Economic Implications of Scaling Blockchains: Why the Consensus Protocol Matters[*]

Kose John[†] Thomas Rivera[‡] Fahad Saleh[§]

May 21, 2021

Abstract

This paper examines the economic implications of scaling blockchains under two different consensus protocols: Proof-of-Work (PoW) and Proof-of-Stake (PoS). We study an economic model whereby agents can store wealth through the blockchain's cryptocurrency but may face a costly delay when liquidating due to the blockchain's finite transaction rate. Agents may expedite processing by paying fees to the blockchain's validators. Within such a model, we study the ability of a malicious agent to compromise the security of the blockchain. We show how improved scaling alleviates congestion, leading to a decrease in equilibrium fees. Under a PoW protocol, this leads validators to earn less revenue and thus spend less on computational power, lowering the cost of a successful attack and therefore the security of the PoW blockchain. Scaling has the opposite effect for the PoS protocol as alleviating congestion increases the demand and therefore the market value of the blockchain's cryptocurrency. That increased market value increases the cost of acquiring enough cryptocurrency necessary for a successful attack and thereby improves PoS blockchain security.

Keywords: Blockchain, Proof-of-Stake, Proof-of-Work, Scale, Security, Fees

JEL Classification: G0, O3

[*] We thank Matthieu Bouvard, Kai-Lung Hui, Urban Jermann, Baixiao Liu, Andreas Park, Julien Prat, Quentin Vandeweyer, Ganesh Viswanath-Natraj and seminar participants at UPenn Wharton, and the Virtual Finance Theory Seminar for valuable comments.

[†] 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

The viability of a widely utilized blockchain technology depends crucially on security and scalability. In this paper, we study the role that the consensus protocol of the blockchain plays in determining the relationship between those two features. We demonstrate that improving the scale (i.e., transaction rate) of a blockchain has a qualitatively different effect on its security depending on whether the consensus protocol is Proof-of-Work (PoW) or Proof-of-Stake (PoS).[1] For a PoW blockchain, improving the transaction rate has the perverse effect of undermining security to the point where an arbitrarily small amount of resources would be sufficient to successfully attack the blockchain. In contrast, for a PoS blockchain, improving the transaction rate enhances security and can render any attack that utilizes a plausible level of resources certain to fail.

We establish our results theoretically via an economic model centered around a single blockchain which is either of type PoW or PoS. We consider an overlapping generations model whereby agents can choose to store their wealth on the blockchain or through an alternative technology. We assume that this alternative technology leads to a depreciation in wealth such as might be experienced by an inflationary fiat currency. On the other hand, storing wealth on the blockchain entails buying cryptocurrency units, also known as *coins*, which are traded and settled on the blockchain. When an agent needs to consume, she sells her cryptocurrency holdings but may incur a delay in her transaction due to congestion on the blockchain. The need to wait arises because the blockchain possesses a finite transaction capacity which implies that all transactions cannot be processed instantaneously. Agents face heterogeneous costs of waiting and, as in practice, can pay competitive fees to have their transaction prioritized since the blockchain endogenously accepts transactions in descending fee order.

To study security, we assume that the blockchain is subject to an attack in each period arising from a malicious agent, hereafter referred to as an attacker. The attacker is deep pocketed and receives an ex-ante random benefit each period from successfully disrupting the transaction activity of the blockchain in that period. In each period the attacker learns the realized benefit she receives from executing a successful attack. In turn, that benefit determines her maximum willingness to pay to perform the attack conditional on the probability that it is successful which depends upon

[1] Irresberger et al. (2020) document that PoW and PoS are the two most widely employed consensus protocols for blockchain.

the equilibrium properties of the blockchain's security. We assume the success of the attacker in any period renders the blockchain inoperable thereafter. Therefore, any user with a cryptocurrency holding at the time of a successful attack loses the ability to liquidate her holdings and hence forgoes any associated consumption utility. Accordingly, the decision to adopt the blockchain depends on the cost of waiting and paying fees, along with the probability that the blockchain is compromised by an attack.

Successfully attacking the blockchain requires the attacker to gain *control* of the blockchain in any given period. Controlling the blockchain requires the ability to add blocks to the blockchain with a sufficient frequency so that the attacker can create a disruptive chain that becomes arbitrarily longer than the main chain. PoW and PoS differ primarily in the conditions that enable an attacker to mount such an attack. In particular, the PoW protocol allocates the right to add a block to the blockchain to any agent who solves a computationally expensive puzzle. Agents who attempt to solve this puzzle are known as *miners* and their attempts to solve the puzzle are known as *mining*. In contrast, the PoS protocol allocates the right to add a block to the blockchain based on a lottery among a set of cryptocurrency holders who agree not to sell their cryptocurrencies in a given period. The agents who partake in this activity are known as *stakers* and the act of holding cryptocurrencies dormant to be eligible for the lottery is known as *staking*. The probability of any agent winning the lottery is equal to the proportion of the coins they stake in the pool of coins that are held dormant (i.e. staked) by all agents in that period.

The PoW governance structure implies that the attacker can gain control of the PoW blockchain if she possesses at least as much computational power than the sum of all other miners (see Nakamoto 2008). In contrast, the PoS governance structure implies that the attacker can gain control of the PoS blockchain only if she possesses at least as many coins than the other stakers (see Saleh 2021). Our analysis of security for PoW and PoS blockchains relies on endogenously deriving the computational power spent in mining and the coins used for staking in equilibrium.

As is the case in practice, the reward for validating transactions includes the fees that agents pay to receive priority along with *block rewards* which are newly issued coins given to validators as a reward for adding blocks to the blockchain. We first study the case whereby the cryptocurrency supply is constant so that there are no block rewards. In this context, Proposition 4.1 establishes that PoW blockchains become *fully insecure* for a sufficiently high transaction rate. What this implies is that for a sufficiently high transaction rate the attacker succeeds in her first attack with certainty so that the blockchain has no hope of facilitating any transaction activity. In contrast, Proposition 4.2 establishes that PoS attains full security for a sufficiently high transaction rate. This implies that, for a sufficiently high transaction rate, the attacker never succeeds in any attack on the PoS blockchain. Consequently, an agent with a cryptocurrency holding may always freely liquidate and therefore faces no security risk in equilibrium.

The aforementioned results rely on the fact that an increase in the blockchain's transaction rate reduces the equilibrium fees paid by the agents. This intermediate finding is important because, in the absence of block rewards, user fees alone finance the computational power of miners under the PoW protocol. Consequently, a reduction in fees corresponds to a reduction in computational power expended by miners which lowers the cost of executing a successful attack and thereby reduces the security of a PoW blockchain. As discussed, PoS blockchains are not secured by computational power and thus are immune to this effect. However, the described reduction in fees is not irrelevant for PoS blockchain security because reduced fees lead to an increase in the market value of the PoS blockchain's coin. Namely, a higher transaction rate generates lower fees which makes using the blockchain more attractive relative to the alternative technology, thereby increasing the demand for the blockchain's cryptocurrency and thus the cryptocurrency's equilibrium market value. Therefore, a decrease in fees increases the financial cost necessary for the attacker to successfully attack the PoS blockchain as doing so requires purchasing sufficiently many coins.

To clarify why fees decline as the blockchain's transaction rate increases, recall that fees are a choice variable for users and that the blockchain accepts transactions in descending fee order. A user's priority depends only on how her fee relates to all other users' fees; the highest fee user receives first priority followed by the next highest, etc. Therefore, a user may gain priority over some number of other users by paying an incremental fee, but the wait time reduction from paying that incremental fee depends not only on the referenced number of other users but also on the blockchain's transaction rate. As the blockchain transaction rate increases, the wait time reduction experienced by the user decreases which implies that her incentive to pay the incremental fee also decreases. As an example, in the extreme case that the blockchain processes transactions at an infinite rate, all transactions receive immediate processing so that the incentive to pay any fee is entirely absent and equilibrium fees are identically zero. More generally, fees decline as the blockchain transaction rate increases and vanish entirely as the blockchain transaction rate diverges.

Our first main result, Proposition 4.1, establishes that a sufficiently high blockchain transaction rate renders a PoW blockchain entirely insecure. More precisely, as discussed, when there are no block rewards, miners finance their computational expenditures entirely from user fees, which are paid to miners to include the associated transactions in blocks on the blockchain. Thus, an increase in the blockchain's transaction rate reduces not only user fees but also the total computational expenditure of a PoW blockchain. In turn, the reduced computational expenditure lowers the cost of successfully attacking the blockchain and therefore increases the probability that the attack is profitable for the attacker, and therefore successfully executed. Moreover, a sufficiently high transaction rate renders a PoW blockchain entirely insecure because computational expenditure falls to such an extent that all agents prefer the alternative technology in lieu of facing the high probability of a successful attack on the blockchain. Then, if no agents employ the blockchain, the blockchain generates zero fee revenue and is secured by zero computational power, which implies that the attacker will always execute a successful attack in her first attempt. Consequently, per Proposition 4.1, the PoW blockchain becomes fully insecure for a sufficiently high transaction rate.

Our second main result, Proposition 4.2, establishes that a sufficiently high blockchain transaction rate renders a PoS blockchain fully secure. PoS blockchains are secured by the financial cost associated with acquiring sufficiently many coins. In turn, the cost of acquiring sufficiently many coins is proportional to the market value of the cryptocurrency and that market value increases with demand for using the blockchain. Further, the demand for using the blockchain increases with the transaction rate because a higher transaction rate implies faster service at a lower fee expense and thereby improves the incentive to use the blockchain relative to the alternative technology. For a sufficiently high transaction rate, the cryptocurrency demand becomes so large that successfully attacking the blockchain becomes too costly and therfore the attacker never finds it profitable to mount such an attack.[2] Accordingly, per Proposition 4.2, a sufficiently high transaction rate induces full security for a PoS blockchain.

