Yield-Bearing Bridge Tokens: Cross-Chain Capital Efficiency through Composable Yield Strategies

Lux Teleport Omnichain Yield Protocol

Zach Kelling

Lux Industries

2024 (Revised December 2025)

Yield-Bearing Bridge Tokens: Cross-Chain Capital Efficiency through Composable Yield Strategies

Lux Teleport Omnichain Yield Protocol

Zach Kelling* Vishnu Seesahai
Lux Industries, Inc.
research@lux.network

2024 (Revised December 2025)

Abstract

Over $15 billion in assets are locked across cross-chain bridges, yet these assets earn zero yield—a capital inefficiency exceeding $600 million per year in forgone staking and lending returns at prevailing rates. We present the Lux Teleport Yield Protocol, a system that deploys locked bridge assets into yield-generating strategies on their source chains and reflects accrued yield in bridge token share prices on destination chains through ERC-4626-inspired share accounting. The protocol defines a composable `IYieldStrategy` interface implemented by 29 strategies across 9 categories: liquid staking, restaking, lending, stablecoin yield, LP/DEX, Bitcoin-native yield, Solana DeFi, TON DeFi, and perpetuals. We formalize share price dynamics, proving that the share price $p(t)$ is monotonically non-decreasing under non-negative yield and bounded below by the collateralization invariant $p(t) \geq 0.985$. An MPC-attested backing oracle reports aggregate strategy positions at configurable intervals; if the attested backing falls below 98.5% of outstanding shares, all bridge operations halt automatically. We introduce a three-tier risk framework with per-tier allocation caps, analyze the xLUX economic flywheel where protocol fees compound across bridge, DEX, lending, perpetuals, and NFT AMM, and demonstrate that yield-bearing bridge tokens (yLETH, yLBTC, yLUSD) achieve 4.2–23% APY compared to 0% for conventional wrapped assets. The Bitcoin-native yield composition—Babylon staking layered with restaking and DeFi—represents, to our knowledge, the first protocol enabling native BTC yield without custodial wrapping.

1 Introduction

Cross-chain bridges hold over $15 billion in locked assets as of Q1 2025 [1]. These assets—primarily ETH, BTC, and stablecoins—sit idle in bridge vaults while their equivalent representations circulate on destination chains. At prevailing DeFi yields (3–5% for ETH staking [6], 4–8% for stablecoin lending [7]), this idle capital forfeits $600M–$1.2B annually.

The waste is structural. Conventional bridges treat the lock-and-mint operation as a pure custodial function: lock the original, mint a synthetic, return the original upon burn. The locked assets serve no productive purpose during the bridge period. This is equivalent to holding cash in a vault rather than deploying it in interest-bearing instruments—a practice that banking abandoned centuries ago.

We address this inefficiency with a yield-bearing bridge token system built atop the Lux Teleport protocol [2]. The key insight is that bridge vaults can be replaced with yield-bearing vaults that deploy locked assets to on-chain strategies, while maintaining the 1:1 (or better) backing guarantee that bridge security requires.

1.1 Contributions

1. A share-based accounting model for yield-bearing bridge tokens with formal monotonicity and collateralization proofs (Section 3).
2. A composable `IYieldStrategy` interface with 29 concrete implementations across 9 yield categories (Section 4).
3. Bitcoin-native yield composition through Babylon, Lombard, SolvBTC, and CoreDAO—the first non-custodial BTC yield aggregation (Section 5).
4. MPC-attested backing oracle with automatic undercollateralization pause (Section 6).
5. A three-tier risk framework with formal diversification constraints (Section 7).
6. Economic analysis of the xLUX flywheel and capital efficiency comparison against conventional bridge tokens (Section 8).

1.2 Scope and Relationship to Prior Work

This paper extends the Lux Teleport protocol specification [2], which defines the MPC threshold signature scheme (FROST [3] and CGGMP21 [4]), nonce management, sovereign governance, and Shariah compliance. We take the bridge's security model as given and focus exclusively on the yield layer: how locked assets generate returns, how those returns are reflected in bridge token prices, and how the system maintains safety invariants under adversarial conditions.

2 Problem Statement

Definition 2.1 (Bridge Capital Inefficiency)**.** *Let L denote the total value locked across all bridge protocols, and let r denote the risk-adjusted opportunity cost of capital (the yield those assets would earn if not locked). The annual capital inefficiency is:*

$$\mathcal{I} = L \cdot r \tag{1}$$

For $L = \$15B$ and $r = 4.5\%$ (weighted average of ETH staking and stablecoin lending yields), $\mathcal{I} = \$675M/year$.

This inefficiency creates three downstream problems:

Higher bridge fees. Without yield income, bridge operators must charge higher fees to cover infrastructure costs, increasing friction for cross-chain transfers.

Inferior bridge tokens. Wrapped ETH (WETH) on a destination chain earns 0% APY. Native stETH on Ethereum earns 3.5%. A user who bridges ETH pays an implicit cost equal to the forgone staking yield for the duration of the bridge period.

Liquidity fragmentation. Rational capital avoids bridges because the opportunity cost exceeds the utility of cross-chain deployment. This reduces liquidity on destination chains, widening spreads and increasing slippage.

