A Game-Theoretic Model of Staking, Restaking, and Token Inflation

S

January 7, 2025

Abstract

This whitepaper presents a stylized mathematical and game-theoretic model for large-scale staking (or "restaking") of BTC/ETH into protocols that promise yield in their native tokens. We explore the tension that arises when real protocol revenue is insufficient to meet stakers' yield demands. Continuous token inflation can lead to a self-perpetuating cycle of token price declines, prompting an eventual shrinkage or implosion of the ecosystem. We contextualize this with the scenario outlined in discussions about Babylon, EigenLayer, and other shared security solutions.

1 Introduction

Shared security protocols rely on large amounts of capital (e.g., BTC or ETH) staked to secure multiple networks, paying yield in native tokens. When real protocol revenue is insufficient, heavy reliance on inflation can trigger a downward price spiral and cause the protocol to implode or shrink drastically. This paper proposes a series of mechanism-design ideas that aim to align incentives between stakers and the protocol. These mechanisms include forcing stakers to lock the native token, dynamically adjusting yields based on actual revenue, capping staked capital, creating real token utility, introducing slashing and insurance, and building a broad base of fee-paying partners. By implementing these mechanisms, shared security solutions can achieve sustainable profitability and avoid the pitfalls of purely inflation-driven yield.

In traditional staking models, token holders lock up capital in exchange for yield. In *shared security* protocols, large amounts of BTC/ETH can be used to secure multiple smaller networks or services. The hope is that the sum of fees paid by these multiple networks can justify the yield stakers earn.

However, if real network usage (and thus fees) is low, there is a tension: to keep stakers, protocols must issue ample native tokens, exerting downward sell-pressure on the token price. Over time, inflation can become unsustainable, leading to price collapse. This whitepaper outlines various mechanism-design solutions intended to remedy or mitigate this fundamental mismatch.

2 Aligning Stakers with Protocol Success

2.1 Requiring Stakers to Hold/Lock the Native Token

(1) **Mechanism:** BTC/ETH holders must also hold or lock a portion of the protocol's native token to earn yields.

(2) **Rationale:** Having “skin in the game” discourages stakers from immediately dumping their rewards, as they have collateral in the native token itself.

(3) **Outcome:** Stakers share the protocol’s downside risk and have an interest in preserving token value.

2.2 Partial Payment in Stablecoins or Real Revenue

(1) **Mechanism:** Channel a portion of actual protocol fees (or stablecoins) directly into staker rewards.

(2) **Rationale:** Ties yield to real revenue, reducing inflation-based payouts.

(3) **Outcome:** Lowers the net new token supply hitting the market, mitigating sell pressure.

2.3 Vesting and Lockups

(1) **Mechanism:** Impose a vesting schedule for newly minted rewards.

(2) **Rationale:** Delays the immediate sale of reward tokens, giving the protocol time to grow revenue.

(3) **Outcome:** Potentially softens the short-term sell pressure and fosters long-term commitment.

3 Dynamic Yield Adjustment Based on Usage

3.1 Revenue-Proportional Yield

(1) **Mechanism:** A fraction κ of the protocol’s real revenue R_t is allocated as staker rewards each period:

$$\text{Yield}_t = \kappa \times R_t.$$

(2) **Rationale:** Ensures yields are matched to actual usage, avoiding excessive inflation when R_t is low.

(3) **Outcome:** The yield rate naturally scales with protocol success, preventing unrealistic payouts.

3.2 Adaptive Cap on Staked Capital

(1) **Mechanism:** The protocol enforces a dynamic upper limit on total BTC/ETH staked, based on anticipated revenue.

(2) **Rationale:** If only $100M in annual rewards can be sustainably paid, cap the staked capital so that yields remain reasonable.

(3) **Outcome:** Prevents oversubscription of stakers whose demand would otherwise force unsustainable token issuance.

