function theorem in order to derive closed form expressions for $\frac{\partial \sigma_S^\star}{\partial \rho}(\boldsymbol{\sigma}_0, \rho_0)$ and $\frac{\partial \sigma_L^\star}{\partial \rho}(\boldsymbol{\sigma}_0, \rho_0)$ around the solution $\boldsymbol{\sigma}_0 = (\sigma_S, \sigma_L)$ to (14) when $\rho = \rho_0$. In particular, consider the function $f : \mathbb{R}^3 \to \mathbb{R}^2$

$$f(\boldsymbol{\sigma}, \rho) := \begin{bmatrix} f_1(\boldsymbol{\sigma}, \rho) \\ f_2(\boldsymbol{\sigma}, \rho) \end{bmatrix} := \begin{bmatrix} \Pi_S(\boldsymbol{\sigma}, \rho) - \sigma_S \\ \Pi_L(\boldsymbol{\sigma}, \rho) - \sigma_L \end{bmatrix}$$

Then, for any ρ we are considering solutions $\boldsymbol{\sigma}$ to (14) of the form $f(\boldsymbol{\sigma}, \rho) = 0$. Now, let $J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)$ denote the Jacobian matrix of f with respect to $\boldsymbol{\sigma}$ defined as

$$J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0) := \begin{bmatrix} \frac{\partial f_1}{\partial \sigma_S} & \frac{\partial f_1}{\partial \sigma_L} \\ \frac{\partial f_2}{\partial \sigma_S} & \frac{\partial f_2}{\partial \sigma_L} \end{bmatrix}$$

If $J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)$ is invertible, then by the implicit function theorem we know that

$$\frac{\partial \boldsymbol{\sigma}}{\partial \rho}(\rho) = -[J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}(\rho), \rho)]^{-1}[\frac{\partial f}{\partial \rho}(\boldsymbol{\sigma}(\rho), \rho)]$$

for all ρ in some open interval containing ρ_0. Further, $J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)$ is invertible whenever $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) \neq 0$. We proceed by assuming that $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) \neq 0$ noting that by the continuity of our profit functions, $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) = 0$ will only hold for some non-generic set of knife edge cases (i.e. a measure zero set of parameters). Further, we proceed by assuming that $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) > 0$ which we will confirm must be the case in any equilibrium at the end of the proof. In particular, we assume

$$det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) = (\frac{\partial \Pi_S}{\partial \sigma_S} - 1) \cdot (\frac{\partial \Pi_L}{\partial \sigma_L} - 1) - \frac{\partial \Pi_S}{\partial \sigma_L} \cdot \frac{\partial \Pi_L}{\partial \sigma_S} > 0 \tag{1}$$

Now, note that

$$\frac{\partial \Pi_j}{\partial \sigma_k} = \frac{\frac{\partial \overline{\tau}}{\partial \sigma_k} \cdot \theta_j \cdot e^{-\rho} \cdot \eta_j - \frac{\partial \overline{\tau}}{\partial \sigma_k} \cdot (\overline{\tau} - 1) \cdot \theta_j^2 \cdot e^{-\rho}}{\eta_j^2} = \frac{-\frac{\partial \overline{\tau}}{\partial \sigma_k} \cdot \theta_j \cdot (1 - \theta_j) \cdot e^{-\rho} \cdot (1 - e^{-\rho})}{\eta_j^2}$$

for each $j, k \in \{S, L\}$ where $\eta_j = (1-\theta_j)\cdot e^{-\rho} + (\theta_j \cdot \overline{\tau} - 1)$. Further,

$$\frac{\partial \overline{\tau}}{\partial \sigma_L} = \frac{G'(\sigma_L)\cdot G(\sigma_S)\cdot p_L \cdot p_S}{(p_S\cdot G(\sigma_S) + p_L \cdot G(\sigma_L))^2}\cdot(\overline{\tau}_L - \overline{\tau}_S) > 0 \qquad \frac{\partial \overline{\tau}}{\partial \sigma_S} = \frac{G'(\sigma_S)\cdot G(\sigma_L)\cdot p_L \cdot p_S}{(p_S\cdot G(\sigma_S) + p_L \cdot G(\sigma_L))^2}\cdot(\overline{\tau}_S - \overline{\tau}_L) < 0 \tag{2}$$