Remark 2.1. *The capital inefficiency is not merely theoretical. As of Q1 2025, approximately \$3.8B of the \$15B in bridge TVL is ETH that could be earning 3.5% in Lido [6], \$2.1B is stablecoins that could earn 5–8% in Aave [7], and \$1.4B is BTC that could earn 3–5% through Babylon [9]. The remainder consists of altcoins with varying yield opportunities.*

3 Share-Based Accounting

3.1 Token Model

The Teleport yield system issues three classes of bridge tokens per underlying asset:

Definition 3.1 (Bridge Token Classes)**.** *For an underlying asset A:*

1. ***LA*** *(e.g., LETH): 1:1 wrapped token. Share price fixed at 1.0. No yield.*
2. ***yLA*** *(e.g., yLETH): Yield-bearing token. Share price appreciates as yield accrues. Non-rebasing.*
3. ***syLA*** *(e.g., syLETH): Shariah-compliant yield token. Same mechanics as yLA but restricted to halal-classified strategies [2].*

The yield-bearing variants follow the ERC-4626 tokenized vault standard [5], adapted for cross-chain operation where the vault (source chain) and the share token (destination chain) reside on different chains.

3.2 Share Price Dynamics

Definition 3.2 (Share Price)**.** *Let $B(t)$ denote the total backing assets on the source chain at time t, and $S(t)$ denote the total outstanding shares (yield-bearing bridge tokens) on all destination chains. The share price is:*

$$p(t) = \frac{B(t)}{S(t)} \tag{2}$$

The backing $B(t)$ evolves as:

$$B(t) = B(t_0) + \underbrace{\int_{t_0}^{t} Y(\tau)\, d\tau}_{\text{yield accrued}} - \underbrace{\int_{t_0}^{t} F(\tau)\, d\tau}_{\text{fees extracted}} - \underbrace{\int_{t_0}^{t} W(\tau)\, d\tau}_{\text{withdrawals}} \tag{3}$$

where $Y(\tau)$ is the instantaneous yield rate, $F(\tau)$ is the performance fee rate, and $W(\tau)$ is the withdrawal rate.

The share supply evolves as:

$$S(t) = S(t_0) + \underbrace{D(t_0, t)}_{\text{new deposits}} - \underbrace{R(t_0, t)}_{\text{redemptions}} \tag{4}$$

where D and R are cumulative deposits and redemptions respectively.

Theorem 3.1 (Share Price Monotonicity)**.** *If the net yield rate after fees is non-negative, i.e., $Y(\tau) - F(\tau) \geq 0$ for all $\tau \in [t_0, t]$, and no withdrawals reduce backing below the collateralization threshold, then for any $t_1 < t_2$:*

$$p(t_2) \geq p(t_1) \tag{5}$$

Proof. New deposits of amount a at time t simultaneously increase $B(t)$ by a and increase $S(t)$ by $a/p(t)$ shares, leaving $p(t)$ unchanged. Redemptions of s shares decrease $S(t)$ by s and decrease $B(t)$ by $s \cdot p(t)$, also leaving $p(t)$ unchanged. Between deposits and redemptions, only yield and fees affect the price:

$$\frac{dp}{dt} = \frac{Y(t) - F(t)}{S(t)} \geq 0 \tag{6}$$

Since $S(t) > 0$ (the token has nonzero supply) and $Y(t) - F(t) \geq 0$ by assumption, $dp/dt \geq 0$, so p is monotonically non-decreasing. □

3.3 Conversion Functions

Following ERC-4626 semantics with virtual offset for first-depositor protection:

$$\texttt{convertToShares}(a) = \left\lfloor \frac{a \cdot (S(t) + V_S)}{B(t) + V_A} \right\rfloor \tag{7}$$

$$\texttt{convertToAssets}(s) = \left\lfloor \frac{s \cdot (B(t) + V_A)}{S(t) + V_S} \right\rfloor \tag{8}$$

where $V_S = V_A = 10^8$ (`VIRTUAL_SHARES` and `VIRTUAL_ASSETS`) provide production-grade first-depositor inflation attack protection. The matched pair ensures the initial `pricePerShare` and `exchangeRate` start at 1:1 with virtual offset applied consistently across all share price calculations. Rounding is always in favor of the vault (floor for shares on deposit, floor for assets on withdrawal), preventing rounding-based extraction attacks [5]. Per-operation `forceApprove` (approve to zero then to exact amount) eliminates infinite approval risks; each strategy interaction approves only the exact amount needed for that operation.

3.4 Cross-Chain State Synchronization

The share price on destination chains is updated through MPC-attested backing reports (Section 6). Between attestations, the share price on the destination chain is stale by at most one attestation interval Δ:

$$|p_{\text{dest}}(t) - p_{\text{source}}(t)| \leq \frac{Y_{\max} \cdot \Delta}{S(t)} \tag{9}$$

where $Y_{\max}$ is the maximum yield rate across all active strategies. For $\Delta = 1$ hour and $Y_{\max}$ corresponding to 30% APY, the maximum staleness on a \$100M vault is approximately 0.0034%, which is negligible relative to bridge fees.

