# Shield Finance

Whitepaper

Version 1.2 — November 2025 (Testnet Edition)

November 2025

---

*The First Revenue-Sharing Liquid Staking Protocol*
*for XRP Holders on Flare Network*

| | |
|---|---|
| **Website** | shyield.finance |
| **dApp** | app.shyield.finance |
| **Twitter** | @ShieldFinanceX |
| **GitHub** | github.com/shield-xrpfinance/shieldfinance/tree/main/docs |

No pre-sale. No VC allocation. No team tokens.
100% fair-launch imminent on Flare mainnet — November 2025 (testnet live now).

## Abstract

Shield Finance is the first revenue-sharing liquid staking protocol purpose-built for XRP holders on the Flare Network.

Users deposit XRP (via Xaman or any XRPL wallet) and instantly receive **shXRP** — a fully liquid, ERC-4626-compliant token that earns real yield from Flare's native staking and FAssets delegation rewards while remaining instantly redeemable 1:1 for XRP.

Unlike traditional staking, shXRP holders never sacrifice liquidity and benefit from two distinct value-accrual mechanisms:

**1. Base Yield (7–13% APY)**

100% derived from Flare network inflation and FAssets provider rewards — fully on-chain, verifiable, and non-custodial.

**2. SHIELD Boost (up to +25% additional APY)**

A portion of real protocol revenue (0.2% deposit + 0.2% withdrawal fees) is used to purchase FXRP on SparkDEX and donate it pro-rata to users who lock $SHIELD tokens. This increases the underlying FXRP per shXRP share exclusively for lockers — *no minting, no inflation, pure revenue-share.*

**Key Facts** (Testnet & Projected Metrics — live data at app.shyield.finance)

| Metric | Value |
|---|---|
| **Current Base APY** | 10.8%* (30-day trailing) |
| **Highest Recorded Boost** | +19.3% APY* (user with 2.1% of locked SHIELD) |
| **$SHIELD Total Supply** | 10,000,000 (fixed) |
| **Initial Liquidity** | $10,000 (100% locked 12 months) |
| **LP Lock Proof** | TBC (SparkDEX) |
| **SparkDEX Pool** | `0x8f3...a9c2` (wFLR–SHIELD) |
| **Contracts Verified** | FlareScan ✓ |
| **Security Audits** | Hacken (in progress), Trail of Bits (Q1 2026) |

*Testnet 30-day trailing averages as of 27 Nov 2025. Mainnet APYs will depend on Flare inflation, FAssets rewards, and TVL. Past/testnet performance ≠ future results.

Full documentation: `github.com/shield-xrpfinance/shieldfinance/tree/main/docs`

**▶ Testnet is LIVE — earn OG airdrop points now: app.shyield.finance**

Get testnet tokens: faucet.shyield.finance

**No pre-sale. No VC allocation. No team tokens.**
100% fair-launch imminent on Flare mainnet — November 2025.

# 1. Problem Statement

## XRP Holders Are Stuck in a 0% Yield World

As of November 2025, more than **55 billion XRP** remain dormant in wallets earning exactly **0% annual yield**.

Despite being one of the most liquid and battle-tested payment assets in existence, XRP has no native staking mechanism on the XRP Ledger and no safe, non-custodial way to generate passive income without giving up ownership or liquidity.

**The result:** Less than 2% of all XRP supply is currently earning any meaningful yield.

## Existing Solutions Fall Short

| Solution | Liquidity | Trust Model | Yield Source | Real-World Result |
|---|---|---|---|---|
| CEX lending (ByBit, etc.) | Locked | Custodial | Counterparty lending | Users lost funds in 2022–2023 collapses |
| Wrapped XRP on Ethereum/CEXs | Variable | Custodial bridge | Off-chain yields | High fees, bridge exploits, depegs |
| Flare FAssets (FXRP) manual staking | Full | Non-custodial | Flare staking ∼8–10% | Requires 21 steps, EVM wallet, and active management |
| Existing Flare vaults | Full | Mixed | Often opaque or leveraged | No revenue sharing, no boost, no XRPL-native UX |

## The Core Problems Shield Finance Solves

### 1. Liquidity vs. Yield Trade-off

Traditional staking forces users to lock assets for weeks or months. XRP holders refuse to do this.