implies that $\frac{\partial \Pi_S}{\partial \sigma_S} > 0$, $\frac{\partial \Pi_L}{\partial \sigma_L} < 0$, $\frac{\partial \Pi_S}{\partial \sigma_L} < 0$, and $\frac{\partial \Pi_L}{\partial \sigma_S} > 0$. Therefore, whenever $\frac{\partial \Pi_S}{\partial \sigma_S} < 1$, then $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) > 0$ for all values of $(\boldsymbol{\sigma}_0, \rho_0)$ and therefore $J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)$ is invertible.[4]

Next, note that (1) can be expressed as

$$\frac{\partial \boldsymbol{\sigma}}{\partial \rho}(\rho) = \begin{bmatrix} \frac{\partial \sigma_S^\star}{\partial \rho}(\rho) \\ \frac{\partial \sigma_L^\star}{\partial \rho}(\rho) \end{bmatrix} = \frac{-1}{det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}(\rho), \rho))}\cdot \begin{bmatrix} (\frac{\partial \Pi_L}{\partial \sigma_L}(\boldsymbol{\sigma}(\rho),\rho) - 1)\cdot \frac{\partial \Pi_S}{\partial \rho}(\boldsymbol{\sigma}(\rho),\rho) - \frac{\partial \Pi_S}{\partial \sigma_L}(\boldsymbol{\sigma}(\rho),\rho)\cdot \frac{\partial \Pi_L}{\partial \rho}(\boldsymbol{\sigma}(\rho),\rho) \\ -\frac{\partial \Pi_L}{\partial \sigma_S}(\boldsymbol{\sigma}(\rho),\rho)\cdot \frac{\partial \Pi_S}{\partial \rho}(\boldsymbol{\sigma}(\rho),\rho) + (\frac{\partial \Pi_S}{\partial \sigma_S}(\boldsymbol{\sigma}(\rho),\rho) - 1)\cdot \frac{\partial \Pi_L}{\partial \rho}(\boldsymbol{\sigma}(\rho),\rho) \end{bmatrix} \tag{3}$$

where

$$\frac{\partial \Pi_j}{\partial \rho}(\rho) = \frac{(\overline{\tau} - 1)\cdot \theta_j e^{-\rho}}{\eta_j^2}\cdot(1 - \theta_j \cdot \overline{\tau})$$

for each $j \in \{S, L\}$. Now, using the fact that $\theta_S \cdot \overline{\tau} > 1$ and $\theta_L \cdot \overline{\tau} < 1$ implies $\frac{\partial \Pi_L}{\partial \rho} > 0$ and $\frac{\partial \Pi_S}{\partial \rho} < 0$. Further, we have assumed that $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) > 0$ and therefore, using the above proven properties regarding the partial derivatives we can see that $\frac{\partial \sigma_S^\star}{\partial \rho}(\rho) < 0$ for all ρ.

Now, in order to prove Result 1, note that as $\rho \to 0$ then $\frac{\partial \Pi_j}{\partial \sigma_k} \to 0$ for all $j, k \in \{S, L\}$. This implies that $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) \to 1$ as $\rho \to 0$. Further, using the expression for $\frac{\partial \sigma_L^\star}{\partial \rho}$ from (3) this implies that $\frac{\partial \sigma_L^\star}{\partial \rho} \to \frac{\partial \Pi_L}{\partial \rho} > 0$ as $\rho \to 0$. Therefore, by continuity and the fact that in equilibrium $\frac{\partial \sigma_L^\star}{\partial \rho} = \frac{d\Pi_L^\star}{d\rho}$, then there must exist a threshold $\underline{\rho}_L$ such that $\frac{d\Pi_L^\star}{d\rho} > 0$ for all $\rho \in [0, \underline{\rho}_L]$.

