Productivity Enables Security: The Economics of Blockchain Settlement*

Campbell R. Harvey† Kose John‡ Fahad Saleh§
Duke University and NBER *NYU Stern* *University of Florida*

June 11, 2026

Abstract

Blockchain technology holds the promise of transforming our financial system, but a key question lingers regarding whether this technology can ensure secure settlement. We develop an equilibrium model to study that question with regard to the most prominent blockchain type, a Proof-of-Stake (PoS) blockchain. We demonstrate that blockchain settlement security increases with the economic productivity generated by the blockchain. Moreover, we show that blockchain settlement can be secured against arbitrarily large disruption incentives so long as the blockchain generates sufficient economic value.

1 Introduction

The United States Securities and Exchange Commission recently launched *Project Crypto*, an initiative aimed at enabling financial markets to move onchain (Atkins, 2025). A prerequisite for the success of this initiative is that blockchain asset settlement must be secure. To that end, this paper develops an economic model to study the security of blockchain asset settlement. Notably, we show that a blockchain can achieve secure settlement through appropriate economic design so long as it generates sufficient economic productivity.

We focus on Proof-of-Stake (PoS) blockchains, the dominant blockchain architecture (see, e.g., John et al. 2025a). In a PoS system, settlement authority is allocated to participants who hold units of the blockchain's native asset dormant, a process known as *staking*. Crucially, each staking participant's settlement authority is proportional to the quantity of native asset staked. Moreover, the system is open-access: any agent can participate in the settlement process by purchasing and

*We thank Agostino Capponi, Mark Flannery, Co-Pierre Georg, Jiasun Li, Kevin Mei, Ciamac Moallemi, Mahendrarajah Nimalendran, Gregory Phelan, and Baolian Wang, as well as seminar participants at the Frankfurt School of Finance and Management, George Mason University, and the University of Florida and conference participants at the 2026 SFS Cavalcade North America and the 2026 Designing DeFi Conference, for helpful comments.

†email: cam.harvey@duke.edu
‡email: kj1@stern.nyu.edu
§email: fahad.saleh@ufl.edu

staking the blockchain's native asset. As a consequence, an attacker could, in principle, disrupt settlement by purchasing and staking a sufficiently large quantity of the native asset. The cost of such an attack depends critically on the price the attacker must pay, and since a large acquisition of any asset increases its price, the attacker faces an endogenous *price impact*. Importantly, this price impact corresponds to a real cost: the attacker pays a price above equilibrium value, and this excess cost is not recouped even if the attacker can subsequently sell at equilibrium value without price impact.

Prior analyses of blockchain settlement security (e.g., Budish 2025) overlook this price impact, assuming instead that an attacker can acquire the necessary position at the same equilibrium price that would prevail in the absence of the attacker's purchase. In contrast, we model price impact explicitly and show how it plays a primary role in generating blockchain settlement security. Notably, we demonstrate that price impact can be engineered to be arbitrarily large when the blockchain generates sufficient economic value, thereby rendering settlement disruption attacks non-incentive-compatible. The underlying channel operates as follows. Price impact arises from the attacker seeking to purchase a specific quantity of the native asset from a limited circulating supply. When circulating supply is small, price impact is commensurately large, which increases the attacker's cost. Crucially, staked assets are locked and unavailable for trading, so the circulating supply from which the attacker must purchase consists of only unstaked assets.[1] Importantly, newly issued units of the native asset accrue to stakers as compensation for locking their assets. In turn, we show that, when the blockchain generates sufficient economic value, the supply growth rate can be set high enough to induce staking investment that reduces circulating supply to the point where price impact renders attacks prohibitively costly.

Formally, we provide two main results that establish how economic productivity generated by a blockchain can enhance its security. First, we demonstrate that both absolute and relative settlement disruption costs increase with blockchain productivity when the native asset supply growth rate is adjusted appropriately (Proposition 5.1). Second, we establish that, for a sufficiently productive blockchain, the native asset supply growth rate can be engineered so that both absolute and relative disruption costs exceed any attack benefit (Proposition 5.7). Here, the absolute disruption cost refers to the total cost of disrupting settlement, whereas the relative disruption cost normalizes this total cost by the native asset's market value. Examining both costs is important because whether a disruption attack is profitable depends on the nature of the attack benefit. The absolute cost is the relevant metric when the attack benefit is exogenous, whereas the relative cost is relevant when the attack benefit scales with the native asset's market value. Since both costs can be made arbitrarily large, our results establish settlement security under either assumption, provided the blockchain is sufficiently productive.

Proposition 5.1 follows from an equilibrium decomposition of the absolute disruption cost into

[1]Note that purchasing liquid staking tokens would not help the attacker execute an attack. More concretely, participating in the settlement process requires digitally signing with the cryptographic keys associated with staked native assets (see John et al. 2025a). Crucially, liquid staking tokens (e.g., stETH, wstETH) convey cash-flow rights and provide no access to the cryptographic keys associated with the underlying staked native assets.

three components: the share of the native asset required for a successful attack, the price impact from that purchase, and the native asset's market value (Proposition 5.2). Notably, as referenced earlier, all newly issued units of the native asset accrue to stakers, thereby serving as an inflationary welfare transfer from existing native asset holders to stakers. The holders include users because users require the native asset to pay for subsequent blockchain execution. Importantly, when the economic value generated by blockchain execution rises, the supply growth rate can be increased so as to transfer a portion of the gains to investors while users remain net beneficiaries. All three components of the disruption cost then increase (Proposition 5.3). The higher supply growth rate increases staking investment (Proposition 5.5), which raises both the share of the native asset required for an attack and the associated price impact (Proposition 5.4). Simultaneously, the net gain to users raises their demand for the native asset and thereby its market value (Proposition 5.6).

Proposition 5.7 strengthens the link between blockchain economic productivity and blockchain settlement security: for sufficiently productive blockchains, the native asset supply growth rate can be engineered so that both absolute and relative disruption costs exceed any attack benefit. The key insight is that there exists a finite productivity threshold above which the blockchain can be secured against arbitrary attack incentives. The underlying economic channel involves a trade-off. Increasing the native asset supply growth rate induces greater staking investment, which reduces circulating supply and increases the price impact faced by an attacker. However, native asset supply growth constitutes an inflationary welfare transfer from users to investors. Users rationally anticipate this transfer and reduce their demand for the native asset when the supply growth rate increases. This reduction in demand lowers the native asset's market value, serving as a countervailing force that reduces disruption costs. We show that, above the productivity threshold, users maintain sufficient demand even as the native asset supply growth rate is raised to the level at which price impact diverges (Proposition 5.8). In turn, for sufficiently productive blockchains, the native asset supply growth rate can be set high enough to induce arbitrarily large disruption costs.

Methodologically, our analysis employs standard asset pricing techniques. Equilibrium user demand for the blockchain's native asset is determined by a static optimization whereby users allocate across blockchain execution and traditional consumption. Blockchain execution requires payment in the blockchain's native asset so that user demand arises through a standard cash-in-advance constraint (see, e.g., Lucas and Stokey 1987). The user population evolves stochastically and constitutes the primary source of risk within our framework. We specify a stochastic discount factor as exponential-affine in innovations to the user population, equivalent to specifying a measure change to the risk-neutral probability (see, e.g., Harrison and Kreps 1979). In turn, equilibrium staking investment is determined by pricing the staking investment under the risk-neutral measure. This specification is standard in the asset pricing literature (see, e.g., Rubinstein 1976 and Lucas 1978) and accommodates arbitrary levels of risk aversion. Our model entails both endogenous demand and endogenous supply for the unstaked native asset with the former arising from users seeking blockchain execution and the latter determined as the residual of the total native asset supply after subtracting staking investment. An attacker seeking to disrupt settlement must compete with user

demand for this residual supply, and the price impact from the attacker's purchase is determined accordingly. Notably, our model admits a closed-form equilibrium (Proposition 3.1), enabling explicit characterization of attack costs and a clear understanding of how protocol design choices affect settlement security. Our contribution arises from identifying the economic channel through which endogenous staking, circulating supply, and price impact interact to generate settlement security, as formalized in Section 5.

At a practical level, our framework reveals that prior literature has conflated the marginal price of acquiring the native asset with the average price an attacker would actually face. As an example, the base case of Budish (2025) presumes that an attacker could acquire 143% of "units of trust support" of the blockchain network at a constant per unit cost equal to the marginal cost that existing participants have paid. Our model shows that an attacker would pay a significantly higher average price due to equilibrium supply-and-demand dynamics. Taking Ethereum as an example, approximately 30% of its native asset, ether, is currently staked, so that a majority attack would require purchasing an additional 30% of ether from the 70% not currently staked. This would require the attacker to pay a price 75% above the current market price, implying a higher level of settlement security than suggested by the current literature.[2] Moreover, the staking ratio is endogenous and can be increased through adjustments to the native asset supply growth rate. Our results establish that, for sufficiently productive blockchains, the staking ratio can be engineered to reduce circulating supply to the point where the price impact renders any attack prohibitively expensive, regardless of the magnitude of the attack benefit (Proposition 5.7).

Our paper contributes to the literature on blockchain settlement security. Nakamoto (2008) and Saleh (2021) establish that investment capital increases settlement security in Proof-of-Work and PoS blockchains respectively, but both model investment as exogenous. Budish (2025) and John et al. (2025b) incorporate endogenous investment but do not incorporate price impact. Our framework incorporates both endogenous investment and endogenous price impact, yielding a qualitatively different conclusion: a PoS blockchain can achieve settlement security against arbitrarily large attack incentives so long as the blockchain is sufficiently productive. Our work thereby also extends the broader class of PoS economic models (e.g., Roşu and Saleh 2021, Cong et al. 2025a, Jermann 2025).

Our work also relates to the literature on price impact in financial engineering. We study price impact in a setting with symmetric information akin to Bertsimas and Lo (1998), Almgren and Chriss (2001), Obizhaeva and Wang (2013), and Capponi et al. (2025). Price impact in our model arises because the attacker competes with user demand for a finite supply of unstaked native assets. As in Capponi et al. (2025), the effective supply in our model is endogenous, determined as the residual native asset after endogenous staking investment. As in Bertsimas and Lo (1998), Almgren and Chriss (2001), and Obizhaeva and Wang (2013), demand is also endogenous, with

[2]The price impact calculation relies on a function that we derive explicitly in Equation (4.4). That derived function establishes that acquiring $x\%$ of the circulating supply entails a price which is $\frac{1}{1-x}$ of the equilibrium price. Since a 30% staking ratio implies $100\% - 30\% = 70\%$ is in circulation and a majority attack requires acquiring 30% of the total supply, the price from an attack would therefore be $\frac{1}{1-\frac{30\%}{70\%}} = 175\%$ of the current price, implying the attacker's price would be 175% - 100% = 75% above the current price.

users optimally determining their demand for the native asset.

2 Model

We study a discrete-time infinite horizon setting with time indexed by $t \in \mathbb{N} = \{1, 2, ...\}$. At the beginning of each period t, a new measure of investors and a new measure of users arrive. We normalize the measure of investors to unity whereas we allow that the measure of users evolves randomly as follows:

$$\eta_{t+1} = \eta_t \, \varepsilon_{t,t+1} \tag{2.1}$$

with η_t denoting the measure of new users at the beginning of period t and $\log(\varepsilon_{t,t+1}) \overset{i.i.d.}{\sim} N(\mu - \frac{\sigma^2}{2}, \sigma^2)$ with $\mu > \frac{\sigma^2}{2}$ and $\sigma > 0$.

