Onyx Protocol
A Zcash Backed Private Stablecoin on Aztec

Onyx Labs
SerPepe (@SerPepeXBT)
serpepexbt@gmail.com

Draft v0.1

Abstract

Onyx Protocol is a privacy focused stablecoin system that issues USDO, a dollar pegged asset backed by Zcash and settled privately on the Aztec network. The protocol combines three ingredients. First, ZEC is used as the base collateral, taking advantage of the Zcash privacy stack at the L1 level. Second, Aztec provides a private rollup execution environment, where smart contracts written in Noir manage minting, redemption and risk logic without leaking user balances or positions in the clear. Third, a multi zone pricing function and bond layer splits collateral value into a conservative floor and a volatile surplus. USDO is backed at a conservative floor price of ZEC. The surplus above that floor is tokenized as xUSDO and absorbed by risk takers. Onyx does not rely on purely algorithmic promises. Every USDO is backed by real ZEC held in a bridge vault and accounted for in Aztec state. Stability comes from overcollateralization, a piecewise minting function, time based redemption bonuses, a volatility absorption pool and standard DeFi mechanics such as liquidation and arbitrage. The design goal is simple and a little ambitious: make a private, credibly backed, crypto native stablecoin that behaves like digital cash with a brain.

1. Introduction

Stablecoins are the closest thing crypto has to everyday money. They are used for trading, savings, DeFi, off ramping and peer to peer payments. Right now privacy conscious users are stuck between two incomplete choices.

- Privacy coins such as Zcash and Monero provide strong anonymity but are volatile.
- Most stablecoins provide price stability but live on fully transparent ledgers.

You can have price stability or transactional privacy, but not both together in a clean, credibly decentralized way.

There have been early attempts to bridge this gap. Algorithmic models that mint private stablecoins from a volatile governance asset. Wrapped assets that rely on centralized custodians. Most of these either inherit centralization risk or concentrate volatility in ways that break under stress.

Onyx takes a different route:

- Use ZEC as base collateral.
- Use Aztec as a private execution and settlement layer.
- Use explicit and conservative math to separate safe users and risk takers.

The user experience we want is straightforward.

You hold ZEC in the Zcash shielded pool. You move some ZEC into an Onyx vault. Aztec contracts privately mint you USDO. You move and spend USDO inside the Aztec ecosystem like a normal stablecoin. At any time you can repay and redeem back into ZEC, subject to the protocol rules.

From the outside, observers see ZEC moving into and out of a vault and public aggregate stats on Aztec such as total USDO supply and reserves. They do not see which address owns which position, what collateral ratio any particular vault has or which specific position was liquidated.

This document describes the goals, economic design and technical architecture of Onyx Protocol, with enough detail that protocol developers and privacy focused DeFi users can reason about the trade offs.

2. Design Goals

2.1 Privacy

On the collateral side, ZEC deposits and withdrawals can use the Zcash shielded pool. On the stablecoin side, USDO and xUSDO are implemented as Aztec private tokens, represented as encrypted notes managed by Noir contracts.

The protocol should not require a central authority to know the real world identity behind a position or to link a vault to an off chain profile. Privacy is a first order design objective, not an afterthought.

2.2 Hard Collateral Backing

USDO is always backed by ZEC held in a vault on the Zcash chain. Invariant checks on Aztec track reserves and total USDO supply. The protocol enforces a coverage inequality relative to a conservative floor price of ZEC.

There is no unbacked algorithmic expansion. If the reserves and floor support are insufficient, minting is denied.

2.3 Explicit Risk Separation

The protocol separates three economic roles.

- USDO holders seek a private, stable, dollar like asset.
- xUSDO holders absorb surplus and tail risk from ZEC volatility.
- Governance token holders manage parameters and backstop rare shortfalls.

This separation keeps the mental model clean. Stablecoin users get something boring. Risk takers explicitly opt into surplus and drawdown.

2.4 Smooth Volatility Handling

Instead of a single binary liquidation threshold, Onyx uses a three zone regime for minting based on the ZEC price relative to a floor. In each zone the minting function for USDO and xUSDO is continuous in price.

This keeps the system conservative when ZEC trades near or below the floor, while allowing it to capture surplus when ZEC trades far above the floor.

2.5 Implementable with Aztec and Noir

All mechanisms described here are designed to be implementable with current Aztec architecture and Noir circuits, plus a realistic Zcash bridge. No speculative cryptography is required, although upgrades can move in that direction later.