4 Yield Strategy Interface

4.1 Interface Definition

Every yield source implements the `IYieldStrategy` interface:

Listing 1: IYieldStrategy interface

```
interface IYieldStrategy {
    function deposit(uint256 amount)
        external returns (uint256 shares);
    function withdraw(uint256 shares)
        external returns (uint256 assets);
    function totalAssets()
        external view returns (uint256);
    function currentAPY()
        external view returns (uint256);
    function harvest()
        external returns (uint256 harvested);
    function isActive()
        external view returns (bool);
    function riskTier()
        external view returns (uint8);
}
```

Definition 4.1 (Strategy Properties)**.** *A compliant strategy satisfies:*

1. ***Idempotent harvest**: Calling `harvest()` twice in succession yields zero on the second call.*
2. ***Withdrawal guarantee**: `withdraw(s)` returns at least `convertToAssets(s)` − `slippageTolerance` assets.*
3. ***Accounting accuracy**: $|$`totalAssets()` $- A_{actual}| \leq \epsilon$ where ϵ is bounded by oracle precision.*
4. ***Risk classification**: `riskTier()` returns a value in $\{1, 2, 3\}$ corresponding to low, medium, or high risk.*

4.2 Strategy Taxonomy

Table 1 enumerates all 29 deployed strategies across 9 categories.

4.3 Yield Composition

Bridge token holders earn layered yield from multiple simultaneous sources. We formalize this as additive yield composition:

Definition 4.2 (Yield Composition)**.** *For a yield-bearing bridge token yLA, the total APY is:*

$$r_{total} = r_{base} + r_{restaking} + r_{bridge} + r_{DeFi} \quad (10)$$

where:

- r_{base}*: primary yield source (staking, lending, LP)*
- $r_{restaking}$*: additional yield from restaking derivatives*
- r_{bridge}*: share of Teleport bridge fees via xLUX*
- r_{DeFi}*: yield from using yLA as collateral/LP on destination chain*

Remark 4.1. *The DeFi layer (r_{DeFi}) is not part of the vault's backing—it is additional yield earned by the token holder through their own DeFi participation on the destination chain. The vault only manages $r_{base} + r_{restaking}$, and r_{bridge} flows through the xLUX staking mechanism.*

Table 2 illustrates the yield stack for three representative bridge tokens.

5 Bitcoin-Native Yield

Bitcoin yield historically required custodial wrapping (WBTC [16]) or centralized lending (BlockFi, Celsius—both insolvent). Babylon [9] changed this by enabling native BTC staking through Bitcoin Script timelock covenants, providing economic security to Proof-of-Stake chains without moving BTC off the Bitcoin network.

Teleport composes Bitcoin-native yield through four protocols:

5.1 Babylon BTC Staking

Babylon enables BTC holders to stake their BTC to secure PoS chains through a covenant-based locking mechanism on Bitcoin L1 [9]:

1. BTC is locked via a self-custodial covenant transaction with a FROST-signed timelock.
2. The locked BTC provides economic security to participating PoS chains.
3. Staking rewards accrue in the secured chain's native token.

4. Unstaking requires a Bitcoin L1 transaction after the timelock expires.

The Teleport bridge vault's BTC is staked through Babylon, with the FROST threshold key serving as both the bridge custody key and the Babylon staking key. This dual use eliminates an additional trust assumption—the same MPC set that secures the bridge also manages the staking position.

5.2 Liquid BTC Derivatives

Definition 5.1 (BTC Yield Stack)**.** *The Teleport BTC yield stack composes four layers:*

$$r_{BTC} = r_{Babylon} + r_{liquid} + r_{restake} + r_{DeFi} \quad (11)$$
$$\approx 4.5\% + 1.5\% + 2.0\% + (5\text{–}15\%)$$

Layer composition:

Layer 1: Babylon staking ($r_{\text{Babylon}} \approx 3$–5%). Raw BTC staking yield from securing PoS chains. The FROST-controlled Taproot address commits to Babylon's staking covenant.

Layer 2: Liquid derivative ($r_{\text{liquid}} \approx 0.5$–2%). Lombard LBTC [10] or SolvBTC [11] wraps the Babylon-staked position into a liquid derivative tradeable on EVM chains. The derivative captures the base staking yield plus protocol-specific incentives.

Layer 3: Restaking ($r_{\text{restake}} \approx 1$–3%). The liquid BTC derivative is restaked through EigenLayer or Symbiotic, providing security to additional AVS protocols in exchange for restaking rewards.

Layer 4: DeFi ($r_{\text{DeFi}} \approx 5$–15%). yLBTC holders on Lux use their tokens as LP capital, collateral in lending markets, or in yield optimization protocols on the destination chain.

5.3 CoreDAO Dual Staking

CoreDAO [12] offers an alternative BTC yield path through dual staking: BTC is delegated to Core validators alongside CORE tokens, earning staking rewards from both networks simultaneously. The yield (3–12% APY) depends on the BTC/CORE delegation ratio and Core network utilization.

5.4 Security Analysis

Property 5.1 (BTC Custody Invariant)**.** *At all times, the BTC backing yLBTC is:*

1. *Held in a FROST 2-of-3 Taproot address (bridge custody), OR*
2. *Locked in a Babylon staking covenant with the same FROST key as the spending condition, OR*
3. *Represented by a liquid derivative (LBTC, SolvBTC) held by a smart contract controlled by the MPC set.*

In all cases, t-of-n MPC signers must cooperate to move the BTC. No single party has unilateral withdrawal authority.