We index each investor by $(i,t) \in [0,1] \times \mathbb{N}$ where t references the period of arrival and i uniquely identifies the investor among all investors arriving in the same period. Upon arrival, each investor (i,t) selects an optimal level of blockchain investment and passively holds this investment over their investment horizon. At the end of their investment horizon, investor (i,t) sells their investment and exits. Additionally, we index each user by $(j,t) \in [0,\eta_t] \times \mathbb{N}$ where t references the period of arrival and j uniquely identifies the user among all users arriving in the same period. Users have two-period horizons with preferences over traditional consumption and blockchain execution in their second period. Consumption requires purchasing fiat money in the prior period whereas blockchain execution requires purchasing the blockchain's native asset in the prior period. Users select an optimal allocation across fiat money and the blockchain's native asset in their initial period to maximize their utility in their terminal period.

2.1 Investors

Investor (i,t) arrives at the beginning of period t with unlimited capital and selects an optimal level of blockchain investment upon arrival. Each investor holds their investment passively until the end of their investment horizon $\tau_{(i,t)} \overset{i.i.d.}{\sim} Geom(\pi)$ with $\pi \in (0,1)$ where $\tau_{(i,t)}$ is realized at the beginning of period t and is independent of all else. At the end of investor (i,t)'s investment horizon $t + \tau_{(i,t)}$, investor (i,t) sells their investment and exits.

We specify investor risk preferences by specifying their stochastic discount factors directly. More concretely, we specify investor (i,t)'s risk pricing in their terminal period as follows:

$$\Lambda^{(i,t)}_{t,t+\tau_{(i,t)}} = \prod_{k=0}^{\tau_{(i,t)}-1} \Lambda_{t+k,t+k+1} \tag{2.2}$$

where $\Lambda_{t+k,t+k+1}$ denotes a one-period pricing kernel from the beginning of period $t+k$ to the beginning of period $t+k+1$. $\Lambda_{t+k,t+k+1}$ is given explicitly as follows:

$$\Lambda_{t+k,t+k+1} = \exp\Big(- r_f - \frac{\lambda^2}{2} - \lambda \, z_{t+k,t+k+1} \Big) \tag{2.3}$$

where $r_f > 0$ denotes the risk-free rate, $\lambda > 0$ denotes the price of risk and $z_{t+k,t+k+1}$ corresponds to normalized shocks from Equation (2.1):

$$z_{t+k,t+k+1} = \frac{\log(\varepsilon_{t+k,t+k+1}) - \left(\mu - \frac{\sigma^2}{2}\right)}{\sigma} \tag{2.4}$$

Note that Equation (2.3) implies that investors discount pay-offs not only because investment entails foregoing investment in a risk-free bond (i.e., $\Lambda_{t+k,t+k+1}$ decreases in r_f) but also because investors are risk-averse (i.e., $\Lambda_{t+k,t+k+1}$ decreases in $\varepsilon_{t+k,t+k+1}$). The latter condition implies that investors require a risk premium for bearing blockchain-related risk and thus equilibrium investment returns with positive risk must exceed the risk-free rate. This notion of investor risk pricing is standard (see, e.g., Markowitz 1952 and Sharpe 1964) and the specific form of the pricing kernel in Equation (2.3) arises naturally from standard assumptions on investor preferences (see, e.g., Rubinstein 1976 and Lucas 1978). As an aside, the normalized pricing kernel also defines a measure change to the risk-neutral probability (see, e.g., Harrison and Kreps 1979) where the price of risk λ parameterizes the measure change. To ensure the absence of arbitrage, we impose $\xi \in \left(\log(1-\pi),\ 0\right)$ where ξ denotes the excess return under the risk-neutral measure associated with $\{\varepsilon_{t,t+1}\}_{t\geq 0}$:

$$\xi := \mu^{\mathbb{Q}} - r_f \tag{2.5}$$

with the expected return for each $\varepsilon_{t,t+1}$ under the risk-neutral measure being given explicitly by $\mu^{\mathbb{Q}} = \mu - \lambda\,\sigma$.

Crucially, all investments involving risk associated with $\{\varepsilon_{t,t+1}\}_{t\in\mathbb{N}}$ must be priced by the stochastic discount factor in Equation (2.2). In particular, letting $R_{t,t+\tau}$ denote the gross return from investing on the blockchain from t to $t+\tau$, then the following equation must hold for all (i,t):

$$\mathbb{E}[\Lambda^{(i,t)}_{t,t+\tau_{(i,t)}} R_{t,t+\tau_{(i,t)}} \mid \mathcal{F}_t] = 1 \tag{2.6}$$

where $\mathcal{F}_t$ denotes the information set at the beginning of period t.

Intuitively, Equation (2.6) states that the marginal investment value must equate with the marginal investment cost. This condition is equivalent to requiring optimal investment because we assume investors possess unlimited capital and thus investors optimally invest until their marginal benefit for each investment equates with their marginal cost for that investment. To add more detail, the right-hand side of Equation (2.6) corresponds to the marginal cost whereas the left-hand side of Equation (2.6) corresponds to the marginal benefit. To see this point, note that a gross return (i.e., $R_{t,t+\tau_{(i,t)}}$) entails normalizing an investment so that its price is unity whereas the price of an investment is its cost to an investor, implying that the right-hand side of Equation (2.6) corresponds to the unit investment cost. Then, since $\Lambda^{(i,t)}_{t,t+\tau_{(i,t)}}$ is the investor's pricing kernel and $R_{t,t+\tau_{(i,t)}}$ corresponds to the pay-off from a unit investment, the left-hand side of Equation (2.6) necessarily corresponds to the investor's marginal valuation for a unit investment.

Although Equation (2.6) can be applied to any investment with blockchain-related risk, we

focus on *staking* investment. Staking entails purchasing the blockchain's native asset and receiving seigniorage rewards. More concretely, all new units of the blockchain's native asset are paid out to those providing staking investment in a pro-rata fashion as follows:

$$R_{t,t+1} = \frac{\mathcal{P}_{t+1}}{\mathcal{P}_t}\Big(1 + \frac{M_{t+1} - M_t}{S_t}\Big) \tag{2.7}$$

where $M_t > 0$ denotes the blockchain native asset's supply at the beginning of period t, $S_t \in [0, M_t]$ denotes the total blockchain native asset units staked during period t and $\mathcal{P}_t$ denotes the blockchain native asset's price at the beginning of period t.

To understand Equation (2.7), note that one unit of numeraire yields $\frac{1}{\mathcal{P}_t}$ units of the blockchain's native asset. Then, since staking is rewarded with seigniorage and $M_{t+1} - M_t$ refers to the new units of the blockchain's native asset, each unit of the blockchain's native asset applied to staking investment therefore accrues a gross return of $1 + \frac{M_{t+1}-M_t}{S_t}$. In turn, each unit of numeraire staked at time t yields $\frac{1}{\mathcal{P}_t}(1 + \frac{M_{t+1}-M_t}{S_t})$ units of the blockchain's native asset and thus $\frac{\mathcal{P}_{t+1}}{\mathcal{P}_t}(1 + \frac{M_{t+1}-M_t}{S_t})$ units of numeraire.

For exposition, we assume that the blockchain native asset supply exhibits constant proportional growth as follows:[3]

$$\log(M_{t+1}) - \log(M_t) = \rho \tag{2.8}$$

where $\rho > 0$ denotes the supply growth rate. Then, applying Equation (2.8) to Equation (2.7) yields the following characterization of staking returns:

$$R_{t,t+1} = \frac{\mathcal{P}_{t+1}}{\mathcal{P}_t}\Big(1 + \frac{e^{\rho} - 1}{\theta_t}\Big) \tag{2.9}$$

where $\theta_t := \frac{S_t}{M_t}$ denotes the proportion of blockchain native asset staked, hereafter the *staking ratio*.

Note that the cumulative blockchain investment return $R_{t,t+\tau_{(i,t)}}$ in Equation (2.6) is given mechanically as the product of period-by-period returns across investor (i,t)'s horizon. More explicitly:

$$R_{t,t+\tau_{(i,t)}} = \prod_{k=0}^{\tau_{(i,t)}-1} R_{t+k,t+k+1} \tag{2.10}$$

where $R_{t+k,t+k+1}$ is given by Equation (2.9).

2.2 Users

User (j,t) arrives at the beginning of period t with a unit of capital. Each user (j,t) values period-$(t+1)$ consumption and period-$(t+1)$ blockchain execution. Notably, we assume that period-$(t+1)$ consumption requires holding fiat money while period-$(t+1)$ blockchain execution requires holding the blockchain's native asset. Thus, user (j,t) allocates their unit of capital across fiat money and

[3]We impose constant proportional growth only to ease exposition of the core economic channel driving our results. More concretely, our results generalize to the case that supply growth varies endogenously with relevant economic quantities (e.g., the staking ratio).

the blockchain's native asset in period t to receive traditional consumption and blockchain execution in period $t+1$. Formally, user (j,t) possesses the following preference structure:

$$U_{(j,t)} = \mathbb{E}[u(c_{(j,t)}^{t+1}) + \upsilon\, b_{(j,t)}^{t+1} \mid \mathcal{F}_t] \tag{2.11}$$

where $c_{(j,t)}^{t+1}$ denotes user (j,t)'s period $t+1$ consumption, $b_{(j,t)}^{t+1}$ denotes the real value user (j,t) applies in period $t+1$ for blockchain execution, $\upsilon > 0$ denotes the economic value of blockchain execution per unit of real value and $u : \mathbb{R}_+ \mapsto \mathbb{R}$ denotes user (j,t)'s period utility function for consumption. We hereafter refer to υ as *blockchain productivity*. This terminology reflects that υ determines the economic value users derive per unit of real value applied to blockchain execution: a more productive blockchain generates more welfare from each unit of user expenditure. In turn, user (j,t)'s optimization problem is given as follows:

$$\begin{aligned} w_{(j,t)} = \underset{w \in L^\infty(\mathcal{F}_t;[0,1])}{\arg\max} \quad & U_{(j,t)} = \mathbb{E}[u(c_{(j,t)}^{t+1}) + \upsilon\, b_{(j,t)}^{t+1} \mid \mathcal{F}_t] \\ \text{s.t.} \quad & c_{(j,t)}^{t+1} = (1-w)\beta \\ & b_{(j,t)}^{t+1} = \frac{w\mathcal{P}_{t+1}}{\mathcal{P}_t} \end{aligned} \tag{2.12}$$

where $w_{(j,t)}$ corresponds to the capital invested in the blockchain's native asset so that $1 - w_{(j,t)}$ corresponds to the capital invested in fiat money. We do not model fiat dynamics endogenously because this is not of interest for our study. Rather, we let $\beta \in (0,1]$ capture fiat inflation in an exogenous manner, hence the period $t+1$ consumption equals the initial fiat investment scaled by β (i.e., $c_{(j,t)}^{t+1} = (1 - w_{(j,t)})\beta$). In contrast, we determine the price dynamics of the blockchain's native asset endogenously and thus the real value applied for blockchain execution, $b_{(j,t)}^{t+1}$, is given by the initial investment in the blockchain's native asset multiplied by the gross return on the blockchain's native asset (i.e., $b_{(j,t)}^{t+1} = \frac{w_{(j,t)}\mathcal{P}_{t+1}}{\mathcal{P}_t}$). Following standard conventions, we assume that $u \in \mathcal{C}^2(0,\infty)$ is strictly increasing (i.e., $u' > 0$), strictly concave (i.e., $u'' < 0$), and satisfies $\lim_{c \to 0^+} u'(c) = \infty$.

