Prism (VerifiedX Privacy Layer)

Prism is VerifiedX's **optional, zero-knowledge-based privacy layer** enabling **shielded transactions and addresses** for both VFX and vBTC (BTC) while preserving **full on-chain verifiability and auditability**.

Core Design Principles

1. Optional Privacy (Not Forced)

- Users can choose between:
  - **Transparent** (fully visible)
  - **Shielded** (privacy-enabled)
- This is critical for regulatory alignment

2. Zero-Knowledge Proofs (PLONK-based)

- Transactions are **cryptographically proven valid**
- Without exposing:
  - Sender
  - Receiver
  - Amount

3. State-Level Integration (Not a Wrapper)

- Privacy is embedded at the **consensus/state layer**
- **Not** reliant on mixers, bridges, or external contracts

Institutional Compliance Compatibility

This is where Prism materially differs from legacy privacy systems.

1. Selective Transparency / Audit Controls

- Institutions can operate **fully transparent wallets**
- Or use **selectively shielded flows**
- Enables **policy-based privacy**, not absolute anonymity

2. Embedded Compliance Tooling

- VerifiedX integrates with **on-chain analytics providers** (Merkle Science):
  - Transaction monitoring
  - Risk scoring
  - KYC, AML, CFTC compliance and tracing

KEY DISTINCTION

Privacy exists at the **data layer**. Compliance exists at the **access + monitoring layer**.

3. Identity & Policy Layer (Institutional Mode)

- Whitelist counterparties
- Enforce transaction rules
- Restrict shielded interactions if required

4. No Obfuscation via Mixing

- Unlike mixers: no commingling of funds, no "black box" pooling
- Each transaction is:
  - Individually provable
  - Deterministically valid

How Prism Can Be Audited

1. Cryptographic Auditability (ZK Proofs)

- Every transaction includes a **zero-knowledge validity proof**
- Validators verify: no double spend, correct balances, valid state transitions

Even when data is hidden, **correctness is publicly verifiable**.

2. Full On-Chain State Integrity

- All balances (including shielded) exist in the **VerifiedX state tree**
- Auditors can verify:
  - Total supply consistency
  - No inflation or hidden minting
  - Deterministic state transitions

How Prism Can Be Audited (continued)

3. View Keys / Disclosure Mechanisms (Institutional)

- Institutions can optionally provide **view access** to auditors/regulators
- Enable **selective disclosure of transaction history**
- Supports: internal audit, regulatory reporting, counterparty verification

4. Third-Party Compliance Monitoring

- Entry/exit points (on/off ramps, counterparties) remain analyzable
- Tools like **Merkle Science** provide risk scoring and pattern detection

5. Code & Security Audits

- VerifiedX core systems (including vBTC (BTC) + network stack) — **audited by Halborn**
- All findings remediated and deployed
- Prism follows the same: cryptographic rigor, formal review, ongoing security (incl. bug bounty)

Key Differentiation vs Traditional Privacy Coins

FEATURE	LEGACY PRIVACY (E.G., ZCASH)	PRISM (VERIFIEDX)
Privacy Model	Strong anonymity by default	Optional / policy-driven
Compliance	Limited institutional tooling	Built-in compliance integrations
Auditability	Cryptographic only	Cryptographic + institutional controls
Transparency Options	Binary (shielded vs transparent)	Granular + programmable
Institutional Fit	Challenging	Designed for institutions

Prism is not designed to obscure accountability — it is designed to separate:

- **Data privacy (what is hidden)**
- **Transaction validity (what is provable)**
- **Compliance visibility (who can see what, when required)**

This results in a system that is:

- **Cryptographically private**
- **Operationally transparent**
- **Institutionally auditable**