FTG Working Paper Series

Economic Implications of Scaling Blockchains

by

Fahad Saleh
Kose John
Thomas Rivera

Working Paper No. 00075-01

Finance Theory Group

www.financetheory.com

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

Kose John† Thomas J. Rivera‡ Fahad Saleh§

October 24, 2022

Abstract

We compare the economic implications of scaling blockchains under the Proof-of-Work (PoW) and Proof-of-Stake (PoS) consensus protocols. We study an economic model whereby agents store wealth on the blockchain and pay fees to expedite their transactions while a malicious agent attempts to compromise the blockchain's security. Improved scaling alleviates congestion, leading to a decrease in equilibrium fees. Under a PoW protocol, this effect lowers the equilibrium expenditure on mining and therefore the security of the PoW blockchain. In contrast, scaling has the opposite effect for the PoS protocol since alleviating congestion increases cryptocurrency demand which 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, Narayana Kocherlakota, Baixiao Liu, Alan Moreira, Christian Opp, Andreas Park, Julien Prat, Quentin Vandeweyer, Ganesh Viswanath-Natraj and seminar participants at the CISDM Conference, ETH Zurich, Monash Business School, UPenn Wharton, the University of Calgary, the University of Rochester, Wake Forest University, 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

Wide user adoption of a blockchain technology depends crucially on the blockchain's scale and security. High scale blockchains (i.e., those with high transaction rates) are intended to bring fast transaction processing to users and therefore to enhance user utility and blockchain adoption. Yet, in order for an increase in the blockchain's scale to improve blockchain adoption, it must be the case that increasing the blockchain's scale does not sufficiently undermine its security. In this paper, we derive the relationship between blockchain scale and security and demonstrate that this relationship crucially depends on the blockchain consensus protocol, i.e., the set of rules that are utilized to govern the blockchain.

We provide the first comparative analysis across the two most commonly utilized blockchain consensus protocols, Proof-of-Work (PoW) and Proof-of-Stake (PoS), to study the economic implications of scaling blockchains. This analysis is of primary importance given that the consensus protocol determines how new transactions are added to the blockchain and therefore fundamentally affects the relationship among scale, security, and adoption. In particular, our main results show that scaling a blockchain has a qualitatively different effect on security and adoption depending on whether the blockchain is governed by PoW or PoS. More explicitly, we establish that improvements in the blockchain's scale can undermine security and adoption for a PoW blockchain, whereas increasing the blockchain's scale enhances security and adoption for a PoS blockchain.

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 transactions 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 from a malicious agent, hereafter referred to as an attacker. The attacker is deep pocketed and possesses an ex-ante random benefit, drawn each period, from successfully disrupting the transaction activity of the blockchain. After learning her realized benefit, the attacker determines the optimal resources to expend in that period to perform such an attack. We assume that a successful attack in any period renders the blockchain inoperable thereafter. Therefore, any user with cryptocurrency holdings 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 not only the cost of waiting and paying fees but also the probability that the blockchain is compromised by an attack.

Successfully attacking the blockchain requires the attacker to gain *control* of the blockchain in a 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 longer than the main chain. The PoW and PoS protocols 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 PoW protocol implies that the attacker can gain control of the PoW blockchain if she expends at least as much computational power as the sum of all other miners, whereas the PoS protocol implies that the attacker can gain control of the PoS blockchain only if she purchases and stakes at least as many coins as the other stakers. Our equilibrium analysis relies upon endogenously deriving both the computational power spent in mining and the market value of coins used for staking.

As an incentive for updating the blockchain with new transactions, validators receive not only the fees that agents pay to receive priority but also *block rewards* which are newly issued coins. We first study the case whereby the cryptocurrency supply is constant so that there are no block rewards

(a case corresponding to Bitcoin's eventual block reward schedule). In this context, Proposition 4.1 establishes that PoW blockchains become *fully insecure* for a sufficiently high transaction rate. This implies that for a high enough transaction rate the attacker succeeds in any attack with certainty so that the PoW blockchain is rendered inoperable. In contrast, Proposition 4.2 establishes that PoS blockchains attain full security for a sufficiently high transaction rate. This implies that for a high enough transaction rate the attacker never succeeds in any attack on the PoS blockchain so that the PoS blockchain always remains operable.

The aforementioned results rely on the fact that an increase in the blockchain's transaction rate reduces the equilibrium fees paid by the users. 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 acquire a sufficient proportion of coins needed to successfully attack the PoS blockchain.

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 transaction 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 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, each transaction receives immediate processing irrespective of its fee payment and thus the incentive to

pay any fee is entirely absent, implying that all equilibrium fees are identically zero in that case. More generally, equilibrium 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 a successful attack occurs in equilibrium. Moreover, a sufficiently high transaction rate renders a PoW blockchain entirely insecure because the 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, since no agents use the blockchain (i.e., zero adoption), 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, the cost of which is proportional to the market value of the cryptocurrency, an endogenous quantity that 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 therefore the attacker never finds it profitable to mount such an attack. 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

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 take-over arises from the fact that executing a take-over of a firm with a large market value involves significant financial costs to purchase a sufficient share of the firm's equity. Analogously, the difficulty of executing an 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 value 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 well governed 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 in that 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 successful 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. In that context, Proposition 4.5 generalizes our results for the PoS blockchain and establishes the same result — a sufficiently high blockchain transaction rate induces full security in the PoS blockchain. On the other hand, for a PoW blockchain, Proposition 4.3 demonstrates how block rewards can generate *some* level of security but that the PoW security level is bounded away from full security.

To understand Proposition 4.3 and 4.5, recall that block rewards correspond to new units of cryptocurrency so that they serve as an inflationary transfer from holders of the cryptocurrency to those receiving the block rewards. In a PoW blockchain, the holders of the cryptocurrency are the blockchain users whereas the recipients of the block rewards are miners, implying that PoW

block rewards constitute an inflationary tax on users and consequently serve as a disincentive for user adoption. In turn, Proposition 4.3 establishes that block rewards cannot resolve the PoW security issue highlighted by Proposition 4.1 because increasing block rewards beyond a certain point will impose a sufficiently large inflationary tax upon users leading to zero adoption of the PoW blockchain and thus zero mining revenues and full insecurity (see Lemma 4.4). Hence, PoW security necessarily relies on the block rewards not exceeding a hard upper bound, and Proposition 4.3 demonstrates that this maximal block reward suffices to only generate partial security. In contrast to a PoW blockchain, a PoS blockchain distributes the revenues from the inflationary tax imposed by block rewards back to the users since PoS blockchain validators are the users. As a consequence, changes in PoS block rewards do not affect the utility of the PoS users in that the inflationary tax imposed on any user by PoS block rewards is exactly offset by the gain received by that user from accruing block rewards (see Lemma 4.6). Then, since user payoffs are invariant to the the level of block rewards in a PoS blockchain, the security of a PoS blockchain with block rewards is guaranteed for sufficiently high blockchain scale for the same reason that PoS security is guaranteed without block rewards as per Proposition 4.2.

Propositions 4.1 - 4.5 focus upon blockchains with large transaction rates, establishing that high scale PoS blockchains generate higher security than high scale PoW blockchains. We conclude by generalizing that comparative insight for any scale of the blockchain. In particular, Proposition 4.7 demonstrates that a PoS blockchain of *arbitrary* scale generates higher security than a PoW blockchain of the same scale. Our work thus establishes that PoS blockchains possess a generic security advantage over PoW blockchains (Proposition 4.7) and that this advantage is most stark when the blockchain possesses a high transaction rate (Propositions 4.1 - 4.5).

Our paper provides the first model of PoS that explicitly incorporates security. In providing such a model, it is convenient to abstract away from staking costs, but we nonetheless emphasize that our main insight holds even in the presence of such costs. More formally, in Appendix A, we allow for an explicit cost of staking, and we generalize our main insight regarding PoS in that context. More precisely, we provide a formal result, Proposition A.1, which demonstrates that a PoS blockchain obtains full security for a sufficiently high scale even with an explicit cost of staking. We note that Proposition A.1 arises under the condition that the PoS protocol pays a block reward above some minimal threshold. Importantly, our earlier results show that block rewards cannot

similarly generate full security for a PoW blockchain. In particular, as previously mentioned, PoW block rewards imply an inflationary tax on users and thus block rewards undermine PoW adoption and PoW security (see Lemma 4.4). In contrast, since PoS users who stake receive the revenues from the inflationary tax (i.e., the block rewards), staking enables a PoS user to avoid the inflationary cost of block rewards. As a consequence, when PoS block rewards are sufficiently high with respect to the cost of staking then all users who hold the cryptocurrency find it optimal to stake implying that the set of agents who pay the inflationary tax from block rewards are equal to the set of agents who receive the block rewards. When this is the case, PoS user utility is invariant to block rewards as in Lemma 4.6 and thus Proposition A.1 follows based on similar economic reasoning as Propositions 4.2 and 4.5.

Our paper relates to a large literature that studies the economics of blockchain protocols. The interested reader may consult John et al. (2022b) for a survey of that literature. Particular papers within the literature that are especially related include papers examining blockchain adoption (e.g., Cong et al. 2021b and Hinzen et al. 2022), papers studying blockchain security (e.g., Biais et al. 2019, Saleh 2021, Garratt and van Oordt 2022 and Pagnotta 2022) and papers modeling key blockchain microstructure elements (e.g., Easley et al. 2019, Huberman et al. 2021 and Basu et al. 2022). Our work builds upon prior literature from a theoretical standpoint in that we provide the first model that determines user fees and adoption decisions endogenously while also explicitly incorporating security. Additionally, we are the first to analyze how the implications of scaling upon security and adoption vary by blockchain protocol.