2.3 Market Clearing

We derive the price of the blockchain's native asset endogenously by equating the market value of the blockchain's native asset supply at the beginning of period t, $\mathcal{M}_t$, with the market value of the blockchain's native asset demand at the beginning of period t, $\mathcal{D}_t$:

$$\mathcal{M}_t = \mathcal{D}_t \tag{2.13}$$

As noted, the blockchain's native asset supply evolves deterministically as per Equation (2.8). In turn, the market value of asset supply is given as follows:

$$\mathcal{M}_t = M_t \mathcal{P}_t \tag{2.14}$$

In contrast, the asset demand is stochastic and entails two components:

$$\mathcal{D}_t = \mathcal{D}_t^I + \mathcal{D}_t^U \tag{2.15}$$

where $\mathcal{D}_t^I$ denotes the blockchain native asset market value held by investors for staking while $\mathcal{D}_t^U$ denotes the blockchain native asset market value held by users for the purpose of period-$(t+1)$ blockchain execution. $\mathcal{D}_t^I$ is given explicitly as follows:

$$\mathcal{D}_t^I = \mathcal{D}_{0_-,t}^I + \sum_{k=1}^{t} \mathcal{D}_{k,t}^I \tag{2.16}$$

with $\mathcal{D}_{k,t}^I$ denoting the market value of demand from investors arriving in period $k > 0$ at the beginning of period $t \geq k > 0$ and $\mathcal{D}_{0_-,t}^I$ denoting the market value of demand at the beginning of period $t > 0$ from investors arriving before period 1. These quantities satisfy the following equations:

$$\mathcal{D}_{k,t}^I = (1-\pi)^{t-k}\Big(\prod_{s=k}^{t-1} R_{s,s+1}\Big)\mathcal{D}_{k,k}^I, \qquad \mathcal{D}_{0_-,t}^I = (1-\pi)^{t-1}\left(\prod_{s=1}^{t-1} R_{s,s+1}\right)\mathcal{D}_{0_-,1}^I \tag{2.17}$$

To understand Equation (2.17), recall that investors exit with probability π in each period but their investments incur a gross return $R_{s,s+1}$ from period s to $s+1$ if the investor does not exit in period s. Thus, an investment in period k grows by $\Big(\prod_{s=k}^{t-1} R_{s,s+1}\Big)$ by period $t > k$ if there is no exit before period t but only $(1-\pi)^{t-k}$ of investors from period k remain at the beginning of period t. In turn, the total investment from investors arriving in period $k > 0$ grows from $\mathcal{D}_{k,k}^I$ in period k to $(1-\pi)^{t-k}\Big(\prod_{s=k}^{t-1} R_{s,s+1}\Big)\mathcal{D}_{k,k}^I$ in period $t \geq k$. Similarly, the total investment from investors arriving before period 1 grows from $\mathcal{D}_{0_-,1}^I$ to $(1-\pi)^{t-1}\Big(\prod_{s=1}^{t-1} R_{s,s+1}\Big)\mathcal{D}_{0_-,1}^I$ in period $t > 0$. Note that Equation (2.17) determines $\mathcal{D}_{k,t}^I$ and $\mathcal{D}_{0_-,t}^I$ given $\mathcal{D}_{k,k}^I$ and $\mathcal{D}_{0_-,1}^I$. We explain how $\mathcal{D}_{k,k}^I$ and $\mathcal{D}_{0_-,1}^I$ are determined in Section 3.1.

We model explicitly only events occurring from period $t = 1$ onward. In turn, we take as given the quantity of stake held at the beginning of period 1 by investors arriving before period 1. We denote this quantity as S_{0_-} and it determines $\mathcal{D}_{0_-,1}^I$ as follows:

$$\mathcal{D}_{0_-,1}^I = \mathcal{P}_1 S_{0_-} \tag{2.18}$$

3 Model Solution

3.1 Equilibrium Definition

We solve for a symmetric equilibrium where all period-t investors invest equally in blockchain investment and where all period-t users equally purchase blockchain execution. More formally, in such an equilibrium, the blockchain native asset market value demand in period t from investors

arriving in period t is given as follows:

$$\mathcal{D}^I_{t,t} = \mathcal{I}_t \tag{3.1}$$

where $\mathcal{I}_t$ is the endogenous blockchain investment by all investors arriving in period t.

Moreover, in such an equilibrium, the blockchain native asset market value demand by users is given as follows:

$$\mathcal{D}^U_t = w_t \eta_t \tag{3.2}$$

where $w_t \in [0, 1]$ is the endogenous blockchain native asset investment by each user arriving in period t.

The comprehensive equilibrium definition is given as follows:

Definition 3.1. Equilibrium

Given a risk-free rate r_f, a price of risk λ, an investor exit probability π, a native asset supply growth rate ρ, a mean and volatility of user-arrival growth (μ, σ), a blockchain productivity υ, a user consumption utility function u, a fiat inflation parameter β, an initial native asset supply M_0 and an initial user measure η_0, an equilibrium is a staking ratio sequence $\{\theta^\star_t\}_{t\geq 0}$, an investor blockchain investment sequence $\{\mathcal{I}^\star_t\}_{t\geq 0}$, a user blockchain investment sequence $\{w^\star_t\}_{t\geq 0}$, an initial amount of staked native assets $S^\star_{0_-}$, an equilibrium price sequence $\{\mathcal{P}^\star_t\}_{t\geq 0}$ and a staking return sequence $\{R^\star_{t,t+1}\}_{t\geq 0}$ such that:

(i) **Optimal Investor Behavior**
Each investor's marginal blockchain investment valuation equals their marginal blockchain investment cost (i.e., Equation 2.6 holds).

(ii) **Optimal User Behavior**
$w^\star_t$ solves the user optimization problem defined in Equation (2.12) for each $t \in \mathbb{N}$.

(iii) **Consistency of Prices and Returns**
The equilibrium prices and returns satisfy Equation (2.9).

(iv) **Market Clearing**
The market for the blockchain's native asset clears each period as specified by Equation (2.13).

3.2 Equilibrium Solution

Lemma A.1 establishes that user demand for the blockchain's native asset is positive (i.e., $w^\star > 0$) if and only if blockchain productivity exceeds a minimal threshold, $\underline{\upsilon}(\rho)$:

$$\upsilon > \underline{\upsilon}(\rho) := \frac{\beta\, u'(\beta)}{e^{\mu-\rho}} \tag{3.3}$$

Crucially, the blockchain is secured by staking, which is incentivized by welfare transfers from users to investors through the native asset supply growth rate. Without sufficient productivity (i.e., $\upsilon \leq \underline{\upsilon}(\rho)$), users do not demand the blockchain's native asset and thus no welfare is available to

transfer, eliminating staking incentives entirely. Lemma A.1 therefore establishes a trivial instance of the productivity enables security channel whereby a minimal productivity threshold, $\underline{\upsilon}(\rho)$, must be met for the blockchain to possess any security. We hereafter focus on the non-trivial case $\upsilon > \underline{\upsilon}(\rho)$ and study how the cost of attack varies with blockchain productivity when the blockchain possesses sufficient productivity for strictly positive staking. We begin by providing the equilibrium solution:

Proposition 3.1. Equilibrium Solution
When the blockchain possesses sufficient productivity for strictly positive staking (i.e., Equation 3.3 holds), the equilibrium is given as follows:

- **Staking Ratio**
  The equilibrium staking ratio is given as follows:

$$\theta_t^\star = \theta^\star := \frac{e^\rho - 1}{e^{-\xi+\rho} - 1} \tag{3.4}$$

- **User Blockchain Investment**
  The equilibrium user blockchain investment is given as follows:

$$w_t^\star = w^\star := 1 - \frac{(u')^{-1}\left(\frac{\upsilon\, e^{\mu-\rho}}{\beta}\right)}{\beta} \tag{3.5}$$

- **Investor Blockchain Investment**
  The equilibrium investor blockchain investment is given as follows:

$$\mathcal{I}_t^\star = \left(1 - e^{-\rho}\right)\left(\frac{\pi}{1 - e^{\xi}} - 1\right) w^\star\, \eta_t \tag{3.6}$$

  where $w^\star$ is given explicitly by Equation (3.5).

- **Initial Stake**
  The staking investment at the beginning of $t = 1$ from investors arriving before $t = 1$ is:

$$S_{0\_}^\star = (1 - \pi)\, \frac{e^\rho - 1}{1 - e^{-\rho+\xi}}\, M_0 \tag{3.7}$$

- **Blockchain Native Asset Price Sequence**
  The equilibrium native-asset price sequence is:

$$\mathcal{P}_t^\star = \frac{e^\rho - e^\xi}{1 + \pi(e^\rho - 1) - e^\xi}\left(e^{-\rho} + \frac{\pi(1 - e^{-\rho})}{1 - e^{\xi}}\right)\frac{w^\star\, \eta_t}{M_0\, e^{\rho t}}, \tag{3.8}$$

  where η_t is exogenous and given by Equation (2.1) whereas $w^\star$ is given explicitly by Equation (3.5).

- **Staking Return Process**

The equilibrium staking returns are given as follows:

$$R^{\star}_{t,t+1} = e^{-\xi}\,\varepsilon_{t,t+1} \tag{3.9}$$

4 Settlement Security

To assess settlement security, we model a malicious agent, hereafter referred to as an *attacker*. The attacker seeks to disrupt blockchain settlement by acquiring a sufficient share of the overall stake. In particular, since the PoS protocol confers authority to participate in the settlement process on the basis of stake (see, e.g., John et al. 2025a and John and Saleh 2025), any particular disruption would require some stake share, and we take that share as an exogenous parameter to accommodate arbitrary attack types. Formally, we model a successful attack as requiring $\alpha \in (\frac{1}{3}, 1)$ of the stake. Notably, settlement authority derives only from staked native assets because participating in the settlement process requires digitally signing with the cryptographic keys associated with staked native assets. Relatedly, liquid staking tokens (e.g., stETH, wstETH) cannot contribute to executing a successful attack because they convey cash-flow rights and provide no access to the underlying cryptographic keys. Thus, the period-t attacker *absolute disruption cost*, κ_t, is given as follows:

$$\kappa_t = \tilde{\mathcal{P}}_t(\tilde{Q}_t)\,\tilde{Q}_t \tag{4.1}$$

where $\tilde{\mathcal{P}}_t(Q)$ denotes the blockchain native asset price given that the attacker purchases $Q \geq 0$ units while $\tilde{Q}_t$ denotes the quantity that the attacker needs to purchase to successfully disrupt blockchain settlement. Crucially, we determine $\tilde{\mathcal{P}}_t(Q)$ and $\tilde{Q}_t$ endogenously based on the optimal actions of users and investors. More explicitly, we augment Equation (2.15) by adding the attacker's demand, apply Equation (2.13), and then invoke the equilibrium solution from Proposition 3.1 to derive the inverse demand curve as follows:

$$\tilde{\mathcal{P}}_t(Q) = \Psi_t(Q)\,\mathcal{P}_t \tag{4.2}$$

where $\Psi_t(Q)$ denotes the *price impact* given a trade of size Q. For simplicity, we derive Equation (4.2) under the assumption of non-anticipation, namely that agents do not anticipate an attack in equilibrium. As we discuss subsequently, our results are robust to relaxing this assumption. More concretely, while relaxing the assumption may alter the demand curve the attacker faces, our main results nonetheless hold under any reasonable demand curve specification (Remark 4.1 and Section 5.2). Importantly, we also show later that our non-anticipation assumption is without loss of generality for sufficiently productive blockchains because the protocol can engineer attacks to be prohibitively expensive in that case (Proposition 5.7). To add further detail, an attack being prohibitively expensive implies that it does not arise in equilibrium, further implying that agents rationally anticipate no attack in equilibrium.