4 Redistributing Risk and Reward

4.1 Slashing for Misbehavior or Failures

(1) **Mechanism:** Penalize stakers (via slashing) for failing to secure the network (e.g., downtime or double-signing).

(2) **Rationale:** Stakers assume real risk and price it into their yield expectations, becoming true underwriters of security.

(3) **Outcome:** Discourages purely extractive yield-farming and makes stakers more conscientious.

4.2 Insurance Fund or Protocol-Owned Liquidity

(1) **Mechanism:** The protocol treasury or an external insurance provider maintains a capital reserve.

(2) **Rationale:** This fund can cover catastrophic losses, stabilizing the ecosystem.

(3) **Outcome:** Encourages stakers to remain, knowing the protocol can handle black-swan events.

5 Building Real Demand for the Token

5.1 Governance and Utility Tokens

(1) **Mechanism:** Give tokens real governance powers or usage (fee payments, DeFi utility, etc.).

(2) **Rationale:** If there is actual demand for the token beyond speculation, some market participants hold it for its usefulness.

(3) **Outcome:** Baseline token demand can offset staker sell pressure.

5.2 Protocol Buy-Back Using Revenue

(1) **Mechanism:** Use a share of protocol revenue to buy tokens on the open market and burn them (or redistribute sustainably).

(2) **Rationale:** Counteracts inflation by creating buy pressure from real income sources.

(3) **Outcome:** Can stabilize or increase token price, making yields more appealing and sustainable.

6 Tiered Staking and Differentiated Risk Classes

6.1 Multiple Staker Classes with Varying APYs

(1) **Mechanism:** Partition stakers into tiers: Tier-1 locks more protocol token (higher APY), Tier-2 provides only BTC/ETH (lower APY).

(2) **Rationale:** Reflects different levels of commitment and risk tolerance, aligning rewards with deeper involvement.

(3) **Outcome:** Reduces inflationary burden on purely extractive stakers while rewarding long-term believers.

6.2 Dynamic Penalties for Early Exits

(1) **Mechanism:** Early withdrawals incur a penalty distributed to remaining stakers or the treasury.

(2) **Rationale:** Deters short-term yield farming and helps maintain staked capital continuity.

(3) **Outcome:** Improves capital stability and security predictability.

7 Cross-Protocol Economies of Scale

7.1 Real Demand for Shared Security

(1) **Mechanism:** Aggregate many smaller chains under a single security umbrella, each paying fees proportionate to the security they use.

(2) **Rationale:** If multiple clients genuinely need shared security, total fees can become large enough to fund meaningful yields.

(3) **Outcome:** A true marketplace for security emerges, with sustainable fee-based payments over inflation.

7.2 Strategic Partnerships and L2 Integrations

(1) **Mechanism:** Integrate with L2 solutions, bridges, and enterprise blockchains that pay stablecoin or major-asset fees.

(2) **Rationale:** Growing a high-value client base raises total protocol revenue, offsetting inflation.

(3) **Outcome:** Steady expansion of real usage and fees underpins sustainable yield for stakers.

8 Summary of Mechanism-Design Principles

(1) **Tie Rewards to Real Revenue:** Link yields to actual protocol fees rather than arbitrary inflation.

(2) **Ensure "Skin in the Game":** Require partial collateral in the native token, slashing, or lockups to align staker incentives.

(3) **Limit Staking Capacity:** Cap or throttle capital inflow to match realistic revenue expectations.

(4) **Strengthen Token Utility:** Drive real demand with governance, fee usage, buy-backs, and DeFi integrations.

(5) **Mitigate Risk via Insurance:** Create a safety net (insurance fund) that protects against black-swan events, lowering the risk premium demanded by stakers.

(6) **Grow Actual Fee-Paying Partnerships:** Scale the underlying revenue from multiple protocols and users to justify substantial staked capital.