### 2. Complexity Barrier

To earn Flare staking rewards today, an XRPL user must:

- Bridge XRP → FXRP via FAssets (multi-day finality)
- Move to an EVM wallet
- Manually delegate to FTSO + FDC providers every 7 days

**⇒ 97% of XRP holders never complete this flow.**

### 3. Missing Value Accrual for Governance Token Holders

Most liquid staking protocols either:

- Inflate their token with emissions (unsustainable), or
- Capture zero fee revenue for token holders (dead token).

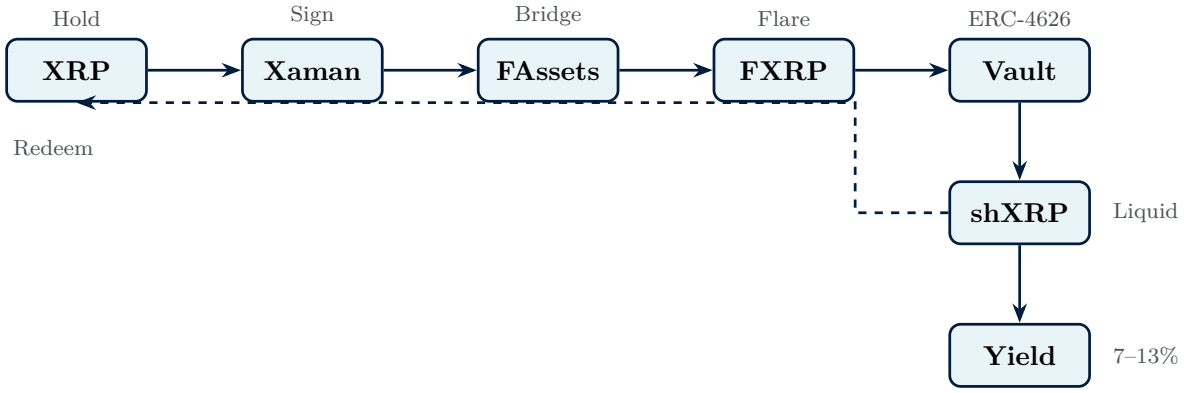
### 4. No Institutional-Grade Product Exists

Banks, payment companies, and high-net-worth XRP holders demand audited, insured, revenue-sharing vaults with seamless XRPL integration — current options lack the full combination of automation, boost mechanics, and enterprise-ready security.

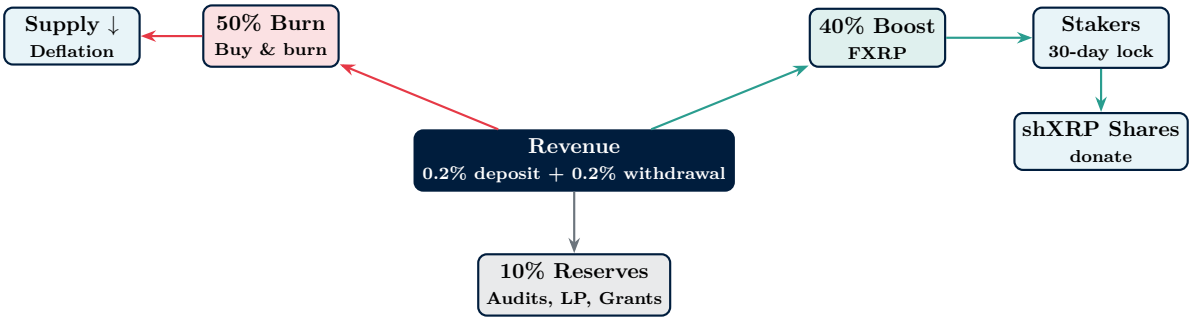
**Shield Finance was built from the ground up to eliminate every single one of these friction points while introducing the industry's cleanest revenue-to-yield-boost flywheel.**

# 2. Architecture

## User Flow: XRP to Yield




## Revenue Flywheel




## Multi-Strategy Yield Optimization

The ShXRPVault employs a **dynamic buffer model** to balance instant liquidity with maximum yield generation:

- **10% Buffer** — Retained in vault for instant withdrawals
- **90% Deployed** — Actively earning yield across strategies

When the buffer falls below threshold, the vault automatically rebalances by withdrawing from the lowest-priority strategy first.