In order to prove Result 2, we use the fact stated above that $\frac{\partial \sigma_S^\star}{\partial \rho}(\rho) < 0$ combined with the fact that $\lim_{\rho\to+\infty}\Pi_S(\rho) = 0$, for all thresholds (σ_S, σ_L). Therefore, there must exist $\overline{\rho}$ such that $\sigma_S^\star = \underline{\sigma}$ whenever $\rho \geqslant \overline{\rho}$ and $\sigma_S^\star \to \underline{\sigma}$ as $\rho \to \overline{\rho}$. Next, we use the fact that as $\rho \to \overline{\rho}$ then $\sigma_S^\star \to \underline{\sigma}$ implies that $\overline{\tau} \to \overline{\tau}_L$. Therefore, this implies that $\frac{\partial \Pi_L}{\partial \rho} \to 0$ as $\rho \to \overline{\rho}$. Finally, we note that $\frac{\partial \Pi_L}{\partial \sigma_S} \to C > 0$ and $\frac{\partial \Pi_S}{\partial \rho} \to C' < 0$ as $\rho \to \overline{\rho}$ for some constants $C > 0$ and $C' < 0$. Therefore $\frac{\partial \sigma_L}{\partial \rho} \to C'' < 0$ as $\rho \to \overline{\rho}$ and thus by continuity there must exist $\overline{\rho}_L < \overline{\rho}$ such that $\frac{d\Pi_L^\star}{d\rho} < 0$ for all $\rho \in [\overline{\rho}_L, \overline{\rho}]$.

Finally, note that if it were the case that $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) < 0$, then we would obtain the opposite results. This would imply that $\sigma_S^\star$ is strictly increasing in ρ and $\sigma_L^\star$ is strictly decreasing

[4] Note that $\lim_{\theta_S\to 1}\frac{\partial \Pi_S}{\partial \sigma_S} = 0$ then implies that there exists $\overline{\theta}_S$ such that $\theta_S > \overline{\theta}_S$ ensures that $J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)$ is invertible.

in ρ for $\rho \in [0, \underline{\rho}_L)$. Yet, we know that $\Pi_L(\rho) \geqslant 1$ and $\Pi_L(0) = 1$, independent of the thresholds σ_S and σ_L. Therefore, it can only be the case that $\sigma^\star_L(\rho) = 1$ for all $\rho \in [0, \underline{\rho}_L)$ contradicting the fact that $\sigma^\star_L$ is strictly decreasing for $\rho \in [0, \underline{\rho}_L)$. Similarly, if both $\sigma^\star_L$ and $\sigma^\star_S$ were strictly increasing for $\rho \in [\overline{\rho}_L, \overline{\rho}]$ then it would imply that $\overline{\rho} = +\infty$ as $\overline{\rho}$ is defined as the largest possible growth rate that supports adoption by both types. Yet, we know that $\Pi_S(\rho) \to 0$ as $\rho \to +\infty$ for any levels of σ_S and σ_L which presents another contradiction as we assume $\underline{\sigma} > 0$. Therefore, it is without loss to assume that in equilibrium $det(J_{f,\boldsymbol{\sigma}}(\boldsymbol{\sigma}_0, \rho_0)) > 0$. $\square$

A.5 Proof of Proposition 4.4

Proof. First, note that we derive the expression for $\tilde{\Pi}_L$ by using the fact that $\pi_L(\rho) = 1 - \pi_S(\rho)$ and therefore $\overline{\tau} = \pi_S(\rho) \cdot (\overline{\tau}_S - \overline{\tau}_L) + \overline{\tau}_L$.

1.) In the proof of Proposition 4.3 we have shown that

$$\frac{\partial \tilde{\Pi}_L}{\partial \rho} = \frac{(\overline{\tau} - 1) \cdot \theta_L e^{-\rho}}{\eta_L^2} \cdot (1 - \theta_L \cdot \overline{\tau})$$

where $\eta_L = (1 - \theta_j) \cdot e^{-\rho} + (\theta_j \cdot \overline{\tau} - 1)$. Thus, using the fact that $\theta_L \cdot \overline{\tau} < 1$, whenever $\rho < \overline{\rho}$ we can see that $\frac{\partial \tilde{\Pi}_L}{\partial \rho} > 0$.

