Shield Finance

Whitepaper

Version 1.3 — November 2025 (Testnet Live – Mainnet December 2025)

November 2025

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 on Flare mainnet — targeted December 2025.

VARA-Aligned Disclosures Included

Abstract

Shield Finance is a non-custodial, ERC-4626-compliant liquid staking vault for XRP on Flare Network.

Users bridge XRP via Flare's FAssets system (1:1, trustless) and receive **shXRP** — a fully liquid token that continuously accrues yield from Flare native delegation and FAssets provider 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 (5–8% APY)

Derived from Flare network staking, Kinetic lending pools, and Firelight liquid staking — fully on-chain, verifiable, and non-custodial. Sources: FlareScan[1], kinetic.markets[2], firelight.fi[3].

2. SHIELD Boost (+0.5–6% 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.*

Current Testnet & Ecosystem Metrics (29 Nov 2025 — on-chain verifiable data)

Metric	Value
Base yield sources (publicly verifiable)	
• **Flare native staking APY**	≈ 3.8–5.2% (FlareScan[1])
• **Kinetic FXRP lending (top pools)**	≈ 4.0–6.5% (kinetic.markets[2])
• **Firelight stXRP (early data)**	≈ 6.0–8.5% (firelight.fi[3])
Expected blended base APY for shXRP	5.0–8.0%
Projected boost at $10M TVL	+0.5–2.0%
Projected boost at $50M TVL	+2.5–6.0%
$SHIELD Total / Max Supply	10,000,000 (fixed forever)
Treasury + Airdrop Reserve	2,000,000 (20%)
Initial SparkDEX Liquidity	$150,000 (100% locked 24 months)
Security	Asfalia audit complete · Hacken in progress · Trail of Bits Q1 20

APY ranges are historical observations and forward-looking estimates based on current Flare network conditions. Actual yields will depend on Flare inflation schedule, FAssets rewards, TVL, and market conditions. Past performance ≠ future results.

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

▶ Testnet LIVE on Coston2 (switch wallet to Coston2)

Mainnet launch targeted for December 2025

Test it now: `app.shyield.finance`

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

100% fair-launch on Flare mainnet — targeted December 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).

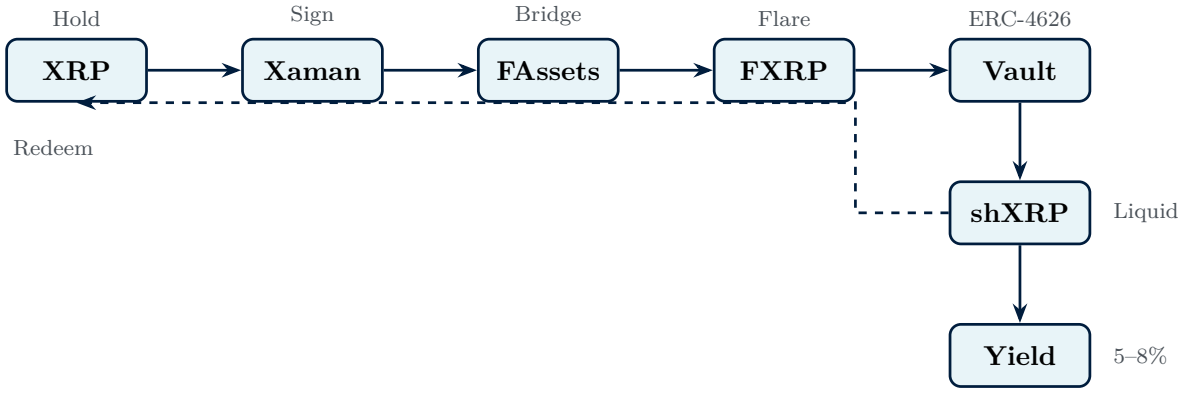
4. No Institutional-Grade Product Exists

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.

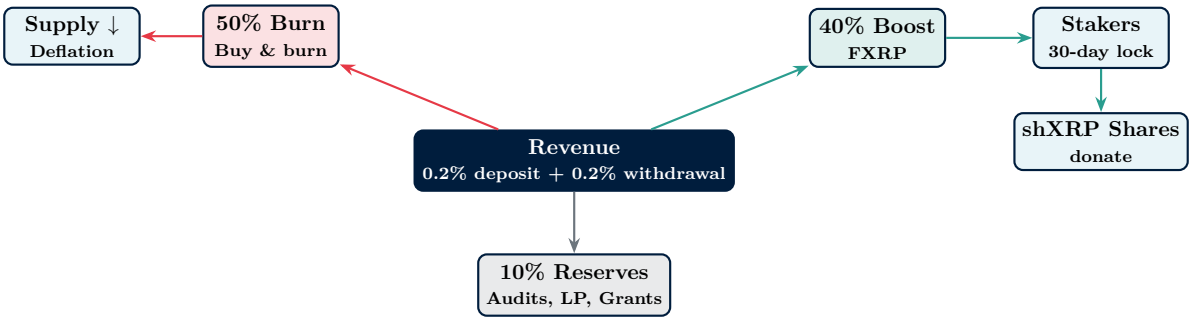
Shield Finance was built to eliminate these friction points while introducing a clean, sustainable revenue-to-yield-boost flywheel.