Of note, the literature that studies blockchain protocols also examines other topics on which we do not focus. In particular, a variety of papers study the industrial organization of either PoW mining or PoS staking. Prominent papers examining the industrial organization of PoW mining include Alsabah et al. (2021), Cong et al. (2021a), Prat and Walter (2021), and Lehar and Parlour (2021b) while Makarov and Schoar (2022) and Mueller (2020) provide related empirical insights. These PoS papers also consider monetary aspects specific to PoS cryptocurrencies, whereas Jermann and Xiang (2022) and Cong et al. (2022) study issues of monetary policy for cryptocurrencies which do not depend on the underlying blockchain protocol.

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 receives utility from 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 period and trade her cryptocurrency holdings for consumption goods during her last period. 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 from consumption 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 in period $t+2$. 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:

$$\mathcal{U}^p_{(i,t)} = \max\{U^p_{(i,t)}, \sigma\} \tag{2.1}$$

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

The decision for Agent (i,t) to adopt the blockchain technology involves two important concerns. First, the blockchain may be successfully attacked while Agent (i,t) holds the cryptocurrency, thereby precluding future transactions from being added to the blockchain 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 $c_{(i,t)}$ Agent (i,t)'s wait disutility per unit time and 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 $f_{-(i,t)}$. 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 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., $\int_0^\infty c \, dG(c) < \infty$).

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

$$f^p_{(i,t)} = \underset{f:\ f \geqslant 0}{\arg\max} \ \underbrace{P^p_{t+2} Q^p_{(i,t),t+1} - f}_{\text{Consumption}} - \underbrace{c_{(i,t)} W^p(f, f_{-(i,t)})}_{\text{Wait Disutility}} \tag{2.2}$$

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 the end of period $t+2$ conditional upon surviving until the beginning of period t. Then, the expected utility of Agent (i,t) from using the blockchain — i.e., purchasing cryptocurrency units in period t and paying the

fee $f^p_{(i,t)}$ in period $t+2$ — is given by:

$$U^p_{(i,t)} = \pi^p_{t\to t+2} \cdot \mathbb{E}_t[P^p_{t+2} Q^p_{(i,t),t+1} - f^p_{(i,t)} - c_{(i,t)} W^p(f^p_{(i,t)}, f_{-(i,t)}) \mid c_{(i,t)}] \tag{2.3}$$

where we assume that the user receives zero consumption utility in the case that a successful attack occurs after she purchases but before she liquidates. 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 that the cost of the cryptocurrency that Agent (i,t) purchases cannot exceed her initial endowment. We proceed by restricting attention to the case whereby agents store all of their wealth either on the blockchain (full adoption) or through the alternative 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 (except for the marginal user who is indifferent).

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 responsible for creating 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 transactions are continuously accepted to the blockchain in infinitesimally small blocks.[1] This enables us to derive the following expression for the expected wait time, $W^p(f, f_{-(i,t)})$:

$$W^p(f, f_{-(i,t)}) = \underbrace{\frac{1}{\Lambda}}_{\text{Service Time Per User}} \times \underbrace{\int \mathbb{1}\{f^p_{(j,t)} \geqslant f\}\, dG(c_{(j,t)})}_{\text{Higher Paying Users}} \tag{2.4}$$

[1] 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.

Equation (2.4) 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 to 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:

$$M_{t+1} = M_t e^{\rho} \tag{2.5}$$

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:

$$R_t \equiv M_{t+1} - M_t = M_t(e^{\rho} - 1) = e^{\rho t}(e^{\rho} - 1) \tag{2.6}$$

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. The value of block rewards in

period t is given by $R_t P_t^{PoW}$ because R_t denotes the period t block reward denominated in units of cryptocurrency and P_t^{PoW} denotes the period t price of the cryptocurrency. Moreover, the value of fees paid in period t is given by $\int f^p_{(i,t-2)} dG(c_{(i,t-2)})$ because the agents paying fees in period t are those who were born in period $t-2$.

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. We assume the mining market is competitive, implying that the following free entry condition must hold in equilibrium:

$$\underbrace{H_t}_{\text{Mining Cost}} = \underbrace{R_t P_t^{PoW}}_{\text{Block Rewards}} + \underbrace{\int f^{PoW}_{(i,t-2)} \, dG(c_{(i,t-2)})}_{\text{User Fees}} \tag{2.7}$$

where we assume that the coins received by miners in a given period are sold at the end of that period. In addition, we assume that miners incur no intra-period dis-utility from waiting, which implies that they pay no fees for their transactions.

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

$$Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} \tag{2.8}$$

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.[2]

2.2.2 PoS Blockchain

A PoS blockchain involves no computational puzzle. Rather, a PoS protocol randomly selects a coin from a set of *staked* coins, each of which the associated coin owner opted to place in the set.

[2]In particular, including users as miners would only lower the amount of total wealth stored on the PoW blockchain as a fraction of user wealth would need to be spent on mining. This has the effect of lowering the total amount of wealth stored on the PoW blockchain which lowers the overall value of 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 our results remain unchanged.

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:

$$S_t = \{(i, t-1) : U^{PoS}_{(i,t-1)} > \sigma\} \tag{2.9}$$

which states that all agents who are born in period $t-1$ and adopt the blockchain stake in period t and no other agents stake in period t. This condition arises because agents born in period t cannot stake, whereas agents born in period $t-2$ do not find staking incentive-compatible. In particular, staking a coin in period t requires ownership of the coin at the beginning of period t, and an agent arriving in period t cannot acquire ownership of a coin until her transaction enters the blockchain which necessarily occurs during period t. Additionally, any agent born in period $t-2$ is in the terminal period of her life so that staking in period t would entail forgoing current period consumption with no opportunity for future consumption, implying that liquidating her holdings for consumption is preferable to staking in period t. In contrast to agents born in period $t-2$ and period t, agents born in period $t-1$ own coins and are in the intermediate period of their lives so that staking enables them to accrue revenues that would yield additional consumption in the terminal period of their lives. Thus, only agents born in period $t-1$ stake coins in period t, and such agents stake if and only if they hold coins (i.e., if they adopt the blockchain), which occurs endogenously for Agent $(i, t-1)$ if and only if $U^{PoS}_{(i,t-1)} > \sigma$.

Our baseline model abstracts from staking costs, which are generally small in practice, but we show that our results hold even with the inclusion of such costs. More formally, we explicitly incorporate staking costs in Appendix A and generalize our main findings regarding PoS to that setting via Proposition A.1.

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:

$$\Delta Q_{(i,t)}^{PoS} = \underbrace{R_{t+1} \times \frac{Q_{(i,t),t}^{PoS}}{\int_{S_{t+1}} Q_{(i,t),t}^{PoS}\, dG(c_{(i,t)})}}_{\text{Block Reward Accrued}} + \underbrace{\frac{\int f_{(i,t-1)}^{PoS}\, dG(c_{(i,t-1)})}{P_{t+1}^{PoS}} \times \frac{Q_{(i,t),t}^{PoS}}{\int_{S_{t+1}} Q_{(i,t),t}^{PoS}\, dG(c_{(i,t)})}}_{\text{Fees Accrued}} \tag{2.10}$$

where

$$\Delta Q_{(i,t)}^{PoS} \equiv \underbrace{Q_{(i,t),t+1}^{PoS}}_{\text{Period t+1 Holding}} - \underbrace{Q_{(i,t),t}^{PoS}}_{\text{Period t Holding}} \tag{2.11}$$

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 (2.10) equal the total rewards and fees multiplied by the probability that Agent (i,t) receives the rewards and fees for a given block. This is because our analysis considers the limiting case of infinitely many blocks of infinitesimal size, which implies that while a staker receiving the rewards and fees from a particular block is random, the total rewards and fees accrued in a period is nonetheless non-random. In turn, the realized rewards and fees accrued by Agent (i,t) equals the expected rewards and fees accrued by Agent (i,t) (i.e., there is no aggregate risk).

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 (2022), we assume that an attack succeeds if and only if the attacker is able to make her forked branch arbitrarily longer than the main chain.[3] Also following Pagnotta (2022), we assume that if the blockchain is successfully attacked in any period then it incurs a crisis of confidence and is no longer operable thereafter. 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.

[3]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.

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, a PoW attack requires the purchase of significant computational power beforehand, whereas a PoS attack requires the purchase of PoS coins beforehand. As a consequence, we assume 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 the beginning of period t the attacker learns the value $B_t \sim U[0, \overline{B}]$ which represents her benefit, denominated in consumption goods, from successfully disrupting the blockchain at the beginning of period $t+1$, with $\overline{B} > 0$ the maximal benefit she can receive from doing so.

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 the beginning of period $t+1$. Denote by $\nu^p_{t+1}(A_t)$ the probability that the attacker successfully attacks the blockchain at the beginning of period $t+1$ when using resources A_t to mount the attack, given the protocol $p \in \{PoW, PoS\}$. Then, the attackers problem is:

$$\max_{A_t \geqslant 0} \; B_t \cdot \nu^p_{t+1}(A_t) - A_t \tag{2.12}$$

whereby, we assume that the attacker selects A_t optimally so as to maximize her consumption utility given B_t and the equilibrium 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.