2.) We directly differentiate $\tilde{\Pi}_L$ to obtain

$$\frac{\partial \tilde{\Pi}_L}{\partial \pi_S} = \frac{\theta_L \cdot (1 - \theta_L) \cdot e^{\rho} \cdot (1 - e^{-\rho})}{\eta_L^2} \cdot (\overline{\tau}_L - \overline{\tau}_S)$$

which using the fact that $(\overline{\tau}_L - \overline{\tau}_S) > 0$ implies $\frac{\partial \tilde{\Pi}_L}{\partial \pi_S} > 0$.

3.) Directly differentiating $\pi_S(\rho)$ and rearranging we obtain

$$\frac{d\pi_S(\rho)}{d\rho} = p_s G'(\sigma^\star_S) \frac{\partial \sigma^\star_S}{\partial \rho} \cdot \pi_L(\rho) - p_L G'(\sigma^\star_L) \frac{\partial \sigma^\star_L}{\partial \rho} \cdot \pi_S(\rho)$$

We know that $\frac{\partial \sigma^\star_S}{\partial \rho} < 0$ for all ρ. Therefore, whenever $\frac{\partial \sigma^\star_L}{\partial \rho} > 0$, then this result holds. We have shown in the proof of Proposition 4.3 that there exists $\underline{\rho}_L$ such that $\frac{\partial \sigma^\star_L}{\partial \rho} > 0$ whenever $\rho < \underline{\rho}_L$ which establishes the first result.

To show that $\frac{d\pi_S}{d\rho}(\rho) < 0$ for sufficiently high ρ, we note we have shown in the proof of Proposition 4.3 that $\frac{\partial \sigma_S^\star}{\partial \rho}(\rho) < 0$ for all ρ. Further, noting that

$$\frac{\partial \sigma_S^\star}{\partial \rho}(\overline{\rho}) = \frac{1}{1 - \frac{\partial \Pi_S}{\partial \sigma_S}(\overline{\rho})} \cdot \frac{(\tau_L - 1) \cdot \theta_S \cdot e^{-\rho}}{\eta_S^2} \cdot (1 - \frac{\theta_S}{\theta_L}) < 0$$

then using the fact that $\overline{\rho} < \infty$, $\frac{\partial \Pi_S}{\partial \sigma_S}(\overline{\rho}) < 1$, and $\frac{\theta_S}{\theta_L} > 1$ implies that $\frac{\partial \sigma_S^\star(\rho)}{\partial \rho}(\overline{\rho}) < C < 0$ for some constant $C < 0$. Finally, note that as $\rho \to \overline{\rho}$ then $\pi_S(\rho) \to 0$ due to the fact that $\sigma_S^\star \to \underline{\sigma}$ as $\rho \to \overline{\rho}$. Hence, as $\rho \to \overline{\rho}$ it must be the case that

$$\frac{d\pi_S}{d\rho} \to p_s G'(\sigma_S^\star) \frac{\partial \sigma_S^\star}{\partial \rho} \cdot \pi_L(\overline{\rho}) < 0$$

and therefore by continuity there must exist $\overline{\rho}_L < \overline{\rho}$ such that $\rho \in (\overline{\rho}_L, \overline{\rho}]$ implies $\frac{d\pi_S}{d\rho}(\rho) < 0$. □

A.6 Proof of Proposition 4.5

Proof. This result was directly proven in the proof of Proposition 4.3. □

A.7 Proof of Proposition 4.6

Proof. In order to prove this result we will directly differentiate $\mathcal{S}$ with respect to ρ to obtain

$$\frac{d\mathcal{S}}{d\rho} = (\overline{\tau} - 1) \cdot (p_S \cdot G'(\sigma_S) \frac{\partial \sigma_S}{\partial \rho} + p_L \cdot G'(\sigma_L) \frac{\partial \sigma_L}{\partial \rho}) + (p_S \cdot G(\sigma_S) + p_L \cdot G(\sigma_L)) \cdot (\frac{\partial \overline{\tau}}{\partial \sigma_S} \cdot \frac{\partial \sigma_S}{\partial \rho} + \frac{\partial \overline{\tau}}{\partial \sigma_L} \cdot \frac{\partial \sigma_L}{\partial \rho})$$

