Economic Implications of Scaling Blockchains: Why the Consensus Protocol Matters

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

January 22, 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 lower fees and thus spend less on computational power. This reduced computational power then lowers 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

[*] 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 with 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 endowed with random wealth, and she seeks to disrupt the transaction activity of the blockchain by investing her wealth for that malicious purpose. Akin to Pagnotta (2020), 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

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

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 that the attacker can create a disruptive chain that becomes arbitrarily longer than the main chain. Our models of 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 composed of coins being held dormant for the period. The PoW governance structure implies that the attacker can gain control of the PoW blockchain only if she possesses more computational power than the sum of all other miners (see, e.g., Nakamoto 2008). In contrast, the PoS governance structure implies that the attacker may gain control of the PoS blockchain only if she possesses more coins than the other stakers (see, e.g., Saleh 2020). 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 increases the likelihood of 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, eventually, the total computational expenditure of a PoW blockchain. In turn, the reduced computational expenditure increases the likelihood that the attacker succeeds in attacking the blockchain. 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 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 succeeds with certainty in her first attack. 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. 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 the attacker cannot mount a successful attack for any plausible level of resources.[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. In particular, one can view a PoS coin as analogous 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

[2] Namely, we show that the attacker would need to have more resources than the entire production in the economy to perform a successful attack when the transaction rate is sufficiently large.

block creation process and the blockchain attack succeeds. In the hostile take-over example, the difficulty of executing the attack arises from the financial cost of the attack in that attempting a take-over of a firm with a large market value involves significant financing costs. Analogously, the difficulty of executing the attack on the blockchain arises from the financial cost of the attack in that successfully attacking a blockchain with a large cryptocurrency market value involves significant financial costs. 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. 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 the rate at which these rewards 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, even for arbitrarily large transaction rates, in that blockchain attacks do not necessarily succeed 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 the attacker will eventually succeed with certainty.

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 (2020) and Saleh (2020), we also provide insights regarding PoS blockchains. Unlike the various referenced papers, we study the economic implications of scaling blockchains and provide findings across 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 agents, hereafter referred to as generation-t agents, being born. We refer to each agent from generation t as Agent (i, t) with $i \in [0, 1]$ denoting the unique identifier for the 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 $\sigma \in (0, 1)$ proportion 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 the act of utilizing the blockchain over the alternative technology as *adoption.*

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 no period $t+2$ consumption. 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. Nonetheless, 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 optimally at the beginning of period $t+2$ according to:

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

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 other agents' fees $f^p_{-(i,t)}$ but we suppress this dependence for ease of notation.

Letting $\pi^p_{t \to t+2} \in [0,1]$ 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 $Q^p_{(i,t),t}$ units of the cryptocurrency and paying fee $f^p_{(i,t)}$— 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 considering 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 enables us to derive the following expression for the expected wait time, $W^p(f, f_{-(i,t)})$:

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

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

[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.

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 user payments denominated in consumption good, and we denote the fee of Agent (i,t) by $f^p_{(i,t)}$. 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, we have that:

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

with M_t denoting the units of cryptocurrency outstanding at the beginning of period t. As a normalization, we assume that the initial cryptocurrency supply is given by $M_0 = 1$. Note then that the block reward B_t distributed across period t is given by:

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

We assume the block reward B_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 consume only in their last period, 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:

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

where we assume 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 assumption 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. Given that mining requires sufficient hardware to solve the computational problem, we make this assumption under the practical limitation that not all agents adopting the blockchain will desire to pursue mining activities (i.e. they will have higher outside options or higher fixed costs to start mining). This assumption will become particularly relevant for blockchains that aim to substitute current transaction systems by generating a large adoption rate. As we discuss subsequently, Equation 8 will not hold in 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 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 cryptocurrencies but not in the terminal period of their life 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 cryptocurrencies cannot stake their coins (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.

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 cryptocurrncy 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:

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

where the rewards and fees are scaled by the probability of receiving them given the number of coins staked by Agent (i, t) and all other agents.

