Onyx Protocol

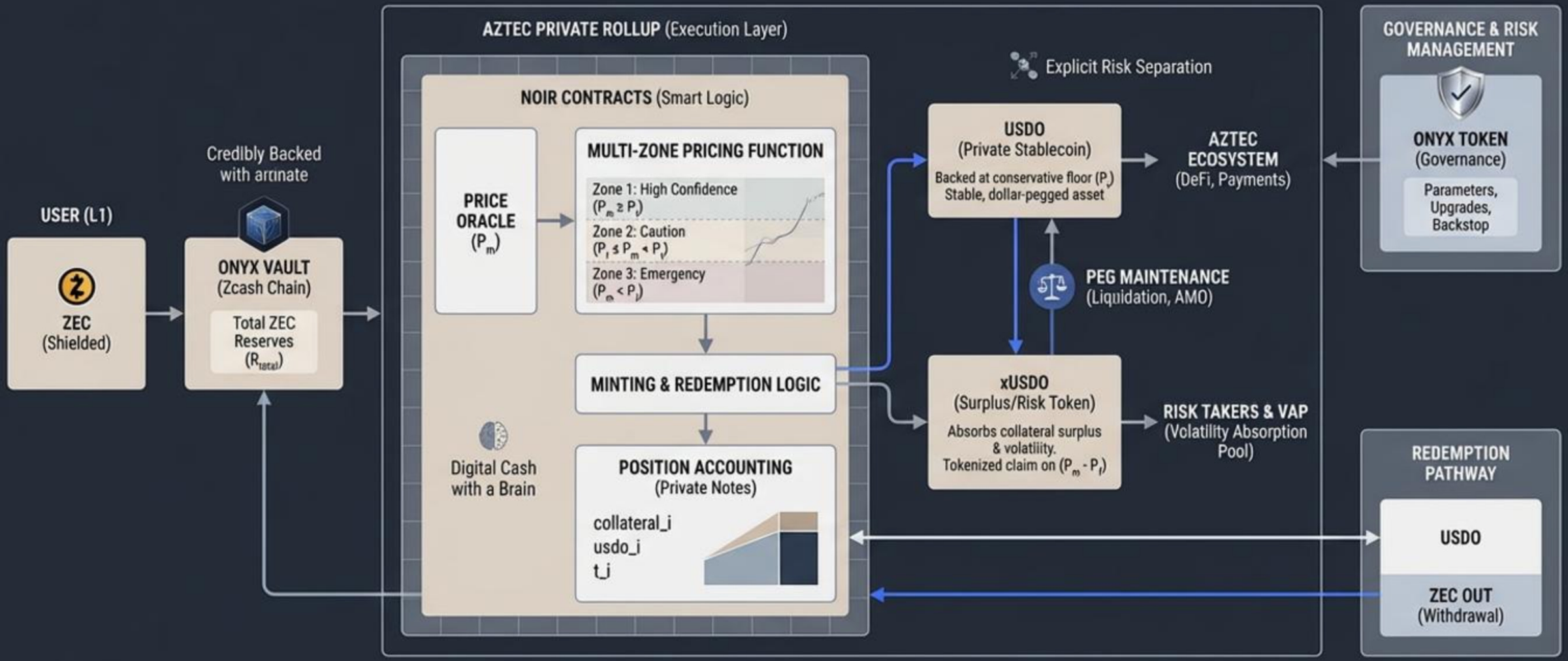
A Zcash Backed Private Stablecoin on Aztec

SerPepe, Onyx Labs

Draft v0.1

Onyx Protocol: A Zcash Backed Private Stablecoin on Aztec

Onyx mints USDO against ZEC collateral inside Aztec's private rollup, splits upside into xUSDO, enforces over-collateralization at a conservative floor, and lets users redeem back to ZEC anytime, delivering digital cash that thinks



ONYX PROTOCOL: PRIVATE ARCHITECTURE ON ZCASH & AZTEC

ZCASH SHIELDED DEPOSITS

Leverage Privacy

AZTEC ENCRYPTED STATE & NOIR CIRCUITS

Noir Circuit

User Balances, Vault Ratios, Liquidation Events are hidden by circuits.

