Multi: A Self-Improving Currency Leveraging Collective Intelligence

Henrik Westerberg
henrik.westerberg@multicurrency.io

January 31, 2025

Abstract

For decentralized, multi-asset-backed currencies, achieving true self-optimization in reserve management represents a significant challenge. We introduce Foresight Protocol, a novel system that manages the Multi currency and solves this through continuous, decentralized competition. In this system, participants stake capital and independently propose changes to the reserve composition, with their decisions implemented immediately. The protocol tracks the performance of these changes over an extended time frame, redistributing stakes among participants to favor strategies with sustained positive performance. The system itself competes by staking newly minted Multi tokens on its existing reserve composition, establishing a benchmark that participants must outperform to earn rewards. This fundamentally establishes a meritocracy where merit drives influence. Through integration with decentralized exchange order books, the protocol enables auto-adjustment of supply to achieve efficient market-based issuance and redemption, providing users with seamless access to the underlying reserve assets.

Contents

1 Introduction

Guaranteed redeemability would represent a major leap forward in currency design. This implies the ability to exchange each currency unit for assets possessing inherent value, meaning the value is derived from the underlying assets themselves and not solely from the belief of others that the currency has value. The guarantee's power is amplified when the underlying assets are decentralized, freeing users from dependence on centralized entities and fostering trust in the delivered value. This kind of system would promote stability and facilitate market activity by providing transparency about the underlying reserve assets.

However, existing cryptocurrencies have not fully delivered on this guarantee of redeemability. Bitcoin [1], despite its pioneering role in decentralized digital currencies, lacks direct redeemability, exposing it to price volatility and dependence on external market forces. Stablecoins [2] address price volatility by being redeemable for fiat currencies, usually through centralized banking infrastructure. But this solution creates a reliance on traditional financial systems, reintroducing the very trust requirements that decentralized currencies aim to eliminate.

To achieve true, decentralized, and trustless redeemability, a currency system would need to manage a diverse reserve of assets in a transparent, automated, and secure manner, without relying on any centralized entity. This ideal system would also need to be scalable and adaptable to changing market conditions. Several on-chain protocols attempt to address aspects of this challenge, including Set Protocol, Enzyme Finance, Betoken, and Yearn Vaults. These protocols utilize various approaches, such as predefined strategies, active management, meritocratic governance, and yield optimization [3]. However, while innovative, these existing solutions are primarily focused on niche investment strategies rather than providing a foundation for a trustless and universally redeemable currency.

We present the Foresight Protocol, a protocol that combines traditional governance with a novel, self-regulating game-theoretic approach to reserve management. The protocol uses traditional DAO governance to define the rules of a competitive game, but then allows the system to evolve organically through the independent actions of its players within those rules. This creates a framework where improvement is driven by individual incentives, under a clear, collectively-determined ruleset, rather than by constant group intervention.

The protocol operates with a dual-token model: Foresight serves as the governance mechanism, allowing holders to stake and participate in the protocol's competitions, while Multi functions as the protocol's redeemable currency, representing claims on the underlying reserve assets. This separation of governance and currency functions allows for specialized incentive alignment within the system.

The protocol centers around a series of structured competitions that drive continuous reserve refinement. In each round, the system takes the lead by announcing competition terms and staking tokens to defend its existing reserve composition. Users then enter the competition, staking both Foresight tokens and Multi tokens and proposing reserve additions. The system prioritizes acquiring these proposed tokens from the open market during settlement; only if this is not possible at a lower price will the system purchase directly from users at the pre-defined competition price. As part of the settlement process, and simultaneous with asset acquisition, the system issues new Multi tokens. Based on performance metrics, the system rewards successful proposals with tokens from its stake and claims the stakes of underperforming proposals. This outcome shapes the subsequent round, creating a dynamic system.

This competitive process is designed to not only optimize the reserve but also to potentially position Multi as a foundation for a decentralized unit of account. Achieving this would require significant scale, likely including various specialized subsidiary multi-asset compositions, robust asset diversification spanning numerous economic sectors, and maturity of the various backing assets, elements that are expected to gradually develop over time as the protocol and ecosystem mature. Another aspect that may contribute to becoming viable as a unit of account is extending performance evaluation periods over market cycles, which should incentivize diversification and risk management.

Beyond functioning as a value anchor in the future tokenized economy, we envision Multi acting as a master key to that economy. In a world where each token functions as a key, unlocking specific utility or access to essential services and resources, managing a multitude of individual tokens could become cumbersome and risky. Multi, by providing access to a dynamic and diverse composition of these underlying utility tokens, simplifies this process. Crucially, the competitive mechanism is designed to ensure that the reserve composition reflects the aggregate demand for these underlying tokens, thus aiming to satisfy the global demand for the essential services they represent. It aims to mitigate the risks associated with individual token volatility and offers a streamlined way to interact with the broader tokenized ecosystem.

1.1 Potential Benefits

The Foresight Protocol offers several potential advantages over existing approaches.

1. **Continuous Reserve Refinement:** The competition mechanism is designed to promote continuous refinement of the reserve. By requiring players to demonstrate sustained success, rather than short-term gains, the protocol incentivizes the submission of proposals that are likely to maintain or improve performance over time. Unsuccessful proposals lose their stakes to potentially better alternatives, creating a natural selection process that refines the reserve composition.