2.3 Attacker

We model a malicious agent, hereafter referred to as an attacker, that seeks to sabotage the blockchain. We follow Pagnotta (2020) and assume that the attacker possesses a use-it-or-lose-it budget in each period and seeks to create a disruptive fork that, if successful, creates a crisis of confidence and renders the blockchain useless thereafter. Formally, we assume that the attacker receives an endowment of consumption good $A_t \sim U[0, 1]$ in period t.[4] The attacker's endowment

[4] Note that $A_t = 1$ represents a scenario whereby the attacker has as many resources than the sum of all agents' endowments in the economy. For this reason we believe this is an appropriate upper bound for the attacker's endowment.

can also be thought of as the random benefit they receive from disrupting the blockchain (and therefore the amount of resources they are willing to expend to do so). The attacker can use her period t endowment, A_t, to acquire resources, computational or financial, to attack the blockchain at time $t+1$ by attempting to create a fork that becomes arbitrarily longer than the main chain in that period. In order to avoid specifying dynamics and beliefs during attacks, we assume that A_t is known at the beginning of each period t and let π_t^p denote the probability that the blockchain survives in period t if it had survived until the beginning of period t. Then, by definition, the following equation holds:

$$\pi^p_{t\to t+2} = \mathbb{E}_t[\pi^p_t \pi^p_{t+1} \pi^p_{t+2}] \tag{11}$$

If the attacker succeeds then we deem the blockchain as having been successfully attacked and no longer an option for transaction activity thereafter. To simplify our analysis, we assume that an attacker attempts the attack only if the attack has a strictly positive probability of succeeding. Additional details regarding security vary by protocol, so we discuss PoW and PoS separately hereafter.

2.3.1 PoW Attacks

For a PoW blockchain, the attacker's ability to create a fork that becomes arbitrarily longer than the main chain depends on her computational power relative to all other miners. Accordingly, if the attacker has a strictly positive probability of succeeding in her attack, she proceeds by acquiring the necessary computational power in period 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 $t+1$, her forked branch grows at a faster rate than the main chain, and her forked branch becomes arbitrarily longer than the main chain with certainty. In that case, her attack succeeds. In contrast, if the attacker possesses less computational power than other miners in period $t+1$, the main chain grows at a faster rate than her forked branch. Moreover, in that case, the likelihood of the attacker's forked branch being (even temporarily) k blocks longer than the main branch vanishes as k diverges so that the likelihood the attacker's branch becomes arbitrarily longer than the main branch is zero an thus her attack fails with certainty. Formally, PoW blockchains possess the following security relationship:

$$\pi_{t+1}^{PoW} = \begin{cases} 0 & \text{if } A_t \geqslant H_{t+1} \\ 1 & \text{if } A_t < H_{t+1} \end{cases} \tag{12}$$

which states that the blockchain survives with probability one whenever the attacker's resources A_t, used to attack the blockchain in period $t+1$, are less than the total amount of resources spent by miners in that period H_{t+1}, and zero otherwise.

2.3.2 PoS Attacks

As shown in Saleh (2020), the attacker's ability to create a disruptive fork within PoS depends upon her share of coins held. Accordingly, if the attacker has a strictly positive probability of succeeding in her attack, she proceeds by acquiring the necessary number of coins in period t and then staking those coins in period $t+1$ to launch an attack in that period. If the attacker has staked more coins than other stakers, then the attacker would be able to grow her forked branch 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. Alternatively, if the attacker has staked fewer coins than the other stakers, then the attacker's forked branch would grow at a slower rate than the main chain and the attacker's forked branch will become arbitrarily longer than the main chain with probability zero so that her attack would fail with certainty. Formally, PoS blockchains possess the following security relationship:

$$\pi_{t+1}^{PoS} = \begin{cases} 0 & \text{if } A_t \geqslant |S_{t+1}| \\ 1 & \text{if } A_t < |S_{t+1}| \end{cases} \tag{13}$$