PRIVATE USER DATA (HIDDEN)

EYE-OFF

PUBLIC AGGREGATE STATE (VISIBLE)

EYE-ON

TOTAL SUPPLY	TOTAL RESERVES
1,000,000	1,000,000

Explicit Risk Separation & Value Segmentation Model.

Onyx Protocol's Economic Architecture: Backing, Surplus, and Governance Roles

ZEC Collateral Vault
(L1 Zcash)

Secure Bridge Vault

Multi-Zone Pricing & Bond Layer
(Aztec L2)

Zone 1: High Confidence

Zone 2: Caution

Zone 3: Emergency

Continuous, explicit math splits collateral value its collateral value into a conservative floor and a volatile surplus, managed by Noir contracts.

Economic Roles & Defined Risk
(Tokenized)

USDO (Stablecoin User)
Dollar-pegged, backed at floor.
Low risk, primary use for stability.
1:1 backing target.

xUSDO (Risk Taker)
Absorbs volatility, captures surplus & tail risk.
High risk, predefined leverage.

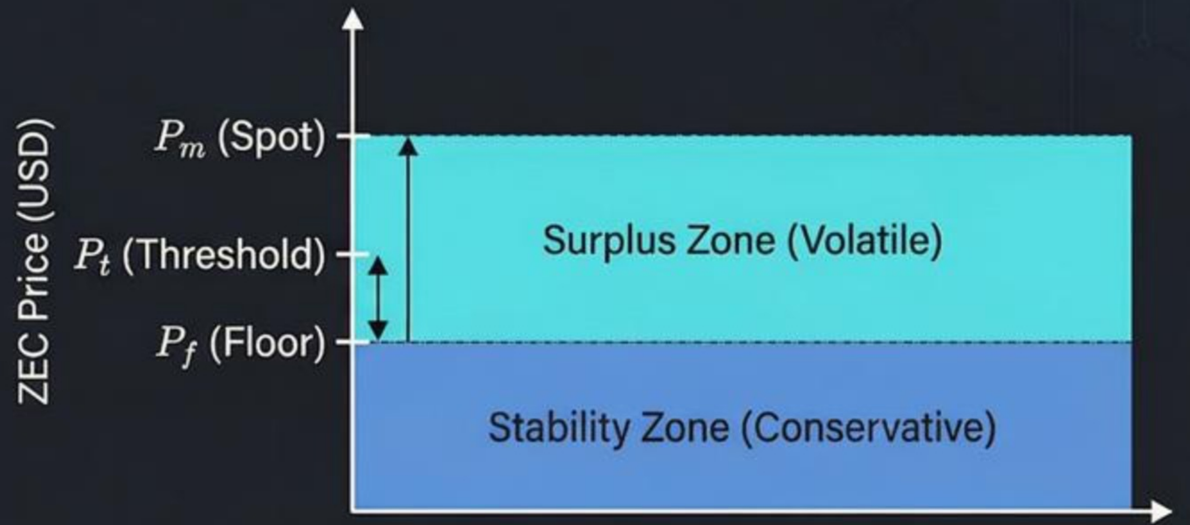
ONYX (Governance & Backstop)
Manages parameters, provides final backstop in shortfalls.
Strategic risk, protocol oversight.

Economic Model & Key Definitions

Key System Variables

P_m	Current ZEC Price (Spot, USD Oracle)
P_f	Conservative Floor Price (ZEC, USD)
P_t	Threshold Price ($P_f * (1 + \alpha)$)
R_{total}	Total ZEC Reserves (ZEC units)
S	Total USDO Supply
B	Total xUSDO Supply

Stability Principle & Surplus



Core Principle: System Only Promises Stability at Floor (P_f). Everything Above is Treated as Surplus.

USDO backing is tied to the conservative floor price, decoupling stability from daily price fluctuations.

