Multi: A Decentralized Currency Backed by a Diversified Token Reserve

Henrik Westerberg
henrik.westerberg@multicurrency.io

July 10, 2024

Abstract

Traditional cryptocurrencies often lack intrinsic value, whereas stablecoins typically depend on centralized benchmarks. We introduce Multi, a decentralized currency that aims to achieve price stability through its dynamic and expanding reserve of diverse tokens. This reserve evolves through a novel token stream mechanism, allowing anyone to contribute approved tokens evenly over time, fostering an inclusive governance model without requiring consensus. To protect the system and ensure high-quality token streams, two key strategies are employed: (1) extending token acquisitions over long timeframes, and (2) utilizing a competitive reward system based on the long-term price performance of contributed tokens. These token streams collectively represent the currency's emergent diversification strategy. Additionally, Multi's supply automatically adjusts to market demand via a market stabilizer, where market participants collaboratively issue and redeem coins. To further expand its reach and utility, Multi can be subdivided into a nested, multi-layered ecosystem of interconnected variants, each tailored to specific economic sectors. This framework aims to eventually mirror the global tokenized economy, ultimately providing a decentralized currency with inherent price stability.

Contents

1 Introduction

Since Bitcoin's inception [1], there have been numerous efforts to create decentralized forms of digital currency. Many of these efforts have addressed Bitcoin's known challenges, including its transaction latency, energy consumption, price volatility, and lack of tangible backing. In this landscape, stablecoins have emerged as significant players [2]. However, their dependence on centralized benchmarks, such as the US Dollar exchange rate, the Special Drawing Rights (SDR), and the Consumer Price Index (CPI), constrains their full potential. Although they may provide price stability, their reliance on external standards undermines the essence of decentralization.

A truly decentralized solution would achieve price stability without relying on centralized benchmarks. It would possess inherent value, ensuring each unit is redeemable for something of worth. This principle of redeemability is already inherent in many Web3 tokens, designed to be exchanged for specific assets, services, or rights through the execution of smart contracts. As the token ecosystem expands, this redeemability can be leveraged to create a novel currency with intrinsic worth.

Such a currency would be backed by a wide variety of tokens, representing a diverse basket of assets. This diversification could be vast, encompassing tokens from every sector and industry, offering a hedge against economic fluctuations. The currency's price would remain relatively stable, adjusting gradually in response to global economic forces, thus embodying a unique form of decentralized price stability. If sufficiently comprehensive, this basket of tokens would mirror the global tokenized economy, reflecting its overall health and performance.

However, the decentralized financial landscape currently lacks a protocol that can effectively manage a diverse basket of assets in a truly decentralized and scalable manner. Various on-chain asset management protocols, such as Set Protocol, Enzyme Finance, Betoken, and Yearn Vaults, have been proposed or developed. These protocols offer different approaches, including following predefined strategies, active management, meritocratic governance, and yield optimization [3]. While innovative and potentially well-suited as specialized investment vehicles, these protocols have not been designed for universal and scalable asset management.

An ideal solution, merging the traits of both currency and fund, remains unrealized. Such a system would be decentralized and inclusive, enabling efficient decision-making on a large scale without requiring unanimous agreement. The system's strategy would be shaped by the collective wisdom of its participants, with performance-based rewards ensuring accountability and aligning the interests of decision-makers with those of users. This approach would foster a decisive, inclusive, evolving, and aligned system, promoting continuous enhancement and mutually beneficial outcomes.

Multi aims to fill this void by employing a unique distributed decision-making mechanism for managing its token reserve. This mechanism allows for autonomous adaptation and evolution over time without requiring community consensus on each decision. As Multi grows, this decision-making process can further subdivide, giving rise to an ecosystem of subsidiary Multi variants. Through this method, Multi strives to redefine benchmarks for decentralized value and stability. If fully realized, this approach could usher in a decentralized universal standard. This new standard draws parallels to the historical gold standard, but with a pivotal distinction: instead of merely backing money with gold, it envisions a system where money is backed by the collective value of all humanity's endeavors.

1.1 Multi

Multi is a decentralized digital currency backed by a dynamic and diverse reserve of blockchain tokens. It is designed with security, scalability, and decentralization as core principles, making it suitable for use as a decentralized currency. The stability and effectiveness of Multi increase as its reserve expands and diversifies. Unlike stablecoins, which maintain price stability by pegging to external assets like fiat currencies or commodities, Multi achieves stability through the strategic diversification of its backing assets.

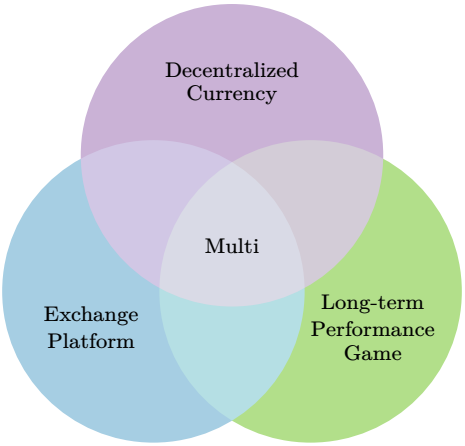


Figure 1: Use cases of Multi.

The reward mechanism of Multi allows anyone to participate in a long-term performance game, where participants compete to provide tokens with the best long-term price performance. Additionally, Multi incorporates unique mechanisms to enhance trade efficiency and liquidity among the tokens within its reserve, effectively functioning as an asset exchange protocol.

1.2 System Overview

The system comprises two interacting components. The market stabilizer dynamically adjusts Multi's supply to match market demand, crucially without changing the proportions or value of its underlying assets. Conversely, the token streams periodically modify Multi's composition, updating its backing ratios and reconfiguring the stabilizer. This interplay is facilitated by the stabilizer's provision of real-time token exchange rates, which are used to calculate the value token streams.

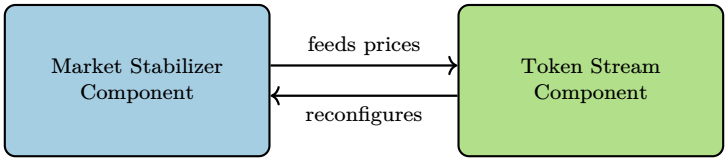


Figure 2: Overview of the two interacting components.

1.3 Market Stabilizer

The market stabilizer is an automated mechanism within the Multi ecosystem that acts as an arbitrageur. When a user places a buy or sell order for Multi with a reserve token, the stabilizer scans the decentralized exchange (DEX) where the algorithm is embedded for arbitrage opportunities. If an arbitrage opportunity is found, the stabilizer initiates a multilateral exchange, which involves simultaneously executing multiple buy or sell orders across different tokens in the reserve. This dynamic process adjusts the supply of Multi, either by minting new coins or redeeming existing ones, to maintain a balance between supply and demand, ensuring the user gets the best possible price while also correcting price discrepancies in the market. The benefits of this mechanism include:

- **Constant Equilibrium:** Multi's supply continuously adjusts to match demand, mitigating price fluctuations.
- **Enhanced Liquidity:** The automated arbitrage mechanism increases liquidity for both Multi and its reserve tokens.
- **Improved Exchange Rates:** Users benefit from more favorable exchange rates due to the automated arbitrage enabled by the stabilizer.
- **Price Stabilization:** Price movements in one reserve token can be mitigated by balancing effects from other tokens, contributing to overall market stability.
- **Collaborative Supply Adjustments:** Multiple parties can participate in the process of creating or removing Multi from circulation.
- **Preventing Bank Runs:** The stabilizer ensures all holders receive the same value upon exiting, fostering fairness and preventing bank runs.
- **Novel Price Oracle:** The multilateral exchange process, involving multiple parties and the system itself, functions as a novel price oracle, potentially providing a more accurate and resilient gauge of true value than traditional exchanges.

1.4 Token Streams

Multi's token reserve is dynamically managed through token streams. The system automatically purchases any approved tokens offered to it at regular intervals. It incentivizes open participation while mitigating risks associated with token acquisition. This is achieved through two key strategies:

1. **Gradual Buying:** The system does not purchase tokens outright. Instead, it acquires them incrementally over a defined period through token stream contracts. The structure and conditions of these token streams ensure a steady flow of assets, averaging the acquisition cost and reducing the risk of overpaying due to short-term price fluctuations or manipulation.
2. **Long-Term Performance Game:** To contribute tokens to the system, stream providers are required to commit governance tokens as a collateral. This collateral is then redistributed based on the long-term price performance of the contributed tokens, creating a long-term performance game where accurate forecasting abilities are rewarded. This incentivizes the contribution of high-quality tokens with long-term potential.

This token stream mechanism, characterized by its decentralized structure, periodic token contributions, and incentivized participation, provides a framework for dynamic on-chain asset management. The approach offers several key features and benefits that shape the Multi's trajectory:

- **Open Participation:** The open participation model allows for a wide range of stream providers, fostering a diversity of ideas and expertise to guide the system's evolution.
- **Incentivized Growth:** Stream providers are motivated to identify and contribute tokens that will appreciate in value, fostering a continuous expansion of the reserve.
- **Achievable State Guarantee:** The system's composition always reflects actually contributed tokens, avoiding the instability risks of target-based systems.
- **Decentralized, Scalable Governance:** The system's governance model is designed to accommodate a growing network of participants while minimizing the need for complex consensus mechanisms, preventing potential conflict and stagnation.
- **Agile Decision-Making:** By streamlining decision-making processes and reducing the need for consensus, the system enables quick and effective responses to evolving market conditions.
- **Merit-Based Decision-Making:** The reward structure inherently favors stream providers who consistently demonstrate skill in identifying promising tokens.
- **Alignment of Interests:** The performance-based rewards create a system where stream providers' interests align with those of Multi users, mitigating the principal-agent problem and fostering trust in the system's decision-making.
- **Evolutionary Governance:** Performance-based governance token redistribution empowers successful stream providers, allowing them to shape future decisions and further refine the system.