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 at the beginning of period $t+1$. If the attacker possesses (weakly) higher computational power than the other miners in period $t+1$ (i.e., $A_t \geqslant H_{t+1}$), 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 the 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 chain by an arbitrary k blocks vanishes to zero as k diverges so that the attack fails with probability one. Taking these features of PoW blockchains into account, $\nu_{t+1}^{PoW}(A_t)$ is given explicitly by:

$$\nu_{t+1}^{PoW}(A_t) = \begin{cases} 1 & \text{if } A_t \geqslant H_{t+1} \\ 0 & \text{if } A_t < H_{t+1} \end{cases} \tag{2.13}$$

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

$$A_t^{\star}(B_t) = \begin{cases} H_{t+1} & \text{if } B_t \geqslant H_{t+1} \\ 0 & \text{if } B_t < H_{t+1} \end{cases} \qquad \nu_{t+1}^{PoW}(A_t^{\star}(B_t)) = \begin{cases} 1 & \text{if } B_t \geqslant H_{t+1} \\ 0 & \text{if } B_t < H_{t+1} \end{cases} \tag{2.14}$$

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 period $t+1$ attack succeeds with probability 1 and otherwise will not find it optimal to expend any resources to attack the blockchain.

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 a number of coins (weakly) greater than those staked by the users, 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 users, then the attacker's forked branch would grow at a slower rate than the main chain so that her attack will fail with certainty. Accordingly, $\nu_{t+1}^{PoS}(A_t)$

is given explicitly by:

$$\nu_{t+1}^{PoS}(A_t) = \begin{cases} 1 & \text{if } A_t \geqslant |S_{t+1}| \\ 0 & \text{if } A_t < |S_{t+1}| \end{cases} \tag{2.15}$$

As noted in Equation (2.15), the security features of the PoS blockchain imply that whenever 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 zero, 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 who adopt in period t and stake in period $t+1$ and thus $|S_{t+1}|$ also represents the total amount of consumption goods spent by users to purchase coin in period t because each user has a unit endowment. Therefore, in order to mount a successful attack in period $t+1$, the attacker would need to spend $A_t \geqslant |S_{t+1}|$ consumption goods in period t to acquire a number of coins (weakly) greater than those staked by the users. Given these features, the optimal expenditure and success probability of the attacker in a PoS blockchain are given by:

$$A_t^{\star}(B_t) = \begin{cases} |S_{t+1}| & \text{if } B_t \geqslant |S_{t+1}| \\ 0 & \text{if } B_t < |S_{t+1}| \end{cases} \qquad \nu_{t+1}^{PoS}(A_t^{\star}(B_t)) = \begin{cases} 1 & \text{if } B_t \geqslant |S_{t+1}| \\ 0 & \text{if } B_t < |S_{t+1}| \end{cases} \tag{2.16}$$

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, to ensure that the attack succeeds with probability 1, and otherwise does not mount an attack because doing so is not incentive compatible.

2.4 Equilibrium

Akin to Huberman et al. (2021) and Hinzen et al. (2022), 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 storage 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 $B_t \sim U[0, \overline{B}]$ 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 her consumption utility according to Equation (2.12).

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 $f^p_{(i,t)} \equiv \phi^p(c_{(i,t)})$ for each Agent (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 probability π^p indicating the likelihood that the blockchain will not be attacked within an agent's lifetime assuming that the blockchain has not already been successfully attacked, and (7) 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):[4]

$$c_{(i,t)} < c^p \Leftrightarrow U^p_{(i,t)} > \sigma \tag{2.17}$$

[4]Note that this definition of optimal adoption decisions assumes positive adoption in equilibrium whenever any agent receives utility from adoption that is strictly higher than the utility they receive from utilizing the alternative technology. Due to the myopic nature of the agents there always exists a trivial equilibrium with zero adoption, regardless of the fundamentals and consensus protocol, as zero adoption implies zero security (see Propositions 3.2 and 3.3 below) and zero security implies that no user will be willing to adopt the blockchain. In what follows, we strictly focus our attention on the non-trivial positive adoption equilibrium whenever there exists a positive adoption threshold that satisfies (2.17).

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

$$Q^p_{(i,t),t} = \frac{1}{P^p_t} \tag{2.18}$$

with $P^p_t \equiv \frac{\mathcal{M}^p}{M_t}$ defined as the price of the cryptocurrency in period t, and $M_t = e^{\rho t}$ being the units of cryptocurrency outstanding at the beginning of period t. In addition, note 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:

$$\text{For all } t : |\{(i,t) : U^p_{(i,t)} > \sigma\}| = |\{(i,t) : c_{(i,t)} < c^p\}| = G(c^p) \tag{2.19}$$

(ii) Equilibrium Fees are Optimal

We require that Agent (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 agents $(j,t) \neq (i,t)$ pay fees according to $f_{(j,t)} = \phi^p(c_{(j,t)})$. Formally, the following condition holds:

$$\text{For all } c : \phi^p(c) = \begin{cases} \underset{f:\ f \geqslant 0}{\arg\max}\ P^p_{t+2} Q^p_{(i,t),t+1} - f - \frac{c}{\Lambda} \int \mathbb{1}\{f^p_{(j,t)} \geqslant f\}\ dG(c_{(j,t)}) & \text{if } c < c^p \\ 0 & \text{if } c \geqslant c^p \end{cases} \tag{2.20}$$

where agents 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 available supply of cryptocurrency units. This supply differs depending on the blockchain protocol and therefore we specify the market clearing condition for each protocol separately.

PoW: the available supply of cryptocurrency units in period t in a PoW blockchain is the total supply, M_t, minus those held by intermediately aged agents, $\frac{G(c^{PoW})}{P^{PoW}_{t-1}}$, who have no need to liquidate given that they derive no utility from consumption in that period.

PoS: the available supply of cryptocurrency units in period t in a PoS blockchain is the total supply, M_t, minus those paid as fees, $\frac{\int f^{PoS}_{(i,t-2)} dG(c_{(i,t-2)})}{P^{PoS}_t}$, which accumulate to the users that stake and are therefore held until period $t+1$, and minus those held by intermediately aged

agents, $\frac{G(c^{PoS})}{P^{PoS}_{t-1}}$, who again have no need to liquidate until time $t+1$.

Therefore, equating the respective expressions and rearranging, we obtain that the PoW and PoS cryptocurrency market clears whenever the following conditions hold:

$$\begin{aligned} \mathcal{M}^{PoW} &= (1+e^{-\rho})G(c^{PoW}) \\ \mathcal{M}^{PoS} &= (1+e^{-\rho})G(c^{PoS}) + \int f^{PoS}_{(i,t-2)} dG(c_{(i,t-2)}) \end{aligned} \tag{2.21}$$

(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:

$$\text{For all } t: H = R_t P_t + \int f^{PoW}_{(i,t-2)}\ dG(c_{(i,t-2)}) \tag{2.22}$$

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

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

$$\text{For all } t: S_t = \{(i, t-1) : c_{(i,t-1)} < c^{PoS}\} \tag{2.23}$$

(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 users receive neither block rewards nor fees. Formally, the following condition holds:

$$\text{For all } (i,t): Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} \tag{2.24}$$

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

$$\text{For all } (i,t): Q^{PoS}_{(i,t),t+1} = Q^{PoS}_{(i,t),t} + R_{t+1}\ \frac{1}{G(c^{PoS})} + \frac{\int f^{PoS}_{(i,t-1)}\ dG(c_{(i,t-1)})}{P^{PoS}_{t+1}}\ \frac{1}{G(c^{PoS})} \tag{2.25}$$

(vi) Blockchain Survival Probability Varies According To Protocol Rules

Given the attacker's problem, the probability that the blockchain survives through period $t+1$ for any fixed realization of the attacker's benefit B_t is given by $\pi^p_{t+1} = 1 - \nu^p_{t+1}(A^\star_t(B_t))$. Furthermore,

$$\pi^p_{t\to t+2} = \pi^p_t \cdot \pi^p_{t+1} \cdot \mathbb{E}_t[\pi^p_{t+2}] \tag{2.26}$$

where throughout, we assume that B_t is public information at the beginning of period t so that the realization of π^p_t and π^p_{t+1} are known at the beginning of period t.[5]

In a PoW equilibrium,

$$\mathbb{E}_t[\pi^{PoW}_{t+2}] = \mathbb{E}_t[1 - \nu^{PoW}_{t+2}(A^\star_{t+1}(B_{t+1}))] = \mathbb{P}(B_{t+1} < H) \tag{2.27}$$

Therefore, given that Agent (i,t) adopts the blockchain only when they know that the blockchain will not be successfully attacked in periods t and $t+1$ (i.e., whenever $\pi^{PoW}_t = \pi^{PoW}_{t+1} = 1$), then $B_{t+1} \sim U[0, \overline{B}]$ for all t, combined with (2.27) yields:

$$\pi^{PoW}_{t\to t+2} = \pi^{PoW} \equiv \mathbb{P}(B_{t+1} < H) = \min\{\frac{H}{\overline{B}}, 1\} \tag{2.28}$$

Similarly, in a PoS equilibrium,

$$\mathbb{E}_t[\pi^{PoS}_{t+2}] = \mathbb{E}_t[1 - \nu^{PoS}_{t+2}(A^\star_{t+1}(B_{t+1}))] = \mathbb{P}(B_{t+1} < |S_{t+2}|) \tag{2.29}$$

As with the PoW case, given that Agent (i,t) adopts the blockchain only when they know that the blockchain will not be successfully attacked in periods t and $t+1$ (i.e., whenever $\pi^{PoS}_t = \pi^{PoS}_{t+1} = 1$), then $B_{t+1} \sim U[0, \overline{B}]$ combined with (2.23) and $|S_{t+2}| = |\{(i, t+1) :$

[5] In particular, we can view the attacker as the agent in the economy that receives the highest private benefit from attacking the blockchain (e.g. a traditional payments processor trying to undermine faith in the blockchain technology or an agent with particular portfolio holdings) and assume that agents can anticipate the benefit that this attacker receives from successfully attacking the blockchain as a function of the state of the world. Once this is the case, agents can anticipate π^p_t from B_{t-1} and π^p_{t+1} from B_t as attacks must be mounted the period before being executed.