In order to clarify this expression, note that if the resources of the attacker A_t are greater than the resources of the agents born in generation t that adopt the blockchain, then the attacker will end up with more coins than the generation t users in period $t+1$ (regardless of price) in which case the attack will be successful. Further, the resources of the agents born in generation t that adopt the blockchain are equivalent to $|S_{t+1}|$ as agents born in generation t who adopt the blockchain stake all of their coins in period $t+1$ and start with a unit endowment. Therefore, whenever $A_t \geqslant |S_{t+1}|$ the attacker succeeds at their period $t+1$ attack with certainty and therefore the probability that the blockchain survives is 0, whereas when $A_t < |S_{t+1}|$ then the period $t+1$ attack fails with certainty and the blockchain survives with probability one.

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 are heterogenous according to a 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, there exists an attacker with exogenous resources $A_t \sim U[0,1]$ in each period. 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):

$$c_{(i,t)} < c^p \Leftrightarrow U^p_{(i,t)} = \pi^p \times \mathbb{E}_t[P^p_{t+2} Q^p_{(i,t),t+1} - f^p_{(i,t)} - \frac{c_{(i,t)}}{\Lambda} \int \mathbb{1}\{f^p_{(j,t)} \geqslant f^p_{(i,t)}\}\, dG(c_{(j,t)}) \mid c_{(i,t)}] > \sigma \tag{14}$$

Note that we only multiply the benefit of using the blockchain by the steady state one period ahead probability π^p as the agent observes A_{t-1} and A_t before adopting and therefore knows for sure whether there will be a successful attack in periods t and $t+1$: $\pi^p_s \in \{0,1\}$ once A_{s-1} is known as given by 12 and 13. Therefore, given that Agent (i,t) will never adopt if the chain will be successfully attacked in periods t or $t+1$, which the agent can determine prior to purchasing coin at time t, then the relevant probability for adoption is π^p.

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

$$\text{For all } (i,t) : Q^p_{(i,t),t} = \frac{1}{P^p_t} \tag{15}$$

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:

$$\text{For all } t : |\{(i,t) : U^p_{(i,t)} > \sigma\}| = |\{(i,t) : c_{(i,t)} < c^p\}| = G(c^p) \tag{16}$$

(ii) <u>Equilibrium Fees are Optimal</u>

We require that User (i,t) with realized cost $c_{(i,t)} \in [0,+\infty)$ finds it optimal to pay the fee $f^p_{i,t} = \phi^p(c)$ 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:

$$\text{For all } c: \phi^p(c) = \begin{cases} \underset{f:\ f\geqslant 0}{\arg\max}\ P^p_{t+2}Q^p_{(i,t),t+1} - f - \frac{c}{\Lambda}\int \mathbb{1}\{f^p_{(j,t)} \geqslant f\}\ dG(c_{(j,t)}) & \text{if } c < c^p \\ 0 & \text{if } c \geqslant c^p \end{cases} \tag{17}$$

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 over that period. Therefore, equating these expressions and rearranging we obtain that the cryptocurrency market clears whenever the following condition holds:

$$\text{For all } t: (1 + e^{-\rho})G(c^p) + \int f^p_{(i,t-2)}\ dG(c_{(i,t-2)}) = \mathcal{M}^p \tag{18}$$

(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:

$$\text{For all } t: H = (B_t + \frac{\int f^{PoW}_{(i,t-2)}\ dG(c_{(i,t-2)})}{P^{PoW}_t}) \times P^{PoW}_{t+1} \tag{19}$$

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

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:

$$\text{For all } t: S_t = \{(i, t-1) : c_{(i,t-1)} < c^{PoS}\} \tag{20}$$

(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:

$$\text{For all } (i,t): Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} \tag{21}$$

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

$$\text{For all } (i,t): Q^{PoS}_{(i,t),t+1} = Q^{PoS}_{(i,t),t} + B_{t+1}\,\frac{1}{G(c^{PoS})} + \frac{\int f^{PoS}_{(i,t-1)}\ dG(c_{(i,t-1)})}{P^{PoS}_{t+1}}\ \frac{1}{G(c^{PoS})} \tag{22}$$