3. Economic Model and Notation

We fix some notation.

- P_m is the current ZEC price in USD from the oracle.
- P_f is a conservative floor price for ZEC. This is a protocol parameter.
- α is a fractional buffer, for example $\alpha = 0.5$.
- P_t is a threshold price
$$P_t = P_f(1 + \alpha). \tag{1}$$
- R_{total} is the total ZEC reserves in the vault, in units of ZEC.
- S is the total supply of USDO.
- B is the total supply of xUSDO.

For each individual deposit we denote

- x as the amount of ZEC deposited.

In contracts we will use fixed point arithmetic. For conceptual exposition we treat all variables as real numbers.

The key idea is simple. The protocol only ever promises stability at the floor. The region between floor and spot is treated as surplus and is pushed into xUSDO and a volatility buffer.

4. Multi Zone Minting Function

When a user deposits x units of ZEC into the vault, the protocol computes how many USDO and xUSDO to mint, based on the current price P_m. There are three price zones.

4.1 Zone 1: High Confidence, $P_m \geq P_t$

In this zone ZEC trades comfortably above the floor. The protocol mints USDO based on the floor and gives the user a small bonus. The surplus above floor is minted as xUSDO with a protocol fee.

Let β be a small bonus fraction, for example $\beta = 0.01$. Let γ be a protocol fee on surplus, for example $\gamma = 0.1$.

Then the USDO minted is
$$\text{USDO}_{\text{minted}} = xP_f(1 + \beta). \tag{2}$$

The xUSDO minted is
$$\text{xUSDO}_{\text{minted}} = x(P_m - P_f)(1 - \gamma). \tag{3}$$

Interpretation. The user gets a floor based loan plus a small bonus because the system is confident. The extra value from $P_m - P_f$ is mostly tokenized into xUSDO. A slice is skimmed as protocol revenue.

4.2 Zone 2: Caution, $P_f \leq P_m < P_t$

Here ZEC is above the floor but approaching it. The system becomes more conservative.

Define the normalized distance

$$d = \frac{P_t - P_m}{P_t - P_f}, \tag{4}$$

so that d runs from 0 near P_t up to 1 at P_f.

Let δ control the discount, for example $\delta = 0.05$.

The USDO minted is

$$\text{USDO}_{\text{minted}} = x P_f \left[1 - \delta d\right]. \tag{5}$$

The xUSDO minted uses a stricter fee on surplus

$$\text{xUSDO}_{\text{minted}} = x(P_m - P_f)(1 - 2\gamma). \tag{6}$$

As P_m approaches P_f, d approaches 1 and the effective factor on USDO tends toward $1 - \delta$, so USDO supply is reduced relative to floor. At the same time surplus becomes small and is further haircutted.

4.3 Zone 3: Emergency, $P_m < P_f$

In this zone ZEC has fallen through the configured floor. The system assumes conditions are bad and becomes strictly conservative. New xUSDO is not minted in this regime.

Let κ be a conservative collateralization factor, for example $\kappa = 0.8$.

The USDO minted is

$$\text{USDO}_{\text{minted}} = x P_m \kappa, \tag{7}$$

and

$$\text{xUSDO}_{\text{minted}} = 0. \tag{8}$$

In words, if ZEC is trading at 60 USD and the floor parameter is 100 USD, the protocol does not pretend that 60 is 100. Borrow capacity is based on the real market price with a haircut.

4.4 Volatility Absorption Pool

Whenever $P_m > P_t$ there is extra cushion between spot and threshold. The protocol tracks this in a separate pool called the volatility absorption pool (VAP).

For each deposit x when $P_m > P_t$, define the increment

$$\Delta\text{VAP} = x(P_m - P_t). \tag{9}$$

VAP is tracked internally in USD terms. It is backed by a portion of ZEC reserves and accumulated fees, and is used as a buffer for bad days and for protocol level market operations.

4.5 Coverage Condition

The core solvency condition is

$$R_{\text{total}} P_f \geq \rho S, \tag{10}$$

where ρ is a coverage ratio such as $\rho = 1.2$ for 120 percent.

The vault contract enforces a stricter version of this condition for each mint. If minting new USDO would push the system below the configured coverage at the floor, the transaction is rejected.

5. Position Accounting and Private State

On Aztec, each deposit and mint produces a private position for the user.