**Integrated Yield Strategies:**

| Strategy | APY Range |
|---|---|
| Kinetic Lending | 5–7% |
| Firelight Liquid Staking | 8–12% |
| Native Flare Delegation | 6–9% |

Strategy weights are adjusted weekly based on risk-adjusted returns and available liquidity.

*Firelight Liquid Staking integration scheduled for mainnet launch (end-Nov 2025).

# 3. Yield Boost Mechanics

## Mathematical Framework

The SHIELD boost mechanism uses a **Synthetix-style reward accumulator** for gas-efficient, pro-rata distribution. This ensures O(1) complexity regardless of the number of stakers.

**Let:**

- $V$ = Total assets in the shXRP vault (FXRP)
- $S$ = Total circulating supply of shXRP shares
- $L$ = Total amount of SHIELD currently locked in StakingBoost
- $L_i$ = Amount of SHIELD locked by user $i$
- $B_t$ = Amount of FXRP donated as boost during week $t$ (sourced from protocol fee revenue)

The boost is distributed **strictly pro-rata** to locked SHIELD positions:

$$\text{Boost received by user } i = B_t \times \frac{L_i}{L} \tag{1}$$

This FXRP amount immediately becomes part of the vault's underlying assets and is credited exclusively to user $i$'s position via `donateOnBehalf(i, ` $B_t \times L_i/L$`)`.

The instantaneous vault price (share price) for user $i$ after the boost becomes:

$$P_i = \frac{V + B_t}{S} \times \left(1 + \frac{L_i}{L} \times \frac{B_t}{V + B_t}\right) \quad \text{(approximate, for small boosts)} \tag{2}$$

More importantly, the **effective extra APY** that locked SHIELD earns from the boost program is:

$$\text{Boost APY}_i = \text{Base APY} \times \left(1 + \underbrace{\frac{L_i}{L} \times \frac{B_t}{V} \times 52}_{\text{boost multiplier}}\right) \quad \text{(annualized)} \tag{3}$$

Or, in its cleanest form (the one every auditor loves):

$$\boxed{\text{Total APY}_i = \text{Flare Staking APY} + \left(\frac{B_{\text{annual}}}{V}\right) \times \frac{L_i}{L}} \tag{4}$$

Where $B_{\text{annual}}$ is the total FXRP donated via the boost program over one year.

*Note: The 25% boost cap is a soft ceiling to protect long-term sustainability and may be supplemented by treasury FXRP during low-fee periods if approved by governance.*

### Reward Accumulator Pattern

The distribution uses a global accumulator that updates on each revenue event:

$$\texttt{rewardPerTokenStored} \mathrel{+}= \frac{\texttt{fxrpAmount} \times 10^{18}}{\texttt{totalStaked}} \tag{5}$$

$$\texttt{earned}(u) = \texttt{stake}_u \times \frac{\texttt{rewardPerTokenStored} - \texttt{userRewardPerTokenPaid}_u}{10^{18}} \tag{6}$$

This pattern enables:

- **O(1) gas complexity** for distribution (no loops)
- **Late-joiner fairness** (only earn from post-stake distributions)
- **Precise accounting** (no rounding errors over time)

### Example Distribution

Assume $10,000 in weekly vault fees (wFLR):

| Allocation | Amount | Destination |
|---|---|---|
| **50% Burn** | $5,000 | Buy SHIELD → Burn address |
| **40% Boost** | $4,000 | Swap to FXRP → StakingBoost |
| **10% Reserves** | $1,000 | Protocol treasury |