2 Market Stabilizer

The market stabilizer is a novel mechanism embedded within a decentralized exchange. Its primary purpose is to minimize trade inefficiencies and maintain Multi at a supply-demand equilibrium by issuing or redeeming coins. From a user perspective, the implementation of this algorithm represents an additional layer on the order book, on top of the orders that already exist, as illustrated in Figure 3. This significantly increases the depth and liquidity of the markets where the stabilizer is embedded.

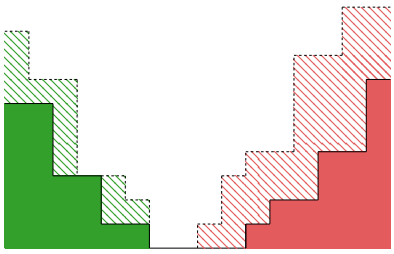


Figure 3: Illustration of the impact of the market stabilizer mechanism on an order book. Existing buy and sell liquidity are depicted in green and red, respectively. The market stabilizer adds additional system buy (green lines) and sell (red lines) liquidity.

The core principle of the stabilizer is to continuously monitor market prices to gauge the current demand for Multi. If prices are high, indicating high demand, new coins are issued. Conversely, if prices are low, suggesting a desire to exit Multi positions, the supply is decreased. The stabilizer achieves this by constantly checking the combined prices of Multi across multiple markets, activating when this combined price level exceeds a threshold defined by the algorithm.

This threshold, determined by the reserve's current backing ratios – the proportion of each backing asset to the circulating supply – serves as a trigger for the algorithm. The stabilizer is designed to trade only when it can fully utilize its available capacity to issue or redeem Multi without altering these backing ratios. By precisely matching its actions to this limit, the stabilizer maintains a constant backing ratio. Thus, after the algorithm has been activated, every Multi remains redeemable for the same quantity of backing tokens as it was before, ensuring that the underlying asset value is preserved for all Multi holders.

When a user submits an order, the stabilizer first evaluates if it can improve the user's price while simultaneously balancing Multi's supply and demand. For example, if a user wants to buy Multi with a reserve token, the stabilizer checks the highest bids on the other markets. If these bids, combined with the user's order, allow the stabilizer to issue new Multi without altering the reserve ratios and stay within its budget, the multilateral exchange is executed, providing the user a better price than they would have otherwise received. The same principle applies when users want to sell their coins, resulting in the redemption of coins and a reduction in the circulating supply.

The stabilizer can be viewed as a form of arbitrage mechanism, albeit one that differs from the traditional definition. While conventional arbitrage involves exploiting price discrepancies between different markets for immediate profit, the stabilizer focuses on a specific discrepancy: the difference between the issue/redeem price of Multi and its prevailing market price. By actively eliminating this discrepancy through multilateral exchanges, the stabilizer not only ensures price stability for Multi but also offers market participants a more favorable exchange rate, benefiting both users and the overall ecosystem by incentivizing trading activity and promoting efficient price discovery.

Since it maintains constant ratios between tokens in its liquidity pool, the stabilizer can be defined as a Constant Ratio Market Maker (CRMM), a type of Automated Market Maker (AMM). However, it differs from conventional AMMs in two key aspects: (1) it relies on Multi as the exchange currency, and (2) it prioritizes user benefit over generating trading fees. The stabilizer aims to execute trades in a way that is neutral for Multi, neither creating profit nor incurring loss, while focusing on providing optimal prices for users.

By operating across multiple markets and providing additional liquidity, the stabilizer creates a dynamic pricing network with stabilizing effects. As Multi gains wider adoption, this interconnected network has the potential to dampen volatility in Web3 markets, fostering a more predictable trading environment. Moreover, the frequent activation of the stabilizer and the resulting price convergence around the multilateral exchange threshold may enable the generation of reliable and secure on-chain price feeds for various Web3 applications, as detailed in Section 2.3.

2.1 Market Stabilizer Definition

Multi, represented as C, has a circulating supply of M. The Multi comprises n unique tokens, $\mathcal{B} = \{T_1, T_2, \dots, T_n\}$, and is supported by the stabilizer, which enables the conversion of units of C to units of the tokens in set $\mathcal{B}$. These conversions take place in a single instance within a block on the blockchain. The minimum number of units of C that can be exchanged during a conversion is defined as u. Additionally, $\boldsymbol{z}$ is defined as a vector of size n, representing the minimum number of units of tokens from set $\mathcal{B}$ that can be exchanged in one instance. The relationship between Multi and its backing tokens can be expressed as: *u units of C can be converted to z_1 units of T_1, z_2 units of T_2, ... and z_n units of T_n,* and similarly, *z_1 units of T_1, z_2 units of T_2, ... and z_n units of T_n can be converted to u units of C.* This relationship is referred to as the strict backing definition.

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

The factor ϕ characterizes the quantity of segments of the minimum amount exchanged within a single instance, where $\phi \in \mathbb{Z}^+$. When the order book design outlined in the subsequent section is applied, the factor ϕ is derived from the aggregation of matches at various price levels, yielding $\phi = \sum_{j=1}^{k} \psi_j$. The current supply can also be expressed as a multiple of the minimum amount, defined as η, with $\eta = \frac{M}{u}$ and $\eta \in \mathbb{Z}^+$. Consequently, if the supply is expanding, the condition $\phi \geq 1$ holds and if the supply is contracting, $\eta \geq \phi \geq 1$ holds.

The reserve quantities of the tokens under the control of Multi are represented by $\boldsymbol{r}$, a vector with a size of n. These quantities are utilized to calculate $\boldsymbol{z}$ in order to ensure that Multi is never insufficiently collateralized. The implementation of token streams leads to modifications in $\boldsymbol{r}$ and the ability to compute a new $\boldsymbol{z}$ whenever there are changes to Multi's contents, thereby allowing for conversions to proceed with the same level of precision. The equation demonstrates that an increase in u results in a heightened degree of overcollateralization and a finer level of granularity.

$$z_i = \left\lfloor \frac{r_i}{\eta} \right\rfloor \tag{2}$$

2.2 Multilateral Order Matching Algorithm

The multilateral order matching algorithm, as detailed in [4], is an order book implementation of the market stabilizer. This algorithm functions symmetrically for both bids and asks, with the former contracting Multi supply, and the latter expanding it. It activates when a combined set of orders on n markets together surpasses a threshold as defined by Multi's current backing. The process is initiated when a user submits a new order, represented as o_i, to the i-th order book, setting the stage for potential multilateral matches and adjustments to the Multi supply.

Multilateral order matches are attempted only if the submitted order o_i is better than the current best bid b_i. If this condition is met, the system enters a loop that continues as long as multilateral matches are possible. In each iteration, the system checks best bid orders on other markets to find the multilateral trade quantity factor ψ_j and the best system offer price $p_{i,j}$. To ensure the user receives the most favorable price, the system prioritizes matching the user with regular asks if a better price than $p_{i,j}$ can be obtained. If quantities still remain, the system executes a multilateral match between o_i, the best bids on other markets, and itself.

Algorithm 1: Multilateral order matching algorithm.

```
if o_i is better than b_i then
    while multilateral matches are possible do
        check o_i, b_{-i} to find ψ_j and best system offer p_{i,j}
        while best market offer is better than p_{i,j} do
            match o_i with best market offer
            update ψ_j to agree with reduced o_i
        end
        match o_i, b_{-i} with system
        add ψ_j to φ
    end
end
if o_i is not filled then
    place o_i in i-th order book
end
```

The set of best bids across all n order books is defined as $\boldsymbol{b}$, with $\boldsymbol{b}_{-i}$ denoting the set of best bids excluding the best bid in the i-th order book. If an order in $\boldsymbol{b}_{-i}$ is filled during the matching process, $\boldsymbol{b}_{-i}$ is updated with the next best bid in that order book. This update necessitates another iteration of the algorithm, as the new best bids may create new opportunities for multilateral matches.

In each iteration, the system trades $\psi_j \cdot \boldsymbol{z}$, and the sum of these trades across iterations determines the number of coins to be redeemed $\phi \cdot u$. Finally, if all possible multilateral matches have been executed and quantities still remain, o_i is placed in the order book.

To encourage participation in multilateral transactions and offset the fees from additional processing, the system could distribute this burden evenly among market participants. One solution is to introduce a modest increase in trading fees, directing the funds to a dedicated pool of native tokens specifically used to cover multilateral order matching costs.

2.3 Multilateral Price Oracle

The stabilizer, with its multilateral exchange capabilities, inherently stabilizes market volatility, potentially offering a more reliable on-chain price feed. This proposal suggests utilizing the multilateral exchange rate as a price feed, either exclusively or in conjunction with bilateral exchanges. Specifically, the multilateral exchange rate can be calculated as the volume-weighted average of all order matches within a given multilateral exchange, as detailed in the multilateral order matching algorithm.

$$\bar{p}_i = \frac{\sum_{j=1}^{k} \psi_j \cdot p_{i,j}}{\phi} \tag{3}$$

The volume-weighted averages can then be employed to determine the relative value of the reserve tokens, where $\boldsymbol{w}$ denotes the relative weight of each asset, expressed as a percentage, in the composition of the reserves.

$$w_i = \frac{\bar{p}_i \cdot z_i}{\sum_{j=1}^{n} \bar{p}_j \cdot z_j} \tag{4}$$

A price feed that adheres to the strict definition of backing, as outlined in equation (1), can then be derived. Here, $S^{\frac{C}{T_i}}$ indicates the number of units of C required to purchase a single unit of T_i at the current market rate.

$$S^{\frac{C}{T_i}} = \frac{w_i \cdot u}{z_i} \tag{5}$$

3 Token Streams

Multi's evolution is driven by token streams. A token stream is a commitment to regularly add a specific approved token to Multi's reserve over a set period. Stream providers agree to deliver a fixed amount of their chosen token according to a predetermined schedule. For example, a provider might contribute 100 units of a specific token every hour for four years. To keep their token stream active, providers must ensure these tokens are available for each scheduled delivery. If they miss a delivery, the agreement is broken. This could result in losing some of the rewards they would have received had they stayed compliant.