$c_{(i,t+1)} < c^{PoS}\}| = G(c^{PoS})$ yields:

$$\pi^{PoS}_{t\to t+2} = \pi^{PoS} \equiv \mathbb{P}(B_{t+1} < G(c^{PoS})) = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} \tag{2.30}$$

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. *Optimal Fees*

Under any $p \in \{PoW, PoS\}$ equilibrium the optimal fees $f^p_{(i,t)}$ are given by:

$$For\ all\ (i,t) : f^p_{(i,t)} = \begin{cases} \frac{1}{\Lambda} \int_0^{c_{(i,t)}} x\ dG(x) & if\ c_{(i,t)} < c^p \\ 0 & if\ c_{(i,t)} \geqslant c^p \end{cases} \tag{3.1}$$

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 market value $\mathcal{M}^{PoW}$, the equilibrium hash rate H, and the blockchain survival probability π^{PoW} are given by

$$\mathcal{M}^{PoW} = (1 + e^{-\rho})G(c^{PoW}) \tag{3.2}$$

$$H = (1 - e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x\ dG(x)\ dG(c) \tag{3.3}$$

$$\pi^{PoW} = \min\{\frac{1}{\overline{B}} \cdot ((1 - e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x\ dG(x)\ dG(c)), 1\} \tag{3.4}$$

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

are given by

$$Q^{PoW}_{(i,t),t} = Q^{PoW}_{(i,t),t+1} = \frac{e^{\rho t}}{(1+e^{-\rho})G(c^{PoW})} \tag{3.5}$$

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

$$\begin{aligned} U^{PoW}_{(i,t)} = \min\{\frac{1}{\overline{B}} \cdot ((1-e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x \; dG(x) \; dG(c)), 1\} \\ \times (e^{-2\rho} - \frac{1}{\Lambda} \int_0^{c_{(i,t)}} x \; dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (G(c^{PoW}) - G(c_{(i,t)}))) \end{aligned} \tag{3.6}$$

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 market value* $\mathcal{M}^{PoS}$*, the equilibrium set of stakers* S_t*, and the blockchain survival probability* π^{PoS} *are given by*

$$\mathcal{M}^{PoS} = (1+e^{-\rho})G(c^{PoS}) + \frac{1}{\Lambda} \int_0^{c^{PoS}} \int_0^{c} x dG(x) dG(c) \tag{3.7}$$

$$S_t = \{(i, t-1) : c_{(i,t-1)} < c^{PoS}\} \quad \textit{for all } t \tag{3.8}$$

$$\pi^{PoS} = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} \tag{3.9}$$

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 blockchain are given by*

$$Q^{PoS}_{(i,t),t} = \frac{e^{\rho t}}{(1+e^{-\rho})G(c^{PoS}) + \frac{1}{\Lambda} \int_0^{c^{PoS}} \int_0^{c} x \; dG(x) \; dG(c)} \tag{3.10}$$

and

$$Q^{PoS}_{(i,t),t+1} = \frac{e^{\rho(t+2)}}{G(c^{PoS})} \times \frac{G(c^{PoS}) + \frac{1}{\Lambda} \int_0^{c^{PoS}} \int_0^{c} x \; dG(x) \; dG(c)}{(1+e^{-\rho})G(c^{PoS}) + \frac{1}{\Lambda} \int_0^{c^{PoS}} \int_0^{c} x \; dG(x) \; dG(c)} \tag{3.11}$$

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

$$U_{(i,t)}^{PoS} = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} \times (1 + \frac{\frac{1}{\Lambda} \int_0^{c^{PoS}} \int_0^{c} x \; dG(x) \; dG(c)}{G(c^{PoS})} - \frac{1}{\Lambda} \int_0^{c_{(i,t)}} x \; dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (G(c^{PoS}) - G(c_{(i,t)})))$$

(3.12)

4 Results

Our analysis in Section 4.1 considers the case of no cryptocurrency growth (i.e., $\rho = 0$), which implies zero block rewards. In Section 4.2, we generalize our results to a setting of arbitrary cryptocurrency growth rates (i.e., $\rho \geqslant 0$). Our results in Sections 4.1 and 4.2 establish that a high scale PoS blockchain generates higher security than a high scale PoW blockchain. We extend that insight in Section 4.3 by demonstrating that a PoS blockchain of arbitrary scale generates higher security than a PoW blockchain of the same scale.

4.1 Constant Cryptocurrency Supply

In the absence of block rewards, improving a PoW blockchain's transaction rate not only undermines security but also 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 whenever the blockchain possesses a higher transaction rate (i.e.,* $\Lambda > \underline{\Lambda}^{PoW}$*) then the blockchain is rendered entirely insecure (i.e.,* $\pi^{PoW} = 0$*).*

To clarify the intuition behind this result, we highlight that, per Equation (3.1), users adopting the blockchain pay an equilibrium fee, $f_{(i,t)}^{PoW}$, given by:

$$f_{(i,t)}^{PoW} = \frac{1}{\Lambda} \int_0^{c_{(i,t)}} x \; dG(x) \tag{4.1}$$

Equation (4.1) 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. To understand this relationship, recall that 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 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 increases.

This relationship between equilibrium fees and the blockchain's transaction rate has important implications for PoW security. To provide intuition, we reproduce Equation (2.22), which determines the equilibrium computational power H, in the case where block rewards are zero (i.e., $\rho = 0$):

$$H = \int f^{PoW}_{(i,t-2)} \, dG(c_{(i,t-2)}) = \frac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x \, dG(x) dG(c) \tag{4.2}$$

Equation (4.2) 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 adoption, c^{PoW}, 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 this 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. Hence, once this is the case the blockchain will generate zero adoption (i.e., $c^{PoW} = 0$) and zero equilibrium computational expenditure (i.e., $H = 0$) making the PoW

blockchain trivial to attack. Thus, a PoW blockchain becomes entirely insecure (i.e., $\pi^{PoW} = 0$) if the blockchain's transaction rate exceeds the finite threshold, $\underline{\Lambda}^{PoW}$.

The notion that a blockchain's scale undermines its security is not generic across all blockchain types. In particular, 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*

Assume that the maximal benefit of attacking the blockchain is less than the total endowment of all agents arriving in each period (i.e., $\overline{B} < 1$). 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 whenever the blockchain possesses a higher transaction rate (i.e., $\Lambda > \underline{\Lambda}^{PoS}$) then the blockchain is rendered fully secure (i.e., $\pi^{PoS} = 1$).

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 fraction 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 control 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 (3.7) (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:

$$\lim_{\Lambda \to \infty} \mathcal{M}^{PoS} = \lim_{\Lambda \to \infty} G(c^{PoS}) \tag{4.3}$$

which highlights a more general fact 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 (3.9).

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 with the PoS blockchain transaction rate which leads to full adoption for a large finite transaction rate, $\underline{\Lambda}^{PoS}$. In turn, for a sufficiently large transaction rate (i.e., $\Lambda > \underline{\Lambda}^{PoS}$), the market value of the cryptocurrency equals the total endowment of the economy. Therefore, a successful attack becomes prohibitively costly and the attacker does not pursue any attacks in equilibrium. Accordingly, in contrast to a PoW blockchain, a PoS blockchain achieves enhanced security from improved scaling.

Proposition 4.2 establishes that a PoS blockchain attains full security (i.e., $\pi^{PoS} = 1$) under the assumption that the attacker's benefit from attacking the blockchain cannot exceed the endowment of the entire economy (i.e., $\overline{B} < 1$). Nonetheless, even without such an assumption, a PoS blockchain generates a higher security level than an otherwise identical PoW blockchain. More explicitly, in Section 4.3, we do not impose any conditions on the attacker's maximum benefit from attacking the blockchain (i.e., $\overline{B}$ is arbitrary), and we demonstrate that a PoS blockchain generates higher security than a PoW blockchain in general (see Proposition 4.7).

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 for positive block rewards by letting the cryptocurrency supply grow at a rate of $\rho \geqslant 0$. Our first result generalizes Proposition 4.1, establishing that a PoW blockchain does not achieve full security for high transaction rates even with positive block rewards:[6]

Proposition 4.3. *High Scale PoW Blockchains Are Insecure, Even With Block Rewards*
Assume that the maximal benefit from attacking the blockchain is greater than the cost of utilizing the alternative technology (i.e., $\overline{B} > 1 - \sigma$). For any cryptocurrency growth rate, ρ, there exists a minimum transaction rate, $\underline{\Lambda_\rho}^{PoW} > 0$, such that whenever the blockchain possesses a higher transaction rate (i.e., any $\Lambda > \underline{\Lambda_\rho}^{PoW}$) then the blockchain is rendered insecure (i.e., $\pi^{PoW} < 1$).

