Astera USD Whitepaper

Beirao[1], Yuval Boneh[2], and Justin Bebis[3]

[1]Astera Head of Security, beirao@conclave.io
[2]Astera CEO, yuvi@conclave.io
[3]Conclave CEO, bebis@conclave.io

Abstract

asUSD is Astera's solution to the stablecoin trilemma - addressing stability, scalability, and security. asUSD is a stablecoin minted predominantly by Facilitators. The primary asUSD Facilitator is Astera Lend, which expands the functionality of traditional cryptocurrency debt by introducing a novel approach to adaptive interest rate management, unified liquidity, and systemic risk management features. asUSD capability is expanded by Algorithmic Market Operations strategies enabling an unbacked line of credit to facilitate autonomous liquidity strategies, whereby unbacked asUSD is not at risk of entering circulation. Astera isolates risk by managing Facilitator limits and repayments, introducing novel yield and scalability opportunities while prioritizing the system's security.

Keywords: Decentralized Finance, Cryptocurrency, Stablecoin, Astera, Collateralized Debt, Algorithmic Market Operation

1. Introduction

asUSD presents a unique implementation of features from the industry's leading Collateralized Debt Position (CDP) platforms, aggregated into a new DeFi primitive that addresses assessed flaws and optimizes for user safety and reduced protocol risk.

The asUSD stablecoin features structural risk mitigations that reinforce its security and enable it to scale yields organically alongside the system.

asUSD is supported by a myriad of features, ranging from cross-chain integrations, to state of the art Astera staking mechanisms. Features are designed to support money markets and credit facilities, as well as more general cross-chain stablecoin capabilities.

Astera Lend architecture and asUSD design autonomously mitigate some of the industry's biggest risks without compromising functionality and scalability. Astera Lend is discussed in this paper, however a detailed Astera Lend Whitepaper will be released in a subsequent publication.

2. Facilitators

Astera asUSD is planned to be available on various EVM chains in the form of an ERC20 Token. Astera is able to create and manage Facilitators, whereby each Facilitator is associated with a strategy that can autonomously mint and burn asUSD tokens. The design allows for flexibility and upgradability on how asUSD is minted, while isolating risk (Figure 1).

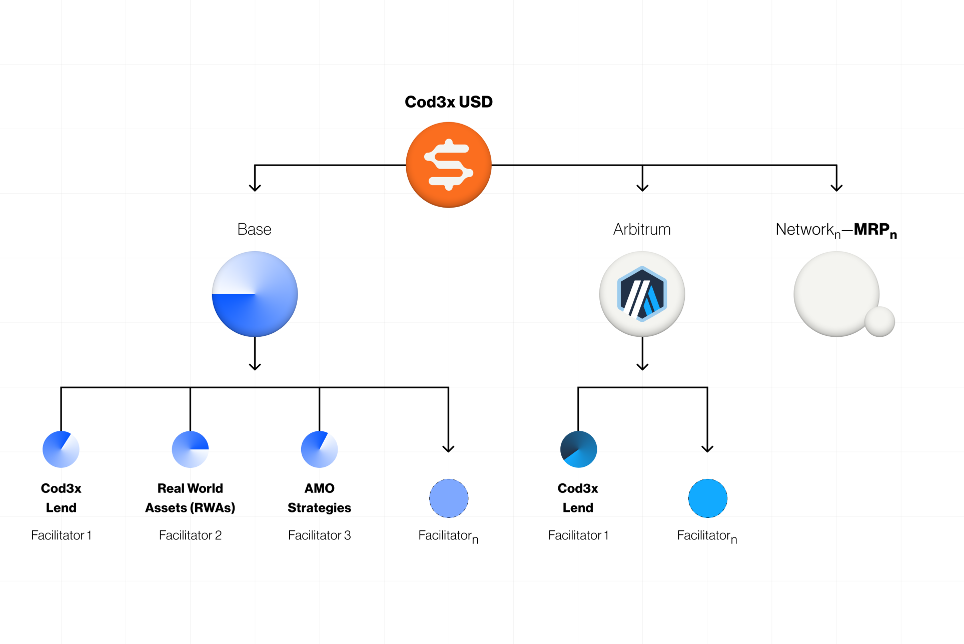


Figure 1: Representation of example asUSD Facilitators.

Astera DAO can limit the amount of asUSD tokens that n number of Facilitators can mint using the bucket model. Each Bucket (B_n) has a Capacity (the maximum amount of asUSD that the Facilitator can mint, C_n), and a Level (the current amount of asUSD the Facilitator has minted, L_n).