Notably, the price impact from an attacker purchase of Q depends upon the circulating supply of the blockchain's native asset. This circulating supply is the residual of the total supply, M_t, after

subtracting $S^{\star}_{(t-1)_-}$, the equilibrium level of staked blockchain native asset units held by investors arriving before period t. $S^{\star}_{(t-1)_-}$ is given explicitly as follows where the subscript $(t-1)_-$ refers to all investor cohorts arriving strictly before period t:

$$S^{\star}_{(t-1)_-} = (1-\pi)\, M_t\, \frac{1-e^{-\rho}}{1-e^{-\rho+\xi}} \tag{4.3}$$

In turn, the price impact function is given as follows:

$$\Psi_t(Q) = \begin{cases} \dfrac{1}{1-\frac{Q}{M_t - S^{\star}_{(t-1)_-}}} & \text{if } Q < M_t - S^{\star}_{(t-1)_-} \\ \infty & \text{otherwise} \end{cases} \tag{4.4}$$

Akin to symmetric information models in financial engineering (e.g., Bertsimas and Lo 1998, Almgren and Chriss 2001, Obizhaeva and Wang 2013, and Capponi et al. 2025), price impact in our setting arises from demand competing for a finite supply. In more detail, supply is the residual of the native asset supply after subtracting the endogenous staking investment, $M_t - S^{\star}_{(t-1)_-}$, while demand $w^{\star}_t \eta_t$ is the endogenous native asset demand of users optimizing their blockchain execution (Equation 2.15). The attacker must compete with user demand for a finite supply, and this generates endogenous price impact. In turn, the price impact $\Psi_t(Q)$ is derived, not assumed: it is the market-clearing consequence of the attacker drawing down a fixed circulating supply, and a price elasticity cannot be imposed in an ad hoc manner.

Remark 4.1. Equation (4.4) shows that the price impact diverges as the attacker's purchase Q approaches the circulating float $M_t - S^{\star}_{(t-1)_-}$. Crucially, this divergence does not depend on narrow assumptions about user demand. Rather, it arises from market clearing: as the float shrinks, the price required to clear the market grows without bound. More formally, the result requires only that the staking level be high enough to leave the circulating float insufficient to satisfy the attacker's demand and that user demand be non-zero. In Section 5, we show that both conditions hold for a sufficiently productive blockchain (Proposition 5.8).

Remark 4.2. We emphasize that the price impact can be engineered to diverge even when the attacker splits the purchase over multiple periods. In particular, as the float shrinks toward the size of a single period's purchase, the price impact on that purchase grows without bound. As we discuss further in Section 5, our results are consequently robust to a multi-period attacker.

We now derive $\tilde{Q}_t$ explicitly as follows:

$$\tilde{Q}_t = \begin{cases} \dfrac{\alpha\,(M_t - S^{\star}_{(t-1)_-})\,\left(S^{\star}_{(t-1)_-} + I^{\star}_t\right)}{(1-\alpha)\,(M_t - S^{\star}_{(t-1)_-}) + \alpha\, I^{\star}_t} & \text{if } \alpha < 1 - \dfrac{S^{\star}_{(t-1)_-}}{M_t} \\ M_t - S^{\star}_{(t-1)_-} & \text{otherwise} \end{cases} \tag{4.5}$$

where $I^{\star}_t = \frac{\mathcal{I}^{\star}_t}{\mathcal{P}^{\star}_t}$ refers to the equilibrium native asset units purchased by investors arriving in period

t. When acquiring α of the staked blockchain native asset units is not feasible, we assume that purchasing all available units suffices to disrupt the blockchain (i.e., $\tilde{Q}_t = M_t - S^{\star}_{(t-1)_-}$ when $\alpha \geq 1 - \frac{S^{\star}_{(t-1)_-}}{M_t}$).

Ultimately, a blockchain disruption attack arises if and only if the attack benefit exceeds the attack cost. We focus on the two most common cases in the literature where the attack benefit is either exogenous or proportional to the blockchain native asset's market value. In the former case, if the absolute disruption cost κ_t can be made arbitrarily large, then the attack cost can be engineered to exceed any finite benefit, thereby establishing settlement security. In the latter case, if the ratio of disruption cost to market value can be made arbitrarily large, then the attack cost can be engineered to exceed any benefit proportional to market value, thereby establishing settlement security. To that end, we define the *relative disruption cost* $\tilde{\kappa}_t$ as follows:

$$\tilde{\kappa}_t := \frac{\kappa_t}{\mathcal{M}^{\star}_t} \tag{4.6}$$

where $\mathcal{M}^{\star}_t$ denotes the equilibrium native asset market value, derived by applying Equation (3.8) to Equation (2.14), and is given explicitly by:

$$\mathcal{M}^{\star}_t = \frac{e^{\rho} - e^{\xi}}{1 + \pi(e^{\rho} - 1) - e^{\xi}} \Big(e^{-\rho} + \frac{\pi(1 - e^{-\rho})}{1 - e^{\xi}} \Big) w^{\star} \, \eta_t \tag{4.7}$$

Crucially, in Section 5, we demonstrate that both κ_t and $\tilde{\kappa}_t$ can simultaneously be made arbitrarily large when the blockchain generates sufficient economic value. This implies that a sufficiently productive blockchain can be engineered so that attack costs exceed attack benefits irrespective of whether attacker benefits are exogenous or proportional to market value.

5 Results

Throughout this section, we analyze how disruption costs, κ_t and $\tilde{\kappa}_t$, respond to changes in blockchain productivity υ and the native asset supply growth rate ρ. As discussed in Section 3.2, we restrict attention to blockchains with sufficient productivity to induce the non-trivial equilibrium (Equation 3.3). Hereafter, we write $\kappa_t(\upsilon, \rho)$ and $\tilde{\kappa}_t(\upsilon, \rho)$ for the absolute and relative disruption costs when blockchain productivity is υ and the native asset supply growth rate is ρ.

We provide two main results. First, in Section 5.1, we demonstrate that *both* the absolute and relative blockchain disruption costs, $\kappa_t(\upsilon, \rho)$ and $\tilde{\kappa}_t(\upsilon, \rho)$, can be made to increase simultaneously when blockchain productivity υ increases with accompanying adjustments to the native asset supply growth rate ρ. Then, in Section 5.2, we demonstrate that, for sufficiently productive blockchains, the supply growth rate can be chosen so that both disruption costs exceed any attack benefit. Overall, our results establish that sufficiently productive PoS blockchains can be secured against arbitrarily large disruption incentives.

5.1 Disruption Costs Increase with Productivity

In this subsection, we let υ and ρ denote the blockchain productivity and the native asset supply growth rate respectively. We consider how disruption costs change when blockchain productivity increases from υ to $\upsilon' > \upsilon$ while the supply growth rate adjusts simultaneously to ρ':

$$\rho'(\upsilon', \upsilon, \rho) := \rho + \phi \log\Big(\frac{\upsilon'}{\upsilon}\Big) \tag{5.1}$$

with $\phi \in (0, 1)$ governing the extent that the supply growth rate increases in response to an increase in blockchain productivity. We specify Equation (5.1) to operationalize a partial transfer of user welfare gains to investors: when blockchain productivity increases, the supply growth rate increases, directing a portion of the user welfare gain to investors. Equation (5.1) is one of many possible parameterizations of this transfer.

Our first main result is as follows:

Proposition 5.1. *Both Disruption Costs Increase with Productivity*
When the disruption costs are finite, both absolute and relative disruption costs, $\kappa_t(\upsilon, \rho)$ and $\tilde{\kappa}_t(\upsilon, \rho)$, increase with blockchain productivity υ:

$$\forall \upsilon' > \upsilon > \underline{\upsilon}(\rho): \quad \kappa_t(\upsilon', \rho'(\upsilon', \upsilon, \rho)) > \kappa_t(\upsilon, \rho) \quad \text{and} \quad \tilde{\kappa}_t(\upsilon', \rho'(\upsilon', \upsilon, \rho)) > \tilde{\kappa}_t(\upsilon, \rho) \tag{5.2}$$

Proposition 5.1 establishes that both absolute and relative disruption costs, κ_t and $\tilde{\kappa}_t$, can be made to increase simultaneously with blockchain productivity υ where this is achieved by increasing the native asset supply growth rate ρ appropriately. The underlying intuition is that the absolute disruption cost, κ_t, can be decomposed into three multiplicative terms: the proportion of native asset supply needed for a successful disruption $\tilde{\alpha}_t$, the price impact from the necessary purchase $\tilde{\Psi}_t$ and the native asset market value $\mathcal{M}_t^\star$. Higher blockchain productivity υ raises native asset user demand $w_t^\star$ and thereby the native asset market value $\mathcal{M}_t^\star$. This directly implies an increase in the absolute disruption cost κ_t but not the relative disruption cost $\tilde{\kappa}_t$. Crucially, to increase not only the absolute disruption cost κ_t but also the relative disruption cost $\tilde{\kappa}_t$, the supply growth rate ρ can be raised (i.e., from ρ to $\rho + \phi \log(\frac{\upsilon'}{\upsilon})$) to generate greater staking investment. This greater staking investment then raises both the needed native asset supply proportion $\tilde{\alpha}_t$ and the associated price impact $\tilde{\Psi}_t$, without decreasing the native asset market value $\mathcal{M}_t^\star$. In turn, both the absolute and relative disruption costs κ_t and $\tilde{\kappa}_t$ increase simultaneously.

We formalize the aforementioned intuition with our subsequent results, Propositions 5.2 - 5.6. More explicitly, Proposition 5.2 establishes the decomposition of the absolute disruption cost κ_t into $\tilde{\alpha}_t$, $\tilde{\Psi}_t$ and $\mathcal{M}_t^\star$. Proposition 5.3 then demonstrates that $\tilde{\alpha}_t$, $\tilde{\Psi}_t$ and $\mathcal{M}_t^\star$ each increase when blockchain productivity rises from υ to any $\upsilon' > \upsilon$ and the native asset supply growth rate simultaneously grows from ρ to $\rho + \phi \log(\frac{\upsilon'}{\upsilon})$. Propositions 5.4 and 5.5 then clarify the economic channel behind $\tilde{\alpha}_t$ and $\tilde{\Psi}_t$ increasing, establishing that $\tilde{\alpha}_t$ and $\tilde{\Psi}_t$ increase due to greater staking investment driven by the higher supply growth rate ρ. Finally, Proposition 5.6 clarifies the economic

channel for the rise in $\mathcal{M}_t^\star$, establishing that $\mathcal{M}_t^\star$ increases because higher blockchain productivity υ raises native asset user demand $w_t^\star$.

Proposition 5.2. *Disruption Cost Decomposition*
When the absolute disruption cost is finite, it decomposes into the required native asset share $\tilde{\alpha}_t$, the price impact $\tilde{\Psi}_t$, and the market value $\mathcal{M}_t^\star$ as follows:

$$\kappa_t = \tilde{\alpha}_t \, \tilde{\Psi}_t \, \mathcal{M}_t^\star \tag{5.3}$$

where $\tilde{\alpha}_t$ and $\tilde{\Psi}_t$ are defined explicitly as follows:

$$\tilde{\alpha}_t := \frac{\tilde{Q}_t}{M_t}, \qquad \tilde{\Psi}_t := \frac{\tilde{\mathcal{P}}_t(\tilde{Q}_t)}{\mathcal{P}_t^\star} \tag{5.4}$$

and Equations (A.21) and (A.22) provide explicit solutions for each of these quantities.

Proposition 5.2 establishes that the absolute disruption cost, κ_t, can be decomposed into three multiplicative components: the share of native asset supply needed to execute the disruption $\tilde{\alpha}_t$, the price impact due to the disruption $\tilde{\Psi}_t$ and the equilibrium native asset market value $\mathcal{M}_t^\star$. This result arises because disrupting blockchain settlement requires acquiring a sufficient share of native asset supply (see, e.g., John et al. 2025a) where $\tilde{\alpha}_t = \tilde{Q}_t / M_t$ corresponds to the endogenous share needed for successful disruption. Crucially, the purchase of these native asset units cannot be executed at the marginal equilibrium price $\mathcal{P}_t^\star$. This is because the purchase constitutes additional demand, increasing the price to $\tilde{\mathcal{P}}_t(\tilde{Q}_t)$. We define the price impact as the proportional price increase due to the attacker's purchase of $\tilde{Q}_t$ native asset units, namely $\tilde{\Psi}_t = \tilde{\mathcal{P}}_t(\tilde{Q}_t)/\mathcal{P}_t^\star$. In turn, the decomposition from Equation (5.3) arises directly from Equation (4.1) as follows:

$$\kappa_t = \tilde{\mathcal{P}}_t(\tilde{Q}_t)\,\tilde{Q}_t = \frac{\tilde{\mathcal{P}}_t(\tilde{Q}_t)}{\mathcal{P}_t^\star}\,\mathcal{P}_t^\star\,\frac{\tilde{Q}_t}{M_t}\,M_t = \frac{\tilde{Q}_t}{M_t}\,\frac{\tilde{\mathcal{P}}_t(\tilde{Q}_t)}{\mathcal{P}_t^\star}\,M_t\mathcal{P}_t^\star = \tilde{\alpha}_t\,\tilde{\Psi}_t\,\mathcal{M}_t^\star \tag{5.5}$$

where we derive the exact solutions for $\tilde{\alpha}_t$ and $\tilde{\Psi}_t$ explicitly in Equations (A.21) and (A.22).