In a standard finance context, our finding regarding the relationship between the blockchain's transaction rate and PoS blockchain security is straight-forward if we view a PoS coin as analogous

[2] Namely, we show that the benefit of a successful attack would have to be greater than the total amount of resources endowed to the agents in the economy in order for an attack to be profitable when the transaction rate is sufficiently large.

to a share of an all-equity firm. Within the context of that analogy, an attack on the blockchain is comparable to a hostile take-over attempt by an outside investor. If the outside investor gains a sufficiently large position in the all-equity firm's shares then she gains control of the firm and the take-over succeeds. Similarly, if the blockchain attacker gains a sufficiently large proportion of the blockchain's coins then the attacker gains control of the PoS blockchain's block creation process and the blockchain attack succeeds. In the hostile take-over example, the difficulty of executing the attack arises from the fact that attempting a take-over of a firm with a large market value involves significant financing costs to purchase a sufficient share of the firm's equity. Analogously, the difficulty of executing the attack on the blockchain arises from the fact that successfully attacking a blockchain with a large cryptocurrency market value involves significant financial costs to purchase a sufficient share of the cryptocurrency. More subtly, the market values of the all-equity firm and the cryptocurrency are themselves endogenous quantities that depend on the quality of the underlying enterprise. In the case of an all-equity firm, a firm that is already governed well would have a higher market value and therefore would be more difficult to take over. In this sense, a well-governed all-equity firm is analogous to a high scale blockchain. This analogy holds because a high scale blockchain implies timely service at low fee costs for users which, in turn, implies higher demand for using the blockchain and thus a higher cryptocurrency market value. Accordingly, just as a larger and better governed firm is less prone to a hostile take-over, a high scale PoS blockchain is similarly less susceptible to a blockchain attack.

As an extension to our main results, we consider the case with positive block rewards whereby the cryptocurrency supply grows at an exogenous rate. As in practice, we assume that the new cryptocurrency units are allocated to validators. Proposition 4.4 generalizes our results for the PoS blockchain to this case and establishes the same result — a sufficiently high blockchain transaction rate induces full security in the PoS blockchain. On the other hand, we show how PoW blockchains with block rewards can generate *some* level of security in that the blockchain is not successfully attacked in each period with certainty. Nonetheless, Proposition 4.3 establishes that for a sufficiently large transaction rate, the blockchain's security level is bounded away from full security so that with probability one the attacker will eventually execute a successful attack, thereby rendering the blockchain inoperable in perpetuity eventually.

Our paper relates to a large literature that studies the economics of blockchain. Akin to Carlsten et al. (2016), Biais et al. (2019), Chiu and Koeppl (2019), Easley et al. (2019), Ebrahimi et al. (2019), Huberman et al. (2019), Prat and Walter (2019), Alsabah and Capponi (2020), Cong et al. (2020), Garratt and van Oordt (2020), Hinzen et al. (2020), Lehar and Parlour (2020), Mueller (2020) and Pagnotta (2020), our work provides insights regarding PoW blockchains. Akin to Fanti et al. (2019), Rosu and Saleh (2021) and Saleh (2021), we also provide insights regarding PoS blockchains. Unlike the aforementioned papers, we examine the economic implications of scaling blockchains and we are the first to provide a comparative analysis on that dimension across the two most prominent blockchain protocols.

2 Model

We model an infinite horizon, discrete-time setting with periods $t \in \mathbb{N}$. The economy is populated by overlapping generations of agents and only one asset, a cryptocurrency, which is settled on a payment system known as a blockchain. Each agent possesses a unit endowment (i.e., savings) only in her first period and incurs utility (i.e., consumption) only in her last period. Each agent has access to an alternative technology that enables her to transfer her endowment from her first to her last period with some spoilage (e.g., inflation). Alternatively, the agent may trade her endowment for the cryptocurrency during her first date and trade her cryptocurrency holdings for consumption goods during her last date. Buying or selling the cryptocurrency requires transacting on the blockchain which faces particular security risks depending on whether the underlying protocol is PoW or PoS.

2.1 Users

Each period t begins with a unit measure of generation-t agents being born. We refer to each individual agent from generation t as Agent (i, t) with $i \in [0, 1]$ denoting the unique identifier for that agent within the generation. Agent (i, t) lives for three periods $t, t + 1, t + 2$. She is endowed with one unit of consumption goods only in her first period, t, and accrues utility only in the terminal period of her life, $t + 2$. Agent (i, t) has access to an alternative technology that enables her to transfer a fraction $\sigma \in (0, 1)$ of her consumption goods two periods ahead for consumption at time $t + 2$. Alternatively, Agent (i, t) may use the blockchain, trading her endowment for units of cryptocurrency during period t and then selling those units of cryptocurrency and any associated proceeds for consumption goods in period $t+2$. We refer to agents that utilize the blockchain as *users* and say that the agent *adopts* the blockchain technology when she utilizes the blockchain over the alternative technology to store her endowment.

We denote Agent (i,t)'s utility as $\mathcal{U}^{p}_{(i,t)}$ with $p \in \{PoW, PoS\}$ denoting the blockchain's protocol. Following the prior discussion, Agent (i,t)'s utility is given by:

$$\mathcal{U}^{p}_{(i,t)} = \max\{U^{p}_{(i,t)}, \sigma\} \tag{1}$$

with $U^{p}_{(i,t)}$ denoting the expected utility of Agent (i,t) if she adopts the blockchain.

The decision to adopt the blockchain technology involves two important concerns. First, the blockchain may be successfully attacked, thereby invalidating user transactions and leaving Agent (i,t) with zero consumption in period $t+2$. We discuss this concern in detail in Section 2.3. Second, even if the blockchain is not successfully attacked, Agent (i,t) may not receive immediate processing because the blockchain possesses a finite transaction rate. We assume that Agent (i,t) possesses utility over period $t+2$ consumption and an intraperiod wait disutility during that period. Further, as in practice, Agent (i,t) may pay a fee, $f^{p}_{(i,t)} \geqslant 0$, denominated in the consumption good, to reduce her wait time because the blockchain processes transactions in descending fee order. Denote by $W^{p}(f, f_{-(i,t)})$ the expected wait time of Agent (i,t) when she pays fee f and the other users pay fees $f_{-(i,t)}$, formally derived below, and denote by $c_{(i,t)}$ Agent (i,t)'s wait disutility per unit time. Then, Agent (i,t)'s total disutility from waiting equals $c_{(i,t)} \cdot W^{p}(f, f_{-(i,t)})$. We assume that $c_{(i,t)}$ is private information of Agent (i,t) and drawn from a smooth cumulative distribution, $G \in \mathcal{C}^{\infty}[0,\infty)$, with a non-negative support and a finite first moment (i.e., $\int\limits_{0}^{\infty} c \; dG(c) < \infty$).

If Agent (i,t) does not use the blockchain then she optimally pays fee $f^{p}_{(i,t)} = 0$; otherwise, she selects her fee to maximize time $t+2$ consumption net the fee and total wait disutility which amounts to choosing $f^{p}_{(i,t)}$ to solve:

$$f^{p}_{(i,t)} = \underset{f:\ f \geqslant 0}{\arg\max} \ \underbrace{P^{p}_{t+2} Q^{p}_{(i,t),t+1} - f}_{Consumption} - \underbrace{c_{(i,t)} W^{p}(f, f_{-(i,t)})}_{Wait\ Disutility} \tag{2}$$

where for any protocol $p \in \{PoW, PoS\}$, P^{p}_{t+2} denotes the cryptocurrency price in period $t+$

2 (denominated in consumption goods) and $Q^p_{(i,t),s}$ denotes Agent (i,t)'s end of period $s \geqslant t$ cryptocurrency holding. Note that $f^p_{(i,t)}$ is a function of Agent (i,t)'s wait disutility $c_{(i,t)}$ and the beliefs Agent (i,t) has regarding the fees $f^p_{-(i,t)}$ chosen by the other agents; in what follows we do not explicitly reference this dependence in order to ease the notation.

Let $\pi^p_{t\to t+2} \in [0,1]$ denote the probability that the blockchain survives until period $t+2$ conditional upon surviving until period t. Then, the expected utility of Agent (i,t) from using the blockchain — i.e., purchasing cryptocurrency units in period t and paying fee $f^p_{(i,t)}$ in period $t+2$ — is given by:

$$U^p_{(i,t)} = \pi^p_{t\to t+2} \cdot \mathbb{E}_t[P^p_{t+2} Q^p_{(i,t),t+1} - f^p_{(i,t)} - c_{(i,t)} W^p(f^p_{(i,t)}, f_{-(i,t)}) \mid c_{(i,t)}] \tag{3}$$

if the blockchain survives until period t and $U^p_{(i,t)} = 0$ otherwise. We use $\mathbb{E}_t[\cdot]$ to denote an expectation conditional on all public information available at the beginning of period t. Note that the budget constraint of Agent (i,t) is represented by $P^p_t \cdot Q^p_{(i,t),t} \leqslant 1$ which states the cost of the cryptocurrency that they purchase cannot exceed their initial endowment. We proceed by restricting to the case whereby agents store all of their wealth either on the blockchain (full adoption) or through the storage technology (no adoption). This assumption is without loss of generality as partial adoption — storing a fraction of wealth on the blockchain and a fraction through the storage technology — is never optimal.

2.2 Blockchain

A blockchain is an electronic ledger that records payments in discrete chunks referred to as *blocks*. The blocks are concatenated together into a single *chain*, hence the term blockchain. For the blockchain to function, there must be some agents that create the blocks because transactions enter the blockchain only by being recorded on blocks that are added to the chain. We let $\Lambda > 0$ denote the blockchain's transaction rate which is the rate at which the blockchain accepts transactions. In order to avoid unnecessary complications, we assume that block sizes are *small* in the sense that transaction's are continuously accepted to the blockchain in infinitesimally small blocks.[3] This

[3] In principle, specifying the blockchain's transaction rate, Λ, allows for an arbitrary block size, b, because the specified transaction rate is achieved by a block arrival rate of $\frac{\Lambda}{b}$. Formally, our analysis considers the limit case when $b \to 0^+$ because arbitrary block sizes complicate the derivation of the wait time without providing incremental economic insight.

enables us to derive the following expression for the expected wait time, $W^p(f, f_{-(i,t)})$:

$$W^p(f, f_{-(i,t)}) = \underbrace{\frac{1}{\Lambda}}_{\textit{Service Time Per User}} \times \underbrace{\int \mathbb{1}\{f^p_{(j,t)} \geqslant f\} \, dG(c_{(j,t)})}_{\textit{Higher Paying Users}} \tag{4}$$

Equation 4 makes explicit that each user must wait for higher fee-paying users but that the total wait varies with the service time per user, which is the inverse of the blockchain transaction rate.