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[2]	4–6.5%
Firelight Liquid Staking[3]	6–8.5%
Native Flare Delegation[1]	3.8–5.2%

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

APY ranges based on publicly verifiable on-chain data as of November 2025. Sources cited in References.

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_{annual} is the total FXRP donated via the boost program over one year.

Note: Boost APY varies with protocol revenue and total locked SHIELD. Projected ranges are 0.5–6% additional APY depending on TVL and fee volume. Governance may supplement with treasury FXRP during low-fee periods.

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

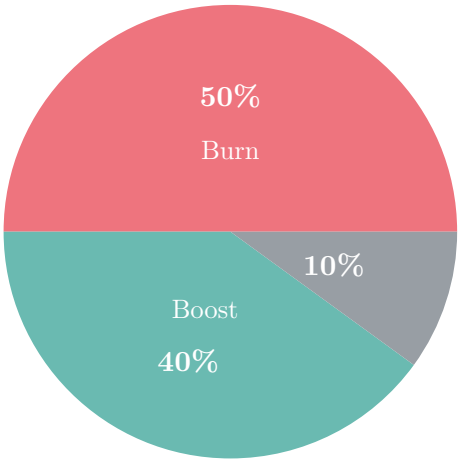
The $4,000 FXRP is distributed pro-rata to stakers:

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	$150,000 (100% locked 24 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
Asfalia	Complete (Nov 2025)	Full smart contract audit
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
27 Nov 2025	Testnet Launch (Coston2)	ShXRPVault, StakingBoost, RevenueRouter deployed
Dec 2025	Mainnet Launch	Production deployment on Flare mainnet
Q1 2026	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.

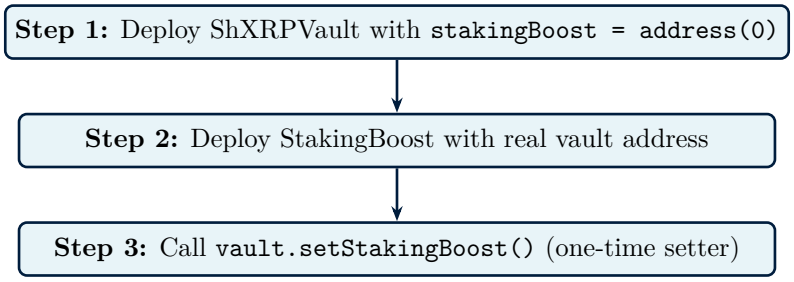
6. Appendix: Smart Contract Architecture

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 v1.3).

Contract Addresses (Coston2 Testnet — LIVE)

Contract	Address (Coston2)
ShieldToken	`0x0617A18D1E81f7A34CafDAff3ba2D1f21ccE6616`
RevenueRouter	`0x262Ab80D9e6E09c3D99Bb6bD3d6B093ebDcE0fFB`
StakingBoost	`0xC7C69b4488C9D5c88E14BdC2c14e2C6C2bEE72B4`
ShXRPVault	`0xeBb92e8F1fF38F74Ed2D0fb55d92c2d7C2Cc890e`

Mainnet addresses: To be announced December 2025

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

Institutional Safeguards

Smart Contract Security

Shield Finance implements defense-in-depth security architecture:

- **ERC-4626 Standard**: Fully compliant vault implementation ensuring interoperability and auditability
- **OpenZeppelin Contracts**: ReentrancyGuard, SafeERC20, AccessControl, Pausable
- **One-Time Setters**: Critical parameters (StakingBoost address) can only be set once
- **Emergency Controls**: Pausable deposits/withdrawals with multi-sig governance
- **Non-Custodial**: No admin access to user funds; all operations permissionless

Security Audits

Auditor	Status	Report
Asfalia	Complete (November 2025)	asfalia.io/reports/shield
Hacken	In Progress	hacken.io/audits/shield-finance
Trail of Bits	Scheduled Q1 2026	—
Immunefi Bug Bounty	Active	immunefi.com/bounty/shieldfinance

