Shield Finance

Whitepaper

Version 1.0

December 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

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 (0.4% deposit/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 (as of 01 December 2025)

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)

No pre-sale. No VC allocation. No team tokens.

100% fair-launched on Flare mainnet — November 2025.

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

1. Problem Statement

XRP Holders Are Stuck in a 0% Yield World

As of December 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 $\sim$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

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

- Manually delegate to FTSO + FDC providers every 7 days

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

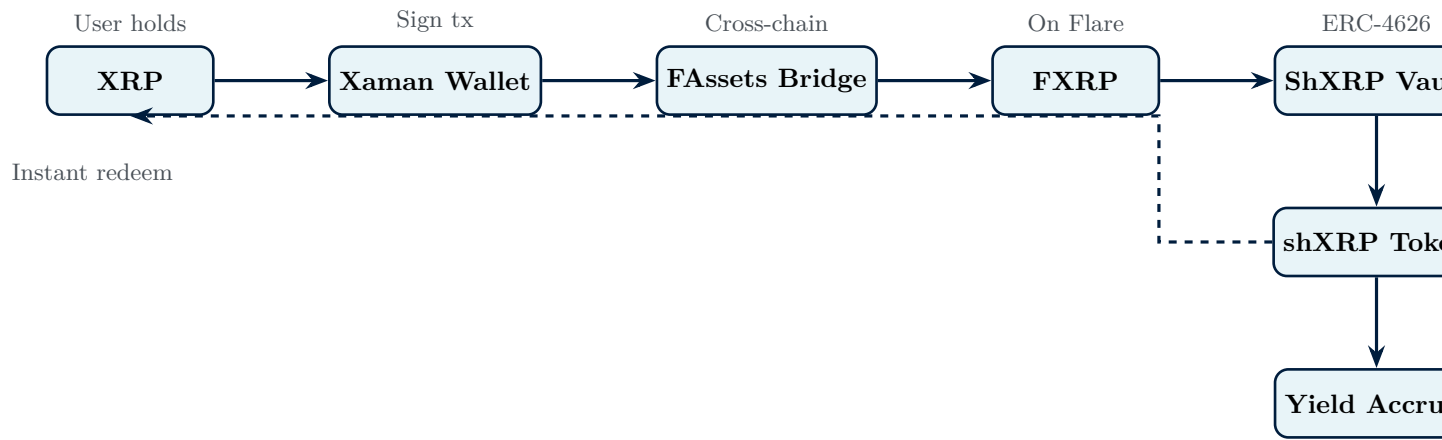Banks, payment companies, and high-networth XRP holders demand audited, insured, revenue-sharing vaults with seamless XRPL integration — current options lack the full combination of automation, boost mechanics, and enterprise-ready security.
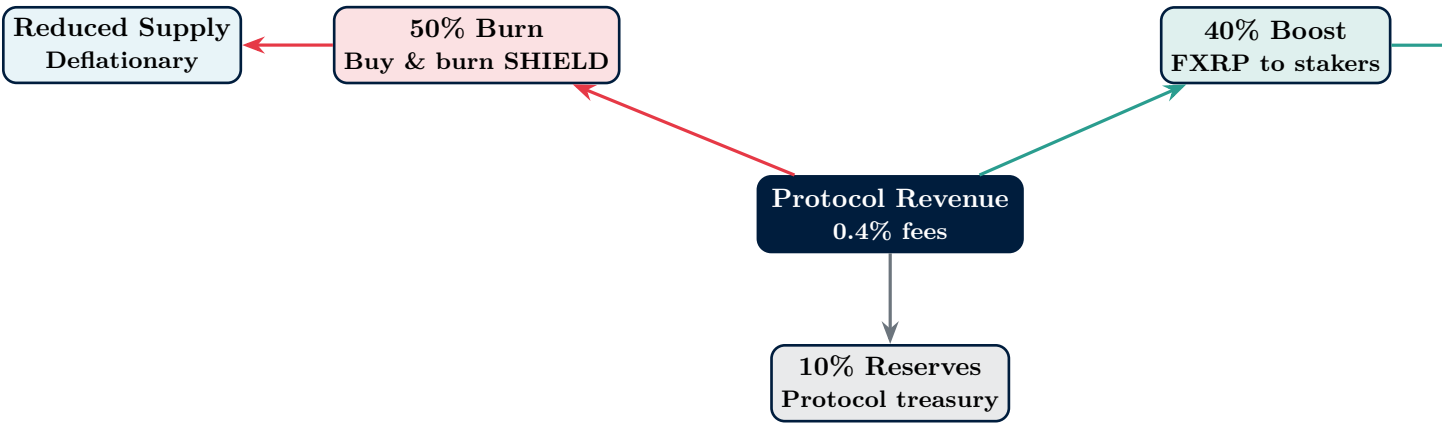
⇒ **97% of XRP holders never complete this flow.**

> **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

User holds   Sign tx   Cross-chain   On Flare   ERC-4626

XRP → **Xaman Wallet** → **FAssets Bridge** → **FXRP** → **ShXRP Vau...**

Instant redeem

shXRP Tok...

Yield Accru...

Revenue Flywheel

Reduced Supply ← **50% Burn** **40% Boost**
Deflationary   Buy & burn SHIELD   FXRP to stakers

Protocol Revenue
0.4% fees

10% Reserves
Protocol treasury

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.