The agents that provide the service of creating blocks are generally known as *validators* but, as discussed earlier, are more specifically referred to as miners for PoW blockchains and stakers for PoS blockchains. In either case, validators receive compensation for creating blocks. That compensation arises in two forms: fees and block rewards. As discussed in Section 2.1, fees refer to the user payments $f^p_{(i,t)}$ denominated in the consumption good. Block rewards refer to newly created units of the cryptocurrency. These coins are distributed into circulation by giving them as rewards for the validators who create new blocks, hence the term block reward. We assume that these block rewards are distributed according to a constant cryptocurrency supply growth rate, $\rho \geqslant 0$. Explicitly, denoting by M_t the units of cryptocurrency outstanding at the beginning of period t, we have that:

$$M_{t+1} = M_t e^{\rho} \tag{5}$$

As a normalization, we assume that the initial cryptocurrency supply is given by $M_0 = 1$. Note then that the total block reward distributed across period t, denoted by R_t, is given by:

$$R_t \equiv M_{t+1} - M_t = M_t(e^{\rho} - 1) = e^{\rho t}(e^{\rho} - 1) \tag{6}$$

We assume the block reward R_t is distributed uniformly across blocks in period t. Additional details regarding the blockchain vary by protocol, so we subsequently detail the PoW and PoS protocols separately.

2.2.1 PoW Blockchain

A PoW blockchain accepts a new block proposed by a miner only if that block contains the solution to a pre-specified computational puzzle. To find the solution for such a puzzle, a miner must expend a large amount of computational power and thereby incur a large financial expense. A miner is willing to bear that expense only because she receives compensation for her service. As discussed, miners receive compensation via block rewards and fees and, as in practice, the fees are paid in cryptocurrency at the time of the transaction. Further, given that agents born in period $t-2$ consume in period t, the sum of fees paid in period t is given by $\int f^{p}_{(i,t-2)} dG(c_{(i,t-2)})$ which, when divided by the period t price of the cryptocurrency P^{p}_{t}, gives the sum of fees paid in cryptocurrency.

We denote by H_t the period t computational power or *hashrate* used by miners. We normalize the financial cost per unit of computational power to unity so that the total computational cost equals the amount of computational power, H_t, directly. Moreover, we assume the mining market is competitive so that the following free entry condition must hold in equilibrium:

$$\underbrace{H_t}_{Mining\ Cost} = (\underbrace{R_t}_{Block\ Rewards} + \underbrace{\frac{\int f^{PoW}_{(i,t-2)}\ dG(c_{(i,t-2)})}{P^{PoW}_{t}}}_{User\ Fees\ in\ Coin}) \times P^{PoW}_{t+1} \tag{7}$$

In deriving this expression, we assume for simplicity of timing that coins received in a given period cannot be sold until the following period, hence the need for the number of coins received by a miner in period t (as a reward for validating) to be scaled by the period $t+1$ price, P^{PoW}_{t+1}.

We assume that users do not serve as miners and therefore the cryptocurrency holdings of generation-t users remains constant until they liquidate so that:

$$Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} \tag{8}$$

This is meant to capture a limiting case whereby the set of miners that are also users is small relative to the total population of users. This assumption is appropriate since most users do not pursue mining activities in practice; nonetheless, our results hold even if we allow users to spend their endowment on mining activities.[4] As we discuss subsequently, Equation 8 will not hold in

[4] In particular, including users as miners would only lower the amount of total wealth stored on the PoW blockchain, lowering demand for the cryptocurrency and therefore the value of the rewards from mining. Thus, when adding users as miners we expect a weakly lower equilibrium hash rate and therefore a weakly lower PoW security so that

general under a PoS blockchain because validators are users by construction and therefore may earn revenues associated with adding blocks to the blockchain.

2.2.2 PoS Blockchain

A PoS blockchain involves no computational puzzle. Rather, a PoS protocol randomly selects a coin among a set of coins, each of which the associated coin owner opted to place in the set. If a user places a coin into the described set then the coin is said to have been staked, and the user is referred to as a staker. The owner of the coin that is randomly selected then creates the next block on the blockchain and, as discussed, receives compensation in the form of block rewards and fees. Staking coins requires foregoing the right to sell those coins in the current period, so that the set of stakers in period t, S_t, is given by the following condition:

$$S_t = \{(i, t-1) : U^{PoS}_{(i,t-1)} > \sigma\} \tag{9}$$

which states that all agents holding the PoS cryptocurrency but not in the terminal period of their life optimally stake their coins. This condition arises because agents in the terminal period of their life would need to forgo consumption with no off-setting gain if they were to stake their coins, whereas agents not holding the cryptocurrency cannot stake (the initial purchase of coins in period t occurs after the period t staking of coins). Moreover, agents in the intermediate period of their lives possess no consumption utility, so they receive no gain from selling their coins and can earn potential block rewards and fees from staking. Thus, only agents born in period $t-1$ stake coins in period t, and such agents stake if and only if they adopt blockchain, which occurs endogenously for for Agent $(i, t-1)$ if and only if $U^{PoS}_{(i,t-1)} > \sigma$.

An important distinction between PoW and PoS is that block rewards and fees are paid to stakers, and stakers are necessarily holders of the cryptocurrency in the PoS case. Accordingly, the cryptocurrency holdings of a PoS user may evolve over time despite not trading. In particular, the following condition holds for all agents that use the blockchain:

our results remain unchanged.

$$\Delta Q^{PoS}_{(i,t)} = \underbrace{R_{t+1} \times \frac{Q^{PoS}_{(i,t),t}}{\int_{S_{t+1}} Q^{PoS}_{(i,t),t}\ dG(c_{(i,t)})}}_{Block\ \ Reward\ \ Accrued} + \underbrace{\frac{\int f^{PoS}_{(i,t-1)}\ dG(c_{(i,t-1)})}{P^{PoS}_{t+1}} \times \frac{Q^{PoS}_{(i,t),t}}{\int_{S_{t+1}} Q^{PoS}_{(i,t),t}\ dG(c_{(i,t)})}}_{Fees\ \ Accrued} \tag{10}$$

where

$$\Delta Q^{PoS}_{(i,t)} \equiv \underbrace{Q^{PoS}_{(i,t),t+1}}_{Period\ t+1\ Holding} - \underbrace{Q^{PoS}_{(i,t),t}}_{Period\ t\ Holding} \tag{11}$$

defines the change in coin holdings for Agent (i, t) from the end of period t (after her initial coin purchase) to the end of period $t + 1$ (after staking). Note that rewards and fees in Equation 10 are scaled by the probability of receiving them given the number of coins staked by Agent (i, t) and all other agents.[5]

2.3 Attacker

We model a malicious agent, hereafter referred to as an attacker, that seeks to sabotage the blockchain. This sabotage entails the attacker forking the blockchain and adding only empty blocks to her forked branch. The attacker adds these empty blocks in an attempt to deny all users from having their transactions processed by the blockchain. Akin to Pagnotta (2020), we assume that an attack succeeds if and only if the attacker is able to make her forked chain arbitrarily longer than the main chain.[6] As we discuss subsequently, the attacker internalizes the difficulty of executing the attack and attacks only if she finds mounting an attack to be incentive compatible.

We assume that the attacker has unlimited resources to perform an attack but receives an ex-ante random benefit from successfully disrupting the blockchain. Moreover, as we discuss in Sections 2.3.1 and 2.3.2, a PoW attack requires the purchase of computational power beforehand whereas a PoS attack requires the purchase of PoS coins beforehand. Therefore, we model this

[5] Recall that our analysis considers the limiting of case of infinitely many blocks of infinitesimal size. As a consequence, while a staker receiving the rewards and fees from a particular block is random, the total rewards and fees accrued is nonetheless non-random (i.e., there is no aggregate risk).

[6] Formally, we consider the probability that the attacker's chain ever exceeds the main chain by $k \in \mathbb{N}_+$ blocks within a period, noting that for a sufficiently large k we expect a crisis of confidence as users and validators learn the attack is occurring. For exposition, we study the limiting case where the crisis of confidence occurs after the attacker's fork exceeds the main chain by an arbitrary number of blocks which is the limiting case as $k \to \infty$. Our main results would hold for finite k as well, but this approach simplifies the solution while preserving the same insights.

feature by assuming that if the attacker wants to attack the blockchain in period $t+1$ then she must spend resources in the prior period t to prepare for the attack. In particular, we assume that at time t the attacker learns the value $B_t \sim U[0,1]$ which represents her benefit, denominated in consumption goods, from successfully disrupting the blockchain at time $t+1$.[7] After learning B_t, the attacker then chooses an amount of resources $A_t \geqslant 0$, also denominated in consumption goods, to mount an attack at time $t+1$. Denote by $\nu^p_{t+1}(A_t)$ the probability that the attacker successfully attacks the blockchain at time $t+1$ when using resources A_t to mount the attack, given the protocol $p \in \{PoW, PoS\}$. Then, the attackers problem is:

$$\max_{A_t \geqslant 0} \; B_t \cdot \nu^p_{t+1}(A_t) - A_t \tag{12}$$

whereby, we assume that the attacker selects A_t optimally so as to maximize her consumption utility given B_t and the equilibrium properties of the probability of a successful attack $\nu^p_{t+1}(A_t)$. We explicitly provide the probability $\nu^p_{t+1}(A_t)$ for each protocol $p \in \{PoW, PoS\}$ in Sections 2.3.1 and 2.3.2 respectively.

If the blockchain is successfully attacked in any period, then we assume that it is no longer an option for transaction activity thereafter, representing a crisis of confidence. Denoting by $A^\star_t(B_t)$ the optimal amount of resources spent by the attacker given the realized benefit B_t, then the probability that the blockchain survives through period t conditional on having survived until the beginning of period t is given by $\pi^p_{t+1} = \mathbb{E}[1 - \nu^p_{t+1}(A^\star_t(B_t))]$, and by definition, the following equation holds:

$$\pi^p_{t\to t+2} = \mathbb{E}_t[\pi^p_{t+1}\pi^p_{t+2}] \tag{13}$$

Note that this expression assumes that agents born in generation t will know if a successful attack is occurring at time t. Given that a successful attack represents a denial of service to these agents (i.e., they will be unable to purchase cryptocurrency with their endowment), this assumption is without loss of generality. Additional details regarding security vary by protocol, so we discuss PoW and PoS separately hereafter.

[7] Note that $B_t = 1$ represents a scenario whereby the benefit to the attacker equals the total endowment of any generation of agents. Accordingly, we believe this is an appropriate upper bound for the attacker's benefit from an attack.