In order to prove 1.) we will first show that

$$p_S \cdot G'(\sigma_S^\star) \frac{\partial \sigma_S^\star}{\partial \rho} + p_L \cdot G'(\sigma_L^\star) \frac{\partial \sigma_L^\star}{\partial \rho} \to 0$$

as $\rho \to 0$. In order to show this, recall that it was shown in the proof of Proposition 4.3 that $\frac{\partial \sigma_L^\star}{\partial \rho} \to \frac{\partial \Pi_L}{\partial \rho}$ as $\rho \to 0$. We can show in an identical fashion that $\frac{\partial \sigma_S^\star}{\partial \rho} \to \frac{\partial \Pi_S}{\partial \rho}$ as $\rho \to 0$. Further,

$$\frac{\partial \Pi_S}{\partial \rho}(0) = \frac{(1 - \theta_S \cdot \overline{\tau})}{\theta_S(\overline{\tau} - 1)} \qquad \text{and} \qquad \frac{\partial \Pi_L}{\partial \rho}(0) = \frac{(1 - \theta_L \cdot \overline{\tau})}{\theta_L(\overline{\tau} - 1)}$$

Next, note that inspection of (14) implies that $\Pi_S(0) = 1 = \Pi_L(0)$ and therefore $\sigma_L^\star(0) = \sigma_H^\star(0) = 1$.

Therefore,

$$(p_S \cdot G'(\sigma_S^\star)\frac{\partial \sigma_S^\star}{\partial \rho} + p_L \cdot G'(\sigma_L^\star)\frac{\partial \sigma_L^\star}{\partial \rho})\Big|_{\rho=0} = \frac{G'(1)}{\overline{\tau}(0)-1} \cdot (\frac{p_S}{\theta_S}(1-\theta_S \cdot \overline{\tau}(0)) + \frac{p_L}{\theta_L}(1-\theta_L \cdot \overline{\tau}(0)))$$

Finally, substituting for $\overline{\tau}(0) = \frac{p_S}{\theta_S} + \frac{p_L}{\theta_L}$ we can see that

$$(p_S \cdot G'(\sigma_S^\star)\frac{\partial \sigma_S^\star}{\partial \rho} + p_L \cdot G'(\sigma_L^\star)\frac{\partial \sigma_L^\star}{\partial \rho})\Big|_{\rho=0} = 0$$

Now, in order to prove the main claim, we note that it was proven in Proposition 4.3 that $\frac{\partial \overline{\tau}}{\partial \sigma_L} > 0$ (provided that $\sigma_L > \underline{\sigma}$), $\frac{\partial \overline{\tau}}{\partial \sigma_S} < 0$, $\frac{\partial \sigma_S^\star}{\partial \rho} < 0$ for all ρ, and $\frac{\partial \sigma_L^\star}{\partial \rho} > 0$ for $\rho < \underline{\rho}_L$. Therefore, whenever $\rho < \underline{\rho}_L$ it must be the case that

$$(\frac{\partial \overline{\tau}}{\partial \sigma_S} \cdot \frac{\partial \sigma_S^\star}{\partial \rho} + \frac{\partial \overline{\tau}}{\partial \sigma_L} \cdot \frac{\partial \sigma_L^\star}{\partial \rho})\Big|_{\rho=0} > 0$$

and therefore, given that the first term of $\frac{d\mathcal{S}}{d\rho}$ goes to zero as $\rho \to 0$ implies that there exists $\underline{\rho}_{\mathcal{S}} > 0$ such that $\rho < \underline{\rho}_{\mathcal{S}}$ implies $\frac{d\mathcal{S}}{d\rho} > 0$.