(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 the following equation holds:

$$\text{For all } t: \pi^{PoW} = \mathbb{P}(A_t < H) = \min\{H, 1\} \tag{23}$$

In a PoS Equilibrium, the one-period-ahead blockchain survival probability varies with the adoption rate, given by c^{PoS}, so that the following equation holds:

$$\text{For all } t: \pi^{PoS} = \mathbb{P}(A_t < G(c^{PoS})) = G(c^{PoS}) \tag{24}$$

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:*

$$\textit{For all } (i,t) : f^{p}_{(i,t)} = \begin{cases} \frac{1}{\Lambda} \int\limits_{0}^{c_{(i,t)}} x \; dG(x) & \textit{if } c_{(i,t)} < c^{p} \\ 0 & \textit{if } c_{(i,t)} \geqslant c^{p} \end{cases} \tag{25}$$

and

$$\mathcal{M}^{p} = (1 + e^{-\rho})G(c^{p}) + \frac{1}{\Lambda} \int\limits_{0}^{c^{p}} \int\limits_{0}^{c} x \; dG(x) \; dG(c) \tag{26}$$

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*

$$H = (1 - e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int\limits_{0}^{c^{PoW}} \int\limits_{0}^{c} x \; dG(x) \; dG(c) \tag{27}$$

$$\pi^{PoW} = \min\{(1 - e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int\limits_{0}^{c^{PoW}} \int\limits_{0}^{c} x \; dG(x) \; dG(c), 1\} \tag{28}$$

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

$$Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} = \frac{e^{\rho t}}{(1 + e^{-\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int\limits_{0}^{c^{PoW}} \int\limits_{0}^{c} x \; dG(x) \; dG(c)} \tag{29}$$

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

$$U_{(i,t)}^{PoW} = \min\{(1-e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda}\int\limits_{0}^{c^{PoW}}\int\limits_{0}^{c} x\ dG(x)\ dG(c), 1\}$$
$$\times(e^{-2\rho} - \frac{1}{\Lambda}\int\limits_{0}^{c_{(i,t)}} x\ dG(x) - \frac{c_{(i,t)}}{\Lambda}\times(G(c^{PoW}) - G(c_{(i,t)}))) \tag{30}$$

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* $U_{(i,t)}^{PoS} > \sigma$*. The equilibrium set of stakers* S_t *and one period ahead blockchain survival probability* π^{PoS} *are given by*

$$S_t = \{(i,t) : c_{(i,t)} < c^{PoS}\} \quad \textit{for all } t \tag{31}$$

and

$$\pi^{PoS} = G(c^{PoS}) \tag{32}$$

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

$$Q_{(i,t),t}^{PoS} = \frac{e^{\rho t}}{(1+e^{-\rho})G(c^{PoS}) + \frac{1}{\Lambda}\int\limits_{0}^{c^{PoS}}\int\limits_{0}^{c} x\ dG(x)\ dG(c)} \tag{33}$$

and

$$Q_{(i,t),t+1}^{PoS} = \frac{e^{\rho(t+2)}}{G(c^{PoS})} \times \frac{G(c^{PoS}) + \frac{1}{\Lambda}\int\limits_{0}^{c^{PoS}}\int\limits_{0}^{c} x\ dG(x)\ dG(c)}{(1+e^{-\rho})G(c^{PoS}) + \frac{1}{\Lambda}\int\limits_{0}^{c^{PoS}}\int\limits_{0}^{c} x\ dG(x)\ dG(c)} \tag{34}$$

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

$$U_{(i,t)}^{PoS} = G(c^{PoS}) \times (1 + \frac{\frac{1}{\Lambda} \int\limits_{0}^{c^{PoS}} \int\limits_{0}^{c} x \; dG(x) \; dG(c)}{G(c^{PoS})} - \frac{1}{\Lambda} \int\limits_{0}^{c_{(i,t)}} x \; dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (G(c^{PoS}) - G(c_{(i,t)}))) \tag{35}$$

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 25, users adopting the blockchain pay an equilibrium fee, $f_{(i,t)}^{PoW}$, given by:

$$f_{(i,t)}^{PoW} = \frac{1}{\Lambda} \int\limits_{0}^{c_{(i,t)}} x \; dG(x) \tag{36}$$

Equation 36 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 associated with this incremental fee paid, $\frac{n}{\Lambda}$, 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 equilibrium fees monotonically decrease towards zero as the scale of the blockchain improves.