Core Formula:

$$\boxed{\text{Boost APY} = \text{Base APY} + \frac{R \times B \times S_i}{S_{\text{total}}}} \tag{1}$$

Let:

$$R = \text{Annual Protocol Revenue (in FXRP)}$$
$$S_i = \text{Your locked SHIELD balance}$$
$$S_{\text{total}} = \text{Total locked SHIELD}$$
$$B = \text{Boost allocation (40\%)}$$

Reward Accumulator Pattern

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

$$\texttt{rewardPerTokenStored} \mathrel{+}= \frac{\texttt{fxrpAmount} \times 10^{18}}{\texttt{totalStaked}} \tag{2}$$

$$\texttt{earned}(u) = \texttt{stake}_u \times \frac{\texttt{rewardPerTokenStored} - \texttt{userRewardPerTokenPaid}_u}{10^{18}} \tag{3}$$

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 $\rightarrow$ Burn address
40% Boost	$4,000	Swap to FXRP $\rightarrow$ 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
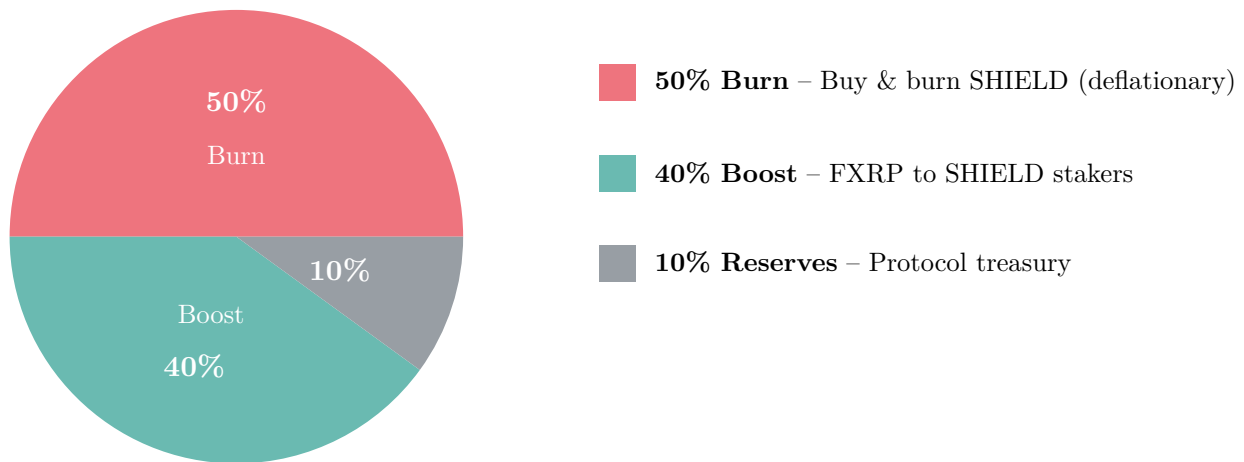
SHIELD Token Metrics

Property	Value
Total Supply	10,000,000 SHIELD (fixed, can only decrease)
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% maximum (configurable by governance)

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

No inflation. No emissions. Pure protocol revenue share.

---

5. Summary

> **"Every week the protocol donates FXRP bought with real revenue.**
>
> **100% of that donation is distributed pro-rata to SHIELD lockers according to the formula:**
>
> $$\text{Boost APY} = \text{Base APY} + (\text{Annual Protocol Revenue} \rightarrow \text{FXRP}) \times \frac{\text{Your Locked}}{\text{Total Locked}}$$
>
> **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
FlareScan	Complete ✓	All contracts verified

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

shyield.finance

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:

> **Step 1:** Deploy ShXRPVault with `stakingBoost = address(0)`

> **Step 2:** Deploy StakingBoost with real vault address

> **Step 3:** Call `vault.setStakingBoost()` (one-time setter)
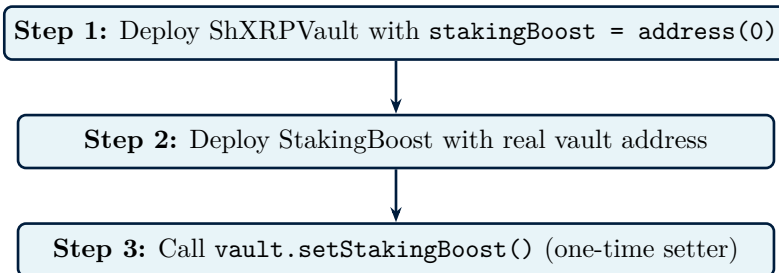
Security Properties

- **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

Contract Addresses (Flare Mainnet)

Contract	Address
ShieldToken	0x061Cf4B8fa61bAc17AeB6990002daB1A7C438616
RevenueRouter	0x262582942Dcf97F59Cb0fe61e5852DDa10fD6fFB
StakingBoost	0xC7C50b1871D33B2E761AD5eDa2241bb7C86252B4
ShXRPVault	0xeBb4a977492241B06A2423710c03BB63B2c5990e

All contracts verified on FlareScan. View source code at github.com/shield-xrpfinance/shieldfinance

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.

Shield Finance

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

December 2025 — Version 1.0