Stayer Finance: Liquid Staking And Stablecoin Protocol

Wynn Chill Lab
University of Engineering and Technology
Vietnam National University, Hanoi
hello@stayer.finance

Abstract—This paper introduces Stayer, a noncustodial dual-layer decentralized finance (DeFi) protocol designed for the Casper Network to enhance capital efficiency and validator accountability. The protocol addresses the inherent tension between network security and liquidity by implementing a performance-based liquid staking mechanism. Unlike traditional liquid staking models, Stayer utilizes a validator performance multiplier system—ranging from 0.5× to 1.5×—to adjust the issuance of the liquid staking token (ySCSPR) based on commission efficiency and operational reliability. This mechanism creates a game-theoretic alignment that incentivizes delegators to support high-performing nodes, thereby strengthening network health. Furthermore, the protocol introduces a second layer consisting of a Collateralized Debt Position (CDP) system, allowing users to mint cUSD, a native overcollateralized stablecoin, against ySCSPR collateral. Security is maintained through a three-layer oracle architecture incorporating Time-Weighted Average Price (TWAP) and circuit-breaker mechanisms. By providing an integrated solution for capital liquidity, merit-based delegation, and native stablecoin primitives, Stayer establishes a robust foundation for the Casper DeFi ecosystem. Our analysis indicates that the auto-appreciating nature of the ySCSPR collateral significantly reduces liquidation risks compared to static assets.

Index Terms—Blockchain, Casper Network, liquid staking, stablecoin, CDP, validator performance, DeFi, ySCSPR, cUSD.

I. INTRODUCTION

The rapid proliferation of Proof-of-Stake (PoS) networks has established a paradigm where network security is directly proportional to the volume of staked capital. However, this security model introduces an inherent conflict between network integrity and capital efficiency. Staked assets on the Casper Network, while vital for consensus, are rendered illiquid for the duration of their delegation. This illiquidity is exacerbated by a 14-hour unbonding period, creating a significant opportunity cost for participants who must choose between securing the network and engaging in decentralized finance (DeFi) activities.

While liquid staking protocols have emerged as a solution by issuing derivative tokens, current implementations often treat validator sets as a monolith. By applying uniform issuance rates, these protocols ignore critical variances in validator performance, such as commission rates and operational uptime. Consequently, capital allocation in the staking ecosystem is frequently driven by marketing visibility rather than technical merit, failing to incentivize the highest standards of network reliability. Furthermore, the Casper ecosystem currently lacks a native, decentralized stablecoin primitive,

forcing users to rely on bridged assets that introduce external custodial and bridge-related risks.

To address these challenges, we present the Stayer Protocol, a dual-layer DeFi framework designed specifically for the Casper Network. Stayer introduces a novel Performance-Based Liquid Staking mechanism that adjusts the issuance of its liquid staking token, ySCSPR, based on validator performance multipliers ranging from 0.5× to 1.5×. This system creates a game-theoretic environment where rational actors are incentivized to delegate to high-performing validators, thereby enhancing overall network health.

The protocol's second layer features a Collateralized Debt Position (CDP) system, enabling users to mint cUSD, a native overcollateralized stablecoin, against their ySCSPR holdings. This architecture allows participants to maintain their staking exposure and performance rewards while simultaneously accessing dollar-denominated liquidity. Supported by a robust three-layer oracle architecture, Stayer Protocol provides a comprehensive solution for liquidity, validator alignment, and decentralized stablecoin utility within the Casper ecosystem.

The Casper Network staking ecosystem faces three primary challenges that impede capital efficiency and network optimization: capital illiquidity, validator incentive misalignment, and the lack of native decentralized liquidity.

II. PROBLEM ANALYSIS

A. Capital Illiquidity and Unbonding Constraints

Proof-of-Stake (PoS) networks necessitate a lock-up period to ensure network security and prevent long-range attacks. On the Casper Network, this is manifested as a 14-hour unbonding period, spanning two eras. During this interval, staked capital is non-transferable and does not generate rewards, creating a significant opportunity cost for participants. This illiquidity prevents the use of the underlying asset in DeFi protocols, forcing a binary choice between earning staking yields and maintaining liquid capital.