If asUSD is deployed on m number of chains and each chain has a set of n_m Facilitators, each associated with a bucket with a capacity ("C_{m,n_m}") and a current level ("L_{m,n_m}"), then asUSD supply must follow Equations 1 and 2:

$$CS_{asUSD} = \sum_{0}^{m}(\sum_{0}^{n_m}(L_{m,n_m})), \tag{1}$$

$$AS_{asUSD} = \sum_{0}^{m}(\sum_{0}^{n_m} min(0, C_{m,n_m} - L_{m,n_m})), \tag{2}$$

where:

- CS_{asUSD} is the Current Supply of asUSD from all Facilitators on all chains
- AS_{asUSD} is the Available Supply of asUSD from all Facilitators on all chains.

3. Primary Facilitator: Astera Lend

3.1 Integration

Astera asUSD operates with a specific liquidity token (cToken) and debtToken. Unlike other assets, direct deposits of asUSD are not supported. Instead, asUSD is minted directly by the Astera Lend main lending pool via the associated cToken, which acts as the Facilitator in this process.

When borrowing asUSD from the Astera Lend main lending pool, the smart contract automatically mints and transfers the corresponding asUSD and asUSD debtTokens to the user, just like other Astera Lend collateral. Simultaneously, the Facilitator's *Bucket* is updated to reflect the newly minted amount.

Liquidation and debt repayment are exactly the same as standard Astera Lend collateral and will be detailed in a subsequent Astera Lend Whitepaper.

3.2 Price Stability

As a Facilitator, Astera Lend implements an over-collateralization strategy (see 3.1), it also utilizes technical mechanisms for price stability:

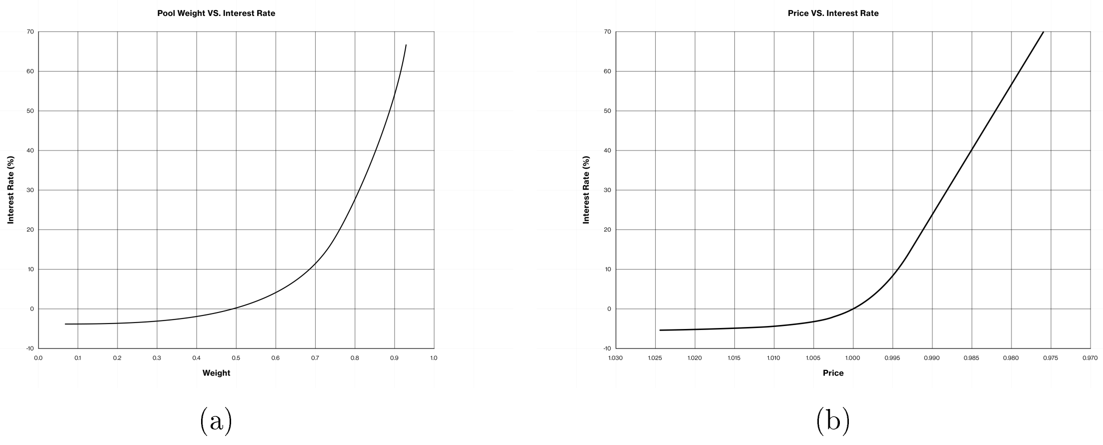
- Price stability is predominantly ensured by the interest rate, which seeks to correct market behaviors based on liquidity conditions, effectively front-running peg deviations. The 'staked asUSD' (see 5) feature automatically manages a liquidity pool and adjusts interest rates based on reserve ratios. If the stablecoin is oversold, the pool balance changes, increasing interest rates. This mechanism autonomously supports yield, security, and scalability by restoring parity and unwinding rate arbitrage (see 3.3).

- Users can always borrow, repay, and liquidate asUSD at $1. This creates an arbitrage opportunity; when the market price of asUSD is below $1, borrowers are incentivized to buy asUSD at a discount and repay/liquidate, profiting from the difference. Conversely, when the asUSD price exceeds $1, there is incentive to generate new asUSD and sell it to the market, repaying once the price corrects enough to be profitable.

3.3 Adaptive Interest Rate Management

Industry leaders like Maker and Aave adjust CDP interest rates manually via governance. This causes a delayed response to shifts in broad economic dynamics, as well as constant effort and human intervention, which results in reduced stablecoin price stability as users seek to arbitrage interest rates. Astera aims to develop towards a highly responsive, governance-free model, starting with asUSD borrow rates.