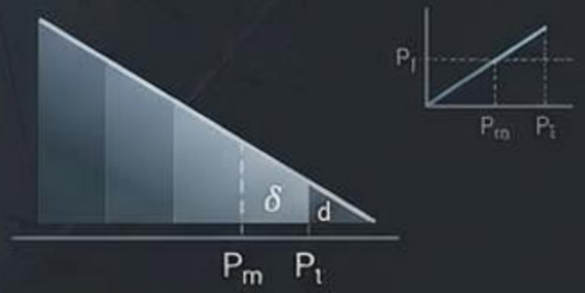
Multi-Zone Minting Function

Zone 1: High Confidence
$(P_m \geq P_t)$

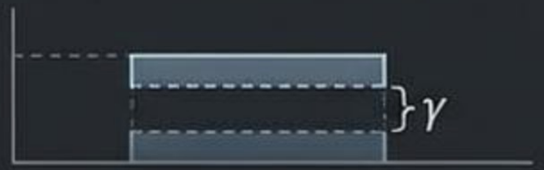
USDO Minted:
$P_f\,(1+\beta)$
(Small Bonus)

xUSDO Minted:
$(P_m - P_f)\,(1-\gamma)$
(Surplus Tokenized)

Zone 2: Caution
$(P_f \leq P_m < P_t)$



USDO Minted:
$P_f\,[1-\delta_d]$
(Linear Discount)



xUSDO Minted:
$(P_m - P_f)\,(1-2\gamma)$
(Tightened Fee)

Zone 3: Emergency
$(P_m < P_f)$

xUSDO Minted: 0
(Halted)

USDO Minted:
$P_m \times \kappa$
(Market Reality Haircut)

Volatility Absorption Pool (VAP) Mechanism & Deployment.

Mechanism (When $P_m > P_t$)

ZEC Deposit (x)

Condition: $P_m > P_t$

Calculate Spread: $P_m - P_t$

VAP Booking:
$\Delta \text{VAP} = x(P_m - P_t)$

Internal USD Buffer

Funding & Structure

ZEC Slices
(Excess Collateral)

Protocol
Fees

USD-Denominated,
Fortified Buffer

Deployment & Benefit

VAP Pool

Buy Back USDO

Peg Maintenance
(below $0.99)

Cover Bad Days

Market Stress /
Shortfalls

No Dilution for
Stable Holders

Floor-Based Solvency Invariant: Mitigating Deep Drawdowns

Systemic Solvency Secured Through Continuous Invariant Checks

The Invariant Formula ($\rho \geq 1.2$)

R: Total ZEC Reserves

ρ: Minimum Coverage Ratio (e.g., 1.2)

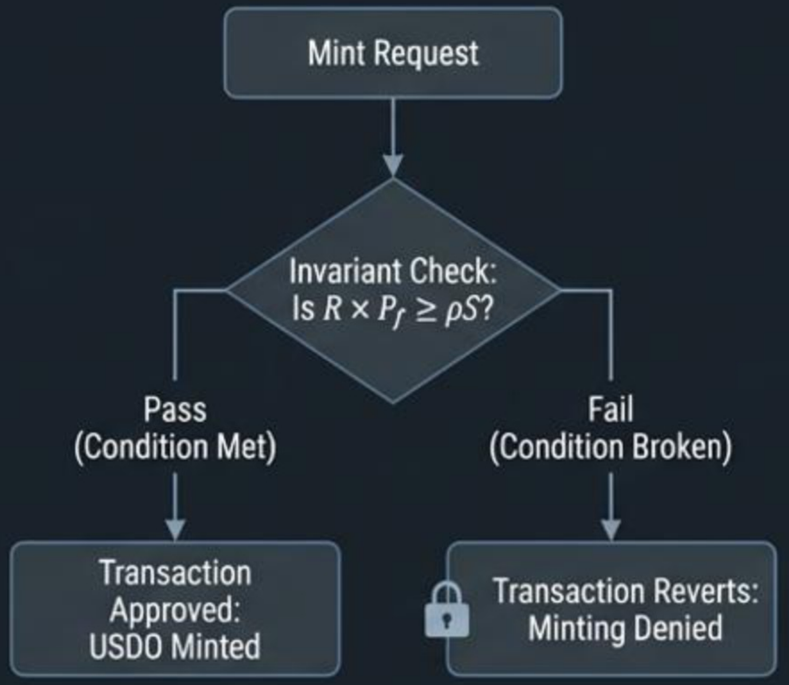
$$R \times P_f \geq \rho S$$

P_f: Conservative ZEC Floor Price

S: Total USDO Supply

This floor-based cushion is the fundamental solvency check.