Having established the decomposition of κ_t into $\tilde{\alpha}_t$, $\tilde{\Psi}_t$ and $\mathcal{M}_t^\star$ via Proposition 5.2, we turn to demonstrating that higher blockchain productivity υ accompanied by an appropriate increase in the native asset supply growth rate ρ increases all three components of the decomposition:

Proposition 5.3. *Disruption Cost Components Increase with Productivity*
When the disruption costs are finite, all three components of the disruption cost decomposition increase with blockchain productivity υ. Making explicit their dependence on υ and ρ:

$$\begin{aligned} \forall \upsilon' > \upsilon > \underline{\upsilon}(\rho): \quad & \tilde{\alpha}_t(\upsilon', \rho'(\upsilon', \upsilon, \rho)) > \tilde{\alpha}_t(\upsilon, \rho) \\ & \tilde{\Psi}_t(\upsilon', \rho'(\upsilon', \upsilon, \rho)) > \tilde{\Psi}_t(\upsilon, \rho) \\ & \mathcal{M}_t^\star(\upsilon', \rho'(\upsilon', \upsilon, \rho)) > \mathcal{M}_t^\star(\upsilon, \rho) \end{aligned} \tag{5.6}$$

Proposition 5.3 demonstrates that higher blockchain productivity υ accompanied by an appropriate increase in the native asset supply growth rate ρ increases all three quantities: (1) the proportion of native asset supply needed for a successful disruption $\tilde{\alpha}_t$, (2) the price impact from a successful disruption $\tilde{\Psi}_t$, and (3) the equilibrium market value $\mathcal{M}_t^\star$. More pointedly, when υ rises to any $\upsilon' > \upsilon$ and the supply growth rate simultaneously grows from ρ to $\rho' = \rho + \phi \log(\frac{\upsilon'}{\upsilon})$, then all three quantities $\tilde{\alpha}_t$, $\tilde{\Psi}_t$ and $\mathcal{M}_t^\star$ increase.

The intuition for Proposition 5.3 is as follows. The equilibrium market value $\mathcal{M}_t^\star$ increases because higher blockchain productivity υ raises native asset user demand $w_t^\star$, which in turn increases the native asset market value $\mathcal{M}_t^\star$. Additionally, a portion $\phi \in (0, 1)$ of the user gain is passed along to investors via an increase in the native asset supply growth rate ρ, and this additional value for investors generates greater staking investment. This greater staking investment then raises both the native asset supply proportion needed for a successful disruption $\tilde{\alpha}_t$ and the associated price impact $\tilde{\Psi}_t$. We formalize the latter channel whereby a higher supply growth rate ρ increases staking investment and thus $\tilde{\alpha}_t$ and $\tilde{\Psi}_t$ via Propositions 5.4 - 5.5. Moreover, we formalize the former channel whereby higher blockchain productivity υ drives greater native asset user demand $w_t^\star$ and thus greater native asset market value $\mathcal{M}_t^\star$ in Proposition 5.6.

Proposition 5.4. *$\tilde{\alpha}_t$ and $\tilde{\Psi}_t$ Both Increase with Staking Investment*
The required share $\tilde{\alpha}_t$ and the price impact $\tilde{\Psi}_t$ depend on staking investment from prior investors, $s^\star_{(t-1)_-}$, and from newly arriving investors, $\iota_t^\star$:

$$\tilde{\alpha}_t := \tilde{\alpha}(s^\star_{(t-1)_-}, \iota_t^\star, \alpha), \qquad \tilde{\Psi}_t := \tilde{\Psi}(s^\star_{(t-1)_-}, \iota_t^\star, \alpha)$$

where explicit expressions are given in Equations (A.30) and (A.31). Crucially, whenever the price impact is finite, both are increasing in staking investment:

$$\begin{aligned} \forall s' > s, \iota' > \iota: \quad & \tilde{\alpha}(s', \iota, \alpha) > \tilde{\alpha}(s, \iota, \alpha), \quad \tilde{\alpha}(s, \iota', \alpha) > \tilde{\alpha}(s, \iota, \alpha) \\ & \tilde{\Psi}(s', \iota, \alpha) > \tilde{\Psi}(s, \iota, \alpha), \quad \tilde{\Psi}(s, \iota', \alpha) > \tilde{\Psi}(s, \iota, \alpha) \end{aligned} \tag{5.7}$$

Proposition 5.4 establishes that the needed native asset attacker share $\tilde{\alpha}_t$ and the associated price impact $\tilde{\Psi}_t$ both increase with staking investment from previously arriving investors $s^\star_{(t-1)_-}$ and with staking investment from newly arriving investors $\iota_t^\star$. The intuition is as follows. The attacker must acquire α of the staked native asset units to successfully disrupt the blockchain. When there is more staking investment, $s^\star_{(t-1)_-}$ or $\iota_t^\star$, then the staked native asset units increase and thus the share of the overall native asset supply needed for a successful attack $\tilde{\alpha}_t$ also increases (i.e., $\tilde{\alpha}(s', \iota, \alpha) > \tilde{\alpha}(s, \iota, \alpha)$ and $\tilde{\alpha}(s, \iota', \alpha) > \tilde{\alpha}(s, \iota, \alpha)$). Additionally, since the attacker requires a larger share of native asset supply for a successful attack, the attacker's purchase is necessarily larger and therefore has a commensurately larger price impact $\tilde{\Psi}_t$ (i.e., $\tilde{\Psi}(s', \iota, \alpha) > \tilde{\Psi}(s, \iota, \alpha)$ and $\tilde{\Psi}(s, \iota', \alpha) > \tilde{\Psi}(s, \iota, \alpha)$). Notably, both staking investment by previously arriving investors, $s^\star_{(t-1)_-}$, and staking investment by newly arriving investors, $\iota_t^\star$, are endogenous, and both increase with the

native asset supply growth rate ρ. We formalize this point with our next result:

Proposition 5.5. *Investment Increases with Supply Growth Rate*
Staking investment increases with the native asset supply growth rate ρ. Making explicit the dependence on ρ:

$$\forall\, \rho' > \rho: \quad s^{\star}_{(t-1)_-}(\rho') > s^{\star}_{(t-1)_-}(\rho), \quad \iota^{\star}_t(\rho') > \iota^{\star}_t(\rho) \tag{5.8}$$

Explicit expressions for $s^{\star}_{(t-1)_-}(\rho)$ and $\iota^{\star}_t(\rho)$ are given in Equation (A.29).

Proposition 5.5 highlights that staking investment, both $s^{\star}_{(t-1)_-}$ and $\iota^{\star}_t$, increases with the native asset supply growth rate ρ. This result arises because a higher supply growth rate ρ implies a larger inflationary transfer from users to investors and thus induces greater staking investment. Importantly, Propositions 5.4 and 5.5 collectively demonstrate the channel whereby a higher supply growth rate ρ raises both the attacker share needed for a successful disruption $\tilde{\alpha}_t$ and the associated price impact $\tilde{\Psi}_t$. In more detail, Proposition 5.5 demonstrates that a higher supply growth rate ρ raises staking investment, $s^{\star}_{(t-1)_-}$ and $\iota^{\star}_t$, whereas Proposition 5.4 establishes that this greater staking investment, $s^{\star}_{(t-1)_-}$ and $\iota^{\star}_t$, increases both $\tilde{\alpha}_t$ and $\tilde{\Psi}_t$.

We now turn to clarifying the economic channel whereby higher blockchain productivity υ drives greater native asset user demand $w^{\star}_t$ and thus increases the native asset market value $\mathcal{M}^{\star}_t$:

Proposition 5.6. *User Demand and Native Asset Market Value Increase with Productivity*
User demand $w^{\star}_t$ and market value $\mathcal{M}^{\star}_t$ both increase with blockchain productivity υ. Making explicit their dependence on υ and ρ:

$$\forall\, \upsilon' > \upsilon > \underline{\upsilon}(\rho): \quad w^{\star}(\upsilon', \rho'(\upsilon', \upsilon, \rho)) > w^{\star}(\upsilon, \rho) \tag{5.9}$$

$$\forall\, \upsilon' > \upsilon > \underline{\upsilon}(\rho): \quad \mathcal{M}^{\star}_t(\upsilon', \rho'(\upsilon', \upsilon, \rho)) > \mathcal{M}^{\star}_t(\upsilon, \rho) \tag{5.10}$$

Explicit expressions for $w^{\star}(\upsilon, \rho)$ and $\mathcal{M}^{\star}_t(\upsilon, \rho)$ are given in Equations (A.23) and (A.24).

Proposition 5.6 demonstrates that higher blockchain productivity υ accompanied by an appropriate increase in the native asset supply growth rate ρ raises native asset user demand $w^{\star}_t$ and thereby the native asset market value $\mathcal{M}^{\star}_t$. Importantly, the increase in native asset user demand $w^{\star}_t$ is specifically driven by higher blockchain productivity υ. In more detail, higher blockchain productivity υ raises user welfare and the countervailing increase in the supply growth rate ρ transfers only a portion $\phi \in (0, 1)$ of that welfare gain to investors, implying that native asset user demand $w^{\star}_t$ increases. More formally, direct verification reveals:

$$\upsilon' e^{-\rho'} > \upsilon e^{-\rho} \tag{5.11}$$

so that applying Equation (5.11) to Equation (3.5) yields the first part of Proposition 5.6:

$$w^{\star}(\upsilon', \rho') > w^{\star}(\upsilon, \rho) \tag{5.12}$$

In turn, applying Equation (5.12) to Equation (3.8) implies that the increase in native asset user demand $w_t^\star$ translates directly into an increase in the native asset market value $\mathcal{M}_t^\star$ as per the second part of Proposition 5.6.

To summarize, we have shown that an arbitrary increase in blockchain productivity from υ to $\upsilon' > \upsilon$ simultaneously raises both the absolute disruption cost, κ_t, and the relative disruption cost, $\tilde{\kappa}_t$, when accompanied by an increase in the native asset supply growth rate from ρ to $\rho' = \rho + \phi \log(\frac{\upsilon'}{\upsilon})$. In particular, the increase in the supply growth rate from ρ to ρ' implies greater staking investment (Proposition 5.5) which raises the native asset supply share needed for an attack $\tilde{\alpha}_t$ and the associated price impact $\tilde{\Psi}_t$ (Proposition 5.4). Moreover, the increase in blockchain productivity from υ to υ' raises native asset user demand $w_t^\star$ and thereby the native asset market value $\mathcal{M}_t^\star$ (Proposition 5.6). Then, since $\tilde{\alpha}_t$, $\tilde{\Psi}_t$ and $\mathcal{M}_t^\star$ each increase under the aforementioned change from (υ, ρ) to (υ', ρ') (Proposition 5.3), the decomposition $\kappa_t = \tilde{\alpha}_t \, \tilde{\Psi}_t \, \mathcal{M}_t^\star$ (Proposition 5.2) implies that the absolute disruption cost κ_t increases (Proposition 5.1). Similarly, since the relative disruption cost satisfies $\tilde{\kappa}_t = \tilde{\alpha}_t \, \tilde{\Psi}_t$ (Proposition 5.2), $\tilde{\alpha}_t$ and $\tilde{\Psi}_t$ both increasing (Proposition 5.3) implies that $\tilde{\kappa}_t$ also increases, establishing that both disruption costs rise simultaneously (Proposition 5.1).