2.3.1 PoW Attacks

For a PoW blockchain, the attacker's ability to create a forked branch that is arbitrarily longer than the main chain depends on her computational power relative to all other miners. In order to initiate the attack, the attacker acquires the necessary computational power in period t by expending A_t and then uses that power to launch an attack in period $t+1$. If the attacker possesses higher computational power than the other miners in period $t+1$ (i.e., $A_t > H_{t+1}$), then her forked branch grows at a faster rate than the main chain, and with certainty her forked branch eventually exceeds the length of the main chain by any arbitrary amount. Thus, in that case, an attack succeeds with probability 1. In contrast, if the attacker possesses less computational power than other miners in period $t+1$ (i.e., $A_t < H_{t+1}$), then the main chain grows at a faster rate than her forked branch. In such a case, the likelihood that the attacker's forked branch ever exceeds the main branch by an arbitrary k blocks vanishes to zero as k diverges so that the attack fails with probability one. Finally, if the attacker possesses computational power equivalent to the other miners in period $t+1$ (i.e., $A_t = H_{t+1}$), the attack succeeds with probability one because the attacker's forked branch will achieve an arbitrarily large lead on the main chain with certainty. Taking these features of PoW blockchains into account, $\nu^{PoW}_{t+1}(A_t)$ is given explicitly by:

$$\nu^{PoW}_{t+1}(A_t) = \begin{cases} 1 & \text{if } A_t \geqslant H_{t+1} \\ 0 & \text{if } A_t < H_{t+1} \end{cases} \tag{14}$$

Moreover, we can derive the attackers optimal expenditure and, as a consequence, the probability of a successful attack as follows:

$$A^{\star}_t(B_t) = \begin{cases} H_{t+1} & \text{if } B_t \geqslant H_{t+1} \\ 0 & \text{if } B_t < H_{t+1} \end{cases} \qquad \nu^{PoW}_{t+1}(A^{\star}(B_t)) = \begin{cases} 1 & \text{if } B_t \geqslant H_{t+1} \\ 0 & \text{if } B_t < H_{t+1} \end{cases} \tag{15}$$

Hence, we see that whenever the attacker's benefit from attacking the blockchain, B_t, is greater than the equilibrium hash rate, H_{t+1}, then the attacker will optimally use sufficient resources A_t to ensure their time $t+1$ attack succeeds with probability 1 and otherwise will not find it optimal to expend any resources to attack the blockchain. This implies that from the agent's perspective, the one period ahead survival probability of the PoW blockchain with hash rate H_{t+1} is given by

$$\pi_{t+1}^{PoW} = \mathbb{E}[1 - \nu_{t+1}^{PoW}(A^\star(B_t))] = Pr(B_t < H_{t+1}) \tag{16}$$

As a technical note, our equilibrium condition for hash rate in Equation 7 assumes that miners anticipate when a successful attack will be executed and therefore do not incur any mining costs in those periods. Formally, we assume that miners know the value of B_t by the beginning of period $t + 1$. Given the nature of our results this assumption is without loss of generality and can be interpreted as a limiting case when miners can quickly abandon their mining activity after observing an attack.[8]

2.3.2 PoS Attacks

As discussed in Saleh (2021), the attacker's ability to create a forked branch within PoS depends upon her share of coins held. Accordingly, if the attacker finds attacking the blockchain optimal, then she acquires the optimal number of coins in period t and stakes those coins in period $t+1$ so that she may execute the attack in period $t+1$. If the attacker acquires and stakes more coins than the other stakers, then her forked branch would grow at a faster rate than the main chain, and her forked branch would become arbitrarily longer than the main chain with certainty. In such a case, the attack would succeed with probability 1. Alternatively, if the attacker stakes fewer coins than the other stakers, then the attacker's forked branch would grow at a slower rate than the main chain so that her attack will fail with certainty. Finally, if the attacker stakes exactly as many coins as other stakers then the attack succeeds with probability one because the attacker's forked branch achieves an arbitrarily large lead on the main chain with certainty. Accordingly, $\nu_{t+1}^{PoS}(A_t)$ is given explicitly by:

$$\nu_{t+1}^{PoS}(A_t) = \begin{cases} 1 & \text{if } A_t \geqslant |S_{t+1}| \\ 0 & \text{if } A_t < |S_{t+1}| \end{cases} \tag{17}$$

As noted in Equation 17, the security features of the PoS blockchain imply that whenever

[8] In such a setting, the miners could potentially face a cost ϵ of mining before learning that an attack was launched with sufficient resources to succeed, in which case we study the limiting case where $\epsilon \to 0$. Including the probability of a successful attack in the zero profit condition 7 would only lower the equilibrium hash rate which would make attacks on the PoW blockchain less costly, lowering security and therefore only strengthening our results.

expending $A_t \geqslant |S_{t+1}|$ the attacker succeeds in their period $t+1$ attack with certainty and therefore the probability that the blockchain survives is 0, whereas when expending $A_t < |S_{t+1}|$ then the period $t+1$ attack fails with certainty and the blockchain survives with probability one. This comes from the fact that $|S_{t+1}|$ represents the measure of agents that adopt at time t and stake at $t+1$ and thus $|S_{t+1}|$ represents the total amount of consumption goods spent by users, who each have a unit endowment, to purchase coin at time t. Therefore, the attacker would need to spend $A_t \geqslant |S_{t+1}|$ consumption goods in acquiring coin at time t in order to mount a successful attack at time $t+1$. Given these features, the optimal expenditure and success probability of the attacker in a PoS blockchain are given by:

$$A_t^\star(B_t) = \begin{cases} |S_{t+1}| & \text{if } B_t \geqslant |S_{t+1}| \\ 0 & \text{if } B_t < |S_{t+1}| \end{cases} \qquad \nu_{t+1}^{PoS}(A^\star(B_t)) = \begin{cases} 1 & \text{if } B_t \geqslant |S_{t+1}| \\ 0 & \text{if } B_t < |S_{t+1}| \end{cases} \tag{18}$$

Namely, similar to the PoW case, if $B_t \geqslant |S_{t+1}|$ then the attacker optimally launches an attack with sufficient resources A_t that ensure the attack succeeds with probability 1, and otherwise spends zero resources on an attack. Finally, given these features of the PoS blockchain and the attackers optimal solution to their expenditure problem we can see that, from the agent's perspective, the time $t+1$ survival probability of the PoS blockchain with set of stakers S_{t+1} is given by

$$\pi_{t+1}^{PoS} = \mathbb{E}[1 - \nu_{t+1}^{PoS}(A^\star(B_t))] = Pr(B_t < |S_{t+1}|) \tag{19}$$

2.4 Equilibrium

Akin to Huberman et al. (2019) and Hinzen et al. (2020), we restrict ourselves to examining a stationary cut-off equilibrium, characterized by an endogenously determined adoption cut-off, c^p such that Agent (i,t) adopts the blockchain technology (over the alternative) if and only if $c_{(i,t)} < c^p$. Furthermore, we suppose that all agents utilize a symmetric ex-ante fee strategy ϕ^p which maps each user's realized cost of waiting c to the fee they pay $f = \phi^p(c)$. For regularity, we impose that ϕ^p is twice continuously differentiable on $(0, c^p)$ and both continuous and strictly increasing on $[0, c_p)$. Consequently, our equilibrium is defined as follows:

Definition 2.1. Equilibrium

Our model is characterized by a blockchain transaction rate, $\Lambda > 0$, an initial cryptocurrency supply $M_0 = 1$, and a cryptocurrency supply growth rate, $\rho \geqslant 0$. Recall that users within our model have heterogenous wait disutility, $c_{(i,t)} \sim G[0, \infty)$, and possess an alternative technology, yielding them $\sigma \in (0,1)$ units of consumption good two periods ahead. Moreover, in each period t, there exists a deep pocketed attacker who draws a benefit $B_t \sim U[0,1]$ from disrupting the blockchain at $t+1$ and spends A_t resources to mount an attack on the blockchain in the following period, where A_t is chosen to maximize their consumption utility according to 12.

Within our model, a $p \in \{PoW, PoS\}$ Equilibrium is (1) an adoption cut-off, c^p, (2) a function, $\phi^p(c)$, that maps user types to their fees, (3) a set of fee realizations $\{f^p_{(i,t)}\}_{(i,t):i\in[0,1],t\geqslant 0}$ such that $f^p_{(i,t)} := \phi^p(c_{(i,t)})$ for each user (i,t), (4) A cryptocurrency market value, $\mathcal{M}^p$, (5) A set of cryptocurrency holdings for each user in each period of her life conditional upon adopting the blockchain, $\{Q^p_{(i,t),t}, Q^p_{(i,t),t+1}\}_{(i,t):i\in[0,1],t\geqslant 0}$, (6), a one-period-ahead survival probability for the blockchain, π^p, and (8) for PoW (a) the total mining computational power, H, and for PoS (b) a sequence of staker sets, $\{S_t\}_{t\in\mathbb{N}}$. All described quantities are conditional on blockchain survival until the relevant period. After a successful blockchain attack, the blockchain is not viable, so no user adopts the blockchain. The equilibrium is defined by the following conditions:

(i) Blockchain Adoption Decisions are Optimal

Agent (i,t) adopting the blockchain entails her selling her endowment for cryptocurrency. More precisely, given the nature of the cut off equilibrium with threshold c^p, all agents adopt whenever $c_{(i,t)} < c^p$. Therefore, c^p must be determined so that this condition represents rational behavior of the agents. In particular, this requires that for all (i,t):

$$c_{(i,t)} < c^p \Leftrightarrow U^p_{(i,t)} = (\pi^p)^2 \times \mathbb{E}_t[P^p_{t+2}Q^p_{(i,t),t+1} - f^p_{(i,t)} - \frac{c_{(i,t)}}{\Lambda}\int \mathbb{1}\{f^p_{(j,t)} \geqslant f^p_{(i,t)}\}\, dG(c_{(j,t)}) \mid c_{(i,t)}] > \sigma \tag{20}$$

As explained when deriving 13, we multiply the benefit of using the blockchain by the steady state one period ahead probability π^p squared as the agent knows if an attack is occurring in period t and therefore only has uncertainty about an attack in period $t+1$ and $t+2$ (before their coin is liquidated).

Whenever Agent (i,t) adopts the blockchain they invest their full wealth and therefore it must be the case that:

$$\text{For all } (i,t) : Q^p_{(i,t),t} = \frac{1}{P^p_t} \tag{21}$$

with $P^p_t \equiv \frac{\mathcal{M}^p}{M_t}$ defined as the price of the cryptocurrency in period t, and $M_t \equiv e^{\rho t}$ defined as the units of cryptocurrency outstanding in period t. Note also that our cut-off equilibrium implies that the total wealth spent on purchasing cryptocurrency in each period t is given by $G(c^p)$ due to the fact that:

$$\text{For all } t : |\{(i,t) : U^p_{(i,t)} > \sigma\}| = |\{(i,t) : c_{(i,t)} < c^p\}| = G(c^p) \tag{22}$$

(ii) Equilibrium Fees are Optimal

We require that User (i,t) with realized cost $c_{(i,t)} \in [0,+\infty)$ finds it optimal to pay the fee $f^p_{i,t} = \phi^p(c_{(i,t)})$ given that all other users $(j,t) \neq (i,t)$ pay fees according to $f_{(j,t)} = \phi^p(c_{(j,t)})$. Formally, the following condition holds:

$$\text{For all } c : \phi^p(c) = \begin{cases} \underset{f:\ f \geqslant 0}{\arg\max}\ P^p_{t+2} Q^p_{(i,t),t+1} - f - \frac{c}{\Lambda} \int \mathbb{1}\{f^p_{(j,t)} \geqslant f\}\ dG(c_{(j,t)}) & \text{if } c < c^p \\ 0 & \text{if } c \geqslant c^p \end{cases} \tag{23}$$

where users optimally pay zero fees whenever they do not adopt.