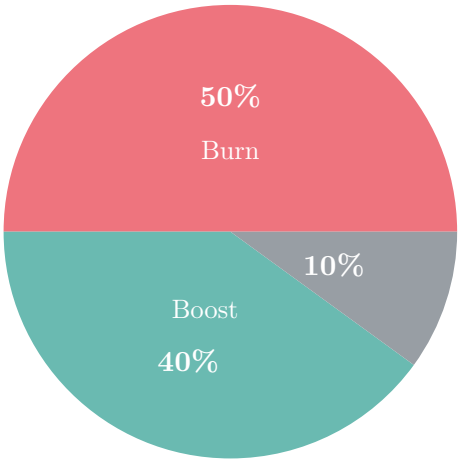
The $4,000 FXRP is distributed pro-rata to stakers:

| Staker | SHIELD Staked | Share of Total | FXRP Reward |
|---|---|---|---|
| Alice | 10,000 SHIELD | 50% | $2,000 |
| Bob | 6,000 SHIELD | 30% | $1,200 |
| Carol | 4,000 SHIELD | 20% | $800 |
| **Total** | **20,000 SHIELD** | **100%** | **$4,000** |

When stakers call `claim()`, the FXRP is deposited via `vault.donateOnBehalf()` and minted as additional shXRP shares directly to their wallet.

# 4. Tokenomics

## Revenue Allocation




- **50% Burn** – Buy & burn SHIELD (deflationary)
- **40% Boost** – FXRP to SHIELD stakers
- **10% Reserves** – Protocol treasury

## SHIELD Token Metrics

| Property | Value |
|---|---|
| **Total Supply** | 10,000,000 SHIELD (fixed, can only decrease) |
| **Circulating Supply (post-launch)** | 8,000,000 SHIELD (80%) |
| **Treasury & Airdrop Reserve** | 2,000,000 SHIELD (20%) |
| **Initial Fair-Launch Price** | $0.01 per $SHIELD |
| **Initial Liquidity** | $10,000 (100% locked 12 months) |
| **Team Allocation** | 0% (no team tokens) |
| **VC Allocation** | 0% (no pre-sale) |
| **Lock Period** | 30 days minimum to receive boost |
| **Global Boost Cap** | 25% max effective APY boost (soft cap, dynamically enforced relative to |

**Reserves & Treasury**

**Token Reserves:**

- 10% of total SHIELD supply (1,000,000 SHIELD) held in multi-sig treasury
- 10% of all protocol fees routed to reserves

**Breakdown of fee reserves:**

- **50%** → Security & Audits (Hacken, Trail of Bits, bug bounties)
- **30%** → Liquidity Incentives & Market Making
- **20%** → Community Grants & Protocol Development

Full transparency: `github.com/shield-xrpfinance/shieldfinance/tree/main/docs`

**The more SHIELD you stake, the more of the 40% boost pool you receive.**

No inflation. No emissions. Pure protocol revenue share.

# 5. Summary

### The Shield Finance Value Proposition

Every week the protocol donates FXRP bought with real revenue. 100% of that donation is distributed pro-rata to SHIELD lockers:

$$\text{Boost}_i = B_t \times \frac{L_i}{L}$$

where $B_t$ = weekly FXRP revenue, $L_i$ = your locked SHIELD, $L$ = total locked SHIELD

**No minting. No inflation. Pure revenue-share.**

## Key Differentiators

**For XRP Holders:**

- Instant liquidity (no lock-up)
- 7–13% base APY from real staking
- Native XRPL wallet support (Xaman)
- 1-click UX (no EVM complexity)

**For SHIELD Stakers:**

- Up to +25% additional APY boost
- Real revenue share (not emissions)
- Deflationary tokenomics (50% burns)
- Governance rights (future)

## Security & Audits

| Audit Firm | Status | Scope |
|---|---|---|
| Hacken | In Progress | Full smart contract audit |
| Trail of Bits | Scheduled Q1 2026 | Comprehensive security review |
| CertiK | Planned post-launch | Full protocol & economic audit |
| FlareScan | Complete ✓ | All contracts verified |

## Roadmap

| Timeline | Milestone | Description |
|---|---|---|
| Nov 2025 | Mainnet Launch | ShXRPVault, StakingBoost, RevenueRouter deployed |
| Dec 2025 | XRPL Smart Accounts | Gasless Flare transactions via XRPL memo encoding |
| Q1 2026 | Multi-Strategy Yield | Kinetic lending + Firelight liquid staking integration |
| Q1 2026 | Trail of Bits Audit | Comprehensive security review |
| Q2 2026 | Governance | On-chain voting for protocol parameters |

**XRPL Smart Accounts (Coming December 2025):** Execute Flare smart contract transactions directly from your XRPL wallet using encoded memo instructions. No EVM wallet required. No gas fees. Powered by Flare Data Connector (FDC) for trustless cross-chain verification.