Conceptually a position i has:

- collateral_i: amount of ZEC backing it,
- usdo_i: amount of USDO debt,
- t_i: timestamp of mint.

These live as private notes and are not visible as a global table on chain. The vault contract only exposes aggregate values such as total collateral and total USDO supply.

When a user wants to redeem, they select one or more positions to close or partially close. A Noir circuit proves ownership of those notes and computes redemption amounts under the protocol rules.

6. Time Based Redemption Function

To avoid a purely static relationship between mint and redeem, Onyx uses a time based redemption value that can share some upside in strong ZEC regimes in a controlled way.

Let U be the USDO amount associated with a given position. Let t_0 be the mint time and t the redemption time. Define $\Delta t = t - t_0$ in days.

Define the redemption value in USD as

$$\mathrm{RV}(U,t) = U\left[1 + \phi\left(\frac{P_m}{P_f} - 1\right)e^{-\lambda\Delta t}\right], \tag{11}$$

where $\phi \in [0,1]$ is a participation factor and $\lambda > 0$ is a decay constant.

When $P_m = P_f$ the boost term vanishes and $\mathrm{RV}(U,t) = U$. You get par back. When $P_m > P_f$ and you redeem soon after mint, the exponential term is close to one and you receive a fraction of upside. As Δt grows, $e^{-\lambda\Delta t}$ shrinks toward zero and the function tends back toward par.

To convert this USD redemption value into ZEC, the protocol divides by a conservative price. Define

$$P_{\min} = \max(P_m,\ \psi P_f), \tag{12}$$

with $\psi > 1$, for example $\psi = 1.1$.

Then the ZEC returned for that position is

$$\mathrm{ZEC}_{\text{out}} = \frac{\mathrm{RV}(U,t)}{P_{\min}}. \tag{13}$$

This prevents the contract from valuing ZEC below ψ times the floor during redemptions, which protects reserves from being drained during odd oracle blips.

For a user with multiple positions, the contract sums over selected positions until the desired redemption USDO amount is reached.

7. Why You Get Around 100 USDO for 350 USD of ZEC

This is the part non DeFi friends always question.

Take a concrete scenario.

Assume:

- $P_f = 100$,
- $\alpha = 0.5$ so $P_t = 150$,
- $\beta = 0.01$,
- $\gamma = 0.1$,
- $\delta = 0.05$,
- $\kappa = 0.8$.

Suppose ZEC is trading at $P_m = 350$ USD and you deposit $x = 1$ ZEC.
Zone check: $P_m = 350 \geq P_t = 150$, so this is Zone 1.
USDO minted:

$$\text{USDO} = xP_f(1+\beta) = 1 \cdot 100 \cdot 1.01 = 101. \tag{14}$$

xUSDO minted:

$$\text{xUSDO} = x(P_m - P_f)(1-\gamma) = 1 \cdot (350 - 100) \cdot 0.9 = 225. \tag{15}$$

You started with 350 USD of ZEC at spot. You get about 101 USDO, plus 225 units of xUSDO which represent a claim on surplus that is more volatile. The remaining few dollars go into protocol fees and VAP.

If ZEC rallies to 700, your 1 ZEC is still in the vault, you still hold 101 USDO and your xUSDO position has exposure to the surplus. If ZEC dumps to 120, you still have the USDO. The floor based logic meant you never borrowed the full 350 USD. The difference between floor and spot sits in surplus instruments that are allowed to ride volatility.

Short answer for the skeptical friend: you did not sell your ZEC for 350 USD. You borrowed against a conservative floor and got a stable asset. The gap is the safety margin that keeps the system solvent when things get ugly.

8. Architecture on Zcash and Aztec

8.1 Zcash Side

On Zcash, Onyx uses a vault address or a set of vault addresses controlled by the operator set using threshold signatures or multi signature.

There are two main flows.

8.1.1 Deposit

A user sends ZEC to a vault address. This can be from a shielded or transparent address depending on wallet support. A memo field or an off chain mapping links the Zcash transaction to a target Aztec address.

Once the transaction has enough confirmations, operators attest to it into the Aztec vault contract.

8.1.2 Withdrawal

When Aztec contracts instruct a withdrawal for a given amount of ZEC and a target address, operators sign a Zcash transaction sending ZEC from the vault to the user. Ideally the recipient is a shielded address to preserve privacy.