We prove the second claim in a similar fashion. Namely, we note that whenever $\rho \in [\overline{\rho}_L, \overline{\rho}]$, then $\frac{\partial \sigma_L^\star}{\partial \rho} < 0$. Therefore, whenever $\rho > \overline{\rho}_L$ the only positive term in $\frac{d\mathcal{S}}{d\rho}$ is

$$(p_S \cdot G(\sigma_S) + p_L \cdot G(\sigma_L)) \cdot (\frac{\partial \overline{\tau}}{\partial \sigma_S} \cdot \frac{\partial \sigma_S}{\partial \rho})$$

we will conclude the proof by showing that

$$[(\overline{\tau}-1) \cdot (p_S \cdot G'(\sigma_S^\star)\frac{\partial \sigma_S^\star}{\partial \rho}) + (p_S \cdot G(\sigma_S^\star) + p_L \cdot G(\sigma_L^\star)) \cdot (\frac{\partial \overline{\tau}}{\partial \sigma_S} \cdot \frac{\partial \sigma_S^\star}{\partial \rho})]\Big|_{\rho=\overline{\rho}} < 0 \tag{4}$$

Then, given that the remaining terms in $\frac{d\mathcal{S}}{d\rho}$ are negative implies, by continuity, that there exists a threshold $\overline{\rho}_{\mathcal{S}} < \overline{\rho}$ such that $\frac{d\mathcal{S}}{d\rho} < 0$ whenever $\rho > \overline{\rho}_{\mathcal{S}}$.

In order to prove that (4) holds, we note that $\sigma_S^\star(\overline{\rho}) = \underline{\sigma}$ and therefore $G(\sigma_S(\overline{\rho})) = 0$. Thus, after substituting for $\frac{\partial \overline{\tau}}{\partial \sigma_S}$ from (2) and rearranging, the left hand side of (4) is equal to

$$\frac{\partial \sigma_S^\star}{\partial \rho} \cdot p_S \cdot G'(\underline{\sigma}) \cdot (\overline{\tau}(\overline{\rho}) - 1 + \overline{\tau}_S - \overline{\tau}_L)$$

Hence, given that $\frac{\partial \sigma_S^\star}{\partial \rho} < 0$ for all ρ, then (4) holds so long as $\overline{\tau}(\overline{\rho}) - 1 + \overline{\tau}_S - \overline{\tau}_L > 0$. Yet, we know that $\overline{\tau}(\overline{\rho}) = \overline{\tau}_L$ and therefore $[\overline{\tau}(\overline{\rho}) - 1 + \overline{\tau}_S - \overline{\tau}_L]\big|_{\rho=\overline{\rho}} = \overline{\tau}_S - 1 > 0$. Thus, we have proven that $\frac{d\mathcal{S}}{d\rho}|_{\rho=\overline{\rho}} < 0$ and therefore by continuity there must exist a threshold $\overline{\rho}_{\mathcal{S}} < \overline{\rho}$ such that $\frac{d\mathcal{S}}{d\rho} < 0$ for all $\rho \in (\overline{\rho}_{\mathcal{S}}, \overline{\rho}]$. □

A.8 Proof of Proposition 4.7

Proof. In order to prove the first result, note that

$$\frac{d}{d\rho}[\mathcal{D}_S + \mathcal{D}_L] = p_S \cdot G'(\sigma_S^\star)\frac{\partial \sigma_S^\star}{\partial \rho} + p_L \cdot G'(\sigma_L^\star)\frac{\partial \sigma_L^\star}{\partial \rho}$$

Further, we have shown in the proof of Proposition 4.6 that this term goes to zero as $\rho \to 0$ and therefore our stated result must be true by continuity.

To prove the second result, note that

$$\frac{d\overline{\tau}}{d\rho} = \frac{\partial \overline{\tau}}{\partial \sigma_S} \cdot \frac{\partial \sigma_S^\star}{\partial \rho} + \frac{\partial \overline{\tau}}{\partial \sigma_L} \cdot \frac{\partial \sigma_L^\star}{\partial \rho}$$