2. **Enhanced Trust:** The protocol enhances trust in reserve management through decentralization, transparency, and mathematical guarantees, rather than reliance on centralized institutions. Traditional systems require trust in managers and institutions. In contrast, the Foresight's game-theoretic mechanisms offer verifiable assurance that reserves are managed in the interests of Multi token holders, as players can only gain influence through demonstrated, long-term success.

3. **Egalitarian Access:** The protocol provides an egalitarian environment where access and influence are determined solely by the objective measurement of a contribution's performance, as measured by the Proof of Improvement mechanism. While staking capital is required to participate in the reserve management competitions, the system is designed to accommodate a wide range of stake sizes; participants, regardless of their stake size, can contribute and earn rewards proportional to their performance.

4. **Agile, Adaptive, and Scalable by Design:** The protocol achieves operational scalability by trusting participants to implement changes first, and then adjusting their influence and rewards retroactively through the stake redistribution algorithm. This "act now, be judged later" approach fosters rapid adaptation and avoids the bottlenecks of traditional consensus mechanisms, while using market performance to determine the long-term impact of each change.

5. **Simplified and Efficient Asset Access:** The protocol incorporates the Market Stabilizer (originally described and implemented in [4]), a multi-party trading algorithm that fundamentally simplifies access to the Multi reserve's underlying assets. By seamlessly integrating Multi token issuance and redemption into decentralized exchange order books, the Market Stabilizer eliminates the need for users to individually acquire each reserve asset before participating. This coordinated access potentially leads to better prices, reduced risk of market manipulation, greater overall market efficiency, and minimized price slippage.

6. **Rewarding Valuable Contributions:** The protocol uses long-term performance evaluations to incentivize and recognize valuable contributions within tokenized systems. When entities create value within external systems and earn tokens anchored to those systems, Foresight Protocol's competitions quantify the merit of these tokens based on objective performance metrics. The entities can then convert their recognized tokens into Multi currency, transforming specialized accomplishments within specific domains into a broadly recognized form of value. While this system might not be a perfect measure of societal value, it aims to better identify and reward valuable contributions within the tokenized economy by linking rewards to sustained market demand.

7. **Multi-Agent Optimization and AI Accountability:** The protocol can be viewed as a framework for multi-agent optimization, where independent agents (human or AI) compete to improve a shared resource (the reserve). This structure directly addresses the principal-agent problem by aligning the incentives of the agents (players) with the interests of the principal (Multi token holders) through measurable outcomes. Because the rules of the game are clearly defined and performance is objectively evaluated, the protocol provides a mechanism for holding AI agents accountable. Furthermore, the competitive environment provides a quantitative benchmark for evaluating the capabilities of different AI strategies in the context of decentralized asset management. By focusing on how to algorithmically coordinate decentralized agents towards a common goal, the Foresight Protocol creates a system where AI agents are incentivized to act in a way that is demonstrably beneficial to the system's overall goals, and in doing so, potentially contributes to the broader AI alignment problem.

2 Performance Competitions

The Foresight network operates through a series of sophisticated competitions, creating a continuous process of reserve refinement. Each competition round follows a clear sequence: competition terms announcement, stake submission, settlement, and reward distribution. The outcome of one round feeds into the next, creating a dynamic and evolving system.

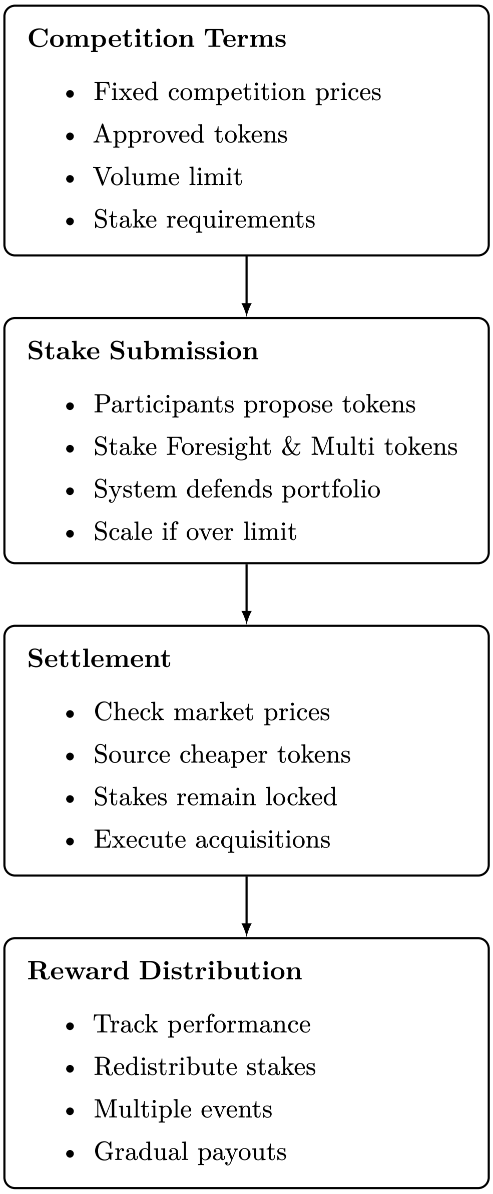

Figure 1: The Foresight Protocol operates in four sequential stages, from parameter announcement through to reward distribution.