5.2 Both Disruption Costs Diverge with Productivity

Previously, the native asset supply growth rate adjusted with blockchain productivity via a specific parameterization. We now treat the native asset supply growth rate ρ as an independent design variable. In doing so, we establish that, for sufficiently productive blockchains, ρ can be chosen to deter arbitrary attack incentives. Our second main result formalizes this point:

Proposition 5.7. *Both Disruption Costs Exceed Any Benefit*
Assume $\pi < \alpha$. Then there exists a productivity threshold $\upsilon_0 > 0$ such that, for any blockchain with higher productivity $\upsilon > \upsilon_0$ and any attack benefits $B_t > 0$ and $\tilde{B}_t > 0$, the native asset supply growth rate ρ can be chosen so that both disruption costs exceed the respective benefits:

$$\exists\, \upsilon_0 > 0 : \ \forall\, \upsilon > \upsilon_0, \ \forall\, B_t > 0, \ \tilde{B}_t > 0, \ \exists\, \rho > 0 : \ \kappa_t(\upsilon, \rho) > B_t \text{ and } \tilde{\kappa}_t(\upsilon, \rho) > \tilde{B}_t \tag{5.13}$$

Proposition 5.7 establishes that a sufficiently productive blockchain ($\upsilon > \upsilon_0$) can be secured against arbitrary attack incentives through an appropriate choice of the native asset supply growth rate ρ. The economic channel operates through the disruption cost decomposition $\kappa_t = \tilde{\alpha}_t \, \tilde{\Psi}_t \, \mathcal{M}_t^\star$ (Proposition 5.2). In particular, a higher supply growth rate ρ raises staking investment $s^\star_{(t-1)_-}$ (Proposition 5.5), which reduces the circulating supply $1 - s^\star_{(t-1)_-}$ and thereby increases the price impact $\tilde{\Psi}_t$ faced by an attacker (Proposition 5.4). However, native asset supply growth constitutes an inflationary transfer from users to investors. Users internalize this cost, so native asset user demand $w_t^\star$ decreases with the supply growth rate ρ (Proposition 3.1). Notably, the native asset market value $\mathcal{M}_t^\star$ grows with native asset user demand $w_t^\star$ (Proposition 3.1), and disruption costs increase with the native asset market value (Proposition 5.2). In turn, a higher supply growth

rate ρ involves a trade-off: a higher supply growth rate ρ increases price impact $\tilde{\Psi}_t$ but decreases native asset market value $\mathcal{M}_t^\star$. The finding of Proposition 5.7 is that, when productivity exceeds the threshold υ_0, users maintain sufficient native asset demand even when the supply growth rate ρ is high, allowing disruption costs, κ_t and $\tilde{\kappa}_t$, to grow without bound. The following result formalizes this channel:

Proposition 5.8. *Price Impact and Disruption Costs Diverge*
Assume $\pi < \alpha$. Then there exists a productivity threshold $\upsilon_0 > 0$ and a native asset supply growth rate threshold $\bar{\rho} > 0$ such that, for any blockchain with higher productivity $\upsilon > \upsilon_0$, the price impact and both disruption costs diverge as the native asset supply growth rate ρ approaches $\bar{\rho}$:

$$\begin{gathered} \exists\, \upsilon_0 > 0 :\ \forall\, \upsilon > \upsilon_0 :\ \lim_{\rho \to \bar{\rho}^-} \tilde{\Psi}_t(\upsilon, \rho) = \infty \\ \lim_{\rho \to \bar{\rho}^-} \kappa_t(\upsilon, \rho) = \infty, \quad \lim_{\rho \to \bar{\rho}^-} \tilde{\kappa}_t(\upsilon, \rho) = \infty \end{gathered} \tag{5.14}$$

where $\bar{\rho}$ is given explicitly by Equation (A.42).

Proposition 5.8 formalizes the channel underlying Proposition 5.7. In more detail, the threshold $\bar{\rho}$ (Equation A.42) is the native asset supply growth rate at which staking investment reaches a level such that the attacker would need to purchase the entire remaining circulating supply to successfully execute the attack. In turn, as the supply growth rate ρ approaches $\bar{\rho}$ from below, the price impact $\tilde{\Psi}_t$ diverges to infinity, driving both disruption costs, κ_t and $\tilde{\kappa}_t$, to infinity. Crucially, this divergence requires that users maintain positive native asset demand even as the supply growth rate ρ approaches $\bar{\rho}$, a condition which holds only when the blockchain is sufficiently productive to sustain user participation despite the high inflationary welfare transfer (i.e., $\upsilon > \upsilon_0$). The key implication is that any finite attack benefit can be exceeded for a sufficiently productive blockchain: since κ_t and $\tilde{\kappa}_t$ diverge as $\rho \to \bar{\rho}^-$, there exists some $\rho < \bar{\rho}$ at which disruption costs exceed any given B_t and $\tilde{B}_t$.

We emphasize that our central conclusion holds under general assumptions about user demand: a sufficiently productive blockchain can be secured against arbitrary attack incentives (Proposition 5.7) because the price impact can be engineered to diverge (Proposition 5.8). In more detail, once the native asset supply growth rate ρ reaches the level $\bar{\rho}$ such that an attacker must purchase the entire unstaked circulating supply, the price impact $\tilde{\Psi}_t$, and hence the disruption costs, κ_t and $\tilde{\kappa}_t$, diverge so long as native asset user demand $\mathcal{D}_t^U$ remains non-zero. Notably, non-zero user demand at $\bar{\rho}$ is exactly what sufficient productivity ($\upsilon > \upsilon_0$) guarantees, so our conclusion requires nothing about demand beyond the productivity condition under which it is stated.

As a related point, our results are also robust to a multi-period attacker. We currently assume the attacker acquires the necessary stake within a single period, but this is only for simplicity. In particular, our results hold even when the acquisition is spread over finitely many periods. Doing so lowers the purchase made in each period, and with it the per-period price impact. Nonetheless, given sufficient productivity, the protocol can shrink the circulating supply far enough that the

price impact remains prohibitive even on these reduced purchases. The required supply growth rate ρ is correspondingly higher than in the single-period case, but achieving it still requires only that the blockchain be sufficiently productive.

Finally, as a technical aside, Propositions 5.7 and 5.8 assume $\pi < \alpha$, a condition that is equivalent to requiring that average investor horizons $\frac{1}{\pi}$ exceed an exogenous threshold $\frac{1}{\alpha}$. This condition is innocuous because it can be ensured through the design of a PoS protocol. In particular, PoS blockchains generally impose withdrawal restrictions (e.g., limits on aggregate staking outflow rates, staking withdrawal lags, etc.), and these restrictions imply a lower bound on average investor horizons. The protocol designer can thus specify withdrawal restrictions to ensure the required condition.

6 Conclusion

This paper establishes that a sufficiently productive Proof-of-Stake blockchain can be engineered to achieve settlement security against arbitrarily large disruption incentives. The key design lever is the native asset supply growth rate: by setting it appropriately, a protocol designer can ensure that the cost of acquiring the stake needed to disrupt settlement exceeds any finite attack benefit. Crucially, this requires that the blockchain generate sufficient economic value because users must derive enough benefit from blockchain execution to sustain demand for the native asset despite the inflationary cost of native asset supply growth. Our work is of particular importance given emerging interest in asset tokenization on blockchains (Malinova and Park 2023; Laschinger et al. 2024; Cong et al. 2025b; Cartea et al. 2026) where the success of these initiatives depends on achieving secure settlement at scale (Harvey et al. 2025). Ultimately, we demonstrate that secure settlement is achievable with appropriate economic design.

References

Almgren R, Chriss N (2001) Optimal execution of portfolio transactions. *Journal of Risk* 3(2):5–39.

Atkins PS (2025) American leadership in the digital finance revolution. URL `https://www.sec.gov/newsroom/speeches-statements/atkins-digital-finance-revolution-073125`, speech at the America First Policy Institute, Washington, D.C., July 31, 2025.

Bertsimas D, Lo AW (1998) Optimal control of execution costs. *Journal of Financial Markets* 1(1):1–50.

Budish E (2025) Trust at scale: The economic limits of cryptocurrencies and blockchains. *The Quarterly Journal of Economics* 140(1):1–62.

Capponi A, Menkveld AJ, Zhang H (2025) Large orders in small markets: Execution with endogenous liquidity supply. *Review of Finance* 29(1):201–239.

Cartea Á, Drissi F, Saleh F (2026) The economics of regulating tokenized securities. *Working Paper* .

Cong LW, He Z, Tang K (2025a) The tokenomics of staking. *NBER Working Paper* (w33640).

Cong LW, Landsman WR, Rabetti D, Zhang C, Zhao W (2025b) Tokenized stocks. *Available at SSRN 5937314* .

Harrison JM, Kreps DM (1979) Martingales and arbitrage in multiperiod securities markets. *Journal of Economic Theory* 20(3):381–408.

Harvey CR, Saleh F, Sverchkov R (2025) An economic model of the l1-l2 interaction. *Available at SSRN 5163823* .

Jermann UJ (2025) A macro finance model for proof-of-stake ethereum. *Available at SSRN 4335835* .

John K, Monnot B, Mueller P, Saleh F, Schwarz-Schilling C (2025a) Economics of ethereum. *Journal of Corporate Finance* 91:102718.

John K, Rivera TJ, Saleh F (2025b) Proof-of-work versus proof-of-stake: A comparative economic analysis. *The Review of Financial Studies* 38(7):1955–2004.

John K, Saleh F (2025) Cryptoeconomics. *Oxford Research Encyclopedia of Economics and Finance*.

Laschinger R, Leonhard H, Dorfleitner G, Schäfers W (2024) Liquidity mechanisms in real-world assets: The empirical case of real estate tokenization. *Available at SSRN 5036350* .

Lucas RE (1978) Asset prices in an exchange economy. *Econometrica* 46(6):1429–1445.

Lucas RE, Stokey NL (1987) Money and interest in a cash-in-advance economy. *Econometrica* 55(3):491–513.

Malinova K, Park A (2023) Tokenized stocks for trading and capital raising. *Available at SSRN 4365241* .

Markowitz H (1952) Portfolio selection. *The Journal of Finance* 7(1):77–91.

Nakamoto S (2008) Bitcoin: A peer-to-peer electronic cash system. *Available at SSRN 3440802* .

Obizhaeva AA, Wang J (2013) Optimal trading strategy and supply/demand dynamics. *Journal of Financial Markets* 16(1):1–32.

Roşu I, Saleh F (2021) Evolution of shares in a proof-of-stake cryptocurrency. *Management Science* 67(2):661–672.

Rubinstein M (1976) The valuation of uncertain income streams and the pricing of options. *The Bell Journal of Economics* 7(2):407–425.

Saleh F (2021) Blockchain without waste: Proof-of-stake. *The Review of financial studies* 34(3):1156–1190.

Sharpe WF (1964) Capital asset prices: A theory of market equilibrium under conditions of risk. *The Journal of Finance* 19(3):425–442.

A Proofs

Lemma A.1. *Optimal User Behavior*
Consider the following optimization problem parameterized by $(\upsilon, \rho, \mu, \beta)$ with $\upsilon > 0$, $\rho > 0$, $\mu > 0$ and $\beta \in (0, 1]$:

$$w^\star = \underset{w\in[0,1]}{\arg\max}\ U(w) := u((1-w)\beta) + \upsilon\, w\, e^{\mu-\rho} \tag{A.1}$$

where $u \in \mathcal{C}^2(0,\infty)$ satisfies $u' > 0$, $u'' < 0$ and $\lim_{c\to 0^+} u'(c) = \infty$. Define:

$$\underline{\upsilon}(\rho) := \beta\, u'(\beta)\, e^{\rho-\mu} \tag{A.2}$$

Then Equation (A.1) has a unique solution characterized as follows:

(i) When $\upsilon > \underline{\upsilon}(\rho)$, the solution is interior:

$$w^\star = 1 - \frac{(u')^{-1}\left(\frac{\upsilon\, e^{\mu-\rho}}{\beta}\right)}{\beta} \in (0,1) \tag{A.3}$$

(ii) When $\upsilon \le \underline{\upsilon}(\rho)$, the solution is $w^\star = 0$.