8.2 Aztec Side

Aztec provides the execution layer where protocol logic lives as Noir contracts.

Core Noir contracts include:

- **PriceOracle**. Stores the latest ZEC USD price as public state. Updated by governance approved feeders.
- **USDOToken**. Private fungible token contract representing USDO. Only the vault contract can mint or burn.
- **XUSDOToken**. Private fungible token contract representing xUSDO.
- **VaultContract**. Holds protocol parameters, tracks aggregate reserves and supplies, creates and updates private position notes, implements the three zone minting function, implements redemption using the time based function and exposes limited public statistics.
- **OperatorBonding**. Contract where operators lock bonds (for example ONYX governance tokens). Handles slashing if proven misbehavior occurs.

Minting flow on Aztec:

1. Operators detect a ZEC deposit on Zcash.
2. They agree on the amount and target Aztec address.
3. A threshold of operators submit a signed attestation into the VaultContract, referencing the Zcash transaction id.
4. VaultContract verifies signatures, updates R_{total} and runs the minting function with current P_m.
5. USDO and xUSDO are minted privately to the user as Aztec notes and a new position note is created with amount and timestamp.

Redemption flow:

1. User selects a position or aggregate amount to redeem.
2. VaultContract computes required USDO burn and ZEC_{out} using the redemption formula.
3. User proves ownership of the position notes in a Noir program, burns the USDO and if required some xUSDO.
4. VaultContract emits a withdrawal instruction with the ZEC amount and target Zcash address.
5. Operators sign and broadcast the ZEC withdrawal transaction.

All Aztec interactions are shielded. Observers see supply and reserve totals and some aggregate events, but not per user positions.

9. Liquidation and Peg Maintenance

Onyx does not rely solely on mint and redeem to keep USDO near one USD. It uses two additional mechanisms: liquidation of unsafe positions and automated market operations.

9.1 Position Level Liquidation

For position i with collateral x_i and USDO debt U_i, define the floor collateral value

$$V_{\text{floor}}^{(i)} = x_i P_f. \tag{16}$$

The floor collateral ratio is

$$\mathrm{CR}_{\text{floor}}^{(i)} = \frac{V_{\text{floor}}^{(i)}}{U_i} = \frac{x_i P_f}{U_i}. \tag{17}$$

The protocol sets a minimum safe ratio θ_{liq}, for example $\theta_{\text{liq}} = 1.5$.

If

$$\mathrm{CR}_{\text{floor}}^{(i)} < \theta_{\text{liq}}, \tag{18}$$

then position i is liquidatable.

Liquidation on Aztec remains private. Liquidators interact with the vault using Noir proofs. At a high level a liquidator:

- repays USDO debt of a position,
- pays a liquidation penalty,
- receives the underlying ZEC.

A simple fixed spread model uses a penalty σ, for example $\sigma = 0.1$. The liquidator pays $U_i(1+\sigma)$ in USDO and receives x_i ZEC. More complex auction mechanisms are possible, but even a simple model provides strong protection if parameters are conservative.

9.2 Peg Operations

Let P_{USDO} be the external market price of USDO in USD on Aztec DEXes or connected venues.

Two simple regimes:

- If $P_{\text{USDO}} < 0.99$ then USDO trades below peg.
- If $P_{\text{USDO}} > 1.01$ then USDO trades above peg.

In the first case the system can spend part of its VAP or surplus reserves to buy USDO on the market and burn it. In the second case the system can mint USDO against surplus collateral and sell it into the market.

These actions can be implemented in an `AMOController` contract that holds USDO, xUSDO and potentially ZEC claims and has limited rights to interact with VaultContract. Governance configures simple bounds so that AMO activity cannot exceed specified limits.

The objective is not to micro manage price to exactly 1.000 at all times, but to lean against persistent deviations.

10. Governance Token and Parameters

Onyx can issue a governance token, denoted ONYX.

ONYX has three main roles:

- Governance of parameters and upgrades.
- Bonding collateral for operator roles.
- Backstop in rare systemic shortfall events.

Examples of parameters that governance can tune:

- Floor price schedule P_f and update rules.
- $\alpha, \beta, \gamma, \delta, \kappa, \phi, \lambda, \psi, \rho$.
- Lists of approved operators and their bond requirements.

- Limits on AMO behavior and risk.
- New collateral types in future versions.

In an extreme event where reserves at floor plus VAP cannot cover S, the vault can enter a recovery mode. New ONYX can be auctioned for ZEC or USDO to fill the hole. This dilutes existing ONYX holders.