2.1 Competition Terms

Before each competition round begins, and potentially after a defined period following the conclusion of the previous round, the system announces the terms of competition. These terms include the eligible tokens, their fixed competition prices, and the total volume limit for new assets in the reserve. It is crucial to note that these competition prices are established at the announcement and remain constant throughout the entire competition round, regardless of market fluctuations. The system also specifies the minimum stake requirements (in both Foresight token and Multi token) to ensure sufficient participant commitment.

2.2 Stake Submission

With the competition terms established, players submit positions for reserve additions. Each player must commit three things: (1) the actual tokens they propose the system should acquire, (2) Foresight tokens as stake, and (3) Multi tokens as stake. The system itself participates by staking tokens against its existing reserve positions. All position submissions are initially accepted, but if their total value exceeds the system's volume limits, each player's proposed token quantity is proportionally scaled down while their stake commitments remain unchanged. This maintains the total stake pool even as acquisition volumes are adjusted to fit within the system bounds.

2.3 Settlement

In this stage, the system attempts to source the proposed tokens at the best available prices. For each position, the system first checks if tokens can be acquired more cheaply from the open market. If lower prices are found, the system acquires tokens from the market instead of from the player, returning the player's committed tokens to them. However, even if a player's tokens are not accepted, their Foresight and Multi token stakes remain locked in the competition.

To maintain stability, the system manages these acquisitions carefully in two ways. First, token purchases can be spread out over time to avoid large market impacts and prevent the reserve from updating too quickly. Second, the system automatically scales down both token acquisitions and Multi token minting when the circulating supply decreases, ensuring all actions remain proportional to the current size of the system. As a consequence of scaling down token acquisitions, players receive a portion of their committed tokens back, and when Multi token minting is scaled down, a corresponding portion of their locked Multi tokens is also returned. These mechanisms help the system adapt smoothly to changing market conditions while preventing destabilizing feedback effects.

2.4 Reward Distribution

In the final stage, the system tracks how well each position performs relative to the others. Based on this performance, stakes are gradually redistributed over multiple distribution events; successful players gain more influence while underperformers lose their stakes. This extended distribution period encourages players to make thoughtful, long-term decisions rather than seeking quick gains. The performance of each position is measured regardless of whether the system acquired tokens from the player or the market.

The system itself also participates in this redistribution. When the system wins stakes from underperforming positions, all Foresight tokens are first sold for Multi tokens. Then, depending on the system's configuration, these Multi tokens (along with any directly won Multi tokens) are either burned to benefit existing holders by reducing the supply, or recycled for use in upcoming competitions. This mechanism ensures that players who make poor token choices are penalized by losing their staked capital, which is then redistributed to reward better performing participants and strengthen the system's reserves.

3 Protocol Security Design

The Foresight Protocol implements a unique approach to security: rather than restricting participation through elaborate permission systems, it establishes economic incentives that make exploitation unprofitable. This security framework emerges from three complementary elements: the core competition mechanics, the evolutionary pressure that rewards long-term value creation, and the governance system that maintains these incentives.

3.1 Core Protection Mechanism

The implementation of this security approach is embedded in the competition structure itself. To propose changes to the system's reserves, players must commit real capital by acquiring and staking both Foresight and Multi tokens. Meanwhile, the system itself participates in these competitions by minting new tokens to defend its existing composition.

This defense mechanism creates an asymmetric advantage for the system. Although players must acquire real capital to participate, the system can mint tokens as needed for defense. When the system mints Multi tokens, this dilutes existing Multi holders, but when it mints Foresight tokens, this has no impact on Multi holders. Even after acquiring tokens, players face multiple hurdles during competitions:

- They compete with other players for limited competition space through their stakes
- They face market-based auctions that ensure fair pricing
- They must maintain strong performance against both other players and the system's existing state
- Poor performance means losing their staked tokens

Consider someone holding a token that they doubt has long-term potential. To add this token to Multi's reserve, they would need to acquire Foresight and Multi tokens (real capital that remains at risk through extended performance evaluations). As their token underperforms, they would gradually lose this capital to other players and the system itself. Meanwhile, they could simply sell questionable tokens on regular exchanges without these complications. This design naturally steers the system toward tokens that players genuinely believe will maintain or increase in value over time.

3.2 Protection Layers

The competition framework creates evolutionary pressure toward valuable reserves through multiple reinforcing mechanisms. The foundation begins with governance-based token approval, which serves as a prerequisite for any token's use in the system. This initial screening ensures basic quality standards by examining factors such as liquidity, market maturity, and technical soundness. While this basic control cannot prevent all problems, it creates an essential first line of defense by excluding unsuitable tokens.

Building on this foundation, competitions implement capacity limits that create automatic protection against concentrated token inflows. If many players attempt to add the same token simultaneously, their combined volume would likely exceed the competition's capacity limit. This naturally leads to higher stake requirements as players compete for the limited space, strengthening security during potentially critical periods. The system adjusts these limits based on its size, maintaining consistent protection as it grows or shrinks.