The effect of this system is that Multi continuously buys approved tokens from various stream providers at current market prices. During each scheduled delivery, the system exchanges newly minted Multi for the provider's tokens at the current market rate. This strategy results in an average acquisition price, balancing out high and low price points. The acquired tokens are added to the reserve, expanding Multi's supply. This increases the proportion of the incoming token relative to existing ones within the reserve, driving the system's evolution.

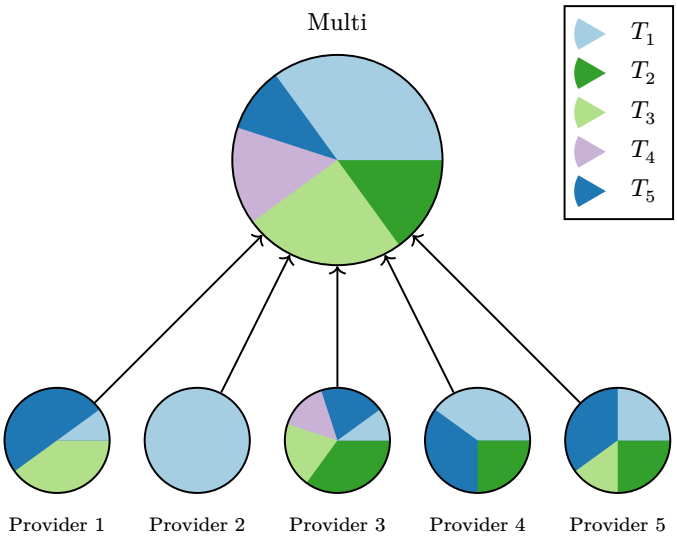


Figure 4: Five distinct strategies, each representing a unique composition of tokens chosen by stream providers as their bets, gradually reshaping the overall asset distribution of Multicoin.

Stream providers are incentivized to select high-quality tokens, as their rewards are directly tied to the long-term price performance of those tokens. As depicted in Figure 4, token streams can be viewed as strategic forecasting decisions, or bets, on the future performance of specific tokens. Given inherent market volatility, it is rational for providers to diversify their bets across a variety of tokens to maximize their potential rewards. This results in a diverse array of strategies being integrated into Multi's reserve, effectively aggregating the collective wisdom and risk appetite of the stream provider community.

3.1 Token Stream Contract

A token stream contract is an immutable, self-executing agreement. It outlines the provider's commitment to periodically supply a fixed quantity of a chosen token to Multi's reserves at predetermined intervals called integration events. The contract specifies the total number of integration events during which the provider must fulfill their obligation. When making this promise, the provider must also stake a proportional number of governance tokens as collateral.

3.1.1 Contract Formation

The contract formation period is an important strategic phase for providers in the Multi system. Each token stream contract formed within the same phase competes with each other. Since contracts share the same starting point and the same length, the competition is inherently fair.

At the start of this period, two key parameters are established: the contract formation price, which indicates the initial valuation of each token, and the participation ratio, which is determined through a governance process and dictates the amount of governance tokens required as collateral per unit of value of a proposed token stream contract. These parameters heavily influence providers' strategic decisions, with bets on perceived undervalued tokens likely being a popular approach.

Once the period begins, token stream contracts are formed. These contracts are irrevocable and publicly visible, enabling strategic signaling. Some providers may signal their intent early by establishing contracts at the outset, while others might wait, potentially aiming to capitalize on the observed choices of others. This dynamic interaction creates a "meta-game" where participants anticipate and respond to each other's actions, which has the potential to improve the diversification of the reserve and foster coordination as providers collectively identify and support promising tokens.

3.1.2 Integration Events

An integration event is a periodic occurrence during which the system interacts with active token stream contracts. These events take place at predefined, regular intervals. During each integration event, the system establishes an integration price for every eligible token. This integration price serves as the exchange rate at which the providers' tokens are converted into Multi. The system then aggregates the tokens from all active token stream contracts and adds them to Multi's reserve. Following the conclusion of the integration event, the yield vesting mechanism is triggered, releasing a portion of the Multi earned by each provider in accordance with the terms outlined in their respective contracts.

3.1.3 Yield Vesting

To incentivize long-term commitment and protect Multi users, the total trade quantity of Multi awarded to providers for their token contributions is not released immediately. Instead, it undergoes a vesting process, where a portion of the Multi is released at each subsequent integration event until the contract's termination. This mechanism ensures that a portion of the provider's potential rewards remains within the system, available for slashing in case of contract breaches followed by underperformance of the contributed tokens.

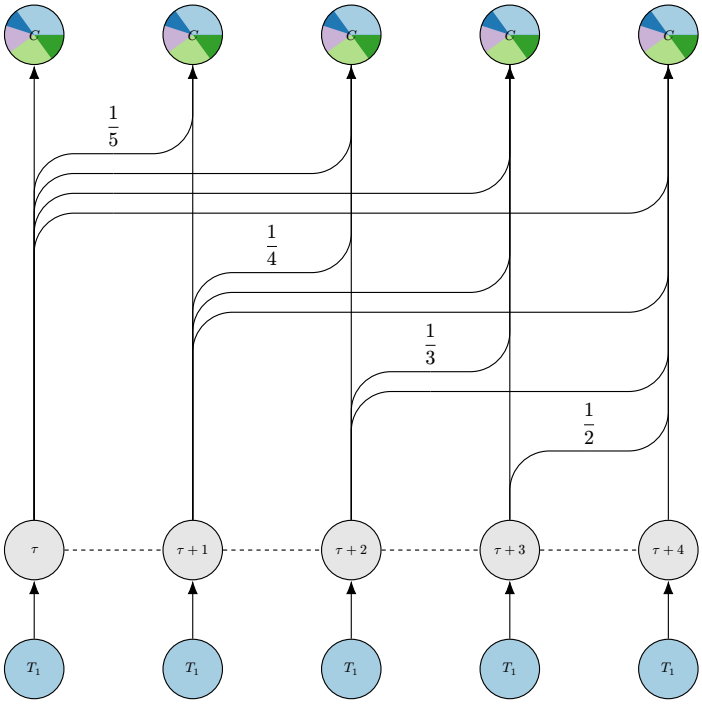


Figure 5: An illustrative token stream contract spanning five integration events. The contributed token T_1 is incrementally converted into Multi C. Simultaneously, the contributor's yield in Multi is released incrementally, with the amount increasing at each subsequent integration event.

The number of coins unlocked at each integration event is not fixed but increases proportionally as the contract progresses. For example, if a provider is due to earn x coins for their first contribution, and the contract has a length of l integration events, they will receive x/l coins. If they earn y coins for the second contribution, they will receive $x/l + y/(l-1)$ coins at the second event, and so on. This increasing yield structure, illustrated in Figure 5, encourages providers to remain active participants in the system for the full duration of their contract.

3.1.4 Contract Breaches

A contract breach occurs when a provider ceases token contributions before the agreed-upon termination date. In such a scenario, the system continues to evaluate the performance of the contributed tokens at each subsequent integration event. The current integration price of the tokens at these events is then compared to the provider's historical average token acquisition price during their active participation period.

If, at any integration event after the breach, the integration price falls below the provider's historical average, a portion of their vested coins will be slashed as a penalty. The severity of this penalty is directly proportional to the degree of underperformance compared to their historical average. However, if the integration price consistently meets or exceeds the provider's historical average at all subsequent integration events, no penalty is incurred, and the full amount of vested coins is unlocked.

Any coins that are slashed as penalties are burned from Multi's total supply. This burning mechanism can lead to a marginal increase in the value of each remaining Multi, benefiting the system's stakeholders. The contract breach and slashing mechanism serves to incentivize responsible participation and safeguard the long-term stability and value of Multi.

3.2 Rewards

Multi incorporates two distinct reward mechanisms to cater to providers: the first is the inflation reward, which utilizes Multi C; the second is the redistribution reward, using the governance and utility token G. These rewards are distributed periodically at integration events based on contract performance, aiming to motivate providers to continuously contribute to the growth of Multi and foster an environment of progressive, performance-based recognition.

3.2.1 Inflation Reward

The inflation reward incentivizes providers by providing them with a more favorable exchange rate for their tokens than the prevailing integration price. This is akin to the advantageous spreads enjoyed by market makers in traditional markets, ensuring that participating in Multi's reward system remains a competitive and attractive option.

To fund the inflation reward, the system issues new coins and distributes them to providers. Each issuance event results in a slight devaluation of existing Multi holdings. The magnitude of this reward is determined by the inflation rate, which is established by the governance population through a voting procedure. The reward size is calculated by multiplying the inflation rate parameter by the current circulating supply of Multi. As the circulating supply fluctuates, the reward size dynamically adjusts to maintain proportionality.

The inflation reward is apportioned among all active contracts based on their proportional contribution to the total value exchanged during the integration event. The value of each contract's exchange is determined by multiplying the quantity of tokens sold by the integration price. Thus, contracts with larger trade values earn a proportionally larger share of the reward pool.

3.2.2 Redistribution Reward

The redistribution reward mechanism introduces a long-term performance game among contracts formed simultaneously. Each new contract formation marks the start of a competition among providers, incentivized to select tokens that will outperform others within their contract period. Unlike the inflation reward, which issues new coins for its reward pool, the redistribution reward utilizes a pool funded by participants' staked governance tokens.

As stated in Section 3.1.1, upon contract creation, providers stake a quantity of governance tokens as collateral, with the amount proportional to the initial value of their contract, as determined by the participation ratio. During each integration event, an even portion of the total staked governance tokens is redistributed among participants based on the relative performance of their chosen tokens compared to the performance of all other tokens selected within the same formation period. Providers whose tokens have appreciated more relative to others in their cohort will receive a larger share of the redistributed governance tokens.