6 MPC Yield Attestation

6.1 Backing Oracle

Because the yield vault (source chain) and the share token (destination chain) exist on different blockchains, destination chains cannot query source-chain vault balances directly. Instead, the MPC signer set periodically attests to the total backing:

Algorithm 1 MPC Backing Attestation

Require: Attestation interval Δ, signer set $\mathcal{S}$, threshold t

At each interval $t_k = t_0 + k\Delta$:
Each signer s_i independently queries all active strategies:
  $B_i \leftarrow \sum_{j=1}^{m} \texttt{strategy}_j\texttt{.totalAssets}()$
Signers exchange B_i values and verify $|B_i - B_j| \leq \epsilon$ for all i, j
if consensus on $B^* = \text{median}(B_1, \ldots, B_n)$ **then**
  Produce threshold signature: $\sigma \leftarrow \text{Sign}_{t,n}(H(\texttt{"BACKING"} \| B^* \| t_k))$
  Broadcast (B^*, t_k, σ) to all destination chains
else
  Flag disagreement; trigger emergency review
end if

Algorithm 2 Auto-Pause on Undercollateralization

Require: Backing report (B_k^*, t_k, σ_k), current state

Verify σ_k against MPC public key
Verify $t_k > t_{k-1}$ (monotonic timestamps)
Compute collateralization ratio: $\theta_k \leftarrow B_k^*/(S(t_k) \cdot p(t_{k-1}))$
if $\theta_k < \theta_{\min}$ **then**
  Set `bridgePaused` $\leftarrow$ `true`
  Emit `UndercollateralizationDetected`(θ_k, B_k^*, t_k)
  Disable `mintDeposit` and `updateBacking`
  Allow `burnForWithdrawal` (users can always exit)
else
  Update $p(t_k) \leftarrow B_k^*/S(t_k)$
  Emit `BackingUpdated`(B_k^*, $p(t_k)$, t_k)
end if

Definition 6.1 (Attestation Message)**.** *The signed backing report has the form:*

$$m_k = H\big(\texttt{"BACKING"} \,\|\, B_k^* \,\|\, t_k \,\|\, chainId_{source}\big) \tag{12}$$

where B_k^* is the attested backing, t_k is the attestation timestamp, and $chainId_{source}$ identifies the source chain. The signature σ_k is produced via CGGMP21 (for EVM destinations) or FROST (for Ed25519/Schnorr destinations).

6.2 Undercollateralization Detection

Invariant 6.1 (Collateralization Bound)**.** *The protocol enforces:*

$$\frac{B_k^*}{S(t_k) \cdot p(t_{k-1})} \geq \theta_{\min} = 0.985 \tag{13}$$

where $\theta_{\min} = 98.5\%$ is the minimum collateralization ratio. If this invariant is violated, the OmnichainRouter on all destination chains enters `PAUSED` state.

Theorem 6.1 (Pause Liveness)**.** *If the actual backing drops below $\theta_{\min} \cdot S(t) \cdot p(t)$, the bridge pauses within at most $\Delta + \delta_{confirm}$ time, where Δ is the attestation interval and $\delta_{confirm}$ is the destination chain confirmation time.*

Proof. The MPC signer set produces a backing report at each interval Δ. By construction, the attested value B_k^* reflects the actual backing at time t_k (median of independent queries). The attestation transaction is submitted to the destination chain and confirmed within δ_{confirm}. Total worst-case latency: the undercollateralization occurs immediately after attestation k, is detected at attestation $k+1$ (delay Δ), and the pause transaction confirms after δ_{confirm}. □

6.3 Attestation Parameters

7 Risk Framework

7.1 Three-Tier Classification

Definition 7.1 (Risk Tiers)**.** *Each yield strategy is classified into one of three risk tiers:*

- ***Tier 1 (Low)**: Blue-chip protocols with $1B+ TVL, multiple audits, 2+ years of*

production operation, no exploits. Examples: Lido, Aave V3, Compound V3, Curve, Spark, Marinade.

- ***Tier 2 (Medium)**: Established protocols with $100M+ TVL, audited, 1+ year of production operation. Examples: EigenLayer, Symbiotic, Morpho, Pendle, Babylon, Lombard, Jito, Kamino, Tonstakers, CoreDAO.*
- ***Tier 3 (High)**: Newer protocols with elevated yield and correspondingly elevated risk. Examples: Ethena, SolvBTC, STON.fi, LPX Perps.*

7.2 Allocation Constraints

The vault enforces per-tier allocation limits:

$$\begin{aligned} w_1 + w_2 + w_3 &= 1 \\ w_1 &\geq 0.50 \\ w_2 &\leq 0.40 \\ w_3 &\leq 0.10 \end{aligned} \tag{14}$$

where w_i is the fraction of total backing allocated to Tier i strategies. These constraints are enforced on-chain by the `YieldBridgeVault` contract.

Theorem 7.1 (Diversification Bound)**.** *No single strategy may receive more than $\alpha_{\max} = 25\%$ of total backing. Combined with the tier constraints, this ensures:*

$$\max_j \frac{A_j}{B} \leq \alpha_{\max} = 0.25 \tag{15}$$

where A_j is the assets deployed to strategy j and $B = \sum_j A_j$ is total backing.

7.3 Maximum Loss Analysis

Definition 7.2 (Strategy Loss)**.** *Let ℓ_j denote the worst-case loss fraction for strategy j (e.g., smart contract exploit draining all funds: $\ell_j = 1.0$). The maximum portfolio loss under the allocation constraints is:*

$$L_{\max} = \max_{\substack{w \in \mathcal{W} \\ j^* \in \{1,\ldots,m\}}} w_{j^*} \cdot \ell_{j^*} \tag{16}$$

where $\mathcal{W}$ is the feasible allocation set satisfying (14).