Proof.
Direct verification yields:

$$U'(w) = -\beta\, u'((1-w)\beta) + \upsilon\, e^{\mu-\rho} \tag{A.4}$$

$$U''(w) = \beta^2 u''((1-w)\beta) < 0 \tag{A.5}$$

Equation (A.5) and $\lim_{c\to 0^+} u'(c) = \infty$ imply:

$$\lim_{w\to 1^-} U'(w) = -\infty \tag{A.6}$$

Moreover, Equations (A.2) and (A.4) imply:

$$\upsilon > \underline{\upsilon}(\rho) \iff U'(0) > 0 \tag{A.7}$$

Case (i): $\upsilon > \underline{\upsilon}(\rho)$:
$\upsilon > \underline{\upsilon}(\rho)$ and Equation (A.7) imply:

$$U'(0) > 0 \tag{A.8}$$

In turn, Equations (A.5), (A.6) and (A.8) then imply a unique interior $w^\star \in (0,1)$ satisfying:

$$U'(w^\star) = 0 \tag{A.9}$$

Applying Equation (A.4) to Equation (A.9) then yields Equation (A.3).

Case (ii): $\upsilon \leq \underline{\upsilon}(\rho)$:

$\upsilon \leq \underline{\upsilon}(\rho)$ and Equation (A.7) imply:

$$U'(0) \leq 0 \tag{A.10}$$

In turn, Equations (A.5) and (A.10) imply $U'(w) < 0$ for all $w \in (0,1)$, yielding $w^\star = 0$.

□

Proof of Proposition 3.1

(i) **Optimal Investor Behavior**

Applying Equation (3.9) to Equation (2.10) yields:

$$R^\star_{t,t+\tau_{(i,t)}} = e^{-\xi\,\tau_{(i,t)}} \prod_{k=0}^{\tau_{(i,t)}-1} \varepsilon_{t+k,t+k+1} \tag{A.11}$$

Then, combining Equation (A.11) and Equations (2.2) - (2.4) yields:

$$\begin{aligned}
&\mathbb{E}[\Lambda^{(i,t)}_{t,t+\tau_{(i,t)}} R^\star_{t,t+\tau_{(i,t)}} \mid \mathcal{F}_t] \\
&= \mathbb{E}[e^{-\xi\,\tau_{(i,t)}} \prod_{k=0}^{\tau_{(i,t)}-1} \Big(\exp\big(-r_f - \frac{\lambda^2}{2} - \lambda\, z_{t+k,t+k+1}\big)\varepsilon_{t+k,t+k+1}\Big) \mid \mathcal{F}_t] \\
&= e^{-\xi\,\tau_{(i,t)}} \prod_{k=0}^{\tau_{(i,t)}-1} \mathbb{E}[\exp\big(-r_f - \frac{\lambda^2}{2} - \lambda\, z_{t+k,t+k+1}\big)\varepsilon_{t+k,t+k+1} \mid \mathcal{F}_t] \\
&= e^{-\xi\,\tau_{(i,t)}} \prod_{k=0}^{\tau_{(i,t)}-1} e^{\xi} \\
&= 1
\end{aligned}$$

thereby establishing Equation (2.6) as desired.

(ii) **Optimal User Behavior**

Equation (3.8) implies that:

$$\frac{\mathcal{P}^\star_{t+1}}{\mathcal{P}^\star_t} = e^{-\rho}\varepsilon_{t,t+1} \tag{A.12}$$

Then, direct verification from Equation (A.12) yields:

$$\mathbb{E}\left[\frac{\mathcal{P}^\star_{t+1}}{\mathcal{P}^\star_t} \mid \mathcal{F}_t\right] = e^{\mu-\rho} \tag{A.13}$$

Equations (3.3) and (A.13) and Lemma A.1 then yield the interior solution given by Equation (3.5).

(iii) **Consistency of Prices and Returns**

Equations (3.4) and (3.8) directly imply Equation (2.9) holds in equilibrium as desired.

(iv) **Market Clearing**

We prove this result by induction with base case $t = 1$. Equations (2.15) - (3.1), (3.5) - (3.7) and Equation (3.9) imply:

$$\mathcal{D}_1 = \Big(\frac{e^{\rho} - e^{\xi}}{1 + \pi(e^{\rho} - 1) - e^{\xi}}\Big)\Big(e^{-\rho} + \frac{\pi(1 - e^{-\rho})}{1 - e^{\xi}}\Big) w^{\star}\eta_1 \tag{A.14}$$

Additionally, Equations (2.8), (2.14) and (3.8) imply:

$$\mathcal{M}_1 = M_1\mathcal{P}_1^{\star} = \Big(\frac{e^{\rho} - e^{\xi}}{1 + \pi(e^{\rho} - 1) - e^{\xi}}\Big)\Big(e^{-\rho} + \frac{\pi(1 - e^{-\rho})}{1 - e^{\xi}}\Big) w^{\star}\eta_1 \tag{A.15}$$

In turn, Equations (A.14) and (A.15) imply Equation (2.13) for the base case, $t = 1$.

Turning to the inductive step, we assume that Equation (2.13) holds for t and establish the result for $t + 1$. To begin, Equations (2.15) - (3.1), (3.5) - (3.7) and Equation (3.9) imply:

$$\mathcal{D}_{t+1} = (1 - \pi)\, e^{-\xi}\, \varepsilon_{t,t+1}\, \mathcal{D}_t^I + w^{\star}\eta_{t+1}\left(e^{-\rho} + \frac{\pi(1 - e^{-\rho})}{1 - e^{\xi}}\right) \tag{A.16}$$

Then, applying the inductive hypotheses (i.e., $\mathcal{M}_t = \mathcal{D}_t \Leftrightarrow \mathcal{D}_t^I = M_t\mathcal{P}_t - \mathcal{D}_t^U$), Equation (3.2) and Equation (3.5) to Equation (A.16) yields:

$$\mathcal{D}_{t+1} = (1 - \pi)\, e^{-\xi}\, \varepsilon_{t,t+1}\, (M_t\mathcal{P}_t - w^{\star}\eta_t) + w^{\star}\eta_{t+1}\left(e^{-\rho} + \frac{\pi(1 - e^{-\rho})}{1 - e^{\xi}}\right) \tag{A.17}$$

Applying Equation (3.8) to Equation (A.17) then yields:

$$\mathcal{D}_{t+1} = w^{\star}\eta_{t+1}\, \frac{e^{\rho} - e^{\xi}}{1 + \pi(e^{\rho} - 1) - e^{\xi}} \left(e^{-\rho} + \frac{\pi(1 - e^{-\rho})}{1 - e^{\xi}}\right). \tag{A.18}$$

Moreover, Equations (2.8), (2.14) and (3.8) imply:

$$\mathcal{M}_{t+1} = M_{t+1}\mathcal{P}_{t+1}^{\star} = \frac{e^{\rho} - e^{\xi}}{1 + \pi(e^{\rho} - 1) - e^{\xi}}\Big(e^{-\rho} + \frac{\pi(1 - e^{-\rho})}{1 - e^{\xi}}\Big)\, w^{\star}\, \eta_{t+1} \tag{A.19}$$

so that Equations (A.18) and (A.19) imply Equation (2.13) for $t + 1$ thereby completing the proof.

□

Lemma A.2. *Settlement Disruption Cost Decomposition*
The settlement disruption cost can be decomposed as follows:

$$\kappa_t = \tilde{\alpha}_t \, \tilde{\Psi}_t \, \mathcal{M}_t^\star \tag{A.20}$$

where $\tilde{\alpha}_t = \frac{\tilde{Q}_t}{M_t}$ and $\tilde{\Psi}_t = \Psi_t(\tilde{Q}_t)$. Additionally, the following results hold:

$$\tilde{\alpha}_t = \tilde{\alpha}_t(\upsilon, \rho) := \begin{cases} \dfrac{\alpha\, e^{\xi}\,(e^{\rho}-1)\Big[(1-e^{\xi})+\pi\,(e^{\rho}-1)\Big]}{(e^{\rho}-e^{\xi})\Big\{(1-\alpha)\Big[(1-e^{\xi})+\pi\,(e^{\rho}-1)\Big]+\alpha\,(e^{\rho}-1)\,\Big[\pi+e^{\xi}-1\Big]\Big\}} & \text{if } \frac{1-e^{-\rho}}{1-e^{-\rho+\xi}} < \frac{1-\alpha}{1-\pi} \\ 1-(1-\pi)\,\frac{1-e^{-\rho}}{1-e^{-\rho+\xi}} & \text{otherwise} \end{cases} \tag{A.21}$$

$$\tilde{\Psi}_t = \tilde{\Psi}_t(\upsilon, \rho) := \begin{cases} \dfrac{(1-\alpha)\Big[1-e^{\xi}+\pi\,(e^{\rho}-1)\Big]+\alpha\,(e^{\rho}-1)\Big[\pi+e^{\xi}-1\Big]}{(1-\alpha)\,(e^{\rho}-e^{\xi})-(1-\pi)\,(e^{\rho}-1)} & \text{if } \frac{1-e^{-\rho}}{1-e^{-\rho+\xi}} < \frac{1-\alpha}{1-\pi} \\ \infty & \text{otherwise} \end{cases} \tag{A.22}$$

$$w_t^\star = w^\star(\upsilon, \rho) := 1 - \frac{(u')^{-1}\big(\frac{\upsilon\, e^{\mu-\rho}}{\beta}\big)}{\beta} \tag{A.23}$$

$$\mathcal{M}_t^\star = \mathcal{M}_t^\star(\upsilon, \rho) := \frac{e^{\rho}-e^{\xi}}{1+\pi(e^{\rho}-1)-e^{\xi}}\Big(e^{-\rho}+\frac{\pi(1-e^{-\rho})}{1-e^{\xi}}\Big) w^\star(\upsilon, \rho)\, \eta_t \tag{A.24}$$

Proof.
Equations (2.14), (4.1) and (4.2) directly imply Equation (A.20) as follows:

$$\kappa_t = \tilde{\mathcal{P}}_t(\tilde{Q}_t)\, \tilde{Q}_t = \frac{\tilde{\mathcal{P}}_t(\tilde{Q}_t)}{\mathcal{P}_t} \mathcal{P}_t \, \frac{\tilde{Q}_t}{M_t} M_t = \tilde{\alpha}_t \, \tilde{\Psi}_t \, \mathcal{M}_t^\star \tag{A.25}$$

Equation (A.21) follows from applying Equations (4.3) and (4.5) to $\tilde{\alpha}_t = \frac{\tilde{Q}_t}{M_t}$.
Equation (A.22) follows from Equations (4.4) - (4.5).
Equation (A.23) follows from Equation (3.5).
Equation (A.24) follows from Equations (2.14), (3.8), and (A.23).