[6] Proposition 4.3 requires the attacker's maximal benefit, $\overline{B}$, to be sufficiently bounded away from zero. Intuitively, if the attacker's maximal benefit is too small, then the attacker will never receive a benefit large enough to ensure that mounting an attack is profitable, irrespective of the blockchain protocol. A competitive alternative storage technology would correspond to a storage rate, σ, close to unity, implying that our hypothesis (i.e., $\overline{B} > 1 - \sigma$) is likely to be met in practice. It is noteworthy that a PoS blockchain generates a higher level of security than a PoW blockchain for any value of $\overline{B}$ (see Proposition 4.7).

In fact, as the transaction rate diverges (i.e., $\Lambda \to \infty$), the blockchain security possesses an upper-bound, strictly below full security. In particular, $\limsup_{\Lambda \to \infty} \pi^{PoW} < 1$.

To understand Proposition 4.3, it is important to recognize that block rewards correspond to inflation and thereby reduce the value of cryptocurrency holdings.[7] 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, where ρ is the cryptocurrency growth rate. Formally, combining Equations (3.2) and (3.5), one can derive that the proceeds from Agent (i,t)'s period $t+2$ sale of her PoW cryptocurrency holdings is given by:

$$P_{t+2}^{PoW} Q_{(i,t),t+1}^{PoW} = e^{-2\rho} \tag{4.4}$$

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, in order for any user to adopt the PoW 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:

$$\underbrace{e^{-2\rho}}_{\text{Max Consumption From Blockchain}} > \underbrace{\sigma}_{\text{Consumption From Alternative Technology}} \tag{4.5}$$

If Equation (4.5) 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. Similarly, the zero value of fees would arise more directly as the lack of usage would imply zero blockchain transactions and thus zero fees. Therefore as we have just argued, a PoW equilibrium in which the blockchain possesses any level of security (i.e., $\pi^{PoW} > 0$) cannot arise unless the cryptocurrency growth rate satisfies $\rho > \log \sqrt{\frac{1}{\sigma}}$. We formalize this point with the following result:

[7] This point is discussed also in earlier works such as Saleh (2019) and Chiu and Koeppl (2022).

Lemma 4.4. *PoW Block Rewards Undermine Adoption*

The equilibrium adoption of the PoW blockchain, c^{PoW}, is strictly positive only if

$$\rho > \log \sqrt{\frac{1}{\sigma}} \tag{4.6}$$

Otherwise, PoW adoption, hash rate, and security are zero (i.e., $c^{PoW} = 0$, $H = 0$, and $\pi^{PoW} = 0$).

Importantly, Equation (4.6) 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 (3.3) implies that the blockchain's computational power, H, satisfies the following equation:

$$\lim_{\Lambda \to \infty} H = \lim_{\Lambda \to \infty} (1 - e^{-2\rho}) G(c^{PoW}) \tag{4.7}$$

Then, invoking Equation (4.6), which restricts the block reward for any equilibrium with non-zero adoption, and also using the fact that $G(c^{PoW}) \leqslant 1$ further implies:

$$\lim_{\Lambda \to \infty} H \leqslant 1 - \sigma < 1 \tag{4.8}$$

which establishes that the security of high scale PoW blockchains are bounded as given by 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. Hence, block rewards must be bounded to ensure a non-zero level of PoW adoption (see Lemma 4.4) and the maximum block reward given by Equation (4.6) can generate only partial security.

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

Proposition 4.5. *High Scale PoS Blockchains Are Fully Secure*

Assume that the maximal benefit of attacking the blockchain is less than the total endowment of all

agents arriving in each period (i.e., $\overline{B} < 1$). There exists a minimum transaction rate, $\underline{\Lambda}^{PoS} > 0$, such that whenever the blockchain possesses a higher transaction rate (i.e., $\Lambda > \underline{\Lambda}^{PoS}$) then the blockchain is rendered fully secure (i.e., $\pi^{PoS} = 1$).

The intuition for Proposition 4.5 mirrors that for Proposition 4.2, so we opt not to restate it here. Instead, we highlight the intuition as to why Proposition 4.2 obtains regardless of block rewards. 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. We formalize this point with the following result:

Lemma 4.6. *PoS User Utility is Neutral to Block Rewards*

For any Agent (i,t) that adopts the blockchain, the period $t+2$ PoS cryptocurrency holding, $P^{PoS}_{t+2}Q^{PoS}_{(i,t),t+1}$, is invariant to the level of block rewards, ρ. Moreover, the following equation holds:

$$\lim_{\Lambda \to \infty} P^{PoS}_{t+2}Q^{PoS}_{(i,t),t+1} = 1 \tag{4.9}$$

This result establishes that the proceeds from Agent (i,t)'s period $t+2$ sale of cryptocurrency approach her initial endowment of unity as the blockchain transaction rate diverges. This result arises because the liquidation value of Agent (i,t)'s cryptocurrency holding is invariant to the cryptocurrency growth rate, ρ. Therefore, as the transaction rate diverges (i.e., as $\Lambda \to \infty$), fees vanish (see Equation 3.1) and cryptocurrency demand becomes sufficiently large so that full security arises (i.e., $\pi^{PoS} = 1$); in turn, the PoS blockchain approximates a perfect storage technology for large transaction rates.[8]

Propositions 4.3 and 4.5 are established under reasonable sufficient conditions regarding the

[8]Note that modeling users as miners, in the context of PoW, would not generate this same result for a PoW blockchain. The reason for this is that block rewards endogenously affect computational expenditure, and the computational expenditure represents a deadweight loss so that the PoW blockchain cannot serve as a perfect storage technology.

maximal benefit, $\overline{B}$, that the attacker can receive from successfully attacking the blockchain. Nonetheless, our insight, that a PoS blockchain generates higher security than a PoW blockchain, holds even without such conditions (i.e., for general $\overline{B}$). We formalize this point via our subsequent result, Proposition 4.7, which does not impose any conditions on $\overline{B}$.

4.3 A Generalized Result

Our results in Sections 4.1 and 4.2 establish that a PoS blockchain generates a higher level of security than a PoW blockchain for sufficiently high transaction rates (i.e., when Λ is large). We now generalize that comparative insight to arbitrary transaction rates without imposing any conditions on the cryptocurrency supply growth rate (i.e., for arbitrary ρ) or the maximum benefit to the attacker (i.e., for arbitrary $\overline{B}$):

Proposition 4.7. *PoS Blockchains Are More Secure Than PoW Blockchains*
The equilibrium security level of a PoS blockchain with an arbitrary transaction rate exceeds the equilibrium security level of a PoW blockchain with an identical transaction rate (i.e., if $\Lambda^{PoS} = \Lambda^{PoW}$*, then* $\pi^{PoS} \geqslant \pi^{PoW}$*).*

Proposition 4.7 arises because a PoW blockchain is secured by its computational expenditure, whereas a PoS blockchain is secured by user investment in the PoS cryptocurrency. Crucially, the PoW blockchain's computational expenditure is financed fully by users through transaction fees and inflationary block rewards (see Equation 2.7), implying that the computational expenditure of a PoW blockchain is necessarily less than the per period user investment (i.e., $H \leqslant G(c^{PoW})$). Moreover, the user financing of the PoW blockchain's computational expenditure corresponds to a welfare transfer from users to miners. Importantly, this welfare transfer (which does not occur in a PoS blockchain) is internalized by users ex ante so that a PoW blockchain generates lower adoption than a PoS blockchain (i.e., $c^{PoS} \geqslant c^{PoW}$). This lower adoption then implies less per-period user investment in a PoW blockchain relative to a PoS blockchain (i.e., $G(c^{PoS}) \geqslant G(c^{PoW})$) and therefore the user investment in a PoS blockchain exceeds the computational expenditure of a PoW blockchain (i.e., $G(c^{PoS}) \geqslant H$). For this reason, a PoS blockchain is more secure than a PoW blockchain in equilibrium (i.e., $\pi^{PoS} \geqslant \pi^{PoW}$).

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 be self-defeating; in particular, our results indicate that the loss in PoW security from scaling may overwhelm any gains from timely processing of transactions. Notably, 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 blockchains may be better suited for applications that require high volume in order to be economically viable. This insight is likely to be particularly important for applications in the context of Tokenomics (see, e.g., Cong et al. 2021b, Gan et al. 2021a, Gan et al. 2021b, Goldstein et al. 2021 and Mayer 2022) and Decentralized Finance (see, e.g., Lehar and Parlour 2021a, Capponi and Jia 2022, Hasbrouck et al. 2022 and John et al. 2022a).

References

Alsabah, H., A. Capponi, and S. Olafsson. 2021. Proof-of-Work Cryptocurrencies: Does Mining Technology Undermine Decentralization? *Working Paper* .

Basu, S., D. Easley, M. O'Hara, and E. Sirer. 2022. StableFees: A Predictable Fee Market for Cryptocurrencies. *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. 2022. The Adoption of Blockchain-based Decentralized Exchanges. *Working Paper* .

Chiu, J., and T. V. Koeppl. 2022. The Economics of Cryptocurrencies - Bitcoin and Beyond. *Canadian Journal of Economics* Forthcoming.

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

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

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

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

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. 2022. Why Fixed Costs Matter for Proof-of-Work Based Cryptocurrencies. *Working Paper* .

Goldstein, I., D. Gupta, and R. Sverchkov. 2021. Initial Coin Offerings As a Commitment to Competition. *Working Paper* .

Hasbrouck, J., T. Rivera, and F. Saleh. 2022. The Need for Fees at a DEX: How Increases in Fees Can Increase DEX Trading Volume. *Working Paper* .