Under the single-strategy cap of 25%:

Corollary 7.2 (Single-Strategy Failure)**.** *If exactly one strategy suffers a complete loss ($\ell_{j^*} = 1.0$), the maximum portfolio loss is 25%. Combined with the 1.5% collateralization buffer, the bridge pauses before share price drops below $0.985 \times p(t_{k-1})$, protecting holders from losses exceeding 1.5% between attestation intervals.*

Corollary 7.3 (Tier 3 Failure)**.** *If all Tier 3 strategies simultaneously fail ($\ell_j = 1.0$ for all j in Tier 3), the maximum loss is 10% of total backing. The bridge pauses immediately at the next attestation.*

7.4 Strategy Health Monitoring

Each strategy's `isActive()` function is checked at every attestation cycle. A strategy is deactivated when:

1. `totalAssets()` decreases by more than 5% between attestations (abnormal loss).
2. The underlying protocol's TVL drops below $50M (liquidity risk).
3. A security advisory is issued (governance override via SAB or MPC emergency action).
4. `currentAPY()` drops below 0% for two consecutive attestation periods.

Upon deactivation, the vault withdraws all assets from the strategy and reallocates according to the tier-weighted algorithm.

8 Economic Analysis

8.1 Capital Efficiency Comparison

We compare three modes of holding ETH across a bridge:

Definition 8.1 (Capital Efficiency Ratio)**.**

$$\eta = \frac{APY_{\textit{bridge token}}}{APY_{\textit{native}}} \tag{17}$$

where APY_{native} is the yield available on the source chain without bridging.

yLETH achieves $\eta > 1.0$ because the vault captures restaking yield that individual stakers may not access, and bridge fee income from xLUX adds yield not available to direct stETH holders.

8.2 The xLUX Flywheel

On Lux Network, the stakeholder vault for the Teleport OmnichainRouter is LiquidLUX (xLUX). All protocol fees flow to xLUX holders:

$$r_{\text{xLUX}} = \frac{\sum_{p \in \mathcal{P}} f_p \cdot V_p}{\text{totalStaked}_{\text{LUX}}} \tag{18}$$

where $\mathcal{P} = \{\text{bridge, DEX, lending, perps, NFT AMM}\}$ is the set of fee-generating protocols, f_p is the fee rate for protocol p, and V_p is the volume processed by protocol p.

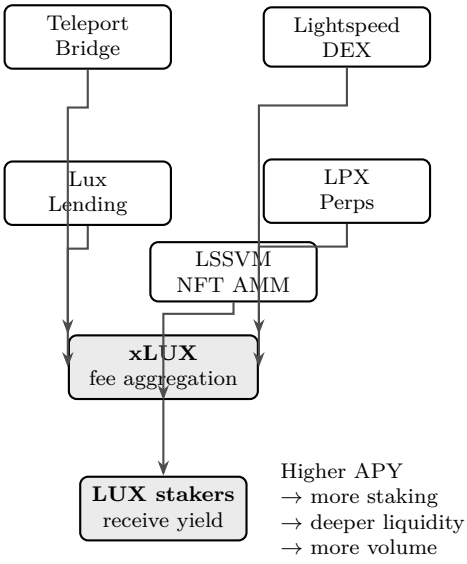

Figure 1: The xLUX fee aggregation flywheel. Fees from all Lux protocols compound into xLUX yield, attracting more staking, deepening liquidity, and generating more fees.

Theorem 8.1 (Flywheel Convergence)**.** *Under the assumption that total protocol volume $V = \sum_p V_p$ is an increasing function of total liquidity $\mathcal{L}$, and liquidity is an increasing function of xLUX APY r_{xLUX}, the system converges to a stable equilibrium. Formally, if:*

$$V = g(\mathcal{L}), \quad g' > 0, \quad g'' < 0 \tag{19}$$

$$\mathcal{L} = h(r_{xLUX}), \quad h' > 0, \quad h'' < 0 \tag{20}$$

$$r_{xLUX} = \frac{f \cdot V}{totalStaked} \tag{21}$$

where g and h are concave increasing functions, then there exists a unique fixed point $(V^*, \mathcal{L}^*, r^*)$ satisfying all three equations.

Proof. Define $\Phi : \mathbb{R}_{>0} \to \mathbb{R}_{>0}$ by $\Phi(r) = f \cdot g(h(r))/\text{totalStaked}$. Since g and h are concave and increasing, Φ is concave and increasing. For sufficiently small r, $\Phi(r) > r$ (the flywheel generates more yield than required). For large r, the concavity of $g \circ h$ ensures $\Phi(r) < r$ (diminishing returns on volume growth). By the intermediate value theorem, there exists a unique r^* with $\Phi(r^*) = r^*$. □

8.3 Fee Flow Quantification

8.4 Yield vs. Risk Frontier

The portfolio of yield strategies traces an efficient frontier in risk-return space. Let $\boldsymbol{r} = (r_1, \ldots, r_m)$ be the vector of strategy APYs and $\boldsymbol{\Sigma}$ be the covariance matrix of strategy returns. The mean-variance optimal allocation is:

$$\max_{\boldsymbol{w}} \boldsymbol{w}^T \boldsymbol{r} - \frac{\lambda}{2} \boldsymbol{w}^T \boldsymbol{\Sigma} \boldsymbol{w} \quad \text{s.t.} \quad \boldsymbol{w} \in \mathcal{W} \tag{22}$$

where λ is the risk aversion parameter and $\mathcal{W}$ is the feasible set defined by the tier constraints (14) and the single-strategy cap.