Pre-Mint Validation Process



Every mint transaction is gated by this real-time verification, ensuring the floor condition is never violated.

Impact During Deep ZEC Drawdown

Even if ZEC price plummets, the protocol denies minting that would breach the conservative floor, preventing unbacked liabiiities.

PRIVATE POSITION ACCOUNTING

ENCRYPTED NOTES & SELECTIVE SPENDING

1. DEPOSIT & CREATION

PRIVATE NOTE

2. REDEMPTION & LIQUIDATION

3. INVISIBLE HISTORY

Each deposit creates an encrypted note recording ZEC collateral, USDO debt, and rnint timestamp; these notes are spent selectively during redemption or liquidation, keeping individual histories invisible to observers.

Time-Based Redemption: Upside Participation, Downside Protection

Redemption Value (RV) Calculation

$$RV(U,t) = U\left[1 + \phi\left(\frac{P_m}{P_f} - 1\right)e^{-\lambda \Delta t}\right]$$

Redemption value includes a dynamic bonus for early exit when the market price (P_m) exceeds the floor price (P_f), decaying over time (Δt) towards par value (U). This incentivizes early exits to share in the surplus while ensuring long-term stability.

Final ZEC Return and Reserve Protection

$$ZEC_{\text{out}} = \frac{RV}{P_{\min}}, \quad P_{\min} = \max(P_m, \psi P_f)$$

The amount of ZEC returned is calculated by dividing the Redemption Value by a conservative minimum price (P_{min}), which is the greater of the current market price (P_m) or a safety buffer above the floor price (ψP_f). This mechanism protects reserves from potential oracle glitches or extreme volatility.

Liquidation Condition

A position becomes liquidatable when its floor collateral ratio falls below the minimum safe ratio θ_{liq}.

Collateral Amount (ZEC)

Conservative Floor Price

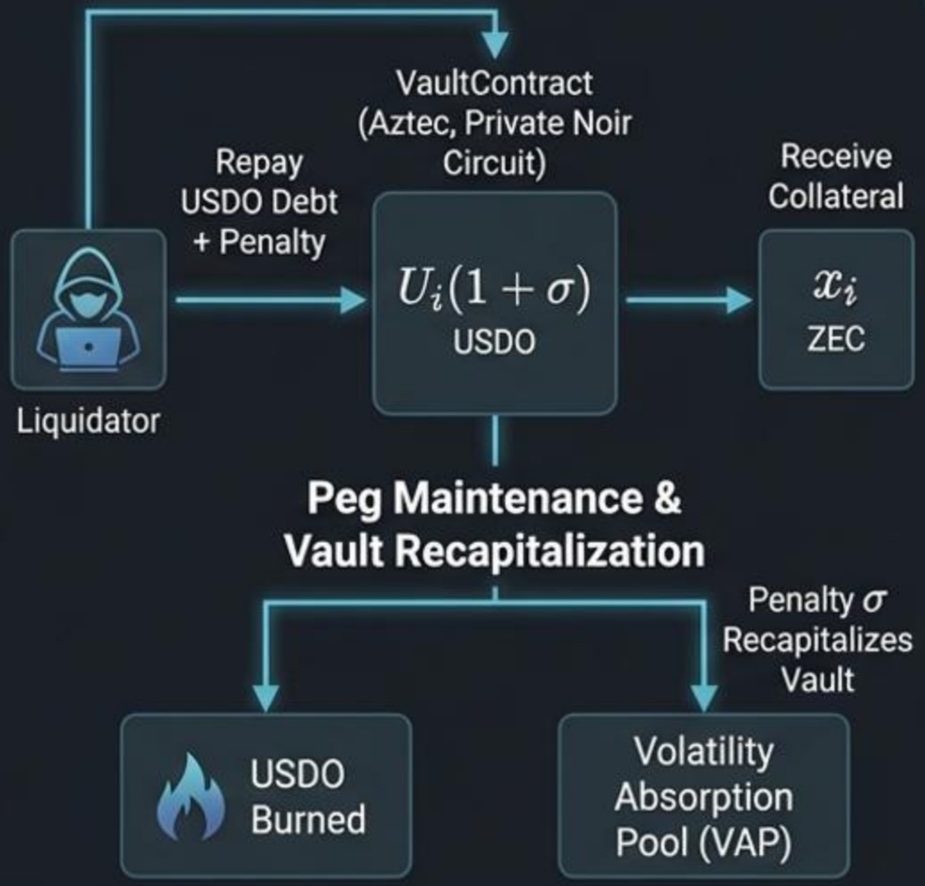
$$\frac{x_i P_f}{U_i} < \theta_{\text{liq}}$$