More specifically, if a participant stakes g amount of governance tokens in a contract with l integration events, they will receive a base reward of g/l governance tokens per event if their chosen tokens perform at the average result level. However, their actual reward will be higher if their tokens outperform the average and lower if their tokens underperform. The earned governance tokens are immediately available to the provider without undergoing vesting, resulting in a linear decrease of their collateral.

3.3 Token Streams Definition

This section outlines the mathematical definitions that underpin the token stream mechanism. It describes how providers initiate and manage token stream contracts during integration events, ensuring these contracts support Multi's strategic objectives. The formulas explain the processes for calculating contract values, determining reward distributions based on performance, and handling consequences when contracts are breached.

3.3.1 Contract Formation

A token stream contract is initiated at the integration event τ and is formulated between times α and τ. Once finalized, these contracts are integrated into Multi.

Contract Formation Process During the formation process, providers initiate contracts, each characterized by the total quantity q_i of token T_k for the entire contract duration, governance tokens stake g_i, and the contract's duration l_i, which is consistent for all contracts in the phase. The contract formation price, S_α^{C/T_k}, represents the exchange rate between Multi C and token T_k at time α. These contracts are binding, meaning once a value for q_i is established, it can only increase. The ratio of stake to value for the i-th contract is given by:

$$b_i = \frac{g_i}{S_\alpha^{\frac{C}{T_k}} \cdot q_i} \tag{6}$$

The contract formation process is fair, meaning that the ratio shown in (6) is the same for all participants, ensuring they all contribute an equal amount of stake per value.

Contract Value After the formation phase, contracts starting at time τ are denoted as $\mathcal{E}_\tau$. The value of each contract at time t is represented by $v_{i,t}$, where S_t^{C/T_k} indicates the integration price between C and T_k.

$$v_{i,t} = \frac{S_t^{\frac{C}{T_k}} \cdot q_i}{l_i} \tag{7}$$

3.3.2 Rewards

The system institutes a bifurcated reward mechanism to motivate participation and commitment: the inflation reward and the redistribution reward. Both reward types are predicated on a performance metric $p_{i,t}(\mathcal{X}_t)$, where $\mathcal{X}_t$ can represent different sets of contracts. Specifically, the term $p_{i,t}(\mathcal{E}_\tau)$ represents a competition among non-expired contracts, including those that have been breached, that started at the same time. Meanwhile, $p_{i,t}(\mathcal{H}_t)$ refers to a contest among all contracts that are currently active, meaning they have not been breached and are not yet complete.

$$p_{i,t}(\mathcal{X}_t) = \frac{v_{i,t}}{\sum_{j \in \mathcal{X}_t} v_{j,t}} \tag{8}$$

Inflation Reward Upon successful allocation of a contract, the contract holder receives inflation reward rewards over the contract duration during each recalibration. Coins are allocated across all active contracts in set $\mathcal{H}_t$, which may have different inception dates. These rewards are proportional to the inflation rate π_t and the circulating supply of Multi M_t. The reward, symbolized as $r_{i,t}$ for the i-th contract at time t, is determined by the contract's performance:

$$r_{i,t} = p_{i,t}(\mathcal{H}_t) \cdot M_t \cdot \pi_t \tag{9}$$

Tokens are dispensed to the provider over time, in proportion to the remaining contract duration. The symbol $C_{i,t}$ signifies the amount of C returned from the contract at time t, assuming there has been no violation of the contract. The contract is expired when $t - \tau \geq l_i$.

$$C_{i,t} = \sum_{m=\tau}^{t} \frac{v_{i,m} + r_{i,m}}{l_i - m + \tau} \tag{10}$$

Redistribution Reward Redistribution rewards are allocated based on a competition among contracts in the set $\mathcal{E}_\tau$, all originating from the same formation process. The quantity of governance tokens that can be redistributed in the competition at time t, specifically pertaining to the i-th contract, is denoted by $\frac{g_i}{l_i}$. These governance tokens are reallocated based on the results of the competition. Hence, the performance-based governance token reward for the i-th contract at time t, denoted as $G_{i,t}$, is computed as:

$$G_{i,t} = p_{i,t}(\mathcal{E}_\tau) \cdot \sum_{j \in \mathcal{E}_\tau} \frac{g_j}{l_j} \tag{11}$$

3.3.3 Contract Breach

In the event of a contract breach, providers face slashing and cease to receive inflation rewards. As a result, $C_{i,\upsilon}$ stays constant for the duration of the contract period, with no new tokens contributed to the system. A contract breach is detected at time υ. The total price that was obtained by the i-th contract, while it was active between τ and υ, is denoted as $\tilde{S}^{C/T_k}_{i,[\tau,\upsilon]}$. This leads to a slashing quantity, represented as $C''_{i,t} = C_{i,\upsilon} - C'_{i,t}$. The quantity $C''_{i,t}$ is subtracted from the circulating supply, thereby causing deflation.

$$C'_{i,t} = \min\left(1, \frac{S_t^{\frac{C}{T_k}}}{\tilde{S}^{\frac{C}{T_k}}_{i,[\tau,\upsilon]}}\right) \cdot C_{i,\upsilon} \tag{12}$$

In the redistribution reward process, breached contracts are treated as active. If a participant's governance token reward surpasses their base reward, those excess tokens are burned from the supply.

$$G'_{i,t} = \min\left(G_{j,t}, \frac{g_j}{l_j}\right) \tag{13}$$

3.4 Token Streams Implementation

The development of the token stream mechanism on a blockchain platform introduces unique challenges and requires specific considerations. This system requires a trustless price feed mechanism to determine both integration and contract formation prices. Additionally, it needs a method for creating token stream contracts and transferring assets from providers to Multi's reserve while minimizing fees and avoiding transaction bottlenecks. The design must also carefully allocate responsibilities for fees and define which parties are responsible for specific actions.

3.4.1 Implementation of Integration Price

The operational efficiency of the token streams significantly depends on a reliable, automated price feed. This feed determines the valuation of token stream contracts at any given moment and directly influences the performance of assets within these contracts. Furthermore, the integration price derived from this feed guides the distribution of the inflation reward and the redistribution reward. By basing the system on a reliable price feed, providers can divert their focus from active price discovery and concentrate on predicting the long-term trajectory of assets.

Exchange rates can be sourced from an internal on-chain oracle or an external decentralized oracle system. Markets with low liquidity often face the risk of price manipulation, necessitating a trustworthy external source, either alongside or as a substitute for the price oracle, as elaborated in Section 2.3. As Multi broadens its scope and influence, the internal on-chain oracle may progressively become a viable source of data, enabling an increase in the weight of that measurement. Such progression could lead to greater system self-sufficiency over time, and it may eventually be feasible to rely solely on the internal on-chain oracle emerging from the market stabilizer.

The appropriate method for deriving the integration price will depend on how frequently integration events occur. Using methods such as moving averages and filtering significant anomalies can contribute to ensuring the system does not purchase tokens at overinflated prices. However, a discrepancy between the integration price and the current market price also carries risks and can lead to instability. Thus, the appropriate method may differ depending on the implementation.

3.4.2 Implementation of Integration Events

Integration events can be implemented by creating a deposit pool and a withdrawal pool. The deposit pool is filled before the event. When the event occurs, the only processing required involves the integration of all tokens from this pool into Multi, thereby increasing the reserve quantities. Simultaneously, using the current integration price, circulating supply, and the existing inflation rate, the system calculates the number of coins to mint and deposit into a withdrawal pool. This approach minimizes the number of calculations that the system needs to make.

The exact amount of rewards a provider is entitled to can be calculated retroactively as they withdraw their rewards. Providers can conduct all necessary computations related to their token stream contract when they interact with the system, such as verifying the completion of the contract, detecting any breaches, or evaluating their results against those of other competitors. This approach helps the system avoid transaction bottlenecks and exorbitant costs. It is also logical to assume that each actor should cover the costs for the actions they perform within the system, maintaining efficiency and fairness.

3.5 Governing List of Approved Tokens

The governance system is responsible for maintaining and updating the list of approved tokens that can be included into Multi. This list is crucial for verifying authenticity, mitigating susceptibility to price manipulation, and excluding tokens with a heavily centralized ownership structure. The governance process for managing the approved token list involves two main aspects: token inclusion and token removal.

3.5.1 Token Inclusion

Adding new tokens to Multi requires a proposal to update the list of approved tokens. The proposal should provide a clear rationale for the token's inclusion, such as its potential to diversify Multi, its proven track record, or its innovative features. Additionally, the proposal should address any potential risks or concerns associated with the token. During a predetermined voting period, governance token holders cast votes either for or against the proposal. The majority vote determines the outcome. To ensure the integrity of Multi, the timing of the proposal period must be strategically designed to prevent the entry of fraudulent or manipulative tokens.

3.5.2 Token Removal

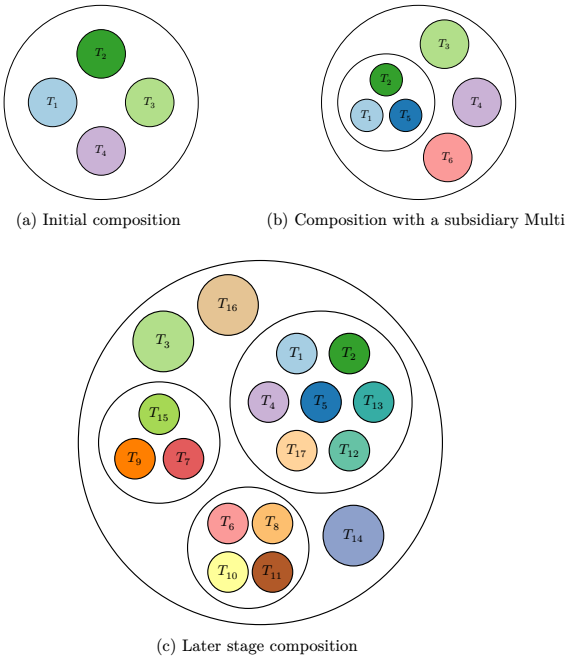
The token removal process is similar, starting with the creation of a proposal. If the majority vote favors the token's removal, it is automatically put up for auction in exchange for coins. The proceeds from this auction are then burned, consequently reducing the overall supply. The auction is open to all, safeguarding Multi's value. To avoid significant shifts in Multi's composition, it is preferable for these removal auctions to occur when the token in question represents a minimal portion of Multi and comprises a low percentage of its total value.