Astera Lend features a unique interest rate controller mechanism that adapts to both user activity and broad market conditions (Boneh, 2024). Contemporary CDP interest rate mechanisms respond to deviations in the price of the stablecoin. While this works generally well, it can be improved by monitoring liquidity conditions instead of token price. asUSD infrastructure monitors a liquidity pool to anticipate price deviations before they occur. The base interest rate is governed by the stablecoin's liquidity conditions, and shifts as pool balance deviates from the target. For example, by leveraging the dynamics of Stableswap architecture, the controller can adjust interest rates before the price of the stablecoin changes. The result is a more responsive interest rate that mitigates price deviations instead of only responding to them, thus leading to a more stable price (Figure 2).



(a)

(b)

Figure 2: Transfer function subset: (a) pool weight vs interest rate, (b) equivalent price vs interest rate.

For each collateral type, the interest rate then proceeds to grow or decay based on the isolated collateralization ratio. Premium collaterals allow for lower ratios and therefore experience slower interest rate growth. More volatile collaterals require higher collateralization ratios and subsequently experience faster interest rate growth, targeting those assets to mitigate stablecoin risk. Growth and decay offsets settle as liquidity conditions correct, which allows the interest rate to be maintained at a level the market deems acceptable. The difference in growth and decay rates means that different collateral types will settle at different market rates based on their respective risk profiles, ensuring the stablecoin can scale effectively.

Interest paid is directed to stablecoin yield, addressing market rate parity, so it is anticipated that market actions will promptly correct liquidity conditions. This is facilitated by the 'staked asUSD' feature (see 5), that automatically manages a Stableswap pool and uses the reserve ratio as the error input for the controller. If the stablecoin is oversold, the pool balance will deviate, causing interest rates to increase. By directing interest to the stablecoin, increased yield will restore parity and unwind the rate arbitrage, restoring the pool balance. This mechanism supports yield, security, and scalability in a completely autonomous and decentralized fashion.

4. Algorithmic Market Operations (AMOs)

4.1 Liquidity AMO Facilitator

In certain cases, asUSD infrastructure can be used to provide unlimited liquidity counterassets for the purpose of raises, launches, and ongoing liquidity. This is possible when 100% of a token's supply is issued via a asUSD liquidity pool, where no additional tokens enter circulation after the point of inception. The varying dynamics of exchange liquidity and slippage characteristics can be used to construct a myriad of liquidity bootstrapping pools, fundraises, etc. so long as asUSD maintains an independent core liquidity pool. By ensuring 100% of the launch token's supply exists in the pool at inception, there is no way for unbacked asUSD to enter circulation.

At the conclusion of the raise event, the liquidity pool can be withdrawn to repay the asUSD line of credit and subsequently seed ongoing liquidity appropriately with backed assets. This can be used to raise funds for protocols, fair-launch meme tokens, and other use cases, in a safe way that mitigates security risks. Astera intends to deploy this product in a permissioned state initially and interate towards a permissionless system (Figure 3).

4.2 Arbitrage AMO Facilitator

The Arbitrage AMO is an implementation of the crvUSD PegKeeper (Curve, 2024) that holds a pre-minted supply of asUSD tokens earmarked for peg stability efforts. The operation of PegKeepers is restricted to only two actions: depositing and withdrawing from liquidity pools. The Arbitrage AMO's supply can not be deposited anywhere else, and should be considered out-of-circulation. Each Arbitrage AMO contract is associated with a specific liquidity pool that includes asUSD and another fiat-redeemable USD stablecoin.