(iii) The Cryptocurrency Market Clears

For each period t, the total user demand for cryptocurrency units, $\frac{G(c^p)}{P^p_t}$, equals the supply of cryptocurrency units, M_t, less those paid as fees, $\frac{\int f^p_{(i,t-2)}\ dG(c_{(i,t-2)})}{P^p_t}$, and those held by intermediately aged agents, $\frac{G(c^p)}{P^p_{t-1}}$, who have no need to liquidate given that they possess no consumption utility in that period. Therefore, equating these expressions and rearranging, we obtain that the cryptocurrency market clears whenever the following condition holds:

$$\text{For all } t : (1 + e^{-\rho})G(c^p) + \int f^p_{(i,t-2)}\ dG(c_{(i,t-2)}) = \mathcal{M}^p \tag{24}$$

(iv) Validators Are Determined According To Protocol Rules

In a PoW Equilibrium, the computational power of miners is determined by free entry so that the following condition holds:

$$\text{For all } t : H = (R_t + \frac{\int f^{PoW}_{(i,t-2)}\ dG(c_{(i,t-2)})}{P^{PoW}_t}) \times P^{PoW}_{t+1} \tag{25}$$

with the block reward being defined as $R_t \equiv M_t(e^\rho - 1) = e^{\rho t}(e^\rho - 1)$.

In a PoS Equilibrium, the set of stakers at time t is determined as the set of users holding coins that prefer to stake rather than consume which is equivalent to the set of users that adopt at time $t-1$. Thus, the following condition holds:

$$\text{For all } t : S_t = \{(i, t-1) : c_{(i,t-1)} < c^{PoS}\} \tag{26}$$

(v) Block Rewards and Fees Are Distributed According To Protocol Rules

In a PoW Equilibrium, block rewards and fees are distributed to miners so that generation-t agents receive neither block rewards nor fees. Formally, the following condition holds:

$$\text{For all } (i, t) : Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} \tag{27}$$

In a PoS Equilibrium, block rewards and fees are distributed to stakers so that the following condition holds:

$$\text{For all } (i, t) : Q^{PoS}_{(i,t),t+1} = Q^{PoS}_{(i,t),t} + R_{t+1}\ \frac{1}{G(c^{PoS})} + \frac{\int f^{PoS}_{(i,t-1)}\ dG(c_{(i,t-1)})}{P^{PoS}_{t+1}}\ \frac{1}{G(c^{PoS})} \tag{28}$$

(vi) Blockchain Survival Probability Varies According To Protocol Rules

In a PoW Equilibrium, the one-period-ahead blockchain survival probability varies with computational power so that $B_t \sim U[0, 1]$ combined with 16 implies:

$$\text{For all } t : \pi^{PoW} = \mathbb{P}(B_t < H) = \min\{H, 1\} \tag{29}$$

In a PoS Equilibrium, the one-period-ahead blockchain survival probability varies with the adoption rate, given by c^{PoS}, so that $B_t \sim U[0,1]$ combined with 19 and 26 implies:

$$\text{For all } t : \pi^{PoS} = \mathbb{P}(B_t < G(c^{PoS})) = G(c^{PoS}) \tag{30}$$

3 Model Solution

We begin by solving for the optimal fees $f^p_{(i,t)}$ and the market value of the cryptocurrency $\mathcal{M}^p$ as given by the following lemma:

Lemma 3.1. *Under any $p \in \{PoW, PoS\}$ equilibrium the optimal fees $f^p_{i,t}$ and market value $\mathcal{M}^p$ are given by:*

$$\textit{For all } (i,t) : f^p_{(i,t)} = \begin{cases} \frac{1}{\Lambda} \int\limits_0^{c_{(i,t)}} x \ dG(x) & \textit{if } c_{(i,t)} < c^p \\ 0 & \textit{if } c_{(i,t)} \geqslant c^p \end{cases} \tag{31}$$

and

$$\mathcal{M}^p = (1 + e^{-\rho}) G(c^p) + \frac{1}{\Lambda} \int\limits_0^{c^p} \int\limits_0^{c} x \ dG(x) \ dG(c) \tag{32}$$

Proof. See appendix Section A.1. □

The remaining equilibrium solutions vary by protocol, so we discuss PoW and PoS separately in the remainder of this section. The following proposition characterizes the main features of the PoW equilibrium.

Proposition 3.2. *PoW Equilibrium*

Any PoW equilibrium is characterized by an adoption cut-off, c^{PoW} such that $c_{(i,t)} < c^{PoW}$ if and only if $U^{PoW}_{(i,t)} > \sigma$. The equilibrium hash rate H and one period ahead blockchain survival probability π^{PoW} are given by

$$H = (1 - e^{-2\rho}) G(c^{PoW}) + \frac{1}{\Lambda} \int\limits_0^{c^{PoW}} \int\limits_0^{c} x \ dG(x) \ dG(c) \tag{33}$$

$$\pi^{PoW} = \min\{(1-e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x \; dG(x) \; dG(c), 1\} \tag{34}$$

For all Agents (i,t) the equilibrium user holdings $Q^{PoW}_{(i,t),t}$ conditional on adopting the blockchain are given by

$$Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} = \frac{e^{\rho t}}{(1+e^{-\rho})G(c^{PoW}) + \frac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x \; dG(x) \; dG(c)} \tag{35}$$

The equilibrium expected benefit from PoW blockchain adoption $U^{PoW}_{(i,t)}$ is given by

$$\begin{aligned} U^{PoW}_{(i,t)} &= (\min\{(1-e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x \; dG(x) \; dG(c), 1\})^2 \\ &\times(e^{-2\rho} - \frac{1}{\Lambda}\int\limits_0^{c_{(i,t)}} x \; dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (G(c^{PoW}) - G(c_{(i,t)}))) \end{aligned} \tag{36}$$

Proof. See appendix Section A.2. □

Next, we proceed to characterize the main properties of the PoS equilibrium.

Proposition 3.3. *PoS Equilibrium*

Any PoS equilibrium is characterized by an adoption cut-off, c^{PoS} such that $c_{(i,t)} < c^{PoS}$ if and only if $U^{PoS}_{(i,t)} > \sigma$. The equilibrium set of stakers S_t and one period ahead blockchain survival probability π^{PoS} are given by

$$S_t = \{(i,t) : c_{(i,t)} < c^{PoS}\} \quad \textit{for all } t \tag{37}$$

and

$$\pi^{PoS} = G(c^{PoS}) \tag{38}$$

For all Agents (i,t) the equilibrium user holdings $Q^{PoS}_{(i,t),t}$ and $Q^{PoS}_{(i,t),t+1}$ conditional on adopting the block chain are given by

$$Q^{PoS}_{(i,t),t} = \frac{e^{\rho t}}{(1+e^{-\rho})G(c^{PoS}) + \frac{1}{\Lambda}\int\limits_0^{c^{PoS}}\int\limits_0^{c} x \; dG(x) \; dG(c)} \tag{39}$$

and

$$Q^{PoS}_{(i,t),t+1} = \frac{e^{\rho(t+2)}}{G(c^{PoS})} \times \frac{G(c^{PoS}) + \frac{1}{\Lambda} \int\limits_0^{c^{PoS}} \int\limits_0^{c} x \ dG(x) \ dG(c)}{(1+e^{-\rho})G(c^{PoS}) + \frac{1}{\Lambda} \int\limits_0^{c^{PoS}} \int\limits_0^{c} x \ dG(x) \ dG(c)} \tag{40}$$

The equilibrium expected benefit from PoS blockchain adoption $U^{PoS}_{(i,t)}$ *is given by*

$$U^{PoS}_{(i,t)} = (G(c^{PoS}))^2 \times (1 + \frac{\frac{1}{\Lambda} \int\limits_0^{c^{PoS}} \int\limits_0^{c} x \ dG(x) \ dG(c)}{G(c^{PoS})} - \frac{1}{\Lambda} \int\limits_0^{c_{(i,t)}} x \ dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (G(c^{PoS}) - G(c_{(i,t)}))) \tag{41}$$

Proof. See appendix Section A.3. □

4 Results

Our analysis in the following Section 4.1 considers the case of no cryptocurrency growth (i.e., $\rho = 0$). That case, by construction, precludes block rewards and reflects Bitcoin's eventual design whereby block rewards are eventually phased out. In Section 4.2, we generalize our results to a setting of arbitrary cryptocurrency growth rates (i.e., $\rho \geqslant 0$).

4.1 Constant Cryptocurrency Supply

In the absence of block rewards, improving a PoW blockchain's transaction rate not only undermines security but makes the blockchain entirely insecure. Our first main result formalizes this assertion:

Proposition 4.1. *High Scale PoW Blockchains Are Fully Insecure*

If a PoW Blockchain possesses no block rewards (i.e., $\rho = 0$), then there exists a minimum transaction rate, $\underline{\Lambda}^{PoW} > 0$, such that the blockchain possessing a higher transaction rate (i.e., $\Lambda > \underline{\Lambda}^{PoW}$) renders the blockchain entirely insecure (i.e., $\pi^{PoW} = 0$) in the unique PoW equilibrium.

Proof. See appendix Section A.4. □

To clarify the intuition behind this result, we highlight that, per Equation 31, users adopting the blockchain pay an equilibrium fee, $f^{PoW}_{(i,t)}$, given by:

$$f^{PoW}_{(i,t)} = \frac{1}{\Lambda} \int\limits_{0}^{c_{(i,t)}} x \; dG(x) \tag{42}$$

Equation 42 shows that Agent (i,t)'s equilibrium fee decreases in the blockchain's transaction rate and that the fee vanishes as the transaction rate diverges. This relationship arises because users dislike waiting and therefore pay fees to reduce their wait times. However, since users are processed in descending fee order, the level of the fee affects the wait time only by influencing the order of processing and not by determining the processing wait time directly. In particular, if a certain incremental fee places a user ahead of a mass of n additional users, then the time saved from paying this incremental fee paid is $\frac{n}{\Lambda}$ which decreases as the blockchain transaction rate increases and vanishes entirely as the transaction rate diverges. Consequently, the incentive to pay higher fees decreases as the transaction rate increases and vanishes as the transaction rate diverges, implying that a user's equilibrium fee monotonically decreases towards zero as the scale of the blockchain improves.