B. Incentive Misalignment in Validator Selection

Existing liquid staking implementations often utilize a uniform issuance model, where the exchange rate between the staked asset and the derivative token is identical across the entire validator set. This model fails to account for the variance in validator performance metrics, specifically:

- **Commission Rates (F_v):** High-fee validators reduce the net yield for delegators without necessarily providing superior service.
- **Operational Reliability:** Factors such as uptime and block production consistency are often ignored in capital allocation.

Under a uniform system, capital allocation is driven by marketing visibility rather than merit. This lacks a game-theoretic mechanism to drive stake toward high-performing nodes, which is essential for long-term network health.

C. Absence of Native Stablecoin Primitives

The Casper ecosystem currently relies heavily on bridged assets to provide dollar-denominated liquidity. This reliance introduces two distinct layers of risk: custodial risk from centralized entities managing reserves, and smart contract/bridge risk from potential vulnerabilities in the bridging infrastructure. The absence of a native, overcollateralized stablecoin prevents the development of a self-sustaining DeFi layer within the network.

D. Mathematical Representation of the Yield Gap

The opportunity cost C_{opp} for a staker can be expressed as the difference between the potential DeFi return R_{defi} and the staking yield R_{stake}, compounded by the liquidity premium L_p:

$$C_{opp} = (R_{defi} + L_p) - R_{stake} \qquad (1)$$

Without a liquid staking solution, C_{opp} remains high, discouraging participation in network security or reducing the total value locked (TVL) in the ecosystem's DeFi protocols.

III. PROTOCOL DESIGN

The Stayer Protocol is architected as a modular dual-layer decentralized finance (DeFi) framework. The first layer focuses on Performance-Based Liquid Staking, while the second layer provides a Collateralized Debt Position (CDP) mechanism for native stablecoin minting.

A. Performance Score System

The defining innovation of the Stayer Protocol is its transition from uniform issuance to a performance-adjusted model.

1) Performance Score (P-Score) Formula: To incentivize network health, each validator v is assigned a Performance Score P_v, which formalizes the trade-off between cost and reliability:

$$P_v = (100 - F_v) \times D_v \qquad (2)$$

where F_v represents the validator's commission rate ($0 \leq F_v \leq 100$), and D_v represents the operational decay factor. This formula ensures that validators with lower commissions and higher uptime receive superior scores, directly benefiting their delegators.

2) Decay Factor Rationale: The decay factor D_v addresses operational reliability by penalizing inactivity:

$$D_v = \max\left(0.5, 1 - \frac{\Delta e}{E_{max}}\right) \qquad (3)$$

where Δe is the number of eras since the validator's last reward and E_{max} is a threshold (default: 10 eras). This mechanism ensures that even a low-fee validator is penalized if they fail to produce blocks, as their D_v will trend toward 0.5, reducing the rewards for their delegators.

3) Multiplier Bounds Analysis: To translate P_v into liquid token issuance, the protocol computes a multiplier M_v based on the network average performance $\bar{P}$:

$$M_v = \frac{P_v \times 10000}{\bar{P}} \qquad (4)$$

To maintain economic stability and prevent extreme issuance anomalies, the protocol applies a bounding function:

$$M_v^{bounded} = \max(5000, \min(15000, M_v)) \qquad (5)$$

This bounds the multiplier between $0.5\times$ and $1.5\times$. This range is wide enough to drive rational delegators toward high-performing validators while protecting the protocol from potential "death spirals" or hyper-inflationary issuance by a single validator.

B. Liquid Staking Layer

The liquid staking layer manages the conversion of CSPR into the yield-bearing ySCSPR token.