Remark 8.1. *The governor (DAO) sets λ based on the chain's risk appetite. A conservative chain (e.g., institutional-focused) uses high λ, concentrating in Tier 1. An aggressive chain uses low λ, allocating more to Tier 2/3 for higher yield.*

9 Performance Fee Mechanics

9.1 Fee Structure

Two fees apply to yield-bearing bridge tokens:

1. **Bridge fee** (f_b, default 10 bps, max 100 bps): Charged on deposit/withdrawal. Applied to the principal.
2. **Performance fee** (f_y, default 1000 bps = 10%): Charged on yield only. Never on principal.

The yield distributed to share holders after fees:

$$Y_{\text{net}}(t) = Y_{\text{gross}}(t) \cdot \left(1 - \frac{f_y}{10{,}000}\right) \tag{23}$$

Performance fees are distributed according to the stakeholder share:

$$\text{toStakeholders} = Y_{\text{gross}} \cdot \frac{f_y}{10{,}000} \cdot \frac{f_s}{10{,}000} \quad (24)$$

where f_s is the stakeholder share (default 9000 bps = 90%). The remaining 10% goes to the protocol treasury.

9.2 Fee Accounting in Share Price

Performance fees are extracted by minting additional shares to the fee recipient rather than reducing the backing:

$$\Delta S_{\text{fee}} = \frac{Y_{\text{gross}} \cdot f_y/10{,}000}{p(t)} \quad (25)$$

This dilution-based approach ensures the share price never decreases due to fee extraction—it simply grows slower than the gross yield rate. The share price after fee extraction:

$$p'(t) = \frac{B(t) + Y_{\text{gross}}}{S(t) + \Delta S_{\text{fee}}} = \frac{B(t) + Y_{\text{gross}}}{S(t) + \frac{Y_{\text{gross}} \cdot f_y/10{,}000}{p(t)}} \quad (26)$$

Since $f_y/10{,}000 < 1$, we have $p'(t) > p(t)$ whenever $Y_{\text{gross}} > 0$, preserving the monotonicity property of Theorem 3.1.

10 Formal Security Properties

We state and prove the key security invariants of the yield system. The implementation includes 54 security tests: unit tests for all share accounting edge cases, fuzz tests (256 runs per property) for conversion function robustness, and invariant tests (128K calls) verifying that share price monotonicity and collateralization bounds hold under arbitrary operation sequences.

Property 10.1 (Conservation)**.** *For every yield-bearing bridge token yT:*

$$S(t) \cdot p(t) \leq B(t) + \epsilon_{rounding} \quad (27)$$

where $\epsilon_{rounding} \leq S(t)$ wei (at most 1 wei per outstanding share due to floor rounding).

Proof. By construction, deposits mint $\lfloor a/p(t) \rfloor$ shares for a assets deposited, so the share value never exceeds the deposit. Withdrawals burn shares before releasing assets. Yield increases $B(t)$ without increasing $S(t)$ (shares are only minted for deposits and fee extraction). Fee shares are minted against yield already in $B(t)$. The rounding bound follows from the floor operation in Equation (7). □

Property 10.2 (Undercollateralization Detection)**.** *If $B(t) < \theta_{\min} \cdot S(t) \cdot p(t_{k-1})$, the bridge pauses within $\Delta + \delta_{confirm}$.*

Proof. Direct from Theorem 6.1. □

Property 10.3 (No Share Price Manipulation)**.** *An external actor cannot decrease $p(t)$ through deposit, withdrawal, or harvest operations.*

Proof. Deposit: increases B by a and S by $a/p(t)$, leaving p unchanged. *Withdrawal*: decreases B by $s \cdot p(t)$ and S by s, leaving p unchanged. *Harvest*: increases B by harvested yield, does not change S, so p increases. *Fee extraction*: mints shares against existing yield in B, yielding $p' > p$ (Section 9). No operation decreases p. □

Property 10.4 (Exit Guarantee)**.** *Users holding yield-bearing bridge tokens can redeem for underlying assets within the MPC liveness bound (7 days worst case under signer rotation) regardless of bridge pause state.*

Proof. The `burnForWithdrawal` function is never disabled, even in `PAUSED` state. Only minting is disabled on pause. The MPC set signs withdrawal releases as long as t-of-n signers are operational. Under signer rotation (7-day timelock), the current signer set remains active until the rotation completes. □

11 Implementation

11.1 Contract Architecture

The yield system comprises four contracts per source chain:

11.2 Gas Costs

11.3 Source Code

All contracts are open-source under the MIT license:

12 Related Work

ERC-4626 Tokenized Vaults [5]. The standard that defines share-based vault accounting on EVM. Teleport adopts the same `convertToShares`/`convertToAssets` semantics but extends them cross-chain, where the vault and share token exist on different blockchains. The key challenge ERC-4626 does not address is cross-chain state synchronization of the share price.

Lido [6]. The largest liquid staking protocol ($14.5B stETH outstanding). Lido's stETH rebasing model inspired yLETH's share-price model, but Lido operates on a single chain. Teleport's contribution is deploying bridge-locked ETH into Lido (and other strategies) while reflecting the yield cross-chain.

EigenLayer [8]. Restaking protocol enabling ETH stakers to provide security to additional services. Teleport uses EigenLayer as one of 29 yield sources, composing restaking yield on top of liquid staking yield for bridge-locked assets.