4 Ecosystem & Growth

Multi is designed to evolve beyond a standalone currency into a comprehensive financial ecosystem that mirrors the global economy. Achieving this requires incorporating tokens from all economic sectors and establishing a scalable infrastructure to manage this diverse asset repository. This section will detail the key factors enabling Multi's transformation into this ambitious vision.

4.1 Hierarchical Structure for Scalability

This organic evolution results in a tiered architecture, as seen in Figure 6, where the main Multi holds subsidiary Multis, which may, in turn, contain their own subsidiaries. This creates a multi-layered, decentralized financial system, where Multi's price stability stems from its vast array of underlying decentralized protocols, making it a robust alternative to traditional stablecoins. If subsidiaries are self-sufficient, this structure could theoretically scale indefinitely.



(a) Initial composition (b) Composition with a subsidiary Multi

(c) Later stage composition

Figure 6: Emergence of a hierarchical Multi structure. The initial composition (a) with four tokens, in (b) the formation of a subsidiary, and finally, in (c), the composition has grown to encompass three subsidiaries.

This hierarchical, modular design offers several distinct advantages. It enables delegated decision-making, allowing each subsidiary Multi to focus on its specific asset class or sector, thereby enhancing overall manageability and expertise. Furthermore, this structure facilitates the distinct management of diverse subsidiary Multi types, catering to the unique characteristics and risk profiles of different asset categories. Additionally, it enables subsidiary Multis to operate on different blockchains, which can then be seamlessly integrated into the main Multi system as backing assets.

Beyond these operational benefits, this design also enhances computational efficiency and security. Computational efficiency is improved compared to a single-layer system, as the stabilizer can execute smaller, more manageable multilateral matches at different levels of the hierarchy. Security is also bolstered by isolating riskier assets to specific branches of the structure, mitigating the potential impact of fraudulent tokens on the overall system.

4.2 Subsidiary Multi Variants

The Multi protocol is designed to be adaptable, supporting a wide range of subsidiary variants tailored to specific use cases within the blockchain ecosystem. These variants may emerge organically, driven by community needs and governance decisions, or be established independently and later integrated into the broader Multi ecosystem.

Each subsidiary Multi will have the autonomy to adopt a governance model and parameters that best suit its specific needs and risk profile, fostering an environment of experimentation and innovation within the ecosystem. These could range from fully independent governance structures to leveraging the parent Multi's mechanisms, or a hybrid approach combining elements of both. Moreover, variants are not constrained to using the same reward mechanisms as the parent Multi, allowing for further customization and adaptation to the specific requirements of each asset class.

The evolving landscape of the tokenized economy will determine the precise nature and focus of these subsidiary Multis. As real-world assets become increasingly tokenized and available for integration, we envision a diverse array of Multi variants catering to specific industries (e.g., energy, agriculture, real estate, manufacturing), emerging technologies (e.g., artificial intelligence, biotechnology, robotics), or financial instruments (e.g., derivatives, insurance, liquid staking). The success of Web3 business models and their integration into value-producing activities will further drive this evolution, ensuring Multi is backed by a robust foundation of intrinsic value.

4.3 Token Swaps within the Ecosystem

In a hierarchical Multi model, exchanging tokens between different branches of the ecosystem would entail a series of trades, analogous to traversing the branches of a tree. The question is whether these multi-step trades would be more cost-effective than using a single exchange currency. The feasibility of this depends on the overall price difference combined with increased fees due to the extra processing required. From a user experience perspective, the difference would likely be negligible, as the series of trades would be bundled into one instant transaction.

What makes multi-step trades appealing is that each subsidiary would have its own stabilizer and trading activity. The frequency of this trading could also be enhanced by strategically placing tokens that frequently trade together within the same subsidiaries. Potentially, these trade routes could be seen as "highways of liquidity," creating a more streamlined and rational exchange market. This structure could potentially decrease the overall market inefficiencies and arbitrage opportunities that currently exist.

5 Design Rationale

Having established a thorough understanding of the system's core mechanisms, including the dynamic stabilizer that adjusts coin supply based on market demands, the token streams' role in modifying Multi's composition, and the projected expansion of a diverse ecosystem, it is now appropriate to explore the rationale behind these design choices. The system leverages principles of mechanism design, a game-theoretic approach that seeks to strategically align individual behaviors with overall system objectives to maximize collective benefits. This section will examine how each component has been meticulously engineered to support an efficient and resilient ecosystem.

5.1 Master Key Analogy

Multi is designed for a future tokenized economy. In this future, tokens are not merely speculative assets, but integral to daily life, powering essential systems and services everyone needs. While this vision may seem distant given the current state of most tokens, the future we anticipate sees tokens fundamentally integrated into the production and exchange of goods and services. Instead of relying solely on traditional companies and their supporting legal structures, tamper-proof systems will emerge to guarantee a steady supply of society's essential needs. These systems will often be built around a specific token, requiring its use to access and operate within that system.

Consider a future where automated systems underpin our essential infrastructure. These systems, powered by tokens, would ensure the seamless operation of power grids, efficient crop harvesting, water purification, transportation networks, and digital communication. In this scenario, tokens are not merely abstract units of value; they are the access keys to these vital systems. Smart contracts, the underlying technology of these tokens, guarantee their exchangeable value and ensure that only the correct token can unlock the desired resource, whether it be a tangible good, a service, an asset, a derivative, or any other item of value.

Every business and individual will need access to a set of these "keys" daily to function effectively. Consequently, every economic actor will need to continuously anticipate which tokens they might require to remain operational. While this may seem cumbersome compared to using a national currency, the numerous benefits – superior business models, reduced costs, increased trust, and enhanced collaboration – make this transition not only worthwhile, but essential for long-term economic growth. The key is ensuring universal access to the necessary tokens, enabling everyone to thrive in this new economy.

This is where Multi becomes essential. If each token is a key to a specific system or service, then Multi functions as the master key or keychain, holding and providing access to all other keys. By utilizing Multi, individuals and businesses gain streamlined access to the tokens they require at any given moment, unlocking the full spectrum of resources and services that underpin society. This direct link to tangible utility is what sets Multi apart from traditional cryptocurrencies. Its value is derived not from speculation or collective trust, but from the real-world functionality of the tokens it represents.

This global repository of tokens can be conceptualized as a vast store. This store must be expansive enough to hold all the tokens people might need, its shelves stocked according to demand, and its layout designed for efficient access to everything. Through its hierarchical structure, where responsibility is delegated to various subsystems, Multi gains the capacity to be backed by an unlimited number of tokens. The token stream mechanism as a demand forecaster, continuously anticipating which tokens will be in demand, as its reward mechanism incentivizes the accumulation of tokens with long-term price potential. Lastly, the market stabilizer enables seamless and efficient swaps for any token at any given time.

By utilizing the global repository that Multi provides, the risks associated with individual token management are mitigated. The alternative – leaving individuals and businesses to predict their future token needs and accumulate accordingly – exposes them to market volatility, potential financial losses, and the risk of manipulation by actors seeking to hoard in-demand tokens. Multi, therefore, paves the way for a more efficient, equitable, and sustainable economy, where individuals and businesses can focus on creating value and collaborating, rather than speculating on token prices.

5.2 Advancing Price Discovery

The system's unique on-chain price oracle, derived from multilateral exchanges (involving multiple parties and the system itself), distinguishes it from traditional oracle designs that rely on bilateral, two-party exchanges. This innovative approach aims to provide more accurate and trustworthy price data. Inaccurate or manipulated price feeds have far-reaching consequences, affecting not only the blockchain ecosystem but also the broader global economy. Improved price oracles could significantly enhance the functionality and reliability of various blockchain-based applications, including decentralized lending platforms, options and derivative contracts, insurance platforms, and prediction markets.

As trading activity within the system increases, the multilateral exchange rate could emerge as a new benchmark for token valuation. This potential arises from the fundamental distinction between traditional bilateral exchanges and multilateral exchanges. Bilateral exchanges match individual buy and sell orders within a single market, where rates are determined by the intersection of supply and demand in that specific market. This can potentially lead to price discrepancies across different markets or vulnerability to localized market manipulation. In contrast, multilateral exchanges facilitate matches across multiple markets simultaneously, imposing strict conditions that bolster the integrity and accuracy of the price discovery process.

These multilateral exchanges must adhere to the circulating supply of Multi and its current true price, which is directly determined by its underlying asset backing. By involving multiple parties in the exchange process, the system strives to achieve a balanced equilibrium in asset valuations. The strict definition of asset backing ensures that any increase in the value of one asset is offset by a proportional decrease in the value of other assets within the reserve. This mechanism, akin to the balancing effects observed in traditional economic systems, ensures price stability. However, unlike traditional systems, the multilateral exchange rate can adapt to market changes in real-time, providing a more agile and responsive price discovery process.

Assets are interconnected within a complex web of relationships, and traditional two-party exchange-based pricing may not fully capture this complexity. The approach outlined in this paper establishes a direct connection between the prices of a set of assets, such that the price of one asset directly influences the prices of others. By incorporating these interdependencies, the multilateral exchange mechanism ensures a more nuanced and accurate price determination process. Consequently, the exchange rate derived from this multilateral approach can be considered a potentially more faithful reflection of the true value of an asset within the broader market context.

5.3 Purpose of Inflation Reward

The inflation reward is designed to compensate providers for their ongoing management and oversight of Multi. Although the system could potentially function without this specific reward, relying solely on the governance token reward may not provide enough incentive to attract and retain skilled providers. To strike a balance, the system implements a variable inflation rate. This allows the rate to be kept as low as possible while still ensuring fair compensation for providers. The flexibility of the system allows it to function effectively even with zero inflation, should that be the optimal configuration determined by governance.