This relationship between equilibrium fees and the blockchain's transaction rate has important implications for security. To intuit that point, we reproduce Equation 19 except with no block rewards:

$$H = \int f^{PoW}_{(i,t-2)}\, dG(c_{(i,t-2)}) = \frac{1}{\Lambda}\int_0^{c^p}\int_0^{c} x\, dG(x)dG(c) \tag{37}$$

Equation 37 highlights that, absent block rewards, the PoW blockchain's computational power is financed entirely by fee revenue. Accordingly, an increase in the blockchain's transaction rate, for a sufficiently high 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}, would fall 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 relevant for securing PoS blockchains. To understand this last point, we revisit our analogy of 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 powers 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 26 (using $\rho = 0$), that as the blockchain's transaction rate diverges (i.e., $\Lambda \rightarrow \infty$), the cryptocurrency market value for a PoS blockchain, $\mathcal{M}^{PoS}$, adheres to the following equation:

$$\lim_{\Lambda \rightarrow \infty} \mathcal{M}^{PoS} = G(c^{PoS}) \tag{38}$$

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 32.

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 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 resources of the attacker cannot exceed the total production of the entire economy in a given period (i.e., $A_t \leqslant 1$ a.s.). Thus, a sufficiently high transaction rate ensures full adoption which ensures that any attack fails with certainty. 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 that the cryptocurrency supply evolves with a growth 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 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.[5] 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 26 and 29, one can derive that the proceeds from Agent (i, t)'s period $t + 2$ sale of her cryptocurrency holdings is given by:

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

$$P_{t+2}^{PoW} Q_{(i,t),t+1}^{PoW} = e^{-2\rho} \tag{39}$$

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:

$$\underbrace{e^{-2\rho}}_{Max\ Consumption\ From\ Blockchain} > \underbrace{\sigma}_{Consumption\ From\ Alternative\ Technology} \tag{40}$$

If Equation 40 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 (i.e., $H = 0$ and therefore $\pi^{PoW} = 0$) as a result. 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:

$$\rho < \log \sqrt{\frac{1}{\sigma}} \tag{41}$$

Importantly, Equation 41 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 diverges (i.e., $\Lambda \to \infty$), Equation 27 implies that the blockchain's computational power, H, adheres to the following equation:

$$\lim_{\Lambda \to \infty} H = (1 - e^{-2\rho}) G(c^{PoW}) \tag{42}$$

Using our restriction on the block reward from Equation 41 and invoking Equation 12 therefore implies:

$$\lim_{\Lambda \to \infty} \pi^{PoW} \leqslant 1 - \sigma < 1 \tag{43}$$

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 26 and 34 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:

$$\lim_{\Lambda \to \infty} P_{t+2}^{PoS} Q_{(i,t),t+1}^{PoS} = 1 \tag{44}$$

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 44 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.

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. Taken together, this paper highlights the need for further work on alternative protocols, particularly PoS.

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.

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.

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* .

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* .

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. Bitcoin as Decentralized Money: Prices, Mining Rewards, and Network Security. *Working Paper* .

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

Rosu, I., and F. Saleh. 2020. Evolution of Shares in a Proof-of-Stake Cryptocurrency. *Management Science* Forthcoming.

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

Saleh, F. 2020. Blockchain without Waste: Proof-of-Stake. *The Review of Financial Studies* URL https://doi.org/10.1093/rfs/hhaa075. Hhaa075.

Appendices

A Proofs

A.1 Proof of Lemma 3.1

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

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

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 25.