USDO Debt

Liquidation Threshold (e.g., 1.5)

Liquidation Triggered

Liquidator Action & Private Settlement



Privacy & Data Leakage Prevention

- Entire process executed within Aztec's private environment.
- User balances and specific position details remain encrypted.
- Only aggregate supply and reserves are visible public state.
- Liquidators interact via Noir proofs, shielding their identity and strategy.

Peg Maintenance & Autonomous Market Operations

Automated mechanisms to stabilize USDO price around the target, using transparent code and bounded interventions.

Below Peg (< 0.99)

Condition: USDO Market Price < 0.99 USD

↓

Action: Volatility Absorption Pool (VAP) Intervention

- ↓ Buys USDO from Market
- 🔥 Burns USDO to Reduce Supply

↓

Outcome: Upward Price Pressure, Peg Restoration

Above Peg (> 1.01)

Condition: USDO Market Price > 1.01 USD

↓

Action: Surplus Collateral Utilization

- ⊕ Mints New USDO from Surplus
- 🛒 Sells USDO into Market

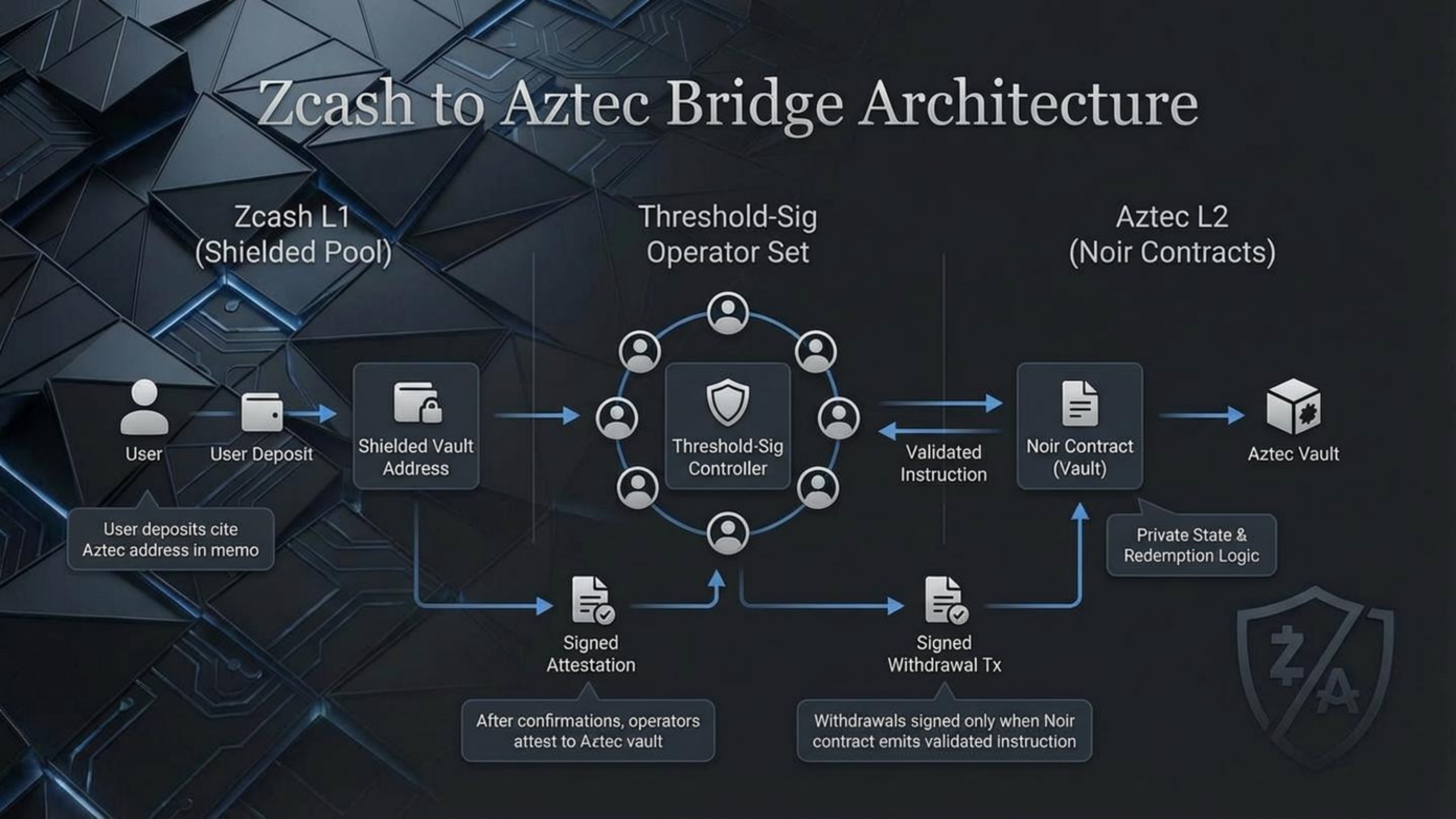
↓

Outcome: Downward Price Pressure, Peg Restoration

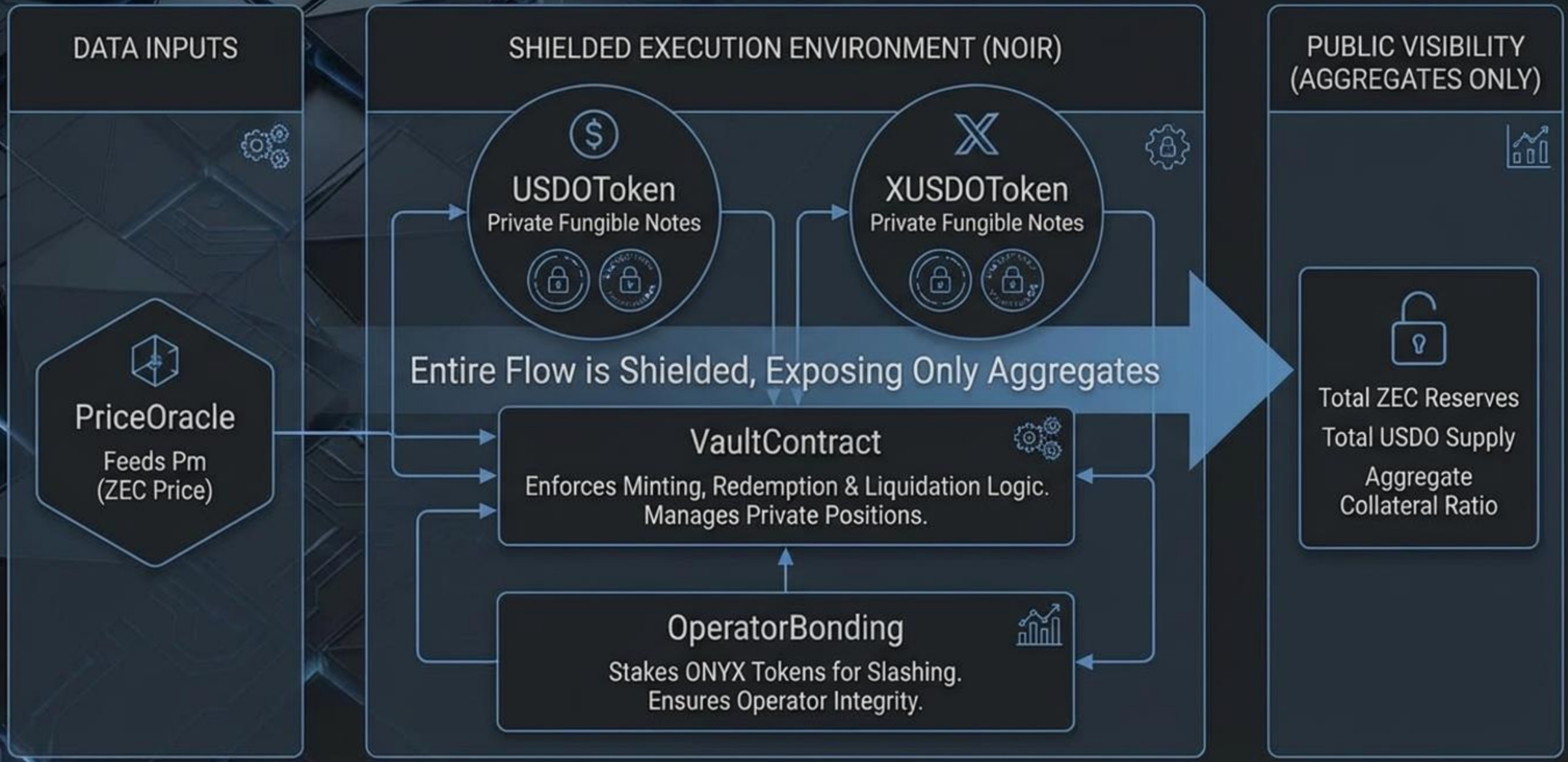
Bounded Autonomous Market Operations (AMO)