5.3.1 Justification for Rewarding Stream Providers

While becoming a stream provider comes with contractual obligations and associated costs, it also presents a unique opportunities. By selling their tokens to the system, providers gain Multi in return, effectively exchanging a portion of their token holdings for a stake in a diversified and decentralized asset that evolves over time. For some, this benefit alone might be enough to justify participating, especially considering Multi's potential utility as a medium of exchange for fast and cost-effective token trading.

Furthermore, Multi's design offers providers several advantages when opening a token stream. The system's unlimited liquidity eliminates concerns about illiquid order books. Because the system purchases tokens at their current market price, these sales do not directly impact the market price of the token. They are only indirectly affected later by the reconfiguration of the market stabilizer. Providers also enjoy a passive trading experience, as they are not burdened with the need for constant market monitoring or precisely timed trades. This experience is akin to contributing tokens to a liquidity pool.

Beyond these benefits, some providers might also value the opportunity to influence Multi's composition by introducing tokens they believe in. This could potentially enhance a token's overall accessibility and visibility within a broader market, aligning with their long-term goals and interests.

Despite these advantages, providers still require a more favorable price than the integration price due to the constraints and potential risks associated with their role. To compensate for these factors and ensure the system remains attractive, providers are offered a price advantage through the issuance of additional coins during integration events. This reward, determined by the inflation rate parameter, is carefully balanced to align the interests of providers with the long-term success of Multi.

5.3.2 Optimal Inflation Rate

The ideal inflation rate is a dynamic equilibrium point that balances the competing interests of providers (who seek higher rewards) and users (who prefer lower dilution). A flexible approach is necessary due to the evolving relationship between these two groups, as well as fluctuating market dynamics. An inappropriate inflation rate could lead to a shortage of either providers or users, hindering Multi's growth potential.

The optimal inflation rate strikes a balance that discourages both providers and users from seeking alternative options. For example, users may consider deploying automated trading scripts that replicate Multi's strategies if the associated costs (token acquisition, development, and maintenance) are lower than the dilution caused by the inflation reward. Similarly, providers might opt to liquidate their tokens elsewhere if comparative cost factors, such as transaction fees, market depth, rewards, and staking requirements in other protocols, outweigh the benefits of participating in Multi.

Several dynamic factors influence the optimal inflation rate for Multi, including Multi's performance, market conditions, and the slashing mechanism. Strong performance may increase tolerance for higher inflation rates, while poor performance may decrease it. Market conditions affect the attractiveness of Multi relative to other investment opportunities. The slashing mechanism, by altering supply-demand dynamics, also impacts the optimal inflation rate. Hence, the ideal inflation rate to maximize Multi's growth is not static; it dynamically shifts in response to these multifaceted factors.

5.3.3 Governance-based Inflation Rate

Due to the complex factors influencing the optimal inflation rate, Multi utilizes a dynamic, governance-based approach for its adjustment. Governance tokens are used to vote on and adjust this parameter, allowing Multi users to remain passive if they wish. This gives providers an active say in the price they charge for their services, as they are the primary holders of governance tokens. This arrangement is logical, as providers are locked into the system through token stream contracts, while users retain the flexibility to exit if inflation becomes excessive. Furthermore, the fees providers earn are directly tied to Multi's growth, incentivizing them to modulate the inflation rate responsibly, as excessive inflation could lead to user attrition and a subsequent decline in their fee revenue.

5.4 Purpose of Redistribution Reward

The redistribution reward system is a core component of Multi's design, aimed at incentivizing the contribution of high-quality tokens to the reserve while promoting a meritocratic governance model. To achieve this, the system introduces a stake-based participation model, requiring providers to commit governance tokens as collateral. While providers whose performance aligns with the average can expect to have their collateral returned, the act of staking itself represents an opportunity cost, as these tokens are temporarily locked and unavailable for withdrawal. To compensate for this opportunity cost and incentivize participation, the redistribution reward system offers providers two potential benefits: access to inflation rewards and the ability to earn additional governance tokens through superior performance relative to their peers.

5.4.1 Incentive Structure and Mechanism

The inflation reward alone cannot function as a purely performance-based incentive because providers must actively supply their own tokens to the token stream and do not receive the full trade quantity back immediately. This makes the cost of participation proportional to the reward, rendering the inflation reward primarily a collective reward shared among all providers based on their level of participation. To incentivize honest participation and differentiate between providers based on their ability to select high-performing assets, a more comprehensive reward structure is necessary. Thus, the redistribution reward mechanism was designed to reintroduce a performance-based element.

The redistribution reward system is designed to incentivize providers to contribute high-quality tokens and punish those who attempt to offload low-quality tokens. It operates under the assumption that the majority of providers are motivated to maintain the stability and growth of Multi to continue receiving inflationary rewards from users. This creates a general incentive to avoid contributing assets that could undermine the system's integrity and deter Multi users. The redistribution of staked governance tokens based on the relative performance of the chosen assets serves to further discourage malicious actors by gradually transferring their staked tokens to providers who consistently make better selections.

In essence, the redistribution mechanism reallocates the entry fees for upcoming competitions, with the most successful providers accumulating more tokens to potentially use in future rounds or sell to other interested participants. This system effectively lowers the cost of participation for proficient decision-makers compared to those who consistently underperform. Over time, this dynamic creates a self-reinforcing cycle where the pool of participants becomes increasingly optimized, consisting of those who have consistently demonstrated their ability to select high-performing assets.

5.4.2 Meritocratic Governance and System Integrity

The redistribution reward system establishes a form of meritocratic governance by rewarding strong prediction abilities with governance tokens. This approach is based on the premise that these abilities correlate with the capacity to identify trends and comprehend technological advancements—skills essential for effective leadership. By attracting and empowering individuals and organizations with forward-looking perspectives, the system has the potential to enhance Multi's technological capabilities and overall decision-making processes.

The dual-purpose nature of the governance token, serving both as a governance tool and an entry fee for participation, enhances its utility and bolsters its tokenomics compared to tokens solely used for governance. This design increases the cost for malicious actors to acquire sufficient tokens to manipulate the system, thus safeguarding Multi from potential attacks or the approval of low-quality tokens.

The efficacy of this mechanism relies heavily on the participation ratio, which determines the amount of governance tokens required as a stake. A ratio that is too low could undermine the competitive aspect of the system, while a ratio that is too high could deter participation and limit the flow of assets into the reserve. Therefore, meticulous calibration of the participation ratio is essential to foster healthy competition among providers, encourage robust participation, and ensure the sustained growth and evolution of Multi.

5.5 Token Stream Contract Design

The token stream contract in Multi serves as the foundation of its token acquisition mechanism, establishing a structured and secure framework for interactions between stream providers and the system. By incorporating gradual contribution, vested rewards, and a slashing mechanism, the contract design aims to incentivize responsible, long-term participation while mitigating risks such as market manipulation and instability. This design fosters a relationship between providers and Multi users that encourages a continuous and sustainable inflow of high-quality tokens into the Multi reserve.

5.5.1 Alternative Designs

The token stream contract mechanism in Multi is designed to offer flexibility to providers while also safeguarding the system. This means that providers can easily enter the system, with the option to contribute tokens gradually rather than requiring a single, upfront deposit. This flexibility enables providers to allocate capital to other activities, such as trading or staking in other protocols. It also gives them the flexibility to terminate the contract if they wish, which adds complexity to the mechanism but increases usability for providers. We will now explore alternative designs that do not have this flexibility, where contract termination is disabled and the system instead relies on single deposits rather than multiple, for a given token stream contract.

The first single-deposit model considered involved an immediate token sale. This meant that the quantity would enter Multi's reserve, new supply would be minted immediately, and then placed in a vesting contract. Over time, depending on the token's subsequent performance, this quantity would be either increased or decreased, leading to either slashing or rewards. However, this alternative design was rejected due to concerns about both the potential for Multi price instability caused by these abrupt changes and the possibility that the retroactive nature of the rewards in this model could incentivize Multi holders to exit the system prematurely to avoid potential dilution of their holdings.

The other single-deposit model considered involved a gradual token sale, as in the original model, but with the full token quantity immediately locked into the contract. This would ensure providers are fully exposed to the asset they contribute, potentially increasing their incentive to contribute high-quality tokens. However, it would also significantly increase the costs and risks for providers, potentially deterring participation and limiting the diversity of assets in the reserve. To compensate for these heightened risks, providers would likely demand much higher rewards, in the form of a higher inflation rate, making it more difficult to maintain the system's economic viability for Multi users.

Another question that may arise concerning the design is why tokens are sourced directly from providers rather than from the open market. One potential alternative would involve the system first attempting to purchase tokens at a lower price from the market, only resorting to the provider for any remaining quantity. While this approach could theoretically lead to more efficient pricing and increased system profits, it also presents significant risks. Providers could manipulate the market by colluding with other actors or acting themselves to sell overvalued tokens to the system. Since market-based sales lack the yield vesting mechanism inherent in token stream contracts, there would be no vested Multi available to slash as a penalty if the provider terminates the contract prematurely, leaving the system vulnerable to exploitation. Therefore, the current design prioritizes direct sourcing from providers to ensure accountability and mitigate the risk of market manipulation.

5.5.2 Ensuring Fair Acquisition Price

The previously explored market-based accumulation alternative highlights the importance of the token stream contract model's key design feature: gradual token acquisition. The design seeks to protect against situations where actors sell tokens to the system only during times of high prices or market cycle peaks, while refraining from selling during periods of low prices. This could lead to the system missing opportunities to acquire tokens at lower prices, resulting in an average accumulation price that does not accurately reflect the asset's true value and ultimately leading to the continuous devaluation of Multi.

However, the effectiveness of this protection depends on the contract length. By aligning the contract length with market cycles, Multi achieves a more balanced and sustainable accumulation strategy. The ideal contract length is not a one-size-fits-all solution and may vary depending on the specific market sector, environment, and asset volatility. It is also influenced by user preferences and the system's ability to implement changes effectively. Therefore, the contract length should be viewed as a dynamic parameter that can be adjusted based on the evolving needs of the ecosystem.