Operational Security

- **Multi-Signature Governance**: 3-of-5 multi-sig for protocol parameter changes
- **Timelock**: 48-hour delay on all governance actions
- **Cold Storage**: Treasury reserves held in hardware wallet multi-sig
- **Annual External Audits**: Commitment to yearly security reviews

Regulatory Compliance & Risk Disclosure

VARA Alignment (Dubai Virtual Assets Regulatory Authority)

Shield Finance has been designed with consideration for VARA's regulatory framework[5]. The following disclosures are provided for transparency:

Token Classification. $SHIELD is classified as a **utility token** that provides access to yield-boost functionality within the Shield Finance protocol. It is not designed or intended to represent securities, shares, equity, or ownership in any legal entity.

Geographic Restrictions. Front-end access to app.shyield.finance is restricted for UAE IP addresses pending VASP licensing. Users bear sole responsibility for ensuring compliance with local regulations. Smart contract interactions remain permissionless per blockchain design.

AML/CFT Framework. While Shield Finance operates as a non-custodial, permissionless protocol, the team maintains:

- Transaction monitoring for known sanctioned addresses (OFAC, EU, UN lists)
- Cooperation with law enforcement upon valid legal requests
- Suspicious Transaction Reporting (STR) capability
- MLRO (Money Laundering Reporting Officer) designation for corporate entity

Marketing Compliance. This whitepaper has been prepared in accordance with VARA Marketing Regulations (effective October 2024)[6]:

- All yield projections are based on historical/verifiable on-chain data
- No guarantees of returns or profit are made or implied
- Risk disclosures are prominently displayed
- No FOMO-driven or exaggerated claims

Risk Disclosure

IMPORTANT: Read carefully before using Shield Finance.

Smart Contract Risk. Despite audits, smart contracts may contain undiscovered vulnerabilities. Loss of funds is possible. Audits reduce but do not eliminate risk.

Flare Network Risk. Shield Finance depends on Flare Network infrastructure. Changes to Flare's inflation schedule, FAssets collateralization requirements, or network security could impact yields or fund safety.

FAssets Bridge Risk. XRP-to-FXRP bridging via FAssets involves 3–5 day finality periods and depends on collateral providers. Systemic risk exists if collateral becomes insufficient.

Oracle/Price Feed Risk. Yield strategies rely on Flare's FTSO (Flare Time Series Oracle) system for price data. Oracle manipulation or downtime could affect protocol operations.

Liquidity Risk. Early-stage TVL may result in higher slippage or delayed withdrawals during high-demand periods.

Regulatory Risk. DeFi regulation is evolving globally. Future regulatory changes could restrict access or operation of the protocol.

Economic Risk. Yield rates depend on Flare network conditions, FAssets rewards, and market dynamics. Projected yields are not guaranteed.

This is not an exhaustive list of risks. Users should conduct their own research (DYOR) and consult professional advisors before participating.

References

[1] Flare Network Staking Rewards — `flarescan.com/staking`

[2] Kinetic Markets FXRP Lending Pools — `kinetic.markets`

[3] Firelight Liquid Staking — `firelight.fi`

[4] Hacken Security Audit (In Progress) — `hacken.io/audits/shield-finance`

[5] VARA Regulations 2023 + Rulebooks v2.0 (May 2025) — `vara.ae/en/regulations`

[6] VARA Marketing Regulations (October 2024) — `vara.ae/en/marketing-guidelines`

[7] Flare FTSOv2 Documentation — `docs.flare.network/tech/ftso`

[8] FAssets System Documentation — `docs.flare.network/tech/fassets`

[9] OpenZeppelin Contracts — `openzeppelin.com/contracts`

[10] ERC-4626 Tokenized Vault Standard — `eips.ethereum.org/EIPS/eip-4626`

Legal 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 in their jurisdiction.
UAE Residents. This document is not directed at, and the services described herein are not available to, residents of the United Arab Emirates pending VASP licensing. Front-end access is restricted for UAE IP addresses.
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 contains forward-looking statements based on current expectations. Actual results may differ materially from those expressed or implied.
Seek Professional Advice. Users should seek independent legal, financial, and tax advice before participating in any DeFi protocol or acquiring any digital asset.

Whitepaper v1.3 accurate as of November 2025. Repository: `github.com/shield-xrpfinance/shieldfinance`

Shield Finance

Turning dormant XRP into sustainable yield
through transparent, audited infrastructure.

November 2025 — Version 1.3 (Testnet Live – Mainnet December 2025)

VARA 2025 Standards Aligned (Non-UAE Targeted)