Then, applying Equation 25 to Equation 18 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 apply Equations 25 and 26 to Equation 19, yielding:

$$H = (1 - e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int\limits_{0}^{c^{PoW}} \int\limits_{0}^{c} x \; dG(x) \; dG(c) \tag{5}$$

Moreover, applying Equation 27 to Equation 23 yields the equilibrium one-period-ahead blockchain survival probability:

$$\pi^{PoW} = \min\{(1 - e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int\limits_{0}^{c^{PoW}} \int\limits_{0}^{c} x \; dG(x) \; dG(c), 1\} \tag{6}$$

Combing Equations 15, 21 and 26 yields the equilibrium holdings for each agent that adopts the blockchain:

$$\text{For all } (i,t) : Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} = \frac{e^{\rho t}}{(1 + e^{-\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int\limits_{0}^{c^{PoW}} \int\limits_{0}^{c} x \; dG(x) \; dG(c)} \tag{7}$$

Finally, plugging in the explicit solutions for $f^{PoW}_{(i,t)}$ from Equation 25, $Q^{PoW}_{(i,t),t+1}$ from Equation 29, P^{PoW}_{t+2} indirectly via Equation 26, and π^{PoW} from Equation 28 delivers Condition 30 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 20. Further, applying Equation 31 to Equation 24 yields the equilibrium one-period-ahead blockchain survival probability 32. Finally, combing Equations 15, 22, 25 and 26 yields the equilibrium holdings for each agent. Finally, plugging in the explicit solutions for $f^{PoS}_{(i,t)}$ from Equation 25, for $Q^{PoS}_{(i,t),t+1}$ from Equation 34, for P^{PoS}_{t+2} indirectly via Equation 26, and for π^{PoS} from Equation 32 delivers Condition 35 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 30:

$$\begin{aligned}
&U^{PoW}_{(i,t)} \\
&= \min\{\tfrac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x \; dG(x) \; dG(c), 1\} \times \{1 - \tfrac{1}{\Lambda} \int_0^{c_{(i,t)}} x \; dG(x) - \tfrac{c_{(i,t)}}{\Lambda} \times [G(c^{PoW}) - G(c_{(i,t)})]^{+}\} \\
&\leqslant \min\{\tfrac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x \; dG(x) \; dG(c), 1\} \\
&\leqslant \min\{\tfrac{1}{\underline{\Lambda}^{PoW}} \int_0^{c^{PoW}} \int_0^{c} x \; dG(x) \; dG(c), 1\} \\
&\leqslant \min\{\tfrac{\sigma}{2}, 1\} \\
&= \tfrac{\sigma}{2}
\end{aligned}$$

which implies that $U^{PoW}_{(i,t)} < \sigma$ for all (i,t) so that Condition 30 holds if and only if $c^{PoW} = 0$ (i.e., no adoption is the unique equilibrium).

In turn, in that unique equilibrium, Equation 28 implies:

$$\begin{aligned}
&\pi^{PoW} = \min\{\tfrac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x \; dG(x) \; dG(c), 1\} \leqslant \min\{\tfrac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c^{PoW}} x \; dG(x) \; dG(c), 1\} \\
&= \min\{\tfrac{1}{\Lambda} \int_0^{0} \int_0^{0} x \; dG(x) \; dG(c), 1\} = \min\{0, 1\} = 0
\end{aligned}$$

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 30, we have that:

$U_{(i,t)}^{PoW}$

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

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

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

$\leqslant \sigma$

Then, $U_{(i,t)}^{PoW} \leqslant \sigma$ for all (i,t) so that $c^{PoW} = 0$. Moreover, Equation 28 implies:

π^{PoW}

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

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

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

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

$= 0$

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.

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

$\rho < \log\sqrt{\frac{1}{\sigma}} \implies 1 - e^{-2\rho} < 1 - \sigma$. 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 28 implies:

π^{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 35:

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

which implies that $c^{PoS} = \infty$ satisfies Condition 35 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 32 implies $\pi^{PoS} = G(c^{PoS}) = G(\infty) = 1$ thereby completing the proof.

□