For example, in a highly volatile market, a longer contract period might be preferable to smooth out price fluctuations and ensure a fair average acquisition price. Conversely, in a more stable market, a shorter contract period might be sufficient. The system's governance mechanism allows for flexibility in adjusting the contract length as needed to adapt to changing market conditions and user preferences.

5.5.3 Slashing Mechanism and Yield Vesting Schedule

Another crucial element in maintaining a fair average acquisition price, particularly when early contract termination is an option, is the slashing mechanism and its associated benchmark. The specific benchmark was chosen because it quantifies the amount of Multi that providers have received for their contributions thus far, effectively representing their "debt" to the system. This design is intentionally flexible, not penalizing providers who terminate their contracts if the token price remains above its historical average, as that would not indicate an unfair acquisition price for the system. Even when confident that the token price will not fall below this average, providers are likely to avoid early termination as they would no longer be eligible for rewards, while still incurring the opportunity cost of having their capital locked in the system.

The quantity of Multi slashed is determined not only by the benchmark but also by the proportion of Multi released to providers at each integration event versus the amount retained for vesting. The chosen yield vesting schedule for Multi is a simple design that distributes their Multi evenly over the remainder of the contract term. This is logical given that the risk for the system is generally higher at the beginning of the contract, when providers can more easily align their actions with their predictions and manipulate the system. Manipulating the system becomes increasingly difficult further into the contract. However, further research is needed to determine whether this particular vesting schedule is the most efficient in ensuring a fair acquisition price while providing maximum flexibility for providers.

5.5.4 Intentional Limitations

The token stream contract design has some apparent limitations. One of these limitations is that tokens can only be sold to the system, not bought from it. This decision is rooted in the inherent asymmetry between selling a trusted asset and buying one lacking confidence. While selling a portion of a high-conviction asset aligns with a provider's belief, buying a distrusted asset seems less congruent. The market stabilizer further complements this design by managing the reserve's composition over time, gradually selling off undesirable assets without impacting the overall distribution, and mitigating the need for buy contracts.

Another limitation is that providers must define the exact amount and duration of their token sales upfront. This process ensures that every token entering the system goes through the same trial of gradual selling, ensuring that the system acquires each token at an average price. Some might consider this approach inflexible, as a decision may last far into the future. However, it also adds a lot of stability and security to the system. It also ensures that every decision-maker is directly responsible for enacting the change they want to make; there is no disconnect between making decisions and their implementation.

Other systems might employ a more active management approach or be target-based, aiming to achieve a specific goal. Examples include on-chain index funds tracking a specific benchmark or stablecoins targeting a specific exchange rate. In both cases, a potential disconnect can arise between the desired state and the actual ability to achieve it, leading to instability and erosion of trust. Many algorithmic stablecoins, for example, have collapsed due to their inability to maintain their peg during periods of market volatility.

5.6 Emergent Diversification Strategy

Multi's decentralized design, wherein the token stream mechanism interacts with the reward system, gives rise to an emergent diversification strategy. This strategy is not dictated by a central authority, but instead self-organizes through the collective decisions of individual providers. By examining the incentives and constraints that guide provider behavior, we can reveal the mechanisms underpinning this emergent strategy and evaluate its potential for constructing a robust and diversified token reserve.

Many entities, whether centralized or decentralized, attempt to manage risk by establishing specific objectives, often based on traditional portfolio theory [5, 6]. This theory focuses on optimizing returns relative to risk, as measured by volatility, and identifying the efficient frontier of portfolios that offer the highest expected return for a defined level of risk. Notably, the portfolio on this frontier with the highest Sharpe ratio, a measure of risk-adjusted return [7], is often sought after, as it theoretically delivers the greatest reward per unit of risk. Fund managers in a traditional system, or even a decentralized protocol, might aim to maintain a portfolio that aligns with this principle of maximizing the Sharpe ratio.

In contrast, Multi's approach to risk management is distinct. Rather than adhering to a fixed objective or relying on various traditional risk metrics, Multi embraces a multifaceted perspective. This open-ended design allows for a comprehensive consideration of various risk factors, including technological, regulatory, and macroeconomic influences, which extend beyond historical performance or volatility measures.

Multi's risk profile is not static but rather emerges organically from its use. Providers, incentivized to maximize their long-term rewards through user growth, are driven to make decisions that contribute to Multi's overall stability and utility. This adaptability allows the system to evolve through different phases, ultimately reaching a level of diversification and risk management that is conducive to its goal of becoming a stable global currency.

5.6.1 Competitive Dynamics in Reserve Diversification

The competitive nature of the reward system encourages a diversified token reserve for several reasons. Firstly, from a rational, game-theoretic perspective, providers are incentivized to diversify their token contributions across multiple assets to maximize their chances of earning rewards. This is because spreading their bets across various assets reduces the risk of any single asset underperforming and increases the likelihood of capturing gains from a broader range of market opportunities.

Secondly, the open and transparent nature of the contract formation process, where providers can observe the choices of others, can influence decision-making and further promote diversification. Observing the actions of others might lead providers to alter their initial strategies, potentially diversifying their contributions to avoid overly concentrated positions.

Finally, the system inherently encourages the selection of high-quality tokens. Providers are more likely to choose tokens they already hold and have thoroughly researched, as they can contribute these assets immediately without additional acquisition costs. Their familiarity with these assets means they better understand their performance characteristics. This tendency to contribute from personal holdings naturally leads to diversification within the reserve, as providers' portfolios are likely to consist of a variety of assets with different risk profiles.

5.6.2 Collaborative Optimization of Reserve Composition

While competition drives diversification, cooperation could emerge as a vital aspect of Multi's strategy. Collaboration involves aligning token stream contracts to achieve beneficial outcomes for Multi and its reserve, such as improving its risk profile and diversification. For example, providers might recognize that a certain token is under- or overrepresented and coordinate their actions to address these imbalances, demonstrating a form of coopetition.

Several factors incentivize collaboration among providers. The requirement to stake governance tokens when creating token stream contracts creates a vested interest in Multi's success. This is because the value of these tokens is directly tied to the overall value of Multi, motivating providers to make decisions that protect and enhance the system. Additionally, the yield in Multi, earned through the yield vesting mechanism of successful token stream contracts, further aligns providers' interests with the Multi's performance.

Another factor is the inflation reward, which increases with the overall success of Multi. As user satisfaction with Multi grows, users are more likely to tolerate higher fees, allowing governance to increase the inflation rate without risking user attrition. Satisfied users are also more likely to recommend Multi to others or use it more extensively, thereby increasing the reserve size and the overall reward given to providers.

The meritocratic redistribution reward system further reinforces this cooperative aspect. As successful providers gain influence and accumulate a greater stake in the system, the overall expertise of the governance population increases. This results in a greater number of rational and skilled actors who understand the benefits of collaboration, leading to a better balance between maximization of individual rewards and optimized outcomes for Multi.

6 Risks and Mitigations

While Multi's design aims to create a robust and secure decentralized currency system, it is not without its challenges and potential vulnerabilities. These risks primarily stem from the token stream mechanism, as it actively changes Multi's reserves. Conversely, the market stabilizer, due to its design, is inherently more secure, maintaining constant backing ratios. This section will examine various risk scenarios and propose potential mitigation strategies, acknowledging that any implemented solution or system alteration may potentially introduce new complexities or vulnerabilities.

6.1 Protecting Against Token Stream Manipulation

The token stream mechanism, while potentially vulnerable due to its open purchasing policy, employs several safeguards to mitigate risk and ensure the integrity of the token acquisition process. Specifically, it spreads purchases out over extended periods and rewards or penalizes providers based on the long-term price performance of their contributed tokens. System security is further influenced by adjustable parameters like inflation rate, participation ratio, and contract length. Optimizing these parameters could further strengthen the system's resilience against various attack vectors, including:

- **Short-term price manipulation:** This involves creating temporary artificial price spikes or exploiting oracle malfunctions to sell tokens to the system at briefly inflated prices.
- **Long-term price manipulation:** This involves maintaining artificial scarcity over extended periods to drive up the selling price of tokens to the accumulator, then selling the hoarded tokens on the open market after the accumulator has completed its purchases.
- **Offloading undesirable tokens:** This involves systematically selling tokens to the system that cannot be liquidated elsewhere without significantly depressing their market price. These actors are motivated not by potential rewards or belief in the tokens' performance, but rather by the opportunity to offload undesirable assets, potentially degrading the overall quality and stability of the reserve.

Each attack vector poses distinct challenges, requiring ongoing refinement and adaptation of mitigation strategies to safeguard Multi's integrity and stability. These strategies include extending contract lengths to deter short-term manipulation, increasing the frequency of accumulation events to limit the impact of price manipulation, enhancing the accuracy and reliability of the price oracle, and ensuring only assets with established use cases and broad token ownership are approved within the system. Furthermore, raising the participation ratio can effectively deter malicious actors by increasing the potential penalties associated with offloading undesirable tokens, making such actions less profitable.

If these problems persist or jeopardize the system, additional solutions could be considered. One approach is to require providers to stake a portion of the token they are selling, aligning their interests with the asset's long-term performance and discouraging manipulative behavior. Another strategy is to implement a hybrid market-based sale approach (as discussed in Section 5.5.1), where the system first attempts to purchase tokens from the open market at potentially lower prices. However, to maintain the system's protection mechanisms, providers would still be obligated to supply the necessary Multi for potential slashing when a market-based sale occurs. This approach could deter providers from offloading overvalued tokens, as market actors would likely capitalize on such opportunities.

6.2 Ensuring System Stability and Adaptability

The Multi system thrives in a state of growth, where an expanding user base fuels a growing reward pool, incentivizing continuous decision-making and adaptation. This growth, coupled with the expiration of older contracts, ensures a steady stream of new decisions, keeping the system dynamic. However, a potential vulnerability arises if the user base initially grows, leading to an expansion of the token reserve, but then contracts. In this scenario, the system could become locked into existing token stream contracts, potentially leading to an unsustainable influx of tokens if demand for Multi decreases. This rigidity could hinder the system's ability to adapt to changing market conditions.