Hinzen, F., K. John, and F. Saleh. 2022. Bitcoin's Limited Adoption Problem. *Journal of Financial Economics* 14:347–369.

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

Jermann, U. J., and H. Xiang. 2022. Tokenomics: Optimal Monetary and Fee Policies. *Working Paper* .

John, K., L. Kogan, and F. Saleh. 2022a. Smart Contracts and Decentralized Finance. *Working Paper* .

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

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

Lehar, A., and C. Parlour. 2021b. Miner Collusion and the BitCoin Protocol. *Working Paper* .

Makarov, I., and A. Schoar. 2022. Blockchain Analysis of the Bitcoin Market. *Working Paper* .

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

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

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

Prat, J., and B. Walter. 2021. An Equilibrium Model of the Market for Bitcoin Mining. *Journal of Political Economy* 129:2415–2452. URL https://doi.org/10.1086/714445.

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 Staking Costs

In this section, we generalize our main insight regarding PoS blockchains to the case whereby any agent that stakes their cryptocurrency in the intermediate period of their life must pay an explicit cost $\kappa > 0$ to do so. More explicitly, we establish that a PoS blockchain of a sufficiently high scale attains full security even in the presence of a staking cost. We demonstrate that insight with the following formal result:

Proposition A.1. *High Scale PoS Blockchains Are Fully Secure, Even With Staking Costs*
Assume that PoS blockchain users face a cost of staking $\kappa > 0$ and that the maximal benefit of attacking the blockchain is less than the total endowment of all agents arriving in each period (i.e. $\overline{B} < 1$). In that context, if the staking cost is reasonably bounded by $\kappa < 1 - \sigma$ and the block reward satisfies $\rho > log(\sqrt{\frac{1}{1-\kappa}})$, then there exists a minimum transaction rate $\underline{\Lambda}^{PoS} > 0$ such that whenever the blockchain possesses a higher transaction rate (i.e., $\Lambda > \underline{\Lambda}^{PoS}$), then the blockchain is rendered fully secure (i.e., $\pi^{PoS} = 1$).

Proof. We will show that there exists a PoS equilibrium that attains full security, under which all agents find it optimal to stake. We start by showing that there exists $\underline{\Lambda}^{PoS} > 0$ such that $\Lambda > \underline{\Lambda}^{PoS}$ implies $\pi^{PoS} = 1$ under the assumption that all agents find it optimal to stake. In order to do so, suppose that all agents stake their tokens and note that $\kappa < 1 - \sigma$ implies that $1 - \sigma - \kappa > 0$. Therefore, there exists $\underline{\Lambda}^{PoS} > 0$ sufficiently large so that $\Lambda > \underline{\Lambda}^{PoS}$ implies $\frac{2}{\Lambda} \int_0^\infty x dG(x) < 1 - \sigma - \kappa$. Then,

$$
\begin{aligned}
&\frac{U^{PoS}_{(i,t)}}{\min\{\frac{1}{\overline{B}}G(c^{PoS}),1\}} = 1 + \frac{\frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x\ dG(x)\ dG(c)}{G(c^{PoS})} - \frac{1}{\Lambda}\int_0^{c_{(i,t)}} x\ dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (G(c^{PoS}) - G(c_{(i,t)})) \\
&\geqslant 1 - \frac{1}{\Lambda}\int_0^{\infty} x\ dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (1 - G(c_{(i,t)})) \\
&= 1 - \frac{1}{\Lambda}\int_0^{\infty} x\ dG(x) - \frac{1}{\Lambda}\int_{c_{(i,t)}}^{\infty} c_{(i,t)} dG(x) \\
&\geqslant 1 - \frac{1}{\Lambda}\int_0^{\infty} x\ dG(x) - \frac{1}{\Lambda}\int_{c_{(i,t)}}^{\infty} x\ dG(x) \\
&\geqslant 1 - \frac{2}{\Lambda}\int_0^{\infty} x\ dG(x) \\
&> \sigma + \kappa
\end{aligned}
$$

which implies that $c^{PoS} = \infty$ satisfies the equilibrium Condition (2.17) as in this case $G(c^{PoS}) = 1$ which implies $\pi^{PoS} = 1$ whenever $\overline{B} < 1$ and therefore $U^{PoS}_{(i,t)} - \kappa > \sigma$ for all (i,t). Hence, for any $\Lambda > \underline{\Lambda}^{PoS}$ there exists a PoS equilibrium with $c^{PoS} = \infty$ provided that it is optimal for all agents to stake their cryptocurrency. Moreover, in such an equilibrium, Equation (3.9) implies $\pi^{PoS} = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} = \min\{\frac{G(\infty)}{\overline{B}}, 1\} = 1$.

The last step is to show that when $\pi^{PoS} = 1$ then all agents strictly prefer to stake and pay the cost κ rather than not staking. To prove this, we will show that whenever $\rho > log(\sqrt{\frac{1}{1-\kappa}})$ and $\pi^{PoS} = 1$ then it is a dominant strategy to stake whenever owning the PoS cryptocurrency. In particular, when $\pi^{PoS} = 1$, then User (i,t) prefers to stake when holding the cryptocurrency v.s. not staking whenever

$$
1 - \kappa + \frac{\frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x\ dG(x)\ dG(c)}{G(c^{PoS})} - \frac{1}{\Lambda}\int_0^{c_{(i,t)}} x\ dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (G(c^{PoS}) - G(c_{(i,t)}))
$$

$$
\geqslant e^{-2\rho} - \frac{1}{\Lambda}\int_0^{c_{(i,t)}} x\ dG(x) - \frac{c_{(i,t)}}{\Lambda} \times (G(c^{PoS}) - G(c_{(i,t)}))
$$

where we note that when holding the cryptocurrency but not staking, the user forgoes any revenues from fees and block rewards. Therefore, when forgoing block rewards, the user's end of life holdings become $P_{t+2}Q_{(i,t),t+1} = \frac{P_{t+2}}{P_t} = e^{-2\rho}$. Further, after rearranging it can be seen that staking is strictly optimal for any Λ whenever $\kappa < 1 - e^{-2\rho}$ which is guaranteed whenever $\rho > log(\sqrt{\frac{1}{1-\kappa}})$. Hence, we have shown that there exists a threshold $\underline{\Lambda}^{PoS} > 0$ such that whenever $\Lambda < \underline{\Lambda}^{PoS}$ then

there exists an equilibrium with full security (i.e., $\pi^{PoS} = 1$) under which all agents find it optimal to stake their cryptocurrency holdings. □

B Proofs

B.1 Proof of Lemma 3.1

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

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

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 (A.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, imposing $f^p_{(i,t)} = \phi^p(c_{(i,t)})$, and rearranging yields

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

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:

$$\text{For all } (i,t) : \phi^p(c) = \begin{cases} \frac{1}{\Lambda} \int_0^c x\ dG(x) & \text{if } c < c^p \\ 0 & \text{if } c \geqslant c^p \end{cases} \tag{A.3}$$

which gives the equilibrium realized fees (3.1).

□

B.2 Proof of Proposition 3.2

Proof. First note that the market value $\mathcal{M}^{PoW}$ comes immediately from the market clearing condition (2.21). To determine the equilibrium computational power we start with Equation (2.22) 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, we substitute for $\mathcal{M}^{PoW}$ from (3.2) and the optimal fees from (3.1) to obtain (after rearranging):

$$H = (1 - e^{-2\rho}) G(c^{PoW}) + \frac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x \; dG(x) \; dG(c) \tag{A.4}$$

Moreover, applying Equation (3.3) to Equation (2.28) yields the equilibrium one-period-ahead blockchain survival probability:

$$\pi^{PoW} = \min\{\frac{1}{B} \cdot ((1 - e^{-2\rho}) G(c^{PoW}) + \frac{1}{\Lambda} \int_0^{c^{PoW}} \int_0^{c} x \; dG(x) \; dG(c)), 1\} \tag{A.5}$$

Combining Equations (2.18), (2.24) and (3.2) yields the equilibrium holdings for each agent that adopts the blockchain:

$$\text{For all } (i,t) : Q_{(i,t),t}^{PoW} = Q_{(i,t),t+1}^{PoW} = \frac{1}{P_t^{PoW}} = \frac{e^{\rho t}}{(1 + e^{-\rho}) G(c^{PoW})} \tag{A.6}$$

Finally, plugging in the explicit solutions for $f_{(i,t)}^{PoW}$ from Equation (3.1), $Q_{(i,t),t+1}^{PoW}$ from Equation (3.5), P_{t+2}^{PoW} indirectly via Equation (3.2) (using $P_{t+2} M_{t+2} = \mathcal{M}^{PoW}$), and π^{PoW} from Equation (3.4) delivers Condition (3.6) and thereby completes the proof. □

B.3 Proof of Proposition 3.3

Proof. Applying Equation (3.1) to Equation (2.21) (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 solution (3.7) for $\mathcal{M}^{PoS}$.

The set of staking nodes, $\{S_t\}_{t\geqslant 0}$, is given directly as a function of the PoS adoption cut-off, c^{PoS}, by Equation (2.23). Further, applying Equation (3.8) to Equation (2.30) yields the equilibrium one-period-ahead blockchain survival probability (3.9).