The third layer of protection comes from the settlement phase, which ensures fair pricing by first attempting to source tokens from the open market. Even if a player commits tokens to the system, they are not guaranteed to be the seller. If better prices are available elsewhere, the system will buy from the market instead. The player must still maintain their stake regardless of where the tokens are sourced, creating strong disincentives against proposing overvalued tokens. By synchronizing trading into competitions, this mechanism concentrates liquidity for efficient price finding.

The final layer emerges from the performance competition that extends across multiple distribution events. By measuring performance over time, the system rewards changes that maintain value while penalizing harmful additions. Successful players grow their influence through redistributed stakes, while poor performers lose their capital. This creates evolutionary pressure that continuously strengthens the system. Players must show sustained positive results over extended periods, naturally leading to more robust and stable reserves.

3.3 Protection Through Competitive Pressure

Beyond these protection layers, the protocol gains additional security through its dual competitive structure. While the system's participation creates a baseline defense, the direct competition between players strengthens this protection by raising performance standards above mere adequacy.

Without player competition, participants would only need to outperform the system's predetermined positions to earn rewards. However, by making players compete for the same stake pool, the protocol ensures participants must demonstrate value against both the system and their peers. This higher standard means that even strategies that marginally improve upon the system's composition may still lose capital if other players find better opportunities.

The combination of system defense and peer competition creates compounding security benefits. The system's participation maintains reserve stability through its stake-backed positions, while competition between players helps identify truly valuable additions rather than just adequate ones. This competitive pressure complements the protection layers by adding dynamic, market-driven security that becomes stronger as more skilled participants engage with the protocol.

3.4 The Role of Governance

While the competition mechanics naturally protect the system, their effectiveness depends on proper parameter calibration by the DAO. The governance population must actively maintain and adjust key aspects of the system as market conditions evolve.

The first responsibility is managing competition structure. The DAO must carefully balance how often competitions occur and how long they last. More frequent competitions help the reserves adapt quickly but require more active price discovery. Longer evaluation periods provide better security by requiring sustained performance but reduce capital efficiency. The DAO must also ensure competition prices are determined in ways that maintain fair and efficient markets.

Managing stake requirements forms another crucial responsibility. The DAO determines how much skin in the game players must commit through both Foresight and Multi token requirements. These stakes can adjust automatically based on competition demand, but the DAO must set appropriate baseline levels and system responses. They must also balance the rewards and penalties players face when competing against the system's existing composition, ensuring incentives remain properly aligned without creating excessive dilution for token holders.

Volume controls represent a third key area of oversight. The DAO must set appropriate limits on how much change can happen in each competition period. These limits need to allow healthy evolution of the reserves while preventing destabilizing shifts. During periods of market stress, tighter limits might provide additional protection, although this protection must be balanced against the need to adapt to changing conditions.

Finally, the DAO must maintain clear asset standards. Beyond initial token approval, this includes establishing standards for continued inclusion and procedures for removing tokens if needed. While future versions might include more automated controls, current governance focuses on thorough initial screening and maintaining clear oversight procedures.

The challenge lies not just in setting individual parameters, but in understanding how they work together and evolve. While some routine adjustments might be automated, major changes require careful consideration to maintain the system's protective qualities. The DAO must develop clear standards for different types of parameter changes while maintaining flexibility to respond to market developments.

4 Formal Definition

This section provides a precise mathematical specification of the Foresight Protocol. For stake token types $\sigma \in \{g, m\}$ where g represents Foresight tokens and m represents Multi tokens, the protocol operates through a sequence of four stages: Competition Terms announcement, where system settings are announced; Stake Submission, where players make their moves; Settlement, where assets are acquired; and Reward Distribution, where performance is evaluated and stakes are redistributed. For each stage, we define the key mechanisms, constraints, and operational rules.

4.1 Core Mechanism

At its core, the protocol uses a unified stake pool as the foundation for a competitive system. Within this system, both players and the protocol itself engage in direct competition, seeking performance-based rewards. A key feature of this mechanism is the volume limit ($\theta \cdot M^{\text{start}}$) imposed on the system's participation, which serves the dual purpose of ensuring bounded system involvement for stake participation and controlling the supply of newly minted Multi tokens for asset acquisition.

4.2 Competition Terms

The system begins each competition by publishing key parameters that govern participation:

4.2.1 Core Parameters

- Volume limit (θ) - maximum competition volume as a portion of current circulating Multi supply (e.g., $\theta = 0.05$ means up to 5% of supply)
- Stake requirements and multipliers:
  - Base stake rates (r^σ) - fixed ratios determining required stake per unit of value for each token type σ
  - System stake multipliers (λ^σ) - determine how much the system stakes relative to players for each token type σ
- Competition pricing:
  - Set of approved tokens $\mathcal{T} = \{T_1, \ldots, T_n\}$
  - Competition prices $P_j^{\text{comp}} = P_j^{\text{oracle}} \cdot (1 + \mu)$ where μ is the markup over oracle prices
- Number of distribution events (l) over which rewards are distributed
- Time parameters:
  - Competition period length (τ_c) - duration of each competition
  - Competition spacing (τ_s) - time between start of consecutive competitions
  - Settlement duration (τ_d) - time over which asset settlement occurs
  - Reward distribution frequency (τ_r) - time between each reward distribution event