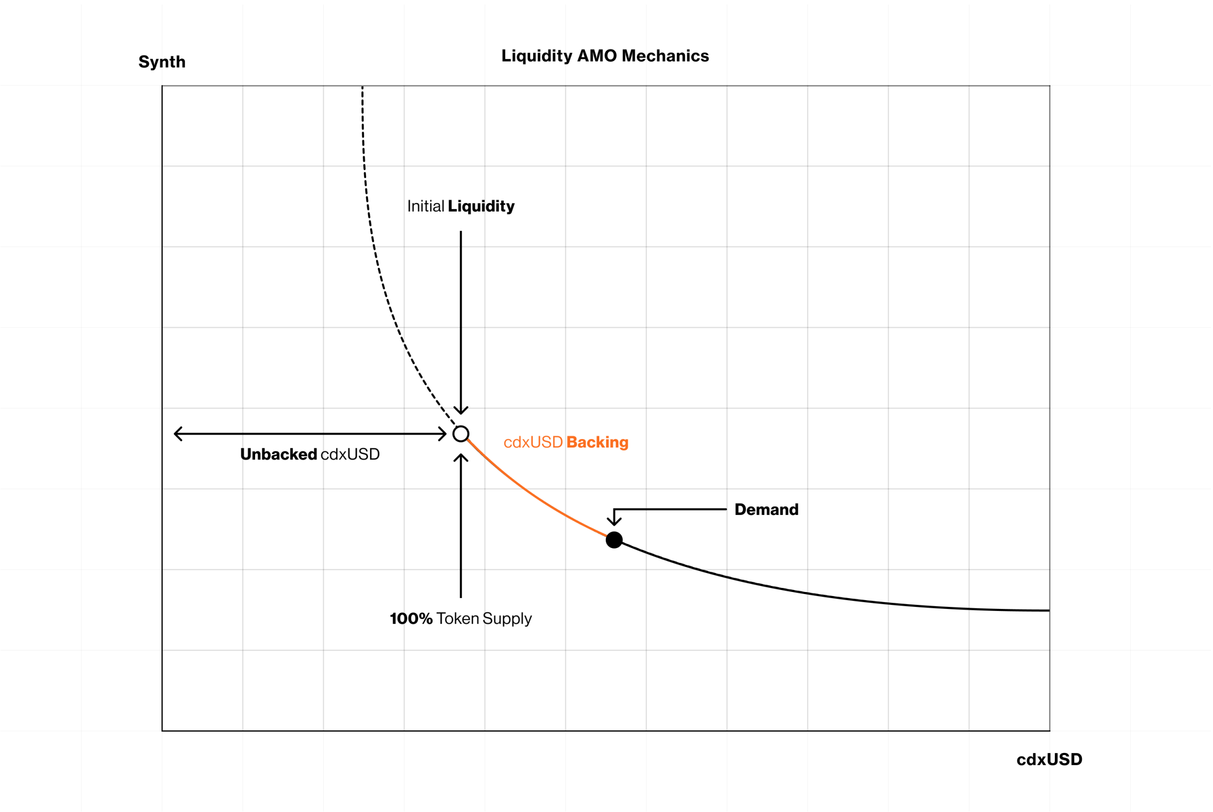


Figure 3: Liquidity AMO mechanics.

The Arbitrage AMO Facilitator monitors the price of asUSD and the balances of the linked pools. When the price of asUSD exceeds $1, the Arbitrage AMO deposits its asUSD into its linked pool and receives LP tokens. This action increases the asUSD balance in the pool, aiding in peg stabilization. Conversely, should the asUSD price fall below $1, the Arbitrage AMO is permitted to burn its LP tokens and withdraw asUSD from the pool, reducing the balance within the pool.

Any EOA or smart contract can call the update function, that deposits and withdraws asUSD via the Arbitrage AMO. Function callers are rewarded with a small share as an incentive.

4.3 Stablecoin Liquidity AMO

The Stablecoin Liquidity AMO Facilitator allows users to single stake counter-asset liquidity for core asUSD liquidity pools. The AMO pairs deposits with pre-minted asUSD and provides liquidity on the user's behalf. The LP gains trading fees and the AMO vault compounds rewards on the user's behalf, further increasing the quantity of tokens in their LP.

This Facilitator has user protections in place to mitigate malicious activities, including minimum deposit times and circuit breakers if the pool balance deviates excessively. This ensures that users do not withdraw at times that will unknowingly result in a net loss for their position. The Stablecoin Liquidity AMO's supply can not be deposited anywhere else, and should also be considered out-of-circulation.

5. Staked asUSD

5.1 Staking Module

The purpose of Staked asUSD is to help maintain the peg by providing an investment opportunity for asUSD and provide a deep native liquidity layer thanks to the Stable Pool investment. Users have the option of compounding their position at base level maturity via asUSDs, or receiving a *Relic* and the potential for additional rewards (Figure 4).