9 Conclusion

Purely inflation-driven yields for large-scale BTC/ETH stakers, absent significant real fees, lead to a fragile economic structure susceptible to downward price spirals. Mechanism design can mitigate these risks by:

1. Setting yield in proportion to revenue;
2. Aligning stakers with the protocol's long-term health;
3. Capping or adjusting staked capital to avoid overshoot;
4. Designing genuine token utility and buy-back models;
5. Introducing risk-sharing through insurance and slashing;
6. Building an ecosystem of fee-paying partners.

These strategies foster sustainability, ensuring that shared security protocols can support large capital inflows without succumbing to inflation-induced collapse. As real usage grows, so does the protocol's capacity to reward stakers profitably and responsibly.

The staking and restaking concept in the blockchain space, notably applied by projects such as Babylon, EigenLayer, and others, envisions a large pool of capital (often in Bitcoin (BTC) or Ether (ETH)) providing security to multiple networks. In theory, these stakers are compensated with yield paid in the various protocols' native tokens. However, there is skepticism as to whether the fees from real network usage can sustainably fund these yield demands. This paper proposes a simple mathematical and game-theoretic framework to analyze this dynamic.

10 Model Setup

10.1 Players and Assumptions

(1) **Stakers (capital providers)**: Large holders of BTC/ETH seeking yield from staking or restaking.

(2) **Protocol/Token Founders**: Those who launch or maintain networks with native tokens and rely on staked capital.

(3) **Token Holders**: Individuals who hold the protocol's native token (e.g., founders, retail, speculators). They are impacted by any inflation or dilution in the token supply.

We denote:

$$S = \text{total staked capital (USD value of BTC/ETH)},$$

$$R = \text{annual protocol fee revenue (USD value)}.$$

We typically assume $R \ll S$ in the scenario of interest, creating a mismatch between demanded yield and real economic value.

10.2 Basic Tension

The protocol must choose how much to inflate its native token supply to reward stakers. If token inflation is too low, stakers may exit for better returns elsewhere. If token inflation is too high, the token price can collapse from excessive sell pressure.

11 Discrete-Time Mathematical Model

We adopt a discrete-time model, indexing time by $t = 0, 1, 2, \dots$ (e.g., months or quarters).

11.1 Protocol Revenue and Payout

$$
\begin{aligned}
R_t &= \text{protocol revenue at time } t \,(\text{USD value}),\\
S_t &= \text{total staked capital at time } t \,(\text{USD value}),\\
\Pi_t &= \text{native token price at time } t \,(\text{USD value per token}),\\
Y_t &= \text{total yield payout at time } t \,(\text{USD value}).
\end{aligned}
$$

Because S_t may be large and R_t relatively small, inflation of the native token may be required to sustain yields.

11.2 Token Emission and Inflation

Let:

$$
\begin{aligned}
\Delta T_t &= \text{number of newly minted tokens in period } t,\\
T_t &= \text{total token supply after period } t.
\end{aligned}
$$

Define the *inflation rate* per period as

$$\alpha_t = \frac{\Delta T_t}{T_{t-1}}.$$

The newly minted tokens are:

$$\Delta T_t,$$

and their USD value (i.e., total yield at time t) is

$$Y_t = \Delta T_t \times \Pi_t.$$

11.3 Staker Utility and Participation Constraint

A BTC/ETH staker compares protocol yield to an *opportunity cost* r_{alt}, which is an annualized yield available elsewhere (e.g., staking ETH natively, or some other low-risk yield).

The staker remains in the protocol if

$$\frac{Y_t}{S_t} \geq r_{\text{alt}}.$$

That is, stakers require that the ratio of USD yield to USD staked capital meets or exceeds their alternative return.

11.4 Token Price Dynamics

Suppose newly minted tokens are sold immediately by stakers, creating strong sell pressure. The simplified dynamic is:

$$\Pi_{t+1} \;=\; \Pi_t \times f\Big(\frac{D(\Pi_t)}{\Delta T_t}\Big),$$

where $D(\Pi_t)$ is the demand for the token from non-stakers, and $f(\cdot)$ is a decreasing function in ΔT_t.