This is intentional. ONYX holders receive upside from fees and system growth. They must also bear downside risk if governance decisions or extreme markets produce bad debt.

11. Numerical Scenarios

11.1 Normal Regime with Strong ZEC

Revisit parameters:

- $P_f = 100$,
- $\alpha = 0.5$ so $P_t = 150$,
- $\beta = 0.01$,
- $\gamma = 0.1$.

Let $P_m = 350$ and user deposits $x = 3$ ZEC.

USDO minted:

$$\text{USDO} = 3 \cdot 100 \cdot 1.01 = 303. \tag{19}$$

xUSDO minted:

$$\text{xUSDO} = 3 \cdot (350 - 100) \cdot 0.9 = 675. \tag{20}$$

Floor value of collateral is $3 \cdot 100 = 300$ USD. USDO supply from this deposit is 303. Coverage from this deposit alone is slightly below 1, which is a sign that in practice either P_f would be set below 100 in this scenario or β would be smaller. This is a reminder that parameter choices matter and should be stress tested.

11.2 Caution Zone Example

Now suppose $P_m = 140$, still above 100 but below $P_t = 150$.

Compute

$$d = \frac{P_t - P_m}{P_t - P_f} = \frac{150 - 140}{150 - 100} = \frac{10}{50} = 0.2. \tag{21}$$

Take a new deposit $x = 1$ ZEC.

USDO minted:

$$\begin{aligned} \text{USDO} &= 1 \cdot 100 \cdot [1 - \delta d] && (22)\\ &= 100 \cdot [1 - 0.05 \cdot 0.2] && (23)\\ &= 100 \cdot (1 - 0.01) = 99. && (24) \end{aligned}$$

xUSDO minted:

$$\begin{aligned} \text{xUSDO} &= 1 \cdot (P_m - P_f)(1 - 2\gamma) && (25)\\ &= 1 \cdot 40 \cdot 0.8 = 32. && (26) \end{aligned}$$

As ZEC moves toward the floor, USDO minted approaches $xP_f(1 - \delta)$ and surplus becomes small.

11.3 Emergency Mint Example

Assume the floor is still $P_f = 100$ but market has crashed to $P_m = 80$.

Zone 3 applies. With $\kappa = 0.8$ and deposit $x = 5$ ZEC, worth 400 USD at spot:

$$\text{USDO} = 5 \cdot 80 \cdot 0.8 = 320, \tag{27}$$

and no xUSDO is minted.

Borrowing capacity is based on actual market value with a strict haircut. The floor is ignored here, which is exactly the point.

11.4 Redemption Example

Take the earlier Zone 1 example. $P_m = 350$, $P_f = 100$, deposit $x = 1$ ZEC yielded $U = 101$ USDO at time t_0.

Set parameters:

- $\phi = 0.7$,
- $\lambda = 0.02$ per day,
- $\psi = 1.1$.

Case A: fast redemption after $\Delta t = 1$ day, price still 350.

Compute:

$$\frac{P_m}{P_f} - 1 = 3.5 - 1 = 2.5, \tag{28}$$

$$e^{-\lambda \Delta t} = e^{-0.02} \approx 0.98. \tag{29}$$

Then

$$\begin{aligned} \text{RV}(U,t) &\approx 101\,[1 + 0.7 \cdot 2.5 \cdot 0.98] && (30)\\ &\approx 101\,[1 + 1.715] && (31)\\ &\approx 101 \cdot 2.715 \approx 274.2. && (32) \end{aligned}$$

$P_{\text{min}} = \max(350,\ 1.1 \cdot 100) = 350$.

So

$$\text{ZEC}_{\text{out}} \approx \frac{274.2}{350} \approx 0.783. \tag{33}$$

You burn 101 USDO and receive about 0.783 ZEC, worth around 274 USD at that price. You originally deposited 1 ZEC worth 350 USD, took out 101 USDO and now take back 0.783 ZEC. The remaining value lives in xUSDO and system buffers.