Babylon [9]. BTC staking protocol using Bitcoin Script covenants. Teleport integrates Babylon as the base layer of the BTC yield stack, with the FROST-controlled Taproot address doubling as both bridge custody and Babylon staking key.

Pendle [13]. Yield tokenization protocol that splits yield-bearing tokens into principal (PT) and yield (YT) components. Teleport yLETH can be deposited into Pendle on the destination chain, enabling fixed-rate yield exposure on bridged assets.

Across Protocol [14]. Optimistic bridge using LP-funded fast fills. Across LPs earn yield by fronting bridge capital, but the bridged assets themselves (held by users) earn no yield. Teleport's yield-bearing tokens ensure the *user's* bridged capital is productive.

Wormhole NTT [15]. Native token transfers without wrapping. NTT addresses token fungibility but not capital efficiency—transferred tokens still earn zero yield during transit.

13 Conclusion

We have presented a comprehensive yield system for cross-chain bridge tokens that eliminates the $675M+ annual capital inefficiency of idle bridge TVL. The system's formal properties—share price monotonicity, automatic undercollateralization pause, tier-based diversification, and exit guarantees—provide the safety invariants required for production bridge operation. Production hardening includes `VIRTUAL_SHARES` = `VIRTUAL_ASSETS` = 10^8 for first-depositor inflation attack protection, per-operation `forceApprove` (no infinite approvals), and 54 security tests including fuzz (256 runs) and invariant (128K calls) suites.

The Bitcoin-native yield composition through Babylon, Lombard, SolvBTC, and CoreDAO represents a qualitative advance: native BTC earning yield without custodial wrapping, with the same FROST threshold key securing both bridge custody and staking positions.

The xLUX flywheel, where fees from bridge, DEX, lending, perpetuals, and NFT AMM compound into staking yield, creates a self-reinforcing economic equilibrium that scales with ecosystem adoption. As cross-chain volume grows, yield-bearing bridge tokens become strictly dominant over conventional wrapped tokens—offering higher capital efficiency with equivalent or superior security guarantees.

References

[1] DefiLlama, "Bridge TVL Rankings," https://defillama.com/bridges, accessed April 2025.

[2] Z. Kelling, "Lux Teleport: A Sovereign Omnichain Liquidity Protocol," Lux Industries, Inc., 2025.

[3] C. Komlo and I. Goldberg, "FROST: Flexible Round-Optimized Schnorr Threshold Signatures," in *Selected Areas in Cryptography (SAC)*, 2020.

[4] R. Canetti, R. Gennaro, S. Goldfeder, N. Makriyannis, and U. Peled, "UC Non-Interactive, Proactive, Threshold ECDSA with Identifiable Aborts," in *ACM CCS*, 2020.

[5] J. Bebis *et al.*, "EIP-4626: Tokenized Vault Standard," Ethereum Improvement Proposal, 2022.

[6] Lido DAO, "Lido: Liquid Staking for Ethereum," https://lido.fi, 2020.

[7] Aave Companies, "Aave V3 Technical Paper," 2022.

[8] S. Kannan *et al.*, "EigenLayer: The Restaking Collective," Whitepaper, 2023.

[9] Babylon Labs, "Bitcoin Staking: Unlocking 21M Bitcoins to Secure the Proof-of-Stake Economy," Whitepaper, 2024.

[10] Lombard Finance, "LBTC: Liquid Bitcoin Staking," https://lombard.finance, 2024.

[11] Solv Protocol, "SolvBTC: Bitcoin Yield Aggregation," https://solv.finance, 2024.

[12] Core Foundation, "CoreDAO: Satoshi Plus Consensus," Whitepaper, 2023.

[13] Pendle Finance, "Pendle: Yield Tokenization Protocol," https://pendle.finance, 2023.

[14] Across Protocol, "Across: Optimistic Cross-Chain Bridge," Whitepaper, 2023.

[15] Wormhole Foundation, "Wormhole: A Generic Message Passing Protocol," Whitepaper, 2022.

[16] BitGo, "Wrapped Bitcoin (WBTC)," https://wbtc.network, 2019.

[17] Rekt News, "Leaderboard," https://rekt.news/leaderboard/, 2024.

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

Table 1: Complete yield strategy taxonomy: 29 strategies across 9 categories. APY ranges reflect Q1 2025 observed rates. Risk tiers: T1 = low (blue-chip, audited, $1B+ TVL), T2 = medium (established, $100M+ TVL), T3 = high (newer protocols, higher yield, elevated risk).