In simpler terms:

- As ΔT_t (new token issuance) grows, token price Π_{t+1} likely decreases.
- The protocol may try to inflate more to keep Y_t stable in USD terms, which further lowers the token price.

This feedback loop (more inflation → lower price → need for even more inflation) can end in a downward spiral.

12 Game-Theoretic Perspective

12.1 Payoff Structure

We can consider this as a repeated game with two main agents:

(1) **Founder (Protocol)** chooses an inflation rate α_t (or total new issuance ΔT_t).

(2) **Stakers** (BTC/ETH holders) decide to stay or leave based on whether

$$\Delta T_t \times \Pi_t \quad\geq\quad r_{\text{alt}} \times S_t.$$

In each period, the founder tries to set ΔT_t to keep stakers interested, but high ΔT_t can reduce token price Π_t in the next period.

12.2 Equilibrium Outcomes

Two broad steady-state outcomes (Nash equilibria) commonly emerge:

Case A. **Shrinking Equilibrium**:

$$S_{t+1} < S_t \quad \text{(as stakers leave)}.$$

Eventually, the protocol gives up on high inflation. The staked capital shrinks until the real revenue R_t can cover the yield. The token price stabilizes at a lower level. The protocol survives in a smaller form.

Case B. **Imploding Equilibrium**:

$$\alpha_t \text{ remains high} \quad\Longrightarrow\quad \Pi_t \downarrow \quad\Longrightarrow\quad S_t \downarrow \quad\Longrightarrow\quad \text{death spiral.}$$

Here, the protocol attempts to keep stakers with large inflation. The token price collapses from persistent sell pressure, stakers exit en masse, and the protocol becomes effectively worthless.

If the protocol attempts to service a very large S_t with minimal real revenue R_t, the system is prone to the “Ponzi” dynamic: minted tokens are used to pay off existing stakers, until the market no longer supports the token price.

13 Numerical Example

Suppose:

$$S_0 = 10 \text{ B USD}, \quad r_{\text{alt}} = 8\%, \quad R = 50 \text{ M USD/year}.$$

To provide stakers with $800M annual yield (8% of $10B), yet only $50M is from real revenue, the protocol must inflate $750M in tokens. If token demand is weak outside stakers, this $750M of new tokens is sold off by stakers each period, depressing the price significantly. To maintain the same $800M yield in the following period, the protocol must inflate even more. Eventually, either:

(1) The protocol chooses a lower inflation path, stakers leave, and S_t shrinks to a level that $50M can cover.

(2) The protocol persists in printing tokens and collapses in a death spiral.

14 Further Considerations

14.1 Discounted Cash Flow Perspective

If stakers foresee the long-run collapse, they may exit immediately. This can spark a faster cascade of token price declines, showcasing the self-fulfilling nature of token price in a low-fundamentals environment.

14.2 Coordination Dynamics

Similar to typical Ponzi schemes, short-term survival can occur if there is collective belief in the protocol's success. Once doubt arises, large-scale exits happen quickly.

14.3 Shared Security Fees vs. Protocol Inflation

Proponents of large staking pools often argue that multiple networks paying for security could generate high enough fees to sustainably pay yield. However, if actual network fees remain limited, this model indicates that heavy reliance on inflation will produce unsustainable outcomes.

15 Conclusion

From a game-theoretic standpoint, the mismatch between large staked capital and insufficient real revenue naturally invites a Ponzi-like scenario, where newly minted tokens compensate stakers until the market can no longer sustain the token's price. The result is either a *shrinking* outcome (with fewer stakers, lower market cap, and only as much yield as fees can support) or an *imploding* outcome (where the protocol collapses entirely).

This framework matches the cautionary observations about ecosystems that attempt to accommodate tens of billions of staked BTC/ETH while relying on token inflation to deliver the yield. Unless real network fees or revenues substantially increase to cover billions in annual staking rewards, the system will fail to escape the fundamental limit of market supply and demand.