This relationship between equilibrium fees and the blockchain's transaction rate has important implications for PoW security. To intuit that point, we reproduce Equation 25, which determines the equilibrium computational power H, in the case where block rewards are zero (i.e. $\rho = 0$):

$$H = \int f^{PoW}_{(i,t-2)} \; dG(c_{(i,t-2)}) = \frac{1}{\Lambda} \int_0^{c^p} \int_0^{c} x \; dG(x) dG(c) \tag{43}$$

Equation 43 highlights that, absent block rewards, the PoW blockchain's computational power is financed entirely by fee revenue. Accordingly, for a sufficiently high transaction rate, increasing the transaction rate not only reduces equilibrium fees but also the blockchain's equilibrium computational power. To clarify this point, note that regardless of how c^p evolves when the transaction rate increases, the equilibrium computational power will decrease to zero as Λ diverges. This comes from the fact that G has a finite first moment so that even if high transaction rates lead to high levels of adoption, the cumulative fees will be decreasing in the transaction rate once it exceeds a certain threshold. Thus, for a sufficiently high transaction rate (i.e., for all $\Lambda \geqslant \underline{\Lambda}^{PoW}$ for some $\underline{\Lambda}^{PoW} < \infty$), the PoW blockchain's equilibrium computational power would necessarily fall to the point that its survival probability, π^{PoW}, falls below the rate of the imperfect storage technology,

σ. In such a case, all agents would prefer to use the storage technology instead of the blockchain (even with zero fees and zero wait time) due to the extreme security risk associated with using the blockchain. In such a case, there will be zero adoption (i.e., $c^{PoW} = 0$) and the blockchain will be trivial for the attacker to successfully attack. Thus, a PoW blockchain becomes entirely insecure (i.e., $\pi^{PoW} = 0$) if the blockchain's transaction rate exceeds a finite threshold, $\underline{\Lambda}^{PoW}$.

The notion that a blockchain's scale undermines its security is not generic across all blockchain types. In fact, our next result highlights that an increased transaction rate enhances security for a PoS blockchain:

Proposition 4.2. *High Scale PoS Blockchains Are Fully Secure*
If a PoS Blockchain possesses no block rewards (i.e., $\rho = 0$), then there exists a minimum transaction rate, $\underline{\Lambda}^{PoS} > 0$, such that the blockchain possessing a higher transaction rate (i.e., $\Lambda > \underline{\Lambda}^{PoS}$) renders the blockchain fully secure (i.e., $\pi^{PoS} = 1$) in a PoS equilibrium.

Proof. See appendix Section A.5. □

As in the PoW case, high transaction rates drive equilibrium fees to zero. However, an important distinction between PoW and PoS arises in the fact that fee revenues are not directly relevant for securing PoS blockchains. To understand this last point, we revisit our analogy of comparing a PoS blockchain to an all-equity firm. To take control of such a firm, it is typically necessary to acquire a significant portion of that firm's shares. In turn, the expense of acquiring such a quantity of shares depends upon the total firm market value. Since a PoS blockchain confers governance power in proportion to coins held, the PoS coins are akin to the shares of the all-equity firm. Moreover, the market value of the all-equity firm is analogous to the market value of the cryptocurrency. It can be seen from Equation 32 (using $\rho = 0$), that as the blockchain's transaction rate diverges (i.e., $\Lambda \to \infty$), the cryptocurrency market value for a PoS blockchain, $\mathcal{M}^{PoS}$, adheres to the following equation:

$$\lim_{\Lambda \to \infty} \mathcal{M}^{PoS} = G(c^{PoS}) \tag{44}$$

which highlights that the PoS cryptocurrency's market value is increasing in the adoption cut-off, c^{PoS}. Therefore, a higher adoption cut-off, c^{PoS}, implies higher demand for the PoS coin, $G(c^{PoS})$, which, in turn, implies higher security, π^{PoS}, per Equation 38.

Thus, the key security question for a PoS blockchain becomes whether the PoS blockchain can generate high adoption. In that regard, an increased blockchain transaction rate helps rather than hampers security. Specifically, as discussed, equilibrium fees vanish as the blockchain transaction rate diverges. More mechanically, wait times also vanish as the blockchain transaction rate diverges. Both of these effects imply that user utility increases and reaches a maximum for a PoS blockchain with infinite transaction capacity. In that case, adoption reaches its maximal value for some finite but large transaction rate and the PoS blockchain survives an attack with certainty as we assume that the benefit to the attacker cannot exceed the total production of the entire economy in any given period (i.e., $B_t < 1$ a.s.). Thus, a sufficiently high transaction rate ensures full adoption which ensures that any attack fails with certainty and therefore no attacks are pursued by the attacker. Accordingly, in contrast to a PoW blockchain, a PoS blockchain achieves enhanced security from improved scaling.

4.2 Non-Constant Cryptocurrency Supply

We next turn to generalizing our results beyond the case of a constant cryptocurrency supply. Accordingly, in this section, we allow the cryptocurrency supply to grow at a rate of $\rho \geqslant 0$, and, as in practice, we assume that all new coins are paid out as block rewards to validators for producing new blocks. Our first result generalizes Proposition 4.1, establishing that a PoW blockchain cannot achieve full security for high transaction rates, even with block rewards:

Proposition 4.3. *High Scale PoW Blockchains Are Insecure, Even With Block Rewards*
For any cryptocurrency growth rate, ρ, there exists a minimum transaction rate, $\underline{\Lambda_\rho}^{PoW} > 0$, such that the blockchain possessing a higher transaction rate (i.e., any $\Lambda > \underline{\Lambda_\rho}^{PoW}$) renders the blockchain insecure (i.e., $\pi^{PoW} < 1$) in any PoW equilibrium. In fact, as the transaction rate diverges (i.e., $\Lambda \to \infty$), blockchain security possesses an upper-bound, strictly below full security. In particular, $\limsup_{\Lambda \to \infty} \pi^{PoW} \leqslant 1 - \sigma < 1$.

Proof. See appendix Section A.6. □

To understand Proposition 4.3, it is important to recognize that block rewards correspond to inflation and thereby reduce the value of cryptocurrency holdings.[9] Thus, a generation-t user who adopts the blockchain incurs a reduction in the real value of her cryptocurrency holdings by a proportional factor of $e^{-\rho}$ in each period with ρ being the cryptocurrency growth rate. Formally, combining Equations 32 and 35, one can derive that the proceeds from Agent (i,t)'s period $t+2$ sale of her cryptocurrency holdings is given by:

$$P_{t+2}^{PoW} Q_{(i,t),t+1}^{PoW} = e^{-2\rho} \tag{45}$$

This is important to note because Agent (i,t) also possesses an alternative technology that entitles her to $\sigma \in (0,1)$ consumption goods in period $t+2$ if she does not adopt the blockchain. Accordingly, for any user to adopt the blockchain, the block reward cannot be too high as otherwise all users would abandon the blockchain in favor of using the storage technology. More precisely, the cryptocurrency growth rate is restricted in any equilibrium with non-zero adoption by the following condition:

$$\underbrace{e^{-2\rho}}_{Max\ Consumption\ From\ Blockchain} > \underbrace{\sigma}_{Consumption\ From\ Alternative\ Technology} \tag{46}$$

If Equation 46 does not hold then all users would opt for the storage technology and not use the blockchain. Moreover, in such a case, both block rewards and fees would have zero value and the blockchain would be entirely insecure as a result (i.e., $H = 0$ and therefore $\pi^{PoW} = 0$). The zero value for block rewards would arise due to the lack of blockchain usage implying zero demand for the cryptocurrency and therefore a zero cryptocurrency price. The zero value of fees would arise more directly as the lack of usage would imply zero blockchain transactions and thus zero fees. Following the stated argument, a PoW equilibrium in which the blockchain possesses any level of security (i.e., $\pi^{PoW} > 0$) cannot arise unless the cryptocurrency growth rate, ρ, satisfies:

$$\rho < \log \sqrt{\frac{1}{\sigma}} \tag{47}$$

Importantly, Equation 47 imposes a limit on block rewards and thus miner revenues and the computational power securing the blockchain. In particular, as the blockchain's transaction rate

[9] This point is discussed also in earlier works such as Chiu and Koeppl (2019) and Saleh (2019).

diverges (i.e., $\Lambda \to \infty$), Equation 33 implies that the blockchain's computational power, H, adheres to the following equation:

$$\lim_{\Lambda \to \infty} H = (1 - e^{-2\rho}) G(c^{PoW}) \tag{48}$$

Using our restriction on the block reward from Equation 47 and invoking Equation 29 therefore implies:

$$\lim_{\Lambda \to \infty} \pi^{PoW} \leqslant 1 - \sigma < 1 \tag{49}$$

which matches the findings of Proposition 4.3.

Intuitively, block rewards involve transferring welfare from users to miners. Yet, we have just shown that while block rewards may improve security by enhancing miner revenues, they may also drive users from the blockchain by lowering the adoption rate and thereby reducing the available resources that could be transferred to miners. Accordingly, block rewards and thus blockchain security are limited to the extent that users have an alternative option to the blockchain.

In contrast to PoW, PoS blockchains can generate full security (i.e., $\pi^{PoS} = 1$) irrespective of the cryptocurrency growth rate. More formally, we have the following result:

Proposition 4.4. *High Scale PoS Blockchains Are Fully Secure*
There exists a minimum transaction rate, $\underline{\Lambda}^{PoS} > 0$, such that the blockchain possessing a higher transaction rate (i.e., $\Lambda > \underline{\Lambda}^{PoS}$) renders the blockchain fully secure (i.e., $\pi^{PoS} = 1$) in a PoS equilibrium.