4.3 Stake Submission

Players submit stakes and select assets to participate in the competition. Each player i commits:

- Stakes of both types ($\sigma \in \{g, m\}$) that participate in performance competition:
  - s_i^g: Foresight tokens that remain locked through the competition period
  - s_i^m: Multi tokens that remain locked through the competition period
- An approved token type k from the set of eligible tokens

Based on the player's stake amount s_i^σ and chosen token k, the system calculates a corresponding token quantity:

$$q_i = \frac{s_i^\sigma}{\tilde{r}^\sigma \cdot P_k^{\text{comp}}}$$

where P_k^{comp} is the competition price for token k and $\tilde{r}^\sigma$ is the current stake rate. The competition has a volume limit of $\theta \cdot M^{\text{start}}$. Initially, when a player submits their position:

- The system uses the base rate r^σ to calculate a preliminary token quantity
- As more players join the competition, the total stake volume may exceed the limit
- If $\sum_{i \in \mathcal{P}} s_i^\sigma > r^\sigma \cdot \theta \cdot M^{\text{start}}$, the stake rate increases

The final stake rate $\tilde{r}^\sigma$ is determined at the end of the submission period:

- If total stake volume is within the limit, $\tilde{r}^\sigma = r^\sigma$
- If volume limit is exceeded, the rate adjusts to:

$$\tilde{r}^\sigma = \max\left(r^\sigma, \frac{\sum_{i \in \mathcal{P}} s_i^\sigma}{\theta \cdot M^{\text{start}}}\right)$$

- When the rate increases, all positions are recalculated:
  - Players' stakes s_i^σ remain unchanged
  - Token quantities q_i are reduced proportionally using the new higher rate
  - The difference between initially submitted tokens and recalculated quantities is returned to players

4.3.1 System Stake

The system participates only up to the volume limit. To match a volume of $\theta \cdot M^{\text{start}}$:

- Required stake would be $\theta \cdot M^{\text{start}} \cdot r^\sigma$ at base rate
- System stakes a proportion λ^σ of this amount

Therefore its maximum stake is:

$$S_{\max}^\sigma = \theta \cdot M^{\text{start}} \cdot r^\sigma \cdot \lambda^\sigma$$

For reserve assets $T_1, \ldots, T_n$ with quantities $q_1, \ldots, q_n$, the system:

- Creates total stake by matching player stakes with multiplier λ^σ:

$$S^\sigma = \lambda^\sigma \cdot \min\left(\sum_{i \in \mathcal{P}} s_i^\sigma, \theta \cdot M^{\text{start}} \cdot r^\sigma\right)$$

- Distributes stake across assets proportionally to maintain current composition:

$$s_k^\sigma = S^\sigma \cdot \frac{q_k \cdot P_k^{\text{comp}}}{\sum_{j=1}^n q_j \cdot P_j^{\text{comp}}}$$

- Creates phantom positions representing hypothetical trades:

$$\hat{q}_k = \frac{s_k^\sigma}{\tilde{r}^\sigma}$$

The competition concludes with:

- $\mathcal{P}$: Player positions (s_i^g, s_i^m, q_i)
- $\mathcal{S}$: System positions $(s_i^g, s_i^m, \hat{q}_i)$
- $\mathcal{A} = \mathcal{S} \cup \mathcal{P}$: All positions

4.4 Settlement

The settlement phase determines the final execution prices and manages token acquisitions. The system processes these acquisitions gradually over time, where each Multi token creation is matched with a corresponding asset deposit.

4.4.1 Supply Creation Bounds

Let M^{settle} denote the total circulating Multi supply at the time of settlement. The parameters establish a maximum supply increase for the competition:

$$M^{\text{max}} = M^{\text{settle}} \cdot (\theta + \lambda^m \cdot r^m \cdot \theta)$$

where $M^{\text{settle}} \cdot \theta$ represents the maximum acquisition supply and $M^{\text{settle}} \cdot \lambda^m \cdot r^m \cdot \theta$ represents the maximum system stake supply. The actual supply increase comes from two sources:

- Acquisition supply: Multi tokens minted to acquire assets from players or the market:

  $$M^{\text{acq}} = \sum_{k \in \mathcal{T}} q_k \cdot P_k^{\text{exec}} \leq M^{\text{settle}} \cdot \theta$$

  where each token type receives Multi tokens based on its execution price.

- System competition supply: Multi tokens minted by the system to participate in competitions:

  $$M^{\text{sys}} = S^m$$

  representing the system's total Multi stake as defined in the Stake Submission section

The total supply after settlement is therefore:

$$M^{\text{new}} = M^{\text{settle}} + M^{\text{acq}} + M^{\text{sys}} \leq M^{\text{settle}} + M^{\text{max}}$$

4.4.2 Market Price Discovery

For each token type k, during price discovery, market players can offer better prices. If a market player offers $P_k^{\text{market}} < P_k^{\text{comp}}$:

- The original tokens are returned to the players who submitted positions in token k
- The market player's tokens are acquired at price P_k^{market}
- All players' stakes s_i^σ for positions in token k remain locked in the competition