#	Category	Protocol	Underlying	Mechanism	APY (%)	Tier
Liquid Staking						
1	Liquid Staking	Lido	ETH	Validator staking, stETH issuance	3.2–3.8	T1
2	Liquid Staking	Rocket Pool	ETH	Permissionless validators, rETH	3.0–3.5	T1
Restaking						
3	Restaking	EigenLayer	ETH/stETH	AVS security, restaking rewards	3.5–6.0	T2
4	Restaking	Symbiotic	ETH/stETH	Flexible restaking, multi-asset	3.0–5.5	T2
5	Restaking	Karak	ETH/stETH	DSS restaking, risk isolation	3.0–5.0	T2
Lending						
6	Lending	Aave V3	ETH/USDC/USDT	Variable-rate lending pools	2.0–8.0	T1
7	Lending	Compound V3	ETH/USDC	Isolated lending markets	2.5–7.0	T1
8	Lending	Morpho	ETH/USDC	Peer-to-peer rate optimization	3.0–9.0	T2
9	Lending	Euler V2	Multi-asset	Modular lending, custom vaults	3.5–10.0	T2
10	Lending	Spark	DAI/ETH	MakerDAO-native lending	4.0–8.0	T1
11	Lending	Fluid	ETH/USDC	Unified liquidity layer	3.0–12.0	T2
Stablecoin Yield						
12	Stablecoin	MakerDAO/Sky	DAI	DSR + Sky savings rate	5.0–8.0	T1
13	Stablecoin	Ethena	USDe	Basis trade (spot + short perp)	8.0–15.0	T3
14	Stablecoin	Frax	FRAX	AMO yield + staking	4.0–7.0	T2
LP / DEX						
15	LP/DEX	Curve	Stablecoins	StableSwap AMM LP fees	5.0–12.0	T1
16	LP/DEX	Convex	CRV/CVX	Boosted Curve LP + CVX rewards	8.0–18.0	T2
17	LP/DEX	Pendle	PT/YT	Yield tokenization, fixed-rate	5.0–20.0	T2
18	LP/DEX	L2 DEX Aggregate	Multi-asset	Concentrated liquidity on L2s	6.0–15.0	T2
Bitcoin Native						
19	BTC Native	Babylon	BTC	BTC staking for PoS security	3.0–5.0	T2
20	BTC Native	Lombard	BTC	LBTC liquid staking derivative	3.5–6.0	T2
21	BTC Native	SolvBTC	BTC	BTC yield aggregation vaults	4.0–8.0	T3
22	BTC Native	CoreDAO	BTC	Dual staking (BTC + CORE)	3.0–12.0	T2
Solana						
23	Solana	Marinade	SOL	mSOL liquid staking	5.0–7.0	T1
24	Solana	Jito	SOL	JitoSOL + MEV rewards	6.0–8.0	T2
25	Solana	Kamino	SOL/USDC	Concentrated liquidity vaults	5.0–10.0	T2
TON						
26	TON	Tonstakers	TON	tsTON liquid staking	5.0–7.0	T2
27	TON	Bemo	TON	stTON liquid staking	5.0–7.0	T2
28	TON	STON.fi	TON/USDT	DEX LP on TON	8.0–15.0	T3
Perpetuals						
29	Perps	LPX Perps	Multi-asset	LP vault earns trading fees	10.0–30.0	T3

Table 2: Yield composition for representative bridge tokens. Rates are Q1 2025 observed medians.

Layer	yLETH	yLBTC	yLUSD
Base yield	3.5%	4.5%	6.0%
Restaking	2.0%	2.0%	
Bridge fees (xLUX)	1.0%	1.0%	1.0%
DeFi on Lux	5–15%	5–15%	5–12%
Total range	**11.5–21.5%**	**12.5–22.5%**	**12.0–19.0%**

Table 3: Default attestation parameters.

Parameter	Value
Attestation interval (Δ)	1 hour
Minimum collateralization ($\theta_{\min}$)	98.5%
Signer disagreement tolerance (ϵ)	0.1%
Pause recovery requires	Governor + MPC joint action
Emergency pause	Any single MPC signer

Table 4: Capital efficiency comparison: ETH across a bridge from Ethereum to Lux. Native stETH APY = 3.5% (Lido, Q1 2025).

Token	APY	η	Source
WETH (Ethereum)	0.0%	0.00	Idle
LETH (Teleport)	0.0%	0.00	1:1 wrapped
stETH (Lido)	3.5%	1.00	Native stake
yLETH (Teleport)	5.5%	1.57	Stake + restake
yLETH + DeFi	11.5–21.5%	3.3–6.1	Full composition

Table 5: Projected annual fee flow to xLUX at varying TVL levels. Assumes: bridge fee 10 bps, DEX fee 5 bps, lending spread 50 bps, perps fee 8 bps, NFT AMM 200 bps. Velocity: bridge 2x/year, DEX 50x/year, lending 3x/year, perps 100x/year, NFT 10x/year. Stakeholder share: 90%.

Total TVL	Annual Fees	xLUX Share	xLUX APY*
\$100M	\$8.2M	\$7.4M	7.4%
\$500M	\$41M	\$37M	7.4%
\$1B	\$82M	\$74M	7.4%
\$5B	\$410M	\$369M	7.4%

*Assumes staked LUX = TVL (simplified). Real APY varies with staking ratio.

Table 6: Yield system contract architecture.

Contract	Function
`YieldBridgeVault`	Manages deposits, withdrawals, strategy routing, tier enforcement
`StrategyRouter`	Allocates capital across strategies per tier weights
`BackingOracle`	Receives MPC attestations, updates share price
`ShariaFilter`	Classifies strategies for Shariah compliance mode

Table 7: Gas costs for yield operations (Ethereum mainnet, 30 gwei gas price).

Operation	Gas	Cost
`deposit` (to vault)	∼120,000	∼\$6.30
`withdraw` (from vault)	∼95,000	∼\$5.00
`harvest` (per strategy)	∼80,000	∼\$4.20
`updateBacking` (attestation)	∼45,000	∼\$2.35
`rebalance` (strategy rotation)	∼250,000	∼\$13.10

Component	Repository
Yield vault	`luxfi/standard`
Strategy adapters	`luxfi/standard`
MPC attestation	`luxfi/mpc`
Threshold crypto	`luxfi/threshold`
Bridge contracts	`luxfi/bridge`