@Cryptis – 09-30-2025

Cryptix Network | https://Cryptix-Network.org | info@cryptix-network.org

---

Anti-Locust Tokenomics: Designing Sustainable Proof-of-Work Networks

This paper proposes a tokenomic framework designed to protect small Proof-of-Work (PoW) blockchains from “locust mining”—a behavior where opportunistic miners, driven purely by profit, extract short-term gains, destroy newly issued coins, and then abandon the chain. Although such miners often claim they are “securing the network,” in reality they do the exact opposite, leaving the blockchain insecure and unstable.

To break this destructive cycle, new coins should be released with mechanisms specifically designed to prevent exploitative behavior. These include reward vesting, loyalty multipliers, stake bonding, hybrid PoW/PoS consensus, merged mining, and dynamic reward scaling. Such defenses stop “helicopter/mining locusts” in their tracks and allow the crypto ecosystem to recover toward the more sustainable, early-era model. Without these safeguards, new coins are launched only to fail quickly, competent developers give up within the first few months, and projects with real potential die before they can grow.

---

1. Core Principles

The design rests on five guiding principles.

First, binding incentives. Miner rewards must not be immediately liquid. Instead, payouts are structured so that miners cannot instantly dump tokens onto the market. This deters extractive behavior and encourages ongoing participation.

Second, dual security. The network's security should not rely solely on hashpower. By requiring miners to also post an economic stake, attacks become more expensive and carry a risk of financial loss.

Third, external reinforcement. When the native chain is too small to guarantee security on its own, it can borrow security from a stronger parent chain through merged mining (AuxPoW).

Fourth, dynamic incentives. Rewards must adapt to miner loyalty and network volatility. A static emission curve encourages mercenary mining, while dynamic adjustments discourage short-term exploitation.

Finally, governance integration. A community treasury, managed under transparent rules, ensures that buybacks, penalties, and parameter changes can be executed in a sustainable and accountable manner.

---

2. Mechanisms

Reward Vesting

One of the most direct ways to prevent mine-and-dump behavior is to time-lock the vast majority of rewards. Each block reward is divided into two parts: a very small fraction (for example, 5%) becomes liquid immediately, while the remaining 95% is locked and released gradually over a vesting period such as 90 days.

Technically, this can be implemented in a UTXO-based system via `OP_CHECKLOCKTIMEVERIFY` or `OP_CHECKSEQUENCEVERIFY`. In account-based models, vesting contracts can manage the gradual release. For instance, if a miner earns 6 tokens, only 0.3 tokens would be spendable at once, while 5.7 tokens remain locked and drip out linearly over the vesting schedule. This simple mechanism alone greatly reduces the profitability of hit-and-run mining strategies.

Loyalty Multiplier

To further reward consistent participation, the system applies a loyalty multiplier. A miner's effective reward increases with the duration of uninterrupted activity. Mathematically, this can be modeled as:

```
Effective reward = Base reward × (1 + Beta × log(1 + T))
```

where *T* represents the number of days of continuous mining, and *Beta* is a scaling constant. For example, with Beta set at 0.12, after 30 days the reward multiplier reaches approximately 1.12, corresponding to a 12% bonus. This structure penalizes opportunistic miners who hop between chains, while long-term contributors benefit from compounding incentives.

Hybrid PoW/PoS with Stake Bonding

Pure PoW systems are relatively cheap to attack if hashpower can be rented. To mitigate this, the proposed design integrates PoS elements. Miners are required to post a stake bond, proportional to their expected earnings—for instance, 20% of projected annual rewards locked for 30 days. In addition, each block requires partial approval from PoS validators before being finalized.

This hybrid mechanism significantly raises the cost of a 51% attack. An adversary cannot simply rent hashpower; they must also acquire and lock a meaningful amount of tokens, which can be slashed if misconduct is detected. The Decred network has successfully demonstrated the viability of such a hybrid approach.

Merged Mining (AuxPoW)

When a chain is too small to defend itself, it can strengthen its security by leveraging an established parent chain through merged mining. In such a system, miners working on the larger chain (for example, Bitcoin) can simultaneously submit proofs that secure the smaller chain without additional work.

This mechanism effectively forces attackers to engage with the parent network as well, making attacks far more expensive and unprofitable. Namecoin's integration with Bitcoin provides a well-known example of this model in practice.

Volatility-Responsive Reward Scaling

Opportunistic hashpower spikes are a recurring problem for small PoW chains. To dampen their effects, the protocol introduces volatility-responsive reward scaling. When the hashrate rises rapidly, block rewards are automatically reduced according to a formula:

```
Adjusted reward = Base reward ÷ (1 + Gamma × max(0, DeltaH / Hbaseline))
```

Here, *DeltaH* is the observed increase in hashrate relative to the baseline average, and *Gamma* is a damping factor. This discourages sudden inflows of

mercenary hashpower, since higher participation temporarily yields lower rewards.