Case B: slow redemption after $\Delta t = 90$ days, price still 350.

$$e^{-\lambda \Delta t} = e^{-0.02 \cdot 90} = e^{-1.8} \approx 0.165. \tag{34}$$

Then

$$\begin{aligned} \text{RV}(U,t) &\approx 101\,[1 + 0.7 \cdot 2.5 \cdot 0.165] && (35)\\ &\approx 101\,[1 + 0.28875] && (36)\\ &\approx 101 \cdot 1.28875 \approx 130.2. && (37) \end{aligned}$$

$$\text{ZEC}_{\text{out}} \approx \frac{130.2}{350} \approx 0.372. \tag{38}$$

As time passes, the bonus term decays and redemption tends closer to par. The user still owns xUSDO and may have benefited or suffered depending on system performance.

The exact numeric choices here are illustrative. The important part is that the curve is explicit and continuous, not tuned by vibes.

12. Risk Discussion

There are several major classes of risk.

12.1 ZEC Price Risk

If ZEC suffers a long and deep drawdown and trades below the configured floor for an extended period, floor assumptions become stale. Governance must be able to adjust P_f downward in a controlled schedule. Floor updates should be conservative but not frozen.

12.2 Oracle Risk

If the oracle price P_m is wrong, all derived values are wrong. Onyx should use multiple feeds and robust aggregation, with guard rails against extreme spikes. Some form of median and time weighting is recommended, along with circuit breakers for obviously impossible prints.

12.3 Bridge and Operator Risk

Operators control the ZEC vault. Their bonds and the slashing logic are the safety net. Until cross chain proofs are cheap and implemented, the system accepts a trust minimized but not entirely trustless bridge. Operators must be diverse and bonds must be sized such that malicious behavior is economically irrational.

12.4 Smart Contract Risk

Bugs in Noir circuits, Aztec rollup code or the vault logic can cause loss. The protocol must be audited, tested on testnets and rolled out with conservative limits. Early versions should cap total USDO supply and per user exposure.

12.5 Governance Risk

Bad parameter choices, adding risky collateral or changing floors aggressively can jeopardize solvency. ONYX holders receive upside from protocol growth and fees. They must also expect downside if governance makes poor choices. This is a feature, not a bug.

13. Roadmap

13.1 Phase 0: Simulation and Parameter Search

- Implement the economic model off chain in Python or Rust.
- Run Monte Carlo simulations of ZEC price paths and vault dynamics.
- Explore sensible ranges for P_f, α, β, γ, δ, κ, ϕ, λ, ψ, ρ.

13.2 Phase 1: Aztec Testnet Deployment

- Implement PriceOracle, USDOToken, XUSDOToken and VaultContract in Noir.
- Deploy an OperatorBonding contract and a small operator set with bonds.
- Use a mocked ZEC bridge on testnet to simulate deposits and withdrawals.

13.3 Phase 2: Zcash Testnet and Real Cross Chain

- Build a Zcash side vault with threshold signatures.
- Wire operators so that real ZEC testnet deposits trigger Aztec minting.
- Test liquidations, redemptions and AMO logic with play capital.

13.4 Phase 3: Guarded Mainnet Launch

- Launch with tight caps on total USDO and per wallet limits.
- Support ZEC only at first.
- Distribute ONYX and set up governance, still with emergency brakes.

13.5 Phase 4: Scaling and Ecosystem

- Increase caps as confidence grows.
- Integrate USDO and xUSDO with Aztec DEXes and private lending.
- Explore issuing USDO as a Zcash shielded asset if and when the stack supports it.

14. Conclusion

Onyx Protocol is an attempt to build a very specific thing.

A private stablecoin backed by a real privacy asset, running on a private rollup, with economics that are explicit rather than mysterious. The design is intentionally conservative. It does not rely on reflexive loops or hidden levers. It uses a floor, a threshold, a few curves and a clear split between stable users and risk takers.

USDO is for people who want a private dollar like object. xUSDO is for people who are willing to absorb the wobbles of ZEC versus that dollar. ONYX is for people who want to steer the parameters and accept that if things go wrong they are in the blast radius.

If this all sounds complicated, that is fair. Money is simple. Building something that behaves like money on adversarial global networks while staying private is not simple. The point of this document is to put the complexity out in the open so that builders, auditors and attackers can all see what is going on.

Onyx Labs will build an initial implementation. The long term owner of this system should be its users and governors. The best outcome is that in a few years nobody cares who wrote this paper and USDO is just the private stablecoin people in the privacy corner of crypto use without thinking too much about it.

Feedback and criticism are welcome.

Contact:
SerPepe, Onyx Labs
Twitter: @SerPepeXBT
Email: `serpepexbt@gmail.com`