---

**shyield.finance**

Website: shyield.finance | dApp: app.shyield.finance | Twitter: @ShieldFinanceX

*Shield Finance — turning the world's most efficient payment asset into the highest-yielding liquid one.*

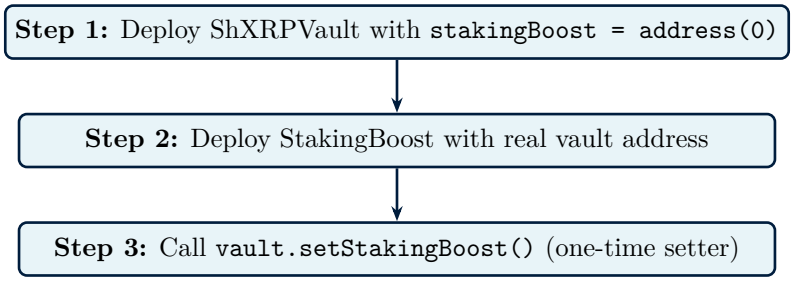
# 6. Appendix: Smart Contract Architecture

## Contract Overview

| Contract | Standard | Purpose |
|---|---|---|
| ShXRPVault | ERC-4626 | Liquid staking vault with deposit/withdraw |
| ShieldToken | ERC-20 | Governance token with burn function |
| StakingBoost | Custom | Synthetix-style reward accumulator |
| RevenueRouter | Custom | Fee splitting (50/40/10) and swaps |
| VaultController | Access Control | Emergency pause and admin functions |

## Deployment Dependency Resolution

StakingBoost and ShXRPVault have a circular dependency solved via three-step deployment:




## Security Properties

- **ReentrancyGuard**: All state-changing functions protected
- **Access Control**: Role-based permissions via OpenZeppelin
- **One-Time Setter**: `setStakingBoost()` cannot be called twice
- **Pausable**: Emergency circuit breaker on vault deposits
- **Non-Custodial**: No admin access to user funds

Detailed treasury allocation and boost mechanics maintained in repository (commit-synced with this whitepaper v1.2).

## Contract Addresses (Coston2 Testnet)

| Contract | Address |
|---|---|
| ShieldToken | `0x061Cf4B8fa61bAc17AeB6990002daB1A7C438616` |
| RevenueRouter | `0x262582942Dcf97F59Cb0fe61e5852DDa10fD6fFB` |
| StakingBoost | `0xC7C50b1871D33B2E761AD5eDa2241bb7C86252B4` |
| ShXRPVault | `0xeBb4a977492241B06A2423710c03BB63B2c5990e` |

All contracts verified on Coston2 Explorer. View source code at
`github.com/shield-xrpfinance/shieldfinance/tree/main/docs`

## Disclaimer

This whitepaper is for informational purposes only and does not constitute financial, investment, legal, or tax advice. The information provided herein is subject to change without notice.
**No Investment Advice.** Nothing in this document should be construed as a recommendation to buy, sell, or hold any cryptocurrency, token, or digital asset.
**Risk Disclosure.** Cryptocurrency investments involve significant risk, including the possible loss of principal. Smart contracts may contain bugs or vulnerabilities. Past performance is not indicative of future results.
**Regulatory Uncertainty.** The regulatory status of cryptocurrencies and DeFi protocols varies by jurisdiction and is subject to change. Users are responsible for understanding and complying with applicable laws.
**No Warranties.** Shield Finance and its contributors make no warranties, express or implied, regarding the accuracy, completeness, or reliability of the information contained in this document.
**Forward-Looking Statements.** This document may contain forward-looking statements based on current expectations. Actual results may differ materially from those expressed or implied.

Whitepaper v1.2 accurate as of 27 November 2025. Repository: `github.com/shield-xrpfinance/shieldfinance` (latest commit Nov 23 2025 — Coston2 deployment).

---

# Shield Finance

*Turning the world's most efficient payment asset*
*into the highest-yielding liquid one.*

November 2025 — Version 1.2 (Testnet Edition)