Proof. See appendix Section A.7. □

The intuition for Proposition 4.4 mirrors that for Proposition 4.2, so we opt not to restate the intuition. Instead, we will highlight the intuition as to why Proposition 4.2 maintains regardless of the cryptocurrency growth rate ρ. In particular, we note that large block rewards (i.e., large ρ) do not impose a loss on cryptocurrency holders in a PoS blockchain due to the fact that even though block rewards constitute inflation, the benefits of that inflation accrue to the stakers, and the stakers are themselves the cryptocurrency holders. More precisely, within our model, Agent (i, t) faces a devaluation in her holdings from t to $t+1$ by a proportional factor of $e^{-\rho}$, but, in period

$t+1$, she serves as a staker and thereby receives block rewards that correspond to an appreciation in her holdings from $t+1$ to $t+2$ by a proportional factor of e^{ρ}. Accordingly, collectively across the two periods, the block reward inflation has no effect on her holdings. To see this within our analysis, note that using Equations 32 and 40 it is possible to show that Agent (i,t)'s period $t+2$ sale of her cryptocurrency holding, $P^{PoS}_{t+2}Q^{PoS}_{(i,t),t+1}$ satisfies:

$$\lim_{\Lambda \to \infty} P^{PoS}_{t+2}Q^{PoS}_{(i,t),t+1} = 1 \tag{50}$$

which establishes that the proceeds from Agent (i,t)'s period $t+2$ sale of cryptocurrency approaches her initial endowment as the blockchain transaction rate diverges. Equation 50 is invariant to the cryptocurrency growth rate, ρ, which highlights the irrelevance of the block reward in a PoS blockchain when the transaction rate is sufficiently large. Therefore, for a sufficiently large transaction rate we obtain negligible fees, full adoption, and full security (i.e., $\pi^{PoS} = 1$) for a PoS blockchain regardless of the cryptocurrency growth rate ρ. It is important to remark here that modeling users as miners would not generate this same irrelevance of block rewards as mining requires computational expenditure and free entry ensures that the expense of the miner is equal to the expected reward. In contrast, staking involves no incremental cost for a cryptocurrency holder.

5 Conclusion

Our work highlights that scaling a PoW blockchain has the perverse effect of undermining its security. Accordingly, proposals to scale PoW blockchains in hopes of improving the user experience may well be self-defeating as our results indicate the loss in security may overwhelm any gains from timely processing of transactions. We also demonstrate that PoS blockchains are immune from the described effect and, in fact, attain enhanced security when the scale of the blockchain is improved. Our results thus suggest that PoS may be better suited to applications in which high volume is necessary for the viability of the economic application. This insight is likely to be particularly important for applications in the context of Tokenomics (see, e.g., Mayer 2020, Cong et al. 2021, Gan et al. 2021a and Gan et al. 2021b) and Decentralized Finance (see, e.g., Capponi and Jia 2021).

References

Alsabah, H., and A. Capponi. 2020. Pitfalls of Bitcoin's Proof-of-Work: R&D Arms Race and Mining Centralization. *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. *Working Paper* .

Carlsten, M., H. Kalodner, S. M. Weinberg, and A. Narayanan. 2016. On the Instability of Bitcoin Without the Block Reward. *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security* pp. 154–167.

Chiu, J., and T. V. Koeppl. 2019. The Economics of Cryptocurrencies - Bitcoin and Beyond. *Working Paper* .

Cong, L. W., Z. He, and J. Li. 2020. Decentralized Mining in Centralized Pools. *Review of Financial Studies* Forthcoming.

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

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.

Ebrahimi, Z., B. Routledge, and A. Zetlin-Jones. 2019. Getting Blockchain Incentives Right. *Working Paper* .

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

Gan, J., G. Tsoukalas, and S. Netessine. 2021a. Inventory, Speculators, and Initial Coin Offerings. *Management Science* 67:914 – 931.

Gan, J., G. Tsoukalas, and S. Netessine. 2021b. To Infinity and Beyond: Financing Platforms With Uncapped Crypto Tokens. *Working Paper* .

Garratt, R., and M. van Oordt. 2020. Why Fixed Costs Matter for Proof-of-Work Based Cryptocurrencies. *Working Paper* .

Hinzen, F., K. John, and F. Saleh. 2020. Bitcoin's Fatal Flaw: The Limited Adoption Problem. *NYU Stern Working Paper* .

Huberman, G., J. D. Leshno, and C. Moallemi. 2019. An Economic Analysis of the Bitcoin Payment System. *Working Paper* .

Irresberger, F., K. John, and F. Saleh. 2020. Bitcoin's User Surplus. *Working Paper* .

Lehar, A., and C. Parlour. 2020. Miner Collusion and the BitCoin Protocol. *Working Paper* .

Mayer, S. 2020. Token-Based Platforms and Speculators. *Working Paper* .

Mueller, P. 2020. Cryptocurrency Mining: Asymmetric Response to Price Movement. *Working Paper* .

Nakamoto, S. 2008. Bitcoin: A peer-to-peer electronic cash system. *https://bitcoin.org/bitcoin.pdf* .

Pagnotta, E. 2020. Decentralizing Money: Bitcoin Prices and Blockchain Security. *Review of Financial Studies* Forthcoming.

Prat, J., and B. Walter. 2019. An Equilibrium Model of the Market for Bitcoin Mining. *Working Paper* .

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

Saleh, F. 2019. Volatility and Welfare in a Crypto Economy. *Working Paper* .

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

Appendices

A Proofs

A.1 Proof of Lemma 3.1

Proof. The optimality of fees requires that for all $c \leqslant c^p$:

$$\phi^p(c) = \underset{f:\ f \geqslant 0}{\arg\max}\ P^p_{t+2} Q^p_{(i,t),t+1} - f - \frac{c}{\Lambda} \times (G(c^p) - G((\phi^p)^{-1}(f))) \tag{1}$$

with $(\phi^p)^{-1}$ denoting the inverse function of ϕ^p over $(0, \phi(c^p))$, $(\phi^p)^{-1}(f) \equiv c^p$ for $f > \phi(c^p)$ and $(\phi^p)^{-1}(0) \equiv 0$. This generalized definition of the inverse function of ϕ^p reflects that any user considering the out-of-equilibrium action of paying a fee higher than that paid in equilibrium internalizes that she would receive immediate service (i.e., $f > \phi(c^p)$ implies $\{G(c^p) - G((\phi^p)^{-1}(f))\} = 0$). Moreover, any user paying a zero fee internalizes that she would have to wait for all other users before receiving service (i.e., $f = 0$ implies $\{G(c^p) - G((\phi^p)^{-1}(f))\} = G(c^p)$).

The first order condition for Equation 1 is given by

$$-1 + \frac{c}{\Lambda} \cdot G'((\phi^p)^{-1}(f)) \cdot \frac{\partial}{\partial f}(\phi^p)^{-1}(f) = 0$$

which after applying the inverse function theorem, applying $f^p_{(i,t)} = \phi^p(c_{(i,t)})$, and rearranging yields

$$\frac{d\phi^p}{dc} = \frac{c}{\Lambda} G'(c) \tag{2}$$

This differential equation is defined over $c_{(i,t)} \in [0, c^p]$ and has the boundary condition $\phi^p(0) = 0$ (i.e., a zero fee is optimal for any agent with wait disutility per unit time of zero). Accordingly, the unique equilibrium fee function, ϕ^p, is given explicitly by:

$$\text{For all } (i,t) : \phi^p(c) = \begin{cases} \frac{1}{\Lambda} \int\limits_0^c x\ dG(x) & \text{if } c < c^p \\ 0 & \text{if } c \geqslant c^p \end{cases} \tag{3}$$

which gives the equilibrium realized fees 31.

Then, applying Equation 31 to Equation 24 (which is derived using the fact that $\frac{P_t^p}{P_{t-1}^p} = \frac{\mathcal{M}^p}{M_t}\frac{M_{t+1}}{\mathcal{M}^p} = e^{-\rho}$) yields the following solution for the cryptocurrency market value:

$$\mathcal{M}^p = (1+e^{-\rho})G(c^p) + \frac{1}{\Lambda}\int\limits_0^{c^p}\int\limits_0^{c} x\; dG(x)\; dG(c) \tag{4}$$

□

A.2 Proof of Proposition 3.2

Proof. To determine the equilibrium computational power we start with Equation 25 and use the fact that

$$P_{t+1}^{PoW} R_t = P_{t+1}^{PoW} M_t (e^{\rho}-1) = P_{t+1}^{PoW} M_{t+1}\frac{(e^{\rho}-1)}{e^{\rho}} = \mathcal{M}^{PoW}(1-e^{-\rho})$$

Then, substituting for $\mathcal{M}^{PoW}$ from 32, substituting the optimal fees from 31, rearranging, and using the fact that $\frac{P_{t+1}}{P_t} = e^{-\rho}$ we obtain.

$$H = (1-e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x\; dG(x)\; dG(c) \tag{5}$$

Moreover, applying Equation 33 to Equation 29 yields the equilibrium one-period-ahead blockchain survival probability:

$$\pi^{PoW} = \min\{(1-e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x\; dG(x)\; dG(c), 1\} \tag{6}$$

Combining Equations 21, 27 and 32 yields the equilibrium holdings for each agent that adopts the blockchain:

$$\text{For all } (i,t): Q_{(i,t),t}^{PoW} = Q_{(i,t),t+1}^{PoW} = \frac{1}{P_t^{PoW}} = \frac{e^{\rho t}}{(1+e^{-\rho})G(c^{PoW}) + \frac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x\; dG(x)\; dG(c)} \tag{7}$$

Finally, plugging in the explicit solutions for $f_{(i,t)}^{PoW}$ from Equation 31, $Q_{(i,t),t+1}^{PoW}$ from Equation 35, P_{t+2}^{PoW} indirectly via Equation 32, and π^{PoW} from Equation 34 delivers Condition 36 and thereby completes the proof. □

A.3 Proof of Proposition 3.3

Proof. The set of staking nodes, $\{S_t\}_{t\geqslant 0}$, is given directly as a function of the PoS adoption cutoff, c^{PoS}, by Equation 26. Further, applying Equation 37 to Equation 30 yields the equilibrium one-period-ahead blockchain survival probability 38.

Finally, combing Equations 21, 28, 31 and 32 yields the equilibrium holdings for each agent. In particular, $Q^{PoS}_{(i,t),t} = \frac{1}{P^{PoS}_t}$ which we derive as 39 by using $P^{PoS}_t = \frac{\mathcal{M}^{PoS}}{M_t}$, $M_t = e^{\rho t}$, and substituting the equilibrium market value $\mathcal{M}^{PoS}$ given by 32. In order to derive 40 we use 28, which after plugging in the the optimal fees from 31 and substituting $\frac{1}{P^{PoS}_{t+1}} = \frac{e^{\rho t}}{\mathcal{M}^{PoS}}$ and rearranging yields

$$\frac{1}{G(c^{PoS}) \times \mathcal{M}^{PoS}}(G(c^{PoS})e^{\rho t} + e^{\rho t+1}(R_{t+1}P^{PoS}_{t+1} + \frac{1}{\Lambda}\int\limits_0^{c^{PoS}}\int\limits_0^{c} x \; dG(x) \; dG(c))) \tag{8}$$

Then, we use the fact that $R_{t+1}P^{PoS}_{t+1} = \mathcal{M}^{PoS}(e^{\rho} - 1)$ and again substituting $\mathcal{M}^{PoS}$ from 32 into this expression implies that

$$R_{t+1}P^{PoS}_{t+1} + \frac{1}{\Lambda}\int\limits_0^{c^{PoS}}\int\limits_0^{c} x \; dG(x) \; dG(c) = G(c^{PoS})(e^{\rho} - e^{-\rho}) + e^{\rho}\frac{1}{\Lambda}\int\limits_0^{c^{PoS}}\int\limits_0^{c} x \; dG(x) \; dG(c)$$

Thus, after plugging this expression into 8 and rearranging we have derived our expression for $Q^{PoS}_{(i,t),t+1}$ in 40.