The final execution price for each token type is:

$$P_k^{\text{exec}} = \min(P_k^{\text{comp}}, P_k^{\text{market}})$$

4.4.3 Settlement Process

For each token type k, divide the total quantity q_k into n segments $\{q_{k,1}, \dots, q_{k,n}\}$ for gradual settlement. For each segment j:

- Asset quantity $q_{k,j}$ enters the reserve
- Two categories of Multi tokens are minted simultaneously:
  - Payment tokens worth $q_{k,j} \cdot P_k^{\text{exec}}$ for acquiring the assets
  - System stake tokens $S_{k,j}^m$ proportional to the system's competition participation

All segments must complete settlement within the settlement duration τ_d. The total supply created for acquisitions must not exceed the volume limit:

$$\sum_{k \in \mathcal{T}} q_k \cdot P_k^{\text{exec}} \leq M^{\text{settle}} \cdot \theta$$

If this limit would be exceeded, quantities are scaled down proportionally and excess tokens are returned to players. All minting and reserve changes occur simultaneously to maintain system backing.

4.5 Reward Distribution

After price discovery completes, the system measures relative performance of positions and redistributes stakes accordingly. This process runs separately for Foresight and Multi token stakes over multiple distribution events.

4.5.1 Performance Calculation

For each position in $\mathcal{A}$, calculate its value at time t:

$$v_{i,t} = P_{i,t} \cdot q_i$$

The relative performance measure for each position i at time t is:

$$\omega_{i,t} = \frac{v_{i,t}}{\sum_{j \in \mathcal{A}} v_{j,t}}$$

4.5.2 Stake Redistribution

Token redistribution occurs over l distribution events. At each event t, position i receives rewards from the unified competition pool:

$$\rho_{i,t}^{\sigma} = \omega_{i,t} \cdot \sum_{j \in \mathcal{A}} \frac{s_j^{\sigma}}{l}$$

where $\sigma \in \{g, m\}$ represents Foresight and Multi tokens respectively. Players can withdraw any rewards they receive after each distribution event. When the system wins stakes:

- Multi tokens are burned directly
- Foresight tokens are sold for Multi tokens, which are then burned

5 Economic Analysis

The Foresight Protocol requires careful parameter calibration to maintain economic stability and encourage productive participation. This section analyzes the economic effects and trade-offs of key system parameters.

5.1 Volume and Supply Parameters

The volume limit θ controls how much the system can change in each competition period. A higher θ allows players to influence the reserves more quickly but increases supply volatility as more Multi tokens need to be minted to acquire assets. A lower θ provides more stability but may make the system slow to adapt.

The token supply changes through two mechanisms: direct minting for asset acquisition (bounded by θ) and system stake minting (determined by λ^m). These changes scale automatically with system size: if supply decreases, both acquisition volumes and stake requirements decrease proportionally. This maintains consistent economic relationships but means changes in one area can affect the entire system.

5.2 Stake Parameters

The reward function in competition events creates natural incentives for decentralization through its asymmetric risk-reward structure. For players with smaller stakes, the potential upside is proportionally larger compared to their downside risk: they can win a significant portion of the reward pool while risking only their small stake. As stake size increases, players can win larger absolute values, but this scaling continues only until they reach 50% of the pool. Beyond this point, their potential gains actually decrease, creating a natural ceiling that discourages stake concentration. This mechanic ensures no rational player would try to control more than 50% of any competition's stake pool.

The ratio requirements r^g and r^m serve as security mechanisms by making players accountable for each unit of change they attempt to make to the system. These requirements must be calibrated carefully; if set too low, players might profit from offloading tokens to the system, particularly when they become the sellers at the competition price. While increasing these ratios provides one form of protection, the system can also require players to source tokens from the market through the purchase ratio γ. Setting γ closer to 1 forces players to acquire most tokens at stake submission placement rather than using existing holdings, making manipulation attempts more difficult and costly by requiring significant market activity before participation.

The system itself acts as a major player through its stake multipliers λ^g and λ^m. Setting these values above 1.0 means the system stakes more than players collectively, potentially creating stronger incentives for participation by offering larger reward pools. However, this comes with significant trade-offs: when the system stakes more than 50% of the pool, it exposes itself to greater potential losses while limiting its possible gains, fundamentally altering the risk-reward balance of the game. This risk is naturally mitigated by the volume limit $\theta \cdot M^{\text{start}}$. When player participation exceeds this limit, the system's fixed stake competes for a larger pool of player stakes, maintaining its original risk while increasing its potential upside.

5.3 Coverage Parameters

The coverage parameters α^g and α^m control when system stakes are minted, with distinct implications for each token type. For Foresight tokens, which are not collateralized, coverage can be flexible (setting $\alpha^g = 0$ simply means tokens are minted exactly when needed for rewards). For Multi tokens, which represent claims on reserves, coverage affects backing and requires careful calibration. Higher α^m values mean immediate minting and clearer price signals but increase short-term supply volatility.

During contractions, retroactive minting presents special challenges. If the system needs to mint tokens to cover previous obligations, these mints must scale down proportionally with the contraction to avoid creating tokens without corresponding asset backing. This means the system effectively reduces its payouts during stressed conditions rather than maintaining full obligation coverage.

6 Game-Theoretic Analysis

We analyze how Multi's security emerges from its game-theoretic properties through formal mechanism design and equilibrium analysis. The key insight is that security arises naturally from carefully designed incentives rather than artificial restrictions.