1) ySCSPR Minting Mechanism: When a user stakes Δ_{CSPR} with validator v, the amount of ySCSPR minted is determined by both the performance multiplier and the current exchange rate R:

$$\Delta_{ySCSPR} = \frac{\Delta_{CSPR} \times M_v^{bounded}}{R \times 10000} \qquad (6)$$

This ensures that users entering the pool at different times or with different validators are treated fairly according to the protocol's game-theoretic incentives.

2) Exchange Rate Dynamics: The exchange rate R represents the ratio of total CSPR staked (including accrued rewards) to the total ySCSPR supply:

$$R = \frac{T_{staked}}{S_{ySCSPR}} \times 10^{18} \qquad (7)$$

As rewards accrue from the Casper auction contract, T_{staked} grows while S_{ySCSPR} remains constant. Consequently, R appreciates over time, allowing ySCSPR to function as a rebasing-free, value-accruing asset.

3) Unbonding Bypass via Secondary Market: While the protocol supports native unstaking, it is subject to Casper's 14-hour unbonding period. To provide immediate liquidity, ySCSPR is designed as a standard CEP-18 token, allowing it to be traded on secondary markets. This market-based exit allows users to bypass the unbonding period at the cost of a potential market discount, providing flexibility for time-sensitive capital deployment.

C. CDP Vault Layer

The CDP layer allows users to unlock liquidity from their ySCSPR holdings without sacrificing staking rewards.

1) Collateralization Model: Users deposit ySCSPR into the `StayerVault` to mint cUSD, a stablecoin pegged to the US Dollar. The system enforces a maximum Loan-to-Value (LTV) of 50% for new positions. A unique advantage of using ySCSPR as collateral is its auto-appreciating nature; as staking rewards accrue, the value of the collateral increases relative to the debt, naturally lowering the LTV over time.

2) Health Factor Computation: The solvency of a position is monitored via the health factor H:

$$H = \frac{C \times P_{ySCSPR} \times L_{threshold}}{D} \quad (8)$$

where C is the collateral amount, P_{ySCSPR} is the oracle price, D is the debt including accrued stability fees, and $L_{threshold}$ is the liquidation threshold (110%). A position is deemed "healthy" and safe from liquidation as long as $H \geq 1$.

3) Liquidation Mechanism: If $H < 1$, the position becomes eligible for liquidation. Any external actor (liquidator) may repay the outstanding debt D to receive an equivalent value of ySCSPR collateral plus a 10% liquidation penalty:

$$Collateral_{received} = D \times (1 + L_{penalty}) \quad (9)$$

This penalty incentivizes borrowers to maintain healthy ratios while ensuring liquidators are compensated for providing capital to secure the protocol's solvency.

IV. ECONOMIC MODEL

The economic viability of the Stayer Protocol is predicated on a self-reinforcing feedback loop between validator performance, capital allocation, and secondary market liquidity. This section analyzes the flow of value, fee structures, and the game-theoretic incentives driving participant behavior.

A. Token Flow Dynamics

The protocol facilitates a circular economy through three primary tokens: CSPR (native), ySCSPR (liquid staking), and cUSD (stablecoin).

1) **Value Capture**: CSPR is deposited into the LiquidStaking contract, which delegates to the Casper auction contract. Staking rewards accrue back to the pool, increasing the internal exchange rate R.
2) **Liquidity Provision**: ySCSPR is issued to users, representing their claim on the pool. This token can be traded on Decentralized Exchanges (DEXs) or used as collateral in the CDP layer.
3) **Debt Cycles**: Users mint cUSD by locking ySCSPR. Repayment involves burning cUSD plus accrued stability fees, which are retained by the protocol treasury.

B. Fee Structure Analysis

To ensure protocol sustainability and solvency, Stayer implements a targeted fee architecture:

- **Stability Fee** (r): A 2% APR is charged on outstanding cUSD debt. This fee compensates the protocol for the risk of maintaining the stablecoin peg and managing the CDP infrastructure.
- **Liquidation Penalty** ($L_{penalty}$): A 10% penalty is applied when a position's health factor $H < 1$. This penalty is split between the liquidator (incentive for providing capital) and the protocol (risk mitigation).
- **Inactivity Decay**: While not a direct fee to the protocol, the decay factor D_v functions as an economic penalty for underperforming validators, redistributing potential issuance toward more reliable nodes.