Finally, plugging in the explicit solutions for $f^{PoS}_{(i,t)}$ from Equation 31, for $Q^{PoS}_{(i,t),t+1}$ from Equation 40, for P^{PoS}_{t+2} indirectly via Equation 32, and for π^{PoS} from Equation 38 delivers Condition 41 and thereby completes the proof.

□

A.4 Proof of Proposition 4.1

Proof. We prove this result constructively. In particular, let $\underline{\Lambda}^{PoW} = \frac{2}{\sigma} \times \int\limits_0^{\infty} x \; dG(x)$. Then, for $\Lambda \geqslant \underline{\Lambda}^{PoW}$, taking $\rho = 0$ in the left-hand side of the consequent of Condition 36:

$$
\begin{aligned}
&U_{(i,t)}^{PoW} \\
&= (\min\{\tfrac{1}{\Lambda}\int\limits_{0}^{c^{PoW}}\int\limits_{0}^{c} x\ dG(x)\ dG(c), 1\})^2 \times \{1 - \tfrac{1}{\Lambda}\int\limits_{0}^{c_{(i,t)}} x\ dG(x) - \tfrac{c_{(i,t)}}{\Lambda} \times [G(c^{PoW}) - G(c_{(i,t)})]^+\} \\
&\leqslant \min\{\tfrac{1}{\Lambda}\int\limits_{0}^{c^{PoW}}\int\limits_{0}^{c} x\ dG(x)\ dG(c), 1\} \\
&\leqslant \min\{\tfrac{1}{\underline{\Lambda}^{PoW}}\int\limits_{0}^{c^{PoW}}\int\limits_{0}^{c} x\ dG(x)\ dG(c), 1\} \\
&\leqslant \min\{\tfrac{\sigma}{2}, 1\} \\
&= \tfrac{\sigma}{2}
\end{aligned}
$$

which implies that $U_{(i,t)}^{PoW} < \sigma$ for all (i,t) so that Condition 36 holds if and only if $c^{PoW} = 0$ (i.e., no adoption is the unique equilibrium).

In turn, in that unique equilibrium, Equation 34 implies:

$$
\begin{aligned}
&\pi^{PoW} = \min\{\tfrac{1}{\Lambda}\int\limits_{0}^{c^{PoW}}\int\limits_{0}^{c} x\ dG(x)\ dG(c), 1\} \leqslant \min\{\tfrac{1}{\Lambda}\int\limits_{0}^{c^{PoW}}\int\limits_{0}^{c^{PoW}} x\ dG(x)\ dG(c), 1\} \\
&= \min\{\tfrac{1}{\Lambda}\int\limits_{0}^{0}\int\limits_{0}^{0} x\ dG(x)\ dG(c), 1\} = \min\{0, 1\} = 0
\end{aligned}
$$

which establishes the desired result. □

A.5 Proof of Proposition 4.2

Proof. Proposition 4.4 proves this result for a general value of $\rho \geqslant 0$, so this result follows trivially as a corollary of that result. The proof of Proposition 4.4 is given below in Section A.7. □

A.6 Proof of Proposition 4.3

Proof. We establish the result in two cases: (i) $\rho \geqslant \log\sqrt{\frac{1}{\sigma}}$ and (ii) $\rho < \log\sqrt{\frac{1}{\sigma}}$.

Case (i): $\rho \geqslant \log\sqrt{\frac{1}{\sigma}}$

In this case, we proceed by construction and set $\underline{\Lambda_\rho}^{PoW} = 1$. Then, taking the consequent of Condition 36, we have that:

$$U^{PoW}_{(i,t)}$$

$$= (\min\{(1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda} \int\limits_0^{c^{PoW}} \int\limits_0^{c} x \; dG(x) \; dG(c), 1\})^2 \times \{e^{-2\rho} - \tfrac{1}{\Lambda} \int\limits_0^{c_{(i,t)}} x \; dG(x) - \tfrac{c_{(i,t)}}{\Lambda} \times [G(c^{PoW}) - G(c_{(i,t)})]^+\}$$

$$\leqslant e^{-2\rho} - \tfrac{1}{\Lambda} \int\limits_0^{c_{(i,t)}} x \; dG(x) - \tfrac{c_{(i,t)}}{\Lambda} \times [G(c^{PoW}) - G(c_{(i,t)})]^+$$

$$\leqslant e^{-2\rho}$$

$$\leqslant \sigma$$

Then, $U^{PoW}_{(i,t)} \leqslant \sigma$ for all (i,t) so that $c^{PoW} = 0$. Moreover, Equation 34 implies:

$$\pi^{PoW}$$

$$= \min\{(1 - e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda} \int\limits_0^{c^{PoW}} \int\limits_0^{c} x \; dG(x) \; dG(c), 1\}$$

$$\leqslant \min\{G(c^{PoW}) + \tfrac{1}{\Lambda} \int\limits_0^{c^{PoW}} \int\limits_0^{c^{PoW}} x \; dG(x) \; dG(c), 1\}$$

$$= \min\{G(0) + \tfrac{1}{\Lambda} \int\limits_0^{0} \int\limits_0^{0} x \; dG(x) \; dG(c), 1\}$$

$$= \min\{0, 1\}$$

$$= 0$$

as desired. Finally, $\limsup\limits_{\Lambda\to\infty} \; \pi^{PoW} = \limsup\limits_{\Lambda\to\infty} \; 0 = 0 \leqslant 1 - \sigma < 1$ which completes the proof for this case.

Case (ii): $\rho < \log\sqrt{\frac{1}{\sigma}}$

$\rho < \log\sqrt{\frac{1}{\sigma}} \implies 1 - e^{-2\rho} < 1 - \sigma$. Let $\varepsilon_\rho \equiv (1 - \sigma) - (1 - e^{-2\rho}) > 0$. Then, note that $\lim\limits_{\Lambda\to\infty} \frac{1}{\Lambda} \int\limits_0^{\infty} x \; dG(x) = 0$ such that, for each $\rho < \log\sqrt{\frac{1}{\sigma}}$, there exists some $\underline{\Lambda_\rho}^{PoW} > 0$ for which $\Lambda > \underline{\Lambda_\rho}^{PoW}$ implies $\frac{1}{\Lambda} \int\limits_0^{\infty} x \; dG(x) \leqslant \frac{\varepsilon_\rho}{2}$. Then, proceeding with a constructive proof, for any ρ and any $\Lambda > \underline{\Lambda_\rho}^{PoW}$, Equation 34 implies:

$$\pi^{PoW}$$

$$
\begin{aligned}
&= \min\{(1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x\ dG(x)\ dG(c), 1\} \\
&\leqslant 1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x\ dG(x)\ dG(c) \\
&\leqslant (1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda}\int\limits_0^{c^{PoW}}\int\limits_0^{c} x\ dG(x)\ dG(c) \\
&< 1-e^{-2\rho} + \tfrac{1}{\Lambda}\int\limits_0^{\infty} x\ dG(x) \\
&= 1-\sigma-\varepsilon_\rho + \tfrac{1}{\Lambda}\int\limits_0^{\infty} x\ dG(x) \\
&\leqslant 1-\sigma-\tfrac{\varepsilon_\rho}{2}
\end{aligned}
$$

Accordingly, for any ρ and any $\Lambda > \underline{\Lambda_\rho}^{PoW}$, $\pi^{PoW} < 1$ as desired. Moreover, $\limsup\limits_{\Lambda\to\infty}\ \pi^{PoW} \leqslant \limsup\limits_{\Lambda\to\infty}\ 1-\sigma-\frac{\varepsilon_\rho}{2} = 1-\sigma-\frac{\varepsilon_\rho}{2} < 1-\sigma < 1$ which completes the proof. □

A.7 Proof of Proposition 4.4

Proof. We proceed with a constructive proof. Let $\underline{\Lambda}^{PoS}$ be such that $\Lambda > \underline{\Lambda}^{PoS}$ implies that $\frac{2}{\Lambda}\int\limits_0^{\infty} x\ dG(x) < \frac{1-\sigma}{2}$. Then, for any $\Lambda > \underline{\Lambda}^{PoS}$, using the left-hand side of the consequent of Condition 41:

$$
\begin{aligned}
&\frac{U^{PoS}_{(i,t)}}{(G(c^{PoS}))^2} = 1 + \frac{\frac{1}{\Lambda}\int\limits_0^{c^{PoS}}\int\limits_0^{c} x\ dG(x)\ dG(c)}{G(c^{PoS})} - \frac{1}{\Lambda}\int\limits_0^{c_{(i,t)}} x\ dG(x) - \frac{c_{(i,t)}}{\Lambda}\times[G(c^{PoS}) - G(c_{(i,t)})]^+ \\
&\geqslant 1 - \tfrac{1}{\Lambda}\int\limits_0^{\infty} x\ dG(x) - \tfrac{c_{(i,t)}}{\Lambda}\times[1-G(c_{(i,t)})] \\
&\geqslant 1 - \tfrac{2}{\Lambda}\int\limits_0^{\infty} x\ dG(x) \\
&\geqslant 1 - \tfrac{1-\sigma}{2} \\
&= \tfrac{1+\sigma}{2} \\
&> \sigma
\end{aligned}
$$

which implies that $c^{PoS} = \infty$ satisfies Condition 41 as then $G(c^{PoS}) = 1$ and $U^{PoS}_{(i,t)} > \sigma$ for all (i,t). Then, applying Proposition 3.3, for any $\Lambda > \underline{\Lambda}^{PoS}$, there exists a PoS equilibrium with $c^{PoS} = \infty$. Moreover, in such an equilibrium, Equation 38 implies $\pi^{PoS} = G(c^{PoS}) = G(\infty) = 1$ thereby completing the proof.

□