6.1 Game-Theoretic Intuition

While earlier sections discuss why manipulation is unprofitable and how capacity limits protect the protocol, here we emphasize the game-theoretic incentives at play. Each player assesses whether to participate based on potential gains versus the cost of staking Foresight tokens and the possibility of being outperformed. Four core elements demonstrate how these incentives guide rational behavior:

- **Volume Constraints as a Strategic Barrier.** The protocol imposes a maximum competition volume of $\theta \cdot M^{\text{settle}}$, capping how much value can be introduced in each round. As more players vie for that capacity, they must stake higher amounts. This "price of admission" scales up under heavy demand, making it disproportionately expensive for players to propose large or dubious asset contributions.
- **Economic Gatekeeping via Opportunity Costs.** Since participation requires staking both Foresight tokens and Multi tokens, a rational player compares this cost to alternatives, such as selling assets on a standard exchange. If the protocol's expected payout (net of stake risks) is not clearly better, the player will not join. This self-screening effect encourages only those players who believe their asset additions will outperform in the long run.
- **Undercuts and Price Discovery.** Even though the protocol defines a competition price for each approved asset, it simultaneously searches external markets for cheaper offers. If it finds a better price than the one announced, the original player's tokens are returned unused; however, the player remains bound by the stake requirement. The player effectively gains nothing while still incurring the stake cost. This mechanism deters attempts to offload overvalued assets at the competition price because being undercut yields no payout and retains the player's locked stake.
- **Collective Improvement through Evolutionary Pressure.** Post-acquisition, performance competitions redistribute staked Foresight tokens based on how well each position performs over time. Underperformers forfeit capital; outperformers grow in influence. Repeated across multiple rounds, this process selectively rewards players who consistently propose high-value assets, gradually refining the reserve toward a more resilient composition.

Viewed together, these rules form a repeated game in which players must carefully evaluate the potential gains from adding assets at the protocol's published competition prices against the risk of being undercut or underperforming. Over many cycles, low-value proposals are weeded out, while constructive strategies gain governance control, which in turn bolsters the protocol's security and overall asset quality.

6.2 Security Properties

We demonstrate two key properties of the Foresight Protocol: economic security against manipulation and guaranteed improvement through competition. These properties emerge directly from the formal system definition.

6.2.1 Economic Security Against Manipulation

Consider a player's utility function from the formal definition:

$$\begin{aligned} U_i(q_i, s_i^g) = {} & \underbrace{(1-p_i)\cdot q_i \cdot (P_i^{\text{comp}} - P_i^{\text{acq}})}_{\text{Expected trading profit/loss}} \\ & - \underbrace{(s_i^g + s_i^m)}_{\text{Initial stake costs}} \\ & + \underbrace{\sum_{t=1}^{l} \mathbb{E}_t\left[\omega_{i,t} \cdot \sum_{j\in\mathcal{A}} \frac{s_j^g}{l}\right]}_{\text{Expected performance rewards}} \end{aligned}$$

where:

- P_i^{acq} is the price at which the player acquired the tokens
- P_i^{comp} is the competition price
- p_i is the probability that market participants undercut the player's offer
- $(1 - p_i)$ is thus the probability of successfully selling to the system

For a player attempting to manipulate with overvalued tokens:

- High probability of being undercut ($p_i \approx 1$) makes trading profit unlikely
- When trades do execute, P_i^{acq} will be close to or higher than P_i^{comp}, making the profit negative
- Initial stake costs are guaranteed and immediate
- Poor expected performance ($\mathbb{E}_t[\omega_{i,t}] < \frac{s_i^g}{\sum_j s_j^g}$) makes expected rewards negative

Therefore $U_i < 0$, making standard market venues more profitable than attempting system manipulation.

6.2.2 Improvement Through Competition

The system's performance is measured through the net change in stake tokens of type $\sigma \in \{g, m\}$:

$$\text{Net System Gain}^\sigma = \sum_{t=1}^{l} \left(\sum_{i \in \mathcal{S}} \rho_{i,t}^\sigma - \frac{\sum_{i \in \mathcal{S}} s_i^\sigma}{l} \right)$$

where:

- $\rho_{i,t}^\sigma$ represents rewards of type σ won by system position i at time t
- s_i^σ represents initial system stake of type σ for position i

When this sum is negative, it proves improvement because:

- System positions $\mathcal{S}$ represent the optimal defense of current composition
- Players can only win system stakes by achieving $v_{i,t} > v_{j,t}$ for system positions j
- Therefore Net System Gain$^\sigma < 0$ implies players demonstrated superior risk-adjusted returns

This creates natural evolutionary pressure: compositions that genuinely improve the system accumulate influence through won stakes, while harmful changes are prevented by stake losses.

This negative Net System Gain formalizes what we term **Proof of Improvement**. This mathematical verification of system enhancement is fundamental to Multi token creation. Multi tokens can only be created in two specific ways: either through depositing all component reserve assets (direct backing), or through demonstrably improving the system as measured by this negative Net System Gain. When participants outperform the system's benchmark (the system's existing reserve composition), the protocol mints new Multi tokens as rewards, creating a direct link between currency creation and verified value addition.