Further, we have shown in the proof of Proposition 4.3 that $\frac{\partial \sigma_S}{\partial \rho} < 0$ for all $\rho \in [0, \overline{\rho}]$ and $\frac{\partial \sigma_L}{\partial \rho} > 0$ whenever $\rho < \underline{\rho}_L$. Finally, (2) tell us that $\frac{\partial \overline{\tau}}{\partial \sigma_S} < 0$ and $\frac{\partial \overline{\tau}}{\partial \sigma_L} > 0$ and therefore whenever $\rho < \underline{\rho}_L$ it must be the case that $\frac{d\overline{\tau}}{d\rho} > 0$. □

A.9 Proof of Proposition 4.8

Proof. In order to prove the first result, we note that

$$\frac{d}{d\rho}[\mathcal{D}_S + \mathcal{D}_L] = p_S \cdot G'(\sigma_S^\star)\frac{\partial \sigma_S^\star}{\partial \rho} + p_L \cdot G'(\sigma_L^\star)\frac{\partial \sigma_L^\star}{\partial \rho}$$

Therefore, as was shown in the proof of Proposition 4.3 we know that there exists $\overline{\rho}_L < \overline{\rho}$ such that $\rho > \overline{\rho}_L$ implies $\frac{\partial \sigma_L^\star}{\partial \rho} < 0$ while it is always the case that $\frac{\partial \sigma_S^\star}{\partial \rho} < 0$. Hence, whenever $\rho > \overline{\rho}_L$ it must be the case that $\frac{d}{d\rho}[\mathcal{D}_S + \mathcal{D}_L] < 0$.

The second result is a direct corollary of Proposition 4.6 as this is precisely the condition required for $\frac{d\mathcal{S}}{d\rho} < 0$. □

A.10 Proof of Proposition 4.9

Proof. We will prove this by showing that $\mathcal{S}(\overline{\rho}) < \mathcal{S}(0)$. Therefore, given that $\mathcal{S}(\rho)$ is decreasing for all $\rho \in [\overline{\rho}_{\mathcal{S}}, \overline{\rho}]$ and fixed when $\rho > \overline{\rho}$ it must imply by continuity that there exists $\overline{\rho}_0 < \overline{\rho}$ such that $\mathcal{S}(\rho) < \mathcal{S}(0)$ for all $\rho > \overline{\rho}_0$.

In order to show that $\mathcal{S}(\overline{\rho}) < \mathcal{S}(0)$ we note that $\sigma_S^\star(0) = \sigma_L^\star(0) = 1$ while $\sigma_S^\star(\overline{\rho}) = \underline{\sigma}$. Therefore $\mathcal{S}(\overline{\rho}) < \mathcal{S}(0)$ if and only if

$$(\overline{\tau}(\overline{\rho}) - 1) \cdot p_L \cdot G(1) < (\overline{\tau}(0) - 1) \cdot G(1)$$

Therefore, noting that

$$\overline{\tau}(0) = \frac{p_S}{\theta_S} + \frac{p_L}{\theta_L} \quad \text{and} \quad \overline{\tau}(\overline{\rho}) = \frac{1}{\theta_L}$$

then after plugging in and rearranging, we can see that $\mathcal{S}(\overline{\rho}) < \mathcal{S}(0)$ if and only if

$$\frac{p_L}{\theta_L} - p_L < \frac{p_S}{\theta_S} + \frac{p_L}{\theta_L} - 1$$

which after substituting $p_L = 1 - p_S$ we can see holds whenever $\frac{p_S}{\theta_S} > p_S$ which is always the case given that $\theta_S \in (0, 1)$. $\square$

A.11 Proof of Proposition 4.10 and Proposition 4.11

Proposition 4.11 can be shown to hold by direct inspection of the payoff functions in (14). In particular, when $\theta_S = \theta_L = \theta$ then we know that $\overline{\tau} = \frac{1}{\theta}$ therefore

$$\Pi_S = \Pi_L = \frac{(\tau - 1)\theta \cdot e^{-\rho}}{(1 - \theta)e^{-\rho} + \theta \cdot \tau - 1} = 1$$

Further, given that Proposition 4.11 holds for all adoption thresholds σ_S and σ_L we know that this must imply that block rewards have no effect on the equilibrium cut-offs $\sigma_S^\star = \sigma_L^\star = 1$.