Lean against persistent deviations while staying transparent in code. Interventions are bounded by defined parameters, avoiding open-ended risks. Governance oversees bounds, not individual actions.

Zcash to Aztec Bridge Architecture



Core Noir Contracts & Architecture



Onyx Protocol Roadmap

PHASE 0: SIMULATION & PARAMETER SEARCH

Monte-Carlo parameter tuning; Implement economic model; Explore sensible ranges.

PHASE 1: AZTEC TESTNET DEPLOYMENT

Aztec testnet with mocked bridge; Implement Noir contracts; Deploy operator set.

PHASE 2: ZCASH TESTNET & REAL CROSS-CHAIN

Zcash testnet plus real threshold vault; Wire operators for minting; Test liquidations and AMO.

PHASE 3: GUARDED MAINNET LAUNCH

Capped mainnet launch with ONYX governance; Support ZEC only; Distribute ONYX, emergency brakes.

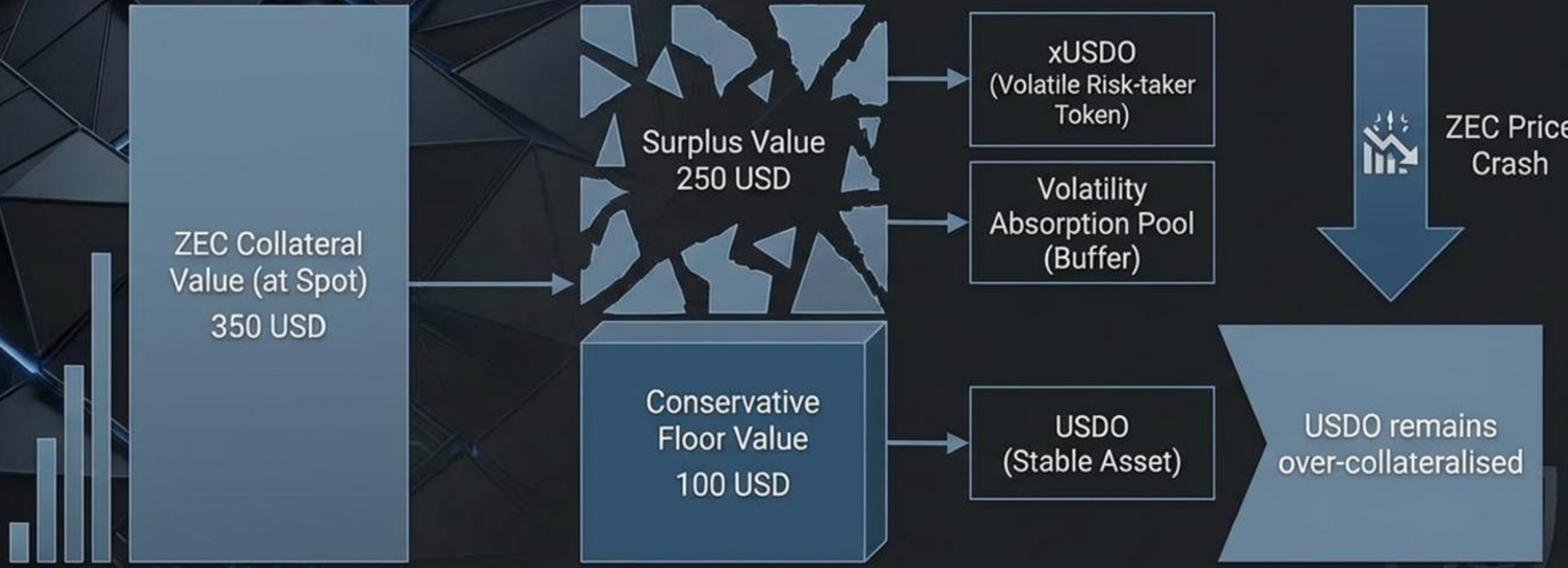
PHASE 4: SCALING & ECOSYSTEM

Raise caps, integrate DEXes, evaluate Zcash shielded USDO; Increase caps, private lending.

Onyx Protocol: Risk and Mitigation Framework

Risk Vectors	Mitigation Strategies
ZEC Long Drawdown, Stale Floor	Conservative Floor Schedule & Dynamic Updates
Oracle Manipulation & Data Corruption	Multi-Feed Oracles, Aggregation, Circuit Breakers
Operator Misbehavior & Bridge Risk	Bonded Diverse Operators, Slashing, Threshold Signatures