□

Lemma A.3. *Settlement Disruption Cost*
The absolute settlement disruption cost, κ_t, can be written as follows:

$$\kappa_t = \kappa_t(\upsilon, \rho) := \begin{cases} \dfrac{\alpha\, e^{\xi-\rho}\,(e^{\rho}-1)}{(1-\alpha)(e^{\rho}-e^{\xi})-(1-\pi)(e^{\rho}-1)} \left(1+\frac{\pi(e^{\rho}-1)}{1-e^{\xi}}\right)\left[1-\frac{(u')^{-1}\big(\frac{\upsilon e^{\mu-\rho}}{\beta}\big)}{\beta}\right]\eta_t & \text{if } \frac{1-e^{-\rho}}{1-e^{-\rho+\xi}} < \frac{1-\alpha}{1-\pi} \\ \infty & \text{otherwise} \end{cases} \tag{A.26}$$

whereas the relative settlement disruption cost, $\tilde{\kappa}_t$, can be written as follows:

$$\tilde{\kappa}_t = \tilde{\kappa}_t(\upsilon, \rho) := \begin{cases} \dfrac{\alpha\, e^{\xi}\,(e^{\rho}-1)\Big[1-e^{\xi}+\pi\,(e^{\rho}-1)\Big]}{(e^{\rho}-e^{\xi})\Big[(1-\alpha)(e^{\rho}-e^{\xi})-(1-\pi)(e^{\rho}-1)\Big]} & \text{if } \frac{1-e^{-\rho}}{1-e^{-\rho+\xi}} < \frac{1-\alpha}{1-\pi} \\ \infty & \text{otherwise} \end{cases} \tag{A.27}$$

Proof.
Lemma A.2 implies Equation (A.26). Then, applying Equations (2.14), (3.8) and (4.6) to Equation (A.26) yields Equation (A.27).

□

Lemma A.4. *Investment-Parameterized Disruption Cost Components*
Let $s^{\star}_{(t-1)_-}$ denote the share of the native asset supply staked by investors arriving before period t and let $\iota^{\star}_t$ denote the share staked by investors arriving in period t. Then:

$$s^{\star}_{(t-1)_-} := \frac{S^{\star}_{(t-1)_-}}{M_t} = s, \qquad \iota^{\star}_t := \frac{I^{\star}_t}{M_t} = \iota \tag{A.28}$$

where:

$$s = \frac{(1-\pi)(1-e^{-\rho})}{1-e^{-\rho+\xi}}, \qquad \iota = \frac{(1-e^{-\rho})(\pi+e^{\xi}-1)}{1-e^{\xi-\rho}} \tag{A.29}$$

Moreover:

$$\tilde{\alpha}_t = \tilde{\alpha}(s, \iota, \alpha) := \begin{cases} \frac{\alpha(1-s)(s+\iota)}{(1-\alpha)(1-s)+\alpha\iota} & \text{if } \alpha < 1-s \\ 1-s & \text{otherwise} \end{cases} \tag{A.30}$$

$$\tilde{\Psi}_t = \tilde{\Psi}(s, \iota, \alpha) := \begin{cases} \left(1-\frac{\tilde{\alpha}(s,\iota,\alpha)}{1-s}\right)^{-1} & \text{if } \alpha < 1-s \\ \infty & \text{otherwise} \end{cases} \tag{A.31}$$

Proof.
Equations (A.28) and (A.29) follow by direct verification from Equations (3.6), (3.8), and (4.3). Equations (A.30) and (A.31) follow from applying Equations (4.5) and (4.4) to Equation (5.4). □

Lemma A.5. *Monotonicity of the Disruption Cost Components*
The following hold:

(i) For $0 < s < 1-\alpha$ and $0 < \iota \leq 1-s$, both $\tilde{\alpha}(s, \iota, \alpha)$ and $\tilde{\Psi}(s, \iota, \alpha)$ are strictly increasing in s and in ι.

(ii) $s^{\star}_{(t-1)_-}(\rho)$ and $\iota^{\star}_t(\rho)$ are strictly increasing in ρ.

(iii) For $\upsilon' > \upsilon$ and $\rho' = \rho'(\upsilon', \upsilon, \rho)$, both $w^{\star}(\upsilon', \rho') > w^{\star}(\upsilon, \rho)$ and $\mathcal{M}^{\star}_t(\upsilon', \rho') > \mathcal{M}^{\star}_t(\upsilon, \rho)$.

(iv) When the disruption costs are finite, $\tilde{\alpha}_t$, $\tilde{\Psi}_t$, and $\mathcal{M}^{\star}_t$ are each strictly larger at (υ', ρ') than at (υ, ρ), for $\upsilon' > \upsilon$ and $\rho' = \rho'(\upsilon', \upsilon, \rho)$.

Proof.
(i): Equations (A.30) and (A.31) imply, for $\alpha < 1 - s$:

$$\tilde{\Psi}(s, \iota, \alpha) = \frac{(1-\alpha)(1-s) + \alpha\iota}{1-\alpha-s} \tag{A.32}$$

Equation (A.32) implies:

$$\frac{\partial \tilde{\Psi}}{\partial s} = \frac{\alpha\,(1-\alpha+\iota)}{(1-\alpha-s)^2} > 0, \qquad \frac{\partial \tilde{\Psi}}{\partial \iota} = \frac{\alpha}{1-\alpha-s} > 0 \tag{A.33}$$

Equation (A.30) implies:

$$\frac{\partial \tilde{\alpha}}{\partial \iota} = \frac{\alpha\,(1-s)(1-\alpha-s)}{\big[(1-\alpha)(1-s) + \alpha\iota\big]^2} > 0, \qquad \frac{\partial \tilde{\alpha}}{\partial s} = \frac{\alpha\big[(1-\alpha)(1-s)^2 + \alpha\iota\,(1-2s-\iota)\big]}{\big[(1-\alpha)(1-s) + \alpha\iota\big]^2} \tag{A.34}$$

Then, $\iota \leq 1 - s$ and $s < 1 - \alpha$ imply:

$$\frac{\partial \tilde{\alpha}}{\partial s} > 0 \tag{A.35}$$

Thus, Equations (A.33), (A.34), and (A.35) imply Part (i).
(ii): Applying direct verification to Equation (A.29) implies Part (ii).
(iii): Equation (5.1), $\upsilon' > \upsilon$, and $\phi \in (0, 1)$ imply:

$$\upsilon' e^{-\rho'} > \upsilon\, e^{-\rho} \tag{A.36}$$

Equations (A.36) and (3.5) imply:

$$w^\star(\upsilon', \rho') > w^\star(\upsilon, \rho) \tag{A.37}$$

Equations (3.4), (A.28), and (A.29) imply:

$$\theta^\star(\rho) = s^\star_{(t-1)_-}(\rho) + \iota^\star_t(\rho) \tag{A.38}$$

Equations (A.24) and (3.4) imply:

$$\mathcal{M}^\star_t(\upsilon, \rho) = \frac{w^\star(\upsilon, \rho)\,\eta_t}{1 - \theta^\star(\rho)} \tag{A.39}$$

Equation (5.1) implies $\rho' > \rho$, so Part (ii) and Equation (A.38) imply:

$$\theta^\star(\rho') > \theta^\star(\rho) \tag{A.40}$$

Thus, Equations (A.37), (A.39), and (A.40) imply:

$$\mathcal{M}^\star_t(\upsilon', \rho') > \mathcal{M}^\star_t(\upsilon, \rho) \tag{A.41}$$

Thus, Equations (A.37) and (A.41) imply Part (iii).

(iv): Equation (5.1) implies $\rho' > \rho$, so Part (ii) implies $s^\star_{(t-1)_-}(\rho') > s^\star_{(t-1)_-}(\rho)$ and $\iota^\star_t(\rho') > \iota^\star_t(\rho)$. When the disruption costs are finite, Part (i) then implies $\tilde{\alpha}_t$ and $\tilde{\Psi}_t$ are strictly larger at (υ', ρ') than at (υ, ρ), and Part (iii) implies the same for $\mathcal{M}^\star_t$. □

Lemma A.6. *Supply Growth Rate Threshold*
Assume $\pi < \alpha$. Then there exists a unique $\bar{\rho} > 0$ satisfying:

$$\frac{1 - e^{-\bar{\rho}}}{1 - e^{-\bar{\rho}+\xi}} = \frac{1-\alpha}{1-\pi} \tag{A.42}$$

Proof.
Define $f(\rho) := \frac{1-e^{-\rho}}{1-e^{-\rho+\xi}}$ for $\rho > 0$. Then, direct verification implies:

$$\lim_{\rho \to 0^+} f(\rho) = 0, \qquad \lim_{\rho \to \infty} f(\rho) = 1, \qquad \frac{df}{d\rho} > 0 \text{ for all } \rho > 0, \qquad \frac{1-\alpha}{1-\pi} \in (0,1) \tag{A.43}$$

Then, Equation (A.43) and the Intermediate Value Theorem imply both existence and uniqueness of $\bar{\rho}$ satisfying Equation (A.42). □

Lemma A.7. *Divergence at Supply Growth Rate Threshold*
Assume $\pi < \alpha$. Then, let $\bar{\rho}$ be the unique solution to Equation (A.42), established in Lemma A.6. Moreover, define $\upsilon_0 := \underline{\upsilon}(\bar{\rho})$. Then, for any $\upsilon > \upsilon_0$, the following results hold:

(i) Equation (3.3) holds for all $\rho \in (0, \bar{\rho})$

(ii) $\lim_{\rho \to \bar{\rho}^-} \tilde{\Psi}_t(\upsilon, \rho) = \infty$

(iii) $\lim_{\rho \to \bar{\rho}^-} \kappa_t(\upsilon, \rho) = \infty$

(iv) $\lim_{\rho \to \bar{\rho}^-} \tilde{\kappa}_t(\upsilon, \rho) = \infty$

Proof.
(i): Direct verification of Equation (A.2) implies:

$$\frac{d\underline{\upsilon}}{d\rho} > 0 \tag{A.44}$$

Then, $\rho \in (0, \bar{\rho})$ and Equation (A.44) imply Equation (3.3) as follows:

$$\underline{\upsilon}(\rho) < \underline{\upsilon}(\bar{\rho}) = \upsilon_0 < \upsilon \tag{A.45}$$

(ii): Equations (A.22) and (A.42) imply the desired result:

$$\lim_{\rho \to \bar{\rho}^-} \tilde{\Psi}_t(\upsilon, \rho) = \infty \tag{A.46}$$

(iii): Part (i), $\upsilon > \upsilon_0 = \underline{\upsilon}(\bar{\rho})$, and Lemma A.1 imply:

$$\lim_{\rho \to \bar{\rho}^-} w^\star(\upsilon, \rho) = w^\star(\upsilon, \bar{\rho}) > 0 \tag{A.47}$$

Equations (A.26), (A.42), and (A.47) imply the desired result:

$$\lim_{\rho \to \bar{\rho}^-} \kappa_t(\upsilon, \rho) = \infty \tag{A.48}$$

(iv): Equations (A.27) and (A.42) imply the desired result:

$$\lim_{\rho \to \bar{\rho}^-} \tilde{\kappa}_t(\upsilon, \rho) = \infty \tag{A.49}$$

□

Proof of Proposition 5.1

When the disruption costs are finite, Lemma A.2 implies $\kappa_t = \tilde{\alpha}_t \, \tilde{\Psi}_t \, \mathcal{M}_t^\star$, and Equation (4.6) then implies $\tilde{\kappa}_t = \tilde{\alpha}_t \, \tilde{\Psi}_t$. Lemma A.5(iv) implies that $\tilde{\alpha}_t$, $\tilde{\Psi}_t$, and $\mathcal{M}_t^\star$ are each strictly larger at (υ', ρ') than at (υ, ρ). Thus, these imply Equation (5.2). □

Proof of Proposition 5.2

This result follows as a corollary of Lemma A.2. □

Proof of Proposition 5.3

Lemma A.5(iv) implies Equation (5.6). □

Proof of Proposition 5.4

Lemma A.5(i) implies Equation (5.7). □

Proof of Proposition 5.5

Lemma A.5(ii) implies Equation (5.8). □

Proof of Proposition 5.6

Lemma A.5(iii) implies Equations (5.9) and (5.10). □

Proof of Proposition 5.7

Lemma A.3 and Lemma A.7 (iii) and (iv) imply Equation (5.13). □

Proof of Proposition 5.8

Lemma A.7 (ii), (iii), and (iv) imply Equation (5.14). □