C. Yield Projections and Scenarios

The total yield for a Stayer participant is a composite of native staking rewards, performance boosts, and DeFi deployment yields.

1) Composite Yield Formula: The total potential annual percentage yield (APY_{total}) is defined as:

$$APY_{total} = (R_{base} \times M_v) + (LTV \times R_{defi}) - r \quad (10)$$

where R_{base} is the Casper base staking rate ($\sim$7–8%), M_v is the performance multiplier, R_{defi} is the yield from deployed cUSD, and r is the stability fee.

2) Scenario Analysis: Table I illustrates the risk-return profile across different user behaviors.

TABLE I
STAYER PROTOCOL YIELD SCENARIOS

Strategy	Risk Level	Estimated APY
ySCSPR Holding (Low P-score)	Low	7% − 12%
ySCSPR Holding (High P-score)	Low	10% − 15%
CDP Borrowing (50% LTV)	Medium	12% − 18%
CDP Leveraged Staking	High	15% − 27%

D. Game Theory: Rational Delegate Behavior

The Performance Score system creates a game-theoretic environment that optimizes network security without manual governance.

1) The Rational Actor's Choice: A rational delegator seeks to maximize their liquid token issuance Δ_{ySCSPR}. Given the issuance formula:

$$\Delta_{ySCSPR} \propto M_v^{bounded} \quad (11)$$

the delegator will always choose the validator v that maximizes $M_v^{bounded}$. Since M_v is a direct function of the P-score ($P_v = (100 - F_v) \times D_v$), capital naturally flows toward validators with:

1) **Low Commission** (F_v): Reducing the fee maximizes the score.
2) **High Reliability** (D_v): Maintaining uptime prevents decay.

2) Validator Competition: This creates a competitive equilibrium. Validators are forced to lower their commissions and invest in robust hardware to attract stake. If a validator increases fees or suffers downtime, the multiplier M_v drops, triggering an immediate exit of rational capital toward higher-performing competitors. This "liquidity-weighted consensus" ensures that Casper's security is concentrated in the hands of the most efficient and reliable operators.

3) Auto-Appreciation as Risk Mitigation: Unlike static collateral, ySCSPR is an auto-appreciating asset because R increases as rewards accrue. This creates a "safety margin" for CDP borrowers; even if the market price of CSPR remains flat, the health factor H of a position will naturally improve over time as the collateral value outpaces the 2% stability fee.

V. ORACLE & SECURITY

The Stayer Protocol's reliance on accurate price data for Collateralized Debt Position (CDP) solvency necessitates a robust and resilient oracle infrastructure. This section details the multi-layered oracle design and the protocol's systemic security mitigations.

A. Three-Layer Oracle Architecture

To ensure the integrity of price feeds against manipulation and technical failure, Stayer implements a hierarchical oracle system.

1) Layer 1: Primary Oracle (Styks TWAP): The primary price feed is derived from the Styks Decentralized Exchange (DEX) using a Time-Weighted Average Price (TWAP). The price is calculated over a 30-minute sliding window to mitigate the impact of flash-loan attacks and temporary volatility:

$$P_{TWAP} = \frac{\sum_{i=t_1}^{t_2} P_i \times \Delta t_i}{t_2 - t_1} \tag{12}$$

This mechanism ensures that a single large trade cannot instantly manipulate the collateral valuation within the vault system.

2) Layer 2: Staleness Detection: The protocol tracks the timestamp of every update (t_{last}). If the duration since the last update exceeds the staleness threshold ($T_{stale} = 2$ hours), the oracle enters a "stale" state. This acts as a safeguard against infrastructure outages or underlying DEX liquidity freezes.