This potential inability to adapt to a shrinking user base can be problematic and could trigger a detrimental feedback loop, akin to a bank run. If users perceive the incoming assets from ongoing token stream contracts as undesirable due to the system's inability to adjust its purchasing behavior, it may cause them to withdraw from Multi. As users leave, the impact of the incoming assets on the remaining users becomes more pronounced, potentially triggering further withdrawals and exacerbating the situation.

Regardless of whether this bank run risk materializes, implementing mechanisms to adapt to a shrinking user base could still be beneficial. A decrease in Multi's user base could indicate dissatisfaction with past decisions regarding token acquisition. These decisions might have been made with the intention of influencing Multi's composition based on its size at that particular time. Thus, when Multi's size subsequently decreases, the reserve's composition might no longer align with the diversification strategy originally envisioned by the providers.

A potential solution to address the issue of a shrinking user base is to proportionally decrease the volume of each token stream contract. However, this raises the question of whether the associated governance token stake should also be reduced proportionally. Reducing the stake might be considered fairer, acknowledging that providers may not be responsible for the system's contraction, which could be due to external factors. Conversely, maintaining the stake could be argued as necessary to hold providers accountable for their decisions, ensuring they remain invested in the system and bear the consequences if their contributions negatively impact Multi.

This adjustment of contract volumes and stakes could be automated, occurring proportionally to the reduction in Multi's supply. Alternatively, a threshold parameter linked to Multi's size could be established, defining the maximum incoming token volume relative to the current supply. This threshold parameter would provide governance stakeholders with a tool to fine-tune the system's response based on the specific circumstances causing the contraction, offering greater flexibility and control.

6.3 Optimizing the Reward Mechanism

In a system with a clearly defined objective, it would potentially be possible to directly measure the impact of each provider's decision on that goal, facilitating a more precise reward allocation. However, Multi's open-ended design, while fostering adaptability and innovation, lacks such a singular objective. Instead, it relies on an emergent strategy where the most effective approaches for achieving price stability and diversification are expected to arise organically.

The current reward system, consisting of redistribution and inflation rewards, aims to address this challenge. While the redistribution system effectively weeds out underperforming providers, the inflation reward, tied to the size of the overall user base, may not fully capture the nuanced impact of each provider's decisions. This could lead to situations where providers who make significant improvements to the system's health and stability are not rewarded proportionally to their impact, potentially discouraging further innovation and optimization.

Several approaches could be considered to strengthen the reward system, although any alteration might introduce new risks and complexity. One potential avenue is to explore reward mechanisms based on the current diversification level of Multi, where providers could receive greater rewards for contributing underrepresented assets and potentially face penalties for actions that increase the overall risk profile of the system. Another approach, also based on the current state of Multi's token reserves, could involve the system actively participating in long-term performance games by creating bets that mirrors its current asset composition. This, or a similar approach, might increase the propensity among participants to make uncorrelated bets, further diversifying the reserve.

6.4 Governance Risks and Challenges

Decentralized governance is essential for Multi's long-term stability and success, but it presents unique challenges. These include optimizing parameters for the dynamic DeFi environment, ensuring the governance process is broadly representative, and aligning the sometimes competing interests of various stakeholders.

6.4.1 Parameter Optimization

Multi's functionality and stability rely on key parameters such as the inflation rate and participation ratio. These parameters require regular adjustments to reflect changing market conditions and user sentiment. Potential solutions include specialized voting mechanisms like token-weighted median voting or bidding processes to determine optimal settings. Additionally, exploring automated parameter adjustments could further streamline governance and improve responsiveness to market dynamics.

The initial configuration of parameters, such as contract length, is also crucial. While fixed parameters may offer initial stability, the evolving DeFi landscape necessitates flexibility to respond to changing market conditions and technological advancements. Ongoing research, analysis of diverse assets and market cycles, and data-driven insights are essential for informed decision-making about token approvals, subsystem formation, and other long-term parameter adjustments. This approach empowers governance participants to make choices that contribute to Multi's sustained success and adaptability.

6.4.2 Addressing Misalignment and Centralization

One concern with the current governance model is the potential concentration of governance tokens among a few successful participants. This could lead to centralized decision-making, undermining the decentralized ethos of Multi. To mitigate this, the system could encourage the wider distribution of governance tokens by allowing users to copy the strategies of successful providers. Additionally, advancements in prediction technologies could empower a broader range of participants to make informed decisions, further decentralizing governance.

Another challenge is the potential misalignment of interests between governance token holders and Multi users, particularly if there's a significant value disparity between the two assets. While legal constraints may deter direct harm to users, this misalignment could erode trust and undermine long-term resilience. Mitigation strategies include imposing limits on actions like inflation adjustments, introducing grace periods for proposal implementation, and exploring weighted voting systems that consider both governance token holdings and Multi ownership. Such measures aim to foster greater alignment between the interests of all stakeholders and ensure that decisions benefit the entire ecosystem.

7 Potential Applications of Multi

Multi, through its innovative design that merges a decentralized currency with an integrated exchange mechanism, aims to fulfill multiple roles within the evolving DeFi ecosystem. This ambition, however, is contingent on successfully navigating potential risk scenarios, adapting to evolving regulatory frameworks, and gaining acceptance from both user and governance communities.

7.1 Currency Use Case

Multi is designed to be a decentralized, adaptive currency that can evolve with market conditions. Unlike traditional cryptocurrencies or stablecoins, Multi has the capacity to integrate new tokens based on shifting economic landscapes, technological advancements, or emerging use cases. This dynamic approach, facilitated by its diversified token reserve, could potentially offer a more resilient and decentralized alternative for achieving price stability.

- **Store of Value:** By maintaining a diversified basket of tokens from multiple economic sectors, Multi has the potential to establish a more stable and resilient store of value. This diversified reserve could buffer the effects of market fluctuations and inflationary pressures, thereby helping to preserve purchasing power over time.
- **Medium of Exchange:** Multi, built on a high-throughput public blockchain, is designed for fast, secure, and borderless transactions. This decentralized structure and rapid processing capability could make it a viable option for everyday use and potentially enable seamless cross-border transactions.
- **Unit of Account:** Multi aims to establish its value based on the collective performance of its underlying reserve assets, rather than relying on external benchmarks like the US dollar exchange rate. This approach creates a more autonomous system for valuing goods and services within the DeFi ecosystem.

7.2 Exchange Platform Use Case

Multi's unique structure, integrating a decentralized currency with an automated arbitrage mechanism, allows it to function as an order book DEX, potentially offering the following advantages:

- **Efficient and Cost-Effective Trading:** The market stabilizer's continuous identification and execution of arbitrage opportunities could lead to reduced slippage and potentially more favorable prices for traders compared to traditional exchanges.
- **Enhanced Liquidity and Asset Diversity:** The diverse token reserve, maintained and updated by the token streams, could offer users seamless access to a wide variety of assets, both popular and niche.
- **On-chain Price Oracle:** The multilateral exchange process, involving simultaneous transactions across multiple tokens, could contribute to robust price discovery and provide a potentially reliable and transparent source of on-chain price information for the DeFi ecosystem.
- **Potential for Earning Trading Fees:** Future iterations may introduce a fee structure that incentivizes liquidity provision, allowing stakeholders to earn a share of trading fees.

7.3 Stream Provider Benefits

Multi's reward system and token stream contract design may offer stream providers distinct advantages and strategies for asset management within the ecosystem:

- **Long-Term Performance Game:** Stream providers can earn governance tokens by accurately predicting token performance, which contributes to the overall price discovery process and provides them with influence over the system's direction.
- **Unit Cost Averaging:** Token stream contracts enable providers to gradually accumulate Multi over time, mitigating the impact of price volatility and offering a reliable, scheduled way to manage their risk exposure.
- **Yield Optimization:** Stream providers could potentially use yield earned from staking or providing liquidity on other DeFi platforms to fulfill their token stream contracts, potentially leading to additional rewards through token streams.

8 Conclusion

This paper introduces Multi, an innovative decentralized currency system designed to address the challenges of price stability and liquidity within the tokenized economy. Multi achieves this through two synergistic mechanisms: the market stabilizer, an automated market maker embedded in on-chain order books, and the token streams, which fosters a diversified asset backing through incentivized participation and token stream contracts. This combined approach enhances liquidity, promotes market stability, and facilitates decentralized decision-making. Additionally, the paper proposes expanding Multi into a hierarchical ecosystem of interconnected variants to achieve greater scalability and ultimately establish itself as a resilient store of value.

Multi is designed to be inclusive, secure, and adaptable, allowing anyone to directly influence its evolving diversification strategy. The gradual token accumulation process aims to mitigate manipulation risks, while the reward system promotes alignment between decision-makers and those who benefit from their decisions, offering a potential solution to the principal-agent problem. Nonetheless, we recognize the need for further research to explore strategies for enhancing the resilience of the accumulation process against manipulation, adapting to changes in the user base, potentially enhancing reward mechanisms, and improving the governance population's ability to optimize parameters.

Multi represents a significant advancement in decentralized currency design, providing a multifaceted approach to risk management and incentivizing long-term strategic thinking among participants. Beyond the fundamental functions of money as a medium of exchange, unit of account, and store of value, Multi offers a platform for competition, risk mitigation, and yield generation. Ultimately, Multi aims to create a future where the concept of money is democratized, empowering individuals and communities worldwide through an inclusive economy where anyone can contribute to its betterment.

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.

[5] H. Markowitz, "Portfolio selection," *The Journal of Finance*, vol. 7, no. 1, pp. 77–91, 1952.

[6] H. M. Markowitz, *Portfolio Selection: Efficient Diversification of Investments*. Yale University Press, 1959.

[7] W. F. Sharpe, "Mutual fund performance," *The Journal of Business*, vol. 39, no. 1, pp. 119–138, 1966.