7 Market Stabilizer

The Market Stabilizer introduces a novel approach to decentralized exchange by embedding a kind of automated market maker (AMM) that differs fundamentally from traditional designs. Unlike standard AMMs that create separate liquidity pools, this mechanism operates as an intelligent arbitrageur within existing order books, continuously analyzing order flows to identify and execute multilateral trades that benefit all participants while maintaining reserve integrity.

7.1 Multilateral Exchange Framework

Let $\mathcal{B} = \{T_1, \dots, T_n\}$ represent the set of reserve tokens with quantities $\mathbf{q} = (q_1, \dots, q_n)$. The exchange system operates under the following mathematical constraints:

- u represents the minimum number of Multi token units that can be exchanged
- $\mathbf{z} = (z_1, \dots, z_n)$ represents the corresponding amounts of each reserve token
- Each z_i is defined as $z_i = \lfloor \frac{q_i}{M} \rfloor$
- M (current supply) can be expressed as $M = \eta \cdot u$ where $\eta \in \mathbb{Z}^+$

This framework ensures that each Multi token always represents the same proportion of the reserve regardless of supply changes. The multilateral exchange can be expressed as:

$$\phi \cdot u \leftrightarrow \{\phi \cdot z_i \mid 1 \leq i \leq n\}$$

Where ϕ represents the quantity factor of minimum amounts exchanged in a single transaction.

7.2 Multilateral Order Matching Algorithm

Algorithm 1: Multilateral order matching algorithm.

```
if $o_i$ is better than $b_i$ then
    while multilateral matches are possible do
        check $o_i, \boldsymbol{b}_{-i}$ to find $\psi_j$ and best system offer $P_{i,j}^{\text{best}}$
        while best market offer is better than $P_{i,j}^{best}$ do
            match $o_i$ with best market offer
            update $\psi_j$ to agree with reduced $o_i$
        end
        match $o_i, \boldsymbol{b}_{-i}$ with system
        add $\psi_j$ to $\phi$
    end
end
if $o_i$ is not filled then
    place $o_i$ in $i$-th order book
end
```

This algorithm triggers when a new order o_i in market i (for reserve token i) offers a better price than the current best bid b_i. Let $\mathbf{b}_{-i}$ represent the set of best bid orders in all markets excluding market i. The algorithm then examines these other markets to identify sets of compatible best bids: either all bids for reserve assets (redemption) or all bids for Multi tokens (issuance). For each market j, the algorithm determines a quantity factor ψ_j representing the potential trade size, and calculates the best system offer price $P_{i,j}^{\text{best}}$ at which the trade could execute in a manner that precisely matches the system's budget.

The algorithm prioritizes matching against existing market offers when they provide more favorable prices. In the absence of better market offers, the algorithm executes a multilateral match by combining compatible orders. These matches must occur in whole multiples of the minimum issuable amount u, maintaining the system's reserve token ratios $\mathbf{z}$. The algorithm tracks its progress through an accumulated quantity factor ϕ, which counts the number of u-sized segments successfully traded. The final exchange converts $\phi \cdot u$ Multi tokens into $\phi \cdot z_i$ units of each reserve token i.

8 Conclusion

This paper has presented a detailed specification of the Foresight Protocol, a decentralized, asset-backed currency system built on game-theoretic principles. The Foresight Protocol addresses the fundamental challenge of creating a trustless, efficiently managed reserve for a digital currency, moving beyond the limitations of traditional governance models. The core innovation lies in the interaction between DAO governance, which sets system parameters, and a unique competition mechanism. Participants stake capital to propose reserve changes, and the system actively defends its existing composition, creating a dynamic and self-optimizing system.

We have demonstrated, through mathematical analysis, how the protocol's security emerges from the interplay of market-based price discovery, capacity constraints, and extended performance evaluation. This makes manipulation economically irrational, as participants are incentivized to contribute assets that provide sustained value. The economic analysis examined how parameters like volume constraints and stake ratios influence system behavior and security as the system scales. Furthermore, the Market Stabilizer facilitates efficient multi-asset trading by integrating directly with decentralized exchange order books.

By strategically leveraging collective intelligence and market-driven competitive dynamics, the Foresight Protocol posits a novel paradigm for decentralized reserve management. This self-improving system, governed by DAO-defined rules and driven by performance-based capital reallocation, demonstrates significant potential to serve as foundational infrastructure for more resilient financial systems, and to function as a ”master key” within a broader, tokenized economy. Further research and empirical validation are recognized as essential to fully realize this potential and to refine the protocol's implementation in practical applications.

References

[1] S. Nakamoto, “Bitcoin: A peer-to-peer electronic cash system.” `https://bitcoin.org/bitcoin.pdf`, 2008.

[2] A. Moin, E. G. Sirer, and K. Sekniqi, “A classification framework for stablecoin designs,” 2019.

[3] F. Schär, “Decentralized finance: On blockchain- and smart contract-based financial markets,” *Federal Reserve Bank of St. Louis Review*, vol. Second Quarter, pp. 153–74, 2021.

[4] H. Westerberg, “Design of a multi-asset-backed stablecoin and a multilateral order matching system,” Master’s thesis, KTH, School of Electrical Engineering and Computer Science (EECS), 2019.