Treasury Buybacks and Burns

Finally, a community treasury captures a share of transaction fees or penalties. The treasury can use these funds to buy back tokens on the open market or to burn them outright. Both actions reduce sell pressure from miners and support price stability. Governance controls ensure transparency and sustainability, for example by limiting buybacks to no more than 2% of supply per month.

---

3. Integrated Tokenomics Example

To illustrate, imagine a chain with a base block reward of 6 tokens. Each block yields 0.3 tokens immediately liquid, while 5.7 tokens are released gradually over 90 days. Miners who maintain continuous activity earn a loyalty bonus of 12% after one month. They must also bond 20% of their annual expected yield, which remains locked for 30 days and is subject to slashing for misconduct.

If the hashrate rises sharply—say more than 30% in a 24-hour period—rewards are damped to prevent exploitative inflows. Meanwhile, 10% of all penalties flow into the treasury, which uses buybacks or burns to stabilize the token economy.

The outcome is that short-term miners receive little immediate liquidity, making hit-and-run strategies unattractive. Long-term miners, by contrast, enjoy loyalty multipliers, bond returns, and a predictable reward stream. Attackers face significantly higher costs, since they must not only control hashpower but also acquire and risk bonded tokens.

---

4. Attack Scenarios and Countermeasures

This integrated design addresses several well-known threats.

- **51% Attacks via hash rental.** Hybrid PoW/PoS requires both hashpower and staked tokens, while merged mining further raises the bar by tying security to the parent chain.
- **Selfish mining and pool hopping.** Loyalty multipliers reduce the profitability of short-term strategies, while volatility-based damping mitigates sudden spikes in returns.

- **Identity faking to exploit loyalty.** Mining pools must sign blocks with a registered PoolID, and solo miners are identified by stable payout addresses.
- **Treasury capture.** Multi-signature requirements, time-locks, and hard-coded spending limits protect against collusion and abuse.

---

5. Implementation Roadmap

Rolling out these mechanisms requires several coordinated steps.

First, the block template must be modified to enforce the immediate-versus-locked reward split. Second, smart contracts are needed for vesting, staking, and slashing logic. Third, consensus rules must be updated to integrate validator approval into block acceptance.

Before deployment, the system should be tested through agent-based simulations that model miner profitability, price feedback loops, and attack scenarios. Formal verification of smart contracts and treasury rules will be necessary to minimize vulnerabilities. Finally, a governance interface must be developed, allowing the community to adjust parameters within strict, audited bounds.

---

6. Simulation Design

The simulation framework considers several types of agents: short-term miners, long-term miners, and opportunistic attackers. Key inputs include electricity costs, hardware efficiency, token price dynamics, and loyalty parameters.

The outputs of interest are:

- The expected value for short-term miners (EV-STM).
- Profitability trajectories for long-term miners.
- The daily rate of reward unlocks, affecting circulating supply.
- The cost of executing a 51% attack under hybrid rules.

These simulations help calibrate parameters so that opportunistic strategies remain unattractive while honest participation remains profitable.

---

7. Risks and Trade-Offs

No system is without drawbacks. Strict vesting schedules may deter legitimate miners who require immediate liquidity. Increased complexity also raises the risk of software bugs, making rigorous audits essential. Treasury governance must be designed to resist collusion, and poorly chosen parameters could still leave openings for locust mining under certain conditions.

Thus, while the proposed system significantly raises security and sustainability, it must be carefully tuned and subject to ongoing community oversight.

---

8. References

- Decred's hybrid PoW/PoS model as a real-world implementation of bonding and validator approval.
- Namecoin's use of Bitcoin's AuxPoW as a precedent for merged mining.
- Research on selfish mining and adaptive difficulty mechanisms.
- Tokenomics design guides, particularly those focusing on vesting schedules and incentive alignment.

Small PoW blockchains are inherently vulnerable to opportunistic miners who exploit short-term rewards. By combining reward vesting, loyalty multipliers, stake bonding, merged mining, volatility damping, and treasury-driven buybacks, the "Anti-Locust" tokenomics framework transforms such strategies into unprofitable options. Instead, miners are incentivized to commit resources over the long term, reinforcing both economic stability and network security.

This design demonstrates that with thoughtful integration of economic and technical tools, PoW systems can remain viable and sustainable, even in environments where mercenary mining would otherwise pose existential risks.