Noir Contract Bugs & Exploits	Audits, Testnet Phase, Guarded Launch, Bug Bounties
Governance Mis-parameterisation & Bad Debt	ONYX Backstop, Parameter Governance, Recovery Auctions

Onyx Protocol: Conservative Floor Collateralisation



Source: Onyx Protocol White Paper. Data is illustrative.

Onyx Protocol: A Private, Backed, Crypto-Native Stablecoin

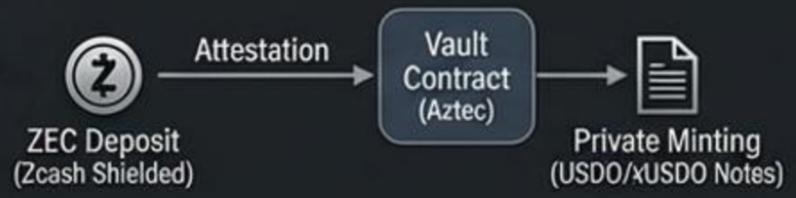
Onyx delivers a private, fully-backed, crypto-native stablecoin without centralised custodians or opaque algorithms; transparent math splits safety and risk, giving users digital cash that preserves confidentiality and maintains dollar parity.

ZEC Base Collateral

- Utilizes Zcash for L1 privacy.
- Conservative floor price backing.
- Held in Zcash Vault addresses.
- No unbacked algorithmic expansion.

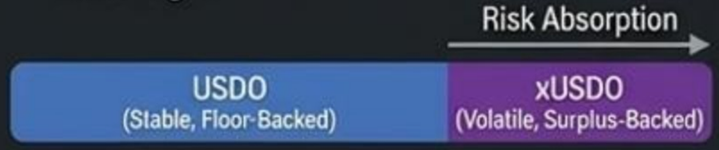
Aztec Private Rollup

- Private Execution Environment.
- Noir smart contracts manage minting/redemption.
- Balances & positions are encrypted notes.
- Privacy is a first-order design objective.



Explicit Risk Separation

- Separates Stable Users (USDO) from Risk Takers (xUSDO).
- Multi-Zone Pricing Function (Floor, Surplus, Threshold).
- Overcollateralization & Time-Based Redemption.
- Standard DeFi mechanics: Liquidation, Arbitrage.



Design Goal: Digital cash with a brain – private, credibly backed, crypto-native stability.