Finally, combing Equations (2.18), (2.25), (3.1) and (3.7) yields the equilibrium holdings for each agent. In particular, $Q_{(i,t),t}^{PoS} = \frac{1}{P_t^{PoS}}$ which we derive as (3.10) by using $P_t^{PoS} = \frac{\mathcal{M}^{PoS}}{M_t}$, $M_t = e^{\rho t}$, and substituting the equilibrium market value $\mathcal{M}^{PoS}$ given by (3.7). In order to derive (3.11) we use (2.25), which after plugging in the the optimal fees from (3.1) and substituting $\frac{1}{P_{t+1}^{PoS}} = \frac{e^{\rho(t+1)}}{\mathcal{M}^{PoS}}$ and rearranging yields

$$\frac{1}{G(c^{PoS})\times\mathcal{M}^{PoS}}(G(c^{PoS})e^{\rho t} + e^{\rho(t+1)}(R_{t+1}P_{t+1}^{PoS} + \frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x\ dG(x)\ dG(c))) \tag{A.7}$$

Then, we use the fact that $R_{t+1}P_{t+1}^{PoS} = \mathcal{M}^{PoS}(e^{\rho}-1)$ which after substituting $\mathcal{M}^{PoS}$ from (3.7) implies that

$$R_{t+1}P_{t+1}^{PoS} + \frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x\ dG(x)\ dG(c) = G(c^{PoS})(e^{\rho}-e^{-\rho}) + e^{\rho}\frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x\ dG(x)\ dG(c)$$

Thus, after plugging this expression into (A.7) and rearranging we have derived our expression for $Q_{(i,t),t+1}^{PoS}$ in (3.11).

Finally, plugging in the explicit solutions for $f_{(i,t)}^{PoS}$ from Equation (3.1), for $Q_{(i,t),t+1}^{PoS}$ from Equation (3.11), for P_{t+2}^{PoS} indirectly via Equation (3.7), and for π^{PoS} from Equation (3.9) delivers Condition (3.12) and thereby completes the proof.

□

B.4 Proof of Proposition 4.1

Proof. We prove this result constructively. In particular, let $\underline{\Lambda}^{PoW} = \frac{2}{\sigma}\times\overline{B}\times\int_0^{\infty} x\ dG(x)$. Then, for $\Lambda \geqslant \underline{\Lambda}^{PoW}$, taking $\rho = 0$ in the left-hand side of the consequent of Condition (3.6):

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

which implies that $U_{(i,t)}^{PoW} < \sigma$ for all (i,t) so that Condition (3.6) holds if and only if the equilibrium level of adoption is zero (i.e., $c^{PoW} = 0$).

In turn, whenever $c^{PoW} = 0$, then Equation (3.4) implies:

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

which establishes the desired result. □

B.5 Proof of Proposition 4.2

Proof. Proposition 4.5 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 4.5 is given below in Section B.8. □

B.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 (3.6), we have that:

$$
\begin{aligned}
&U_{(i,t)}^{PoW} \\
&= \min\{\tfrac{1}{B}((1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda}\int_0^{c^{PoW}}\int_0^{c} x\ dG(x)\ dG(c)), 1\} \times \{e^{-2\rho} - \tfrac{1}{\Lambda}\int_0^{c_{(i,t)}} x\ dG(x) - \tfrac{c_{(i,t)}}{\Lambda} \times \\
&(G(c^{PoW}) - G(c_{(i,t)}))\} \\
&\leqslant e^{-2\rho} - \tfrac{1}{\Lambda}\int_0^{c_{(i,t)}} x\ dG(x) - \tfrac{c_{(i,t)}}{\Lambda} \times (G(c^{PoW}) - G(c_{(i,t)})) \\
&\leqslant e^{-2\rho} \\
&\leqslant \sigma
\end{aligned}
$$

Then, $U_{(i,t)}^{PoW} \leqslant \sigma$ for all (i,t) so that $c^{PoW} = 0$. Moreover, Equation (3.4) implies:

$$
\begin{aligned}
&\pi^{PoW} \\
&= \min\{\tfrac{1}{B}((1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda}\int_0^{c^{PoW}}\int_0^{c} x\ dG(x)\ dG(c)), 1\} \\
&\leqslant \min\{\tfrac{1}{B}(G(c^{PoW}) + \tfrac{1}{\Lambda}\int_0^{c^{PoW}}\int_0^{c^{PoW}} x\ dG(x)\ dG(c)), 1\}) \\
&= \min\{G(0) + \tfrac{1}{\Lambda}\int_0^0\int_0^0 x\ dG(x)\ dG(c), 1\} \\
&= \min\{0, 1\} \\
&= 0
\end{aligned}
$$

as desired. Finally, $\limsup_{\Lambda\to\infty}\ \pi^{PoW} = \limsup_{\Lambda\to\infty}\ 0 = 0 < 1$ which completes the proof for this case.

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

First note that $\rho < \log\sqrt{\frac{1}{\sigma}}$ implies that $1 - e^{-2\rho} < 1 - \sigma$. Let $\varepsilon_\rho \equiv (1-\sigma) - (1-e^{-2\rho}) > 0$. Then, note that $\lim_{\Lambda\to\infty} \frac{1}{\Lambda}\int_0^{\infty} x\ dG(x) = 0$ and therefore, for each $\rho < \log\sqrt{\frac{1}{\sigma}}$, there exists some $\underline{\Lambda_\rho}^{PoW} > 0$ for which $\Lambda > \underline{\Lambda_\rho}^{PoW}$ implies $\frac{1}{\Lambda}\int_0^{\infty} x\ dG(x) \leqslant \frac{\varepsilon_\rho}{2}$. Then, proceeding with a constructive proof, for any ρ and any $\Lambda > \underline{\Lambda_\rho}^{PoW}$, Equation (3.4) implies:

$$
\begin{aligned}
&\pi^{PoW}
\end{aligned}
$$

$$= \min\{\tfrac{1}{\overline{B}}((1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda}\int_0^{c^{PoW}}\int_0^{c} x\ dG(x)\ dG(c)), 1\})$$
$$\leqslant \tfrac{1}{\overline{B}}((1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\Lambda}\int_0^{c^{PoW}}\int_0^{c} x\ dG(x)\ dG(c))$$
$$\leqslant \tfrac{1}{\overline{B}}((1-e^{-2\rho})G(c^{PoW}) + \tfrac{1}{\underline{\Lambda}_\rho^{PoW}}\int_0^{c^{PoW}}\int_0^{c} x\ dG(x)\ dG(c))$$
$$< \tfrac{1}{\overline{B}}(1-e^{-2\rho} + \tfrac{1}{\underline{\Lambda}_\rho^{PoW}}\int_0^{\infty} x\ dG(x))$$
$$= \tfrac{1}{\overline{B}}(1-\sigma-\varepsilon_\rho + \tfrac{1}{\underline{\Lambda}_\rho^{PoW}}\int_0^{\infty} x\ dG(x))$$
$$\leqslant \tfrac{1}{\overline{B}}(1-\sigma-\tfrac{\varepsilon_\rho}{2})$$

Accordingly, whenever $\overline{B} > 1-\sigma$ then for any ρ and any $\Lambda > \underline{\Lambda_\rho}^{PoW}$, $\pi^{PoW} < 1$ as desired. Moreover, $\limsup_{\Lambda\to\infty} \pi^{PoW} \leqslant \limsup_{\Lambda\to\infty} \tfrac{1}{\overline{B}}(1-\sigma-\tfrac{\varepsilon_\rho}{2}) = \tfrac{1}{\overline{B}}(1-\sigma-\tfrac{\varepsilon_\rho}{2}) < \tfrac{1}{\overline{B}}(1-\sigma) < 1$ which completes the proof. □

B.7 Proof of Lemma 4.4

Proof. This result was proven in Case (i) of the proof of Proposition 4.3. □

B.8 Proof of Proposition 4.5

Proof. We proceed with a constructive proof. Let $\underline{\Lambda}^{PoS}$ be such that $\Lambda > \underline{\Lambda}^{PoS}$ implies that $\tfrac{2}{\Lambda}\int_0^{\infty} x\ dG(x) < \tfrac{1-\sigma}{2}$. Then, for any $\Lambda > \underline{\Lambda}^{PoS}$, using the left-hand side of the consequent of Condition (3.12):

$$\frac{U_{(i,t)}^{PoS}}{\min\{\frac{1}{\overline{B}}G(c^{PoS}),1\}} = 1 + \frac{\frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x\ dG(x)\ dG(c)}{G(c^{PoS})} - \tfrac{1}{\Lambda}\int_0^{c_{(i,t)}} x\ dG(x) - \tfrac{c_{(i,t)}}{\Lambda} \times (G(c^{PoS}) - G(c_{(i,t)}))$$
$$\geqslant 1 - \tfrac{1}{\Lambda}\int_0^{\infty} x\ dG(x) - \tfrac{c_{(i,t)}}{\Lambda} \times (1 - G(c_{(i,t)}))$$
$$= 1 - \tfrac{1}{\Lambda}\int_0^{\infty} x\ dG(x) - \tfrac{1}{\Lambda}\int_{c_{(i,t)}}^{\infty} c_{(i,t)} dG(x)$$
$$\geqslant 1 - \tfrac{1}{\Lambda}\int_0^{\infty} x\ dG(x) - \tfrac{1}{\Lambda}\int_{c_{(i,t)}}^{\infty} x\ dG(x)$$
$$\geqslant 1 - \tfrac{2}{\Lambda}\int_0^{\infty} x\ dG(x)$$
$$\geqslant 1 - \tfrac{1-\sigma}{2}$$
$$= \tfrac{1+\sigma}{2}$$

$> \sigma$

which implies that $c^{PoS} = \infty$ satisfies the equilibrium Condition (2.17) as in this case $G(c^{PoS}) = 1$ which implies $\pi^{PoS} = 1$ whenever $\overline{B} < 1$ and therefore $U^{PoS}_{(i,t)} > \sigma$ for all (i,t). Hence, for any $\Lambda > \underline{\Lambda}^{PoS}$ there exists a PoS equilibrium with $c^{PoS} = \infty$. Moreover, in such an equilibrium, Equation (3.9) implies $\pi^{PoS} = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} = \min\{\frac{G(\infty)}{\overline{B}}, 1\} = 1$ thereby completing the proof.