3) Layer 3: Emergency Fallback: In the event of a total failure of on-chain price feeds, the protocol administrators maintain a manual price override capability. This is a last-resort mechanism controlled via multi-signature authority to prevent protocol insolvency during extreme "black swan" events.

B. Circuit Breaker Mechanisms

To protect the system during periods of high uncertainty, Stayer employs automated circuit breakers.

- **Price Staleness Lock**: When the T_{stale} threshold is breached, the protocol automatically halts all borrowing and liquidation operations. This prevents the execution of liquidations based on outdated (and potentially incorrect) market data.
- **Emergency Pause**: A global circuit breaker flag can be toggled by the admin multi-sig to pause all contract interactions in the event of a discovered smart contract vulnerability.

VI. SMART CONTRACT ARCHITECTURE

The Stayer Protocol is implemented as a modular suite of smart contracts on the Casper Network, utilizing the CEP-18 token standard for its liquid assets. The architecture is designed to separate validator logic, liquid staking operations, and collateralized debt management.

A. Contract Interaction Framework

1) System-Wide Interaction Framework: The overall protocol lifecycle, from user staking to oracle price integration, is coordinated through a series of automated interactions between core contracts and external actors.
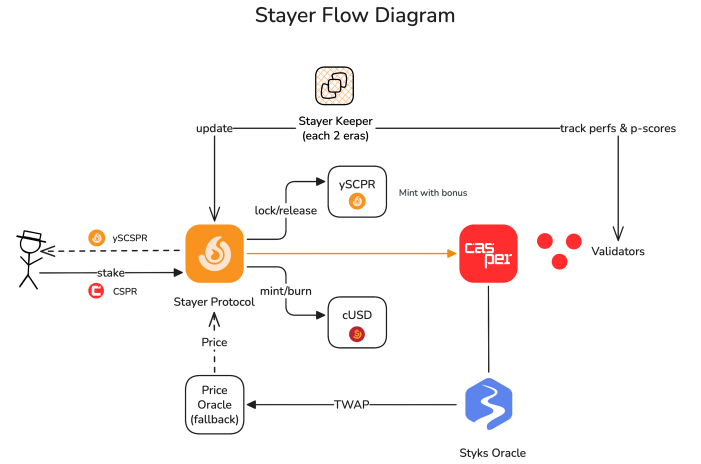

Fig. 1. Stayer Flow Diagram: Illustrating the interaction between users, the Stayer Protocol, Stayer Keepers, and the dual-oracle price feed system.

As shown in Fig. 1, the protocol operations are supported by two critical background processes:

- **Stayer Keepers**: These off-chain entities update the protocol state every 2 eras, tracking validator performance metrics and calculating P-scores to ensure the M_v multipliers remain accurate.
- **Price Oracle Integration**: The protocol consumes Time-Weighted Average Price (TWAP) data from the Styks Oracle, providing a manipulation-resistant price feed for both CSPR and ySCSPR.

2) Lending and Vault Logic: The CDP (Collateralized Debt Position) layer is managed by the Stayer Vault Protocol, which governs the lifecycle of the cUSD stablecoin. This layer allows users to unlock value from their staked assets without losing exposure to Casper network rewards.

The lending process, visualized in Fig. 2, follows a strict "Lock-and-Mint" and "Release-and-Burn" cycle:
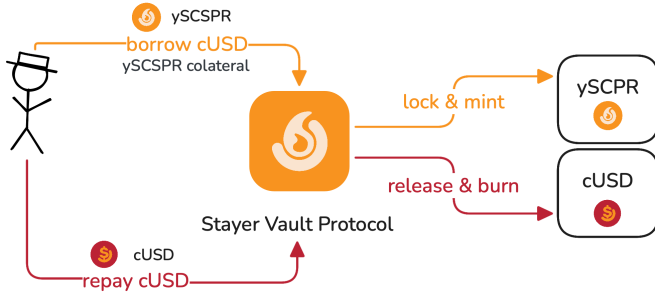
Stayer Lending Flow Diagram

Fig. 2. Stayer Lending Flow Diagram: The mechanism for locking ySCSPR collateral to mint cUSD and the subsequent repayment/burning process.

- **Borrowing Phase**: Users deposit ySCSPR as collateral into the Stayer Vault. Based on the current oracle price and a 50% Loan-to-Value (LTV) ratio, the protocol mints the corresponding amount of cUSD.
- **Repayment Phase**: To reclaim their collateral, users must return the borrowed cUSD. The protocol then burns the stablecoins and releases the ySCSPR back to the user's wallet.

3) Key Contract Components: The architecture is comprised of several specific entry points that facilitate these flows:

- **ValidatorRegistry**: Stores P-scores and operational data for all Casper validators.
- **LiquidStaking**: Handles the conversion of CSPR to ySCSPR using the performance-adjusted formula.
- **StayerVault**: Manages position state, including collateral amounts, debt balances, and health factor calculations for liquidations.

B. Key Functions Overview

The system's operational logic is exposed through several high-level entry points across the core contracts.

1) ValidatorRegistry Entry Points:

- `update_validator`: Used by authorized keepers to submit the latest performance metrics (F_v, D_v) for a specific validator.
- `get_multiplier`: A public view function that returns the bounded performance multiplier ($M_v^{bounded}$) for a given validator address.

2) LiquidStaking Entry Points:

- `stake`: Accepts CSPR deposits, calls the `ValidatorRegistry` for the multiplier, and mints the adjusted amount of ySCSPR to the user.
- `unstake`: Initiates the 14-hour unbonding process by burning ySCSPR tokens and signaling undelegation to the Casper network.

3) StayerVault Entry Points:

- `borrow`: Verifies the user's collateral value against the 50% Loan-to-Value (LTV) limit and mints cUSD stablecoins.
- `liquidate`: Allows third parties to repay debt for unhealthy positions ($H < 1$) in exchange for ySCSPR collateral plus a 10% penalty.

C. Upgrade and Governance Mechanism

The Stayer Protocol follows a path of progressive decentralization to balance initial agility with long-term security.

1) Contract Immutability: By design, the core smart contracts are non-upgradeable to ensure that the protocol's mathematical logic (such as the issuance formula) cannot be altered post-deployment. This provides users with deterministic guarantees regarding their staked assets.

2) Administrative Controls: During the initial bootstrap phase, certain parameters are managed by a core team admin key:

- **Emergency Pause**: An administrative circuit breaker that can halt `borrow` and `liquidate` functions in the event of a discovered vulnerability.
- **Parameter Tuning**: Adjusting LTV ratios, stability fees, and validator whitelists.

3) Progressive Decentralization: The roadmap includes the transition of administrative authority to a 3-of-5 multi-signature wallet, followed by the implementation of a Decentralized Autonomous Organization (DAO). This DAO will eventually assume control over the `PriceOracle` emergency overrides and parameter governance through token-weighted voting.

VII. GOVERNANCE & ROADMAP

Stayer Protocol is designed for progressive decentralization to balance initial stability with long-term community autonomy.

A. Decentralization Path

The protocol follows a three-stage roadmap toward full autonomy:

- **Initial Phase**: Centralized control by the core team over the validator whitelist, oracle updates, and emergency pause authority.
- **Intermediate Phase**: Transition of administrative authority to a 3-of-5 multi-signature wallet and decentralization of the keeper network through stake requirements.
- **Full Decentralization**: Implementation of a Decentralized Autonomous Organization (DAO) with token-weighted voting and the removal of administrative keys.

B. Parameter Governance

Post-decentralization, the DAO will govern critical systemic parameters, including:

- **LTV and Liquidation Ratios**: Adjusting the 50% LTV or the 110% liquidation threshold based on market volatility.

- **Fee Structures**: Modifying the 2% stability fee or the 10% liquidation penalty to optimize protocol revenue and solvency.
- **Validator Management**: Maintaining the validator registry and adjusting the E_{max} decay threshold.