□

B.9 Proof of Lemma 4.6

Proof. To prove the invariance of Agent (i,t)'s utility to ρ we first note that c^{PoS} is determined by the condition

$$\min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} \times (1 + \frac{\frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x\ dG(x)\ dG(c)}{G(c^{PoS})} - \frac{1}{\Lambda}\int_0^{c^{PoS}} x\ dG(x)) = \sigma$$

and therefore c^{PoS} must be invariant to ρ. Therefore, the fact that $U^{PoS}_{(i,t)}$ is only a function of c^{PoS} and exogenously given variables implies that $U^{PoS}_{(i,t)}$ must be invariant to ρ.

The next result is obtained by combining equations (3.7) and (3.11). In particular, $\mathcal{M}^{PoS} = M_{t+2}P^{PoS}_{t+2} = e^{\rho(t+2)}P^{PoS}_{t+2}$ and therefore

$$P^{PoS}_{t+2} = \frac{1}{e^{\rho(t+2)}}\left((1 + e^{-\rho})G(c^{PoS}) + \frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x dG(x) dG(c)\right)$$

and therefore after substituting this expression into (3.11) we obtain

$$\lim_{\Lambda\to\infty} P^{PoS}_{t+2}Q^{PoS}_{(i,t),t+1} = \lim_{\Lambda\to\infty} \frac{G(c^{PoS}) + \frac{1}{\Lambda}\int_0^{c^{PoS}}\int_0^{c} x\ dG(x)\ dG(c)}{G(c^{PoS})} = 1$$

□

B.10 Proof of Proposition 4.7

Proof. Recall that $\pi^{PoW} = \min\{\frac{H(c^{PoW})}{\overline{B}}, 1\}$ and $\pi^{PoS} = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\}$ where the equilibrium hash rate $H(c^{PoW})$, written as a function of the adoption level, c^{PoW}, is given by

$$H(c^{PoW}) = (1 - e^{-2\rho})G(c^{PoW}) + \frac{1}{\Lambda}\int_0^{c^{PoW}}\int_0^{c} x dG(x) dG(c)$$

We will proceed by proving that $c^{PoS} \geqslant c^{PoW}$ and then showing that this implies $\pi^{PoS} \geqslant \pi^{PoW}$.

As a first step, we will show that whenever $c^{PoW} > 0$, then it must be the case that $H(c^{PoW}) < G(c^{PoW})$. Namely, suppose to the contrary that $H(c^{PoW}) \geqslant G(c^{PoW})$. Then, using (3.3) this implies that

$$\frac{1}{\Lambda}\int_0^{c^{PoW}}\int_0^{c} x dG(x) dG(c) \geqslant e^{-2\rho} \cdot G(c^{PoW}) \tag{A.8}$$

Yet, by (2.17), integrating over Equation (3.6) with respect to c (from 0 to c^{PoW}) gives us the aggregate equilibrium utility of users that adopt the PoW cryptocurrency from any given generation. In particular, this aggregate utility is given by

$$\begin{aligned}
&\int_{(i,t):c_{(i,t)}<c^{PoW}} U^{PoW}_{(i,t)} dG(c_{(i,t)}) \\
&= \int_0^{c^{PoW}} \min\{\tfrac{H(c^{PoW})}{\overline{B}}, 1\} \times (e^{-2\rho} - \tfrac{1}{\Lambda}\int_0^{c} x\ dG(x) - \tfrac{c}{\Lambda} \times (G(c^{PoW}) - G(c)))dG(c) \\
&< \min\{\tfrac{H(c^{PoW})}{\overline{B}}, 1\} \times (\int_0^{c^{PoW}} (e^{-2\rho} - \tfrac{1}{\Lambda}\int_0^{c} x\ dG(x))dG(c)) \\
&= \min\{\tfrac{H(c^{PoW})}{\overline{B}}, 1\} \times (e^{-2\rho} \cdot G(c^{PoW}) - \tfrac{1}{\Lambda}\int_0^{c^{PoW}}\int_0^{c} x\ dG(x))dG(c))
\end{aligned}$$

Hence, if $c^{PoW} > 0$ and $H(c^{PoW}) \geqslant G(c^{PoW})$, then Equation A.8 holds which implies that the aggregate utility of adopting users in any generation is weakly negative. Yet, this contradicts the optimality of adoption as $c^{PoW} > 0$ implies that $c_{(i,t)} < c^{PoW}$ if and only if $U^{PoW}_{(i,t)} > \sigma > 0$ and therefore $c^{PoW} > 0$ must imply that the aggregate utility of each generation's adopting users is strictly positive.

We now proceed with three cases:

Case (i): $c^{PoW} \in (0, \infty)$

Assume that $c^{PoW} \in (0, \infty)$ and denote by $U^{PoW}(c^{PoW})$ the utility of the marginal user with wait disutility c^{PoW}. Then, we note that $c^{PoW} < \infty$ implies that $U^{PoW}(c^{PoW}) = \sigma$. Now suppose that $c^{PoW} > c^{PoS}$, then this implies that

$$\begin{aligned}
&\sigma > U^{PoS}(c^{PoW}) = \min\{\tfrac{G(c^{PoW})}{\overline{B}}, 1\} \times (1 - \tfrac{1}{\Lambda} \int_0^{c^{PoW}} x dG(x)) \\
&\geqslant \min\{\tfrac{G(c^{PoW})}{\overline{B}}, 1\} \times (e^{-2\rho} - \tfrac{1}{\Lambda} \int_0^{c^{PoW}} x dG(x)) \\
&\geqslant \min\{\tfrac{H(c^{PoW})}{\overline{B}}, 1\} \times (e^{-2\rho} - \tfrac{1}{\Lambda} \int_0^{c^{PoW}} x dG(x)) \\
&= U^{PoW}(c^{PoW})
\end{aligned}$$

a contradiction given that $U^{PoW}(c^{PoW}) = \sigma$.[9]

We have shown that $c^{PoW} \in (0, \infty)$ implies that $c^{PoS} \geqslant c^{PoW}$. Thus, whenever $c^{PoW} \in (0, \infty)$ then $H(c^{PoW}) \leqslant G(c^{PoW}) < G(c^{PoS})$ and therefore $\pi^{PoS} = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} \geqslant \min\{\frac{G(c^{PoW})}{\overline{B}}, 1\} \geqslant \min\{\frac{H(c^{PoW})}{\overline{B}}, 1\} = \pi^{PoW}$.

Case 2: $c^{PoW} = \infty$ If $c^{PoW} = \infty$ then $c^{PoW} > 0$ and therefore, as shown above, it must be the case that $H(c^{PoW}) < G(c^{PoW})$. Further, we know that $c^{PoW} = \infty$ implies that $U^{PoW}(c^{PoW}) \geqslant \sigma$. Now, suppose that $c^{PoS} < c^{PoW}$, then following the steps of Case 1, it must be the case that $U^{PoS}(c^{PoW}) < \sigma$. Yet, this implies that

$$\begin{aligned}
&\sigma > U^{PoS}(c^{PoW}) = \min\{\tfrac{G(c^{PoW})}{\overline{B}}, 1\} \times (1 - \tfrac{1}{\Lambda} \int_0^{c^{PoW}} x dG(x)) \\
&\geqslant \min\{\tfrac{G(c^{PoW})}{\overline{B}}, 1\} \times (e^{-2\rho} - \tfrac{1}{\Lambda} \int_0^{c^{PoW}} x dG(x)) \\
&\geqslant \min\{\tfrac{H(c^{PoW})}{\overline{B}}, 1\} \times (e^{-2\rho} - \tfrac{1}{\Lambda} \int_0^{c^{PoW}} x dG(x)) \\
&= U^{PoW}(c^{PoW})
\end{aligned}$$

which again presents a contradiction as $c^{PoW} = \infty$ implies $U(c^{PoW}) \geqslant \sigma$. Thus, it must be the case that $c^{PoW} \leqslant c^{PoS}$. Finally, using the aforementioned fact that, in this case, $H(c^{PoW}) < G(c^{PoW})$, we note that $\pi^{PoS} = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} \geqslant \min\{\frac{G(c^{PoW})}{\overline{B}}, 1\} \geqslant \min\{\frac{H(c^{PoW})}{\overline{B}}, 1\} = \pi^{PoW}$.

[9] Note that in this context $U^{PoS}(c^{PoW})$ denotes the utility received by a user with wait disutility $c_{(i,t)} = c^{PoW}$ from adopting the PoS blockchain when users with $c_{(i,t)} \in [0, c^{PoW}]$ adopt the blockchain.

Case 3: $c^{PoW} = 0$ In this case, we know that $H(c^{PoW}) = 0$. Therefore, $G(c^{PoS}) \geqslant 0$ implies that $\pi^{PoS} = \min\{\frac{G(c^{PoS})}{\overline{B}}, 1\} \geqslant 0 = \min\{\frac{H(c^{PoW})}{\overline{B}}, 1\} = \pi^{PoW}$. □