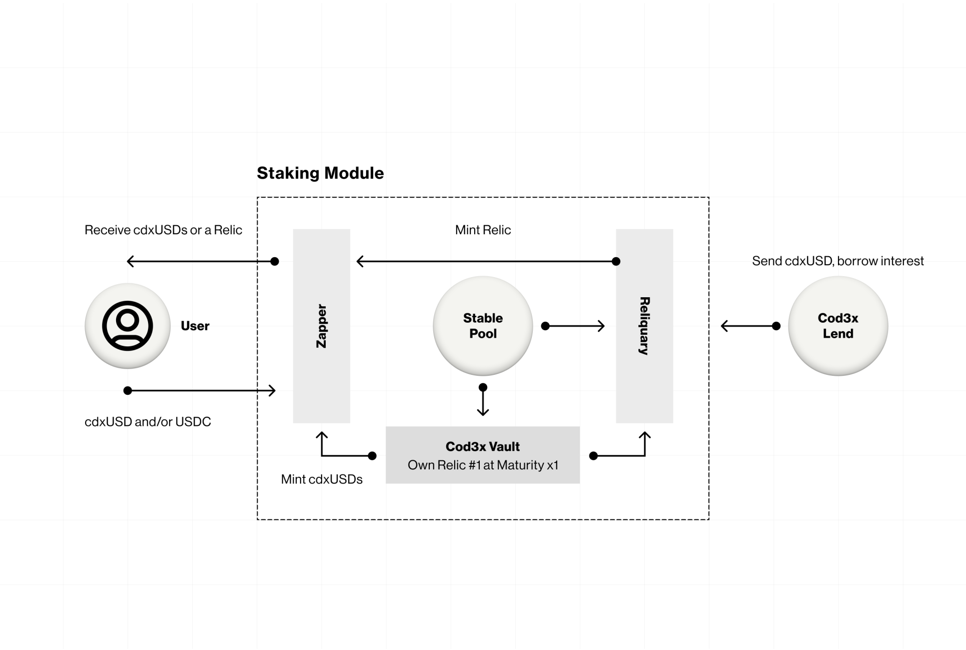


Figure 4: asUSD staking module.

The asUSD Staking Module is composed of:

- Reliquary (Cod3x Labs, 2024b): This is the staking module that deals with reward distribution.
- Cod3x Vault (Cod3x Labs, 2024a): This vault tokenizes the 1st Relic (ERC721) from Reliquary into an ERC20 (asUSDs).
- Stable Pool: This pool can be any stable pool provider. The asUSD counter-asset will predominantly be USDC or USDT, but is not limited to centralized stablecoin issuers.
- Zapper: This contract exists to simplify all staking operations and improve UX.

The Staking Module itself issues a composable ERC20 receipt representing the underlying LP token, that can be deployed throughout DeFi. Astera will offer an ERC721 staked asUSD position that implements Cod3x's Reliquary rewarder contract (Cod3x Labs, 2024b), which applies a time-based weighting to positions. Yield from borrower interest is directed to the Reliquary rewarder, closing the rate parity loop in a fully scalable and sustainable manner.

5.2 Centralization mitigation

The Stableswap pool is composed of asUSD and a counter-asset, serving as the primary liquidity layer for asUSD. To address the centralization risk posed by the counter-asset, we have implemented the following safety mechanisms:

- Depeg Detection and Response: An oracle monitors the peg status of the counter-asset. If depegging is detected, the rate update will be paused until the counter-asset re-pegs. Given the slow setting of the Integrator component of the controller, a temporary peg freeze does not introduce significant risk.

- Manual Adjustment and Migration: In the event of a prolonged depeg, Astera maintains the capability to manually adjust the rate, similar to the approach used by Aave. Additionally, Astera can facilitate the migration of all funds from asUSDs to a new stable pool with a different counter-asset.

6. Multi-Chain Functionality

6.1 Features

Majority of contemporary stablecoins can only be minted on their native chain of origin. For example, LUSD can be purchased and used on many chains, but can only be minted on ETH mainnet.

asUSD seeks to leverage LayerZero OFT technology (LayerZero Labs, 2024) to overcome this in favor of majority user experience, however we have chosen to accept specific system limitations that would otherwise compromise security (Figure 5). It is assessed that multi-chain frameworks improve user experience, but must not be a critical part of the system. That is, if the bridge fails or a network or protocol is compromised, asUSD risk must be isolated.

The asUSD bridging feature is intentionally designed for retail use only, with restrictions in place to prevent excessive bridging. These restrictions can be lifted over time as the system scales.

6.2 Risk Mitigation

The two predominant perceived risks are network liquidity and exploit contagion.

6.2.1 Network Liquidity

Network Liquidity refers to one network taking on a significant amount of collateral and issuing a significant amount of debt, that could be bridged to a network with little relative liquidity. This scenario could cause oracle manipulation, resulting in erratic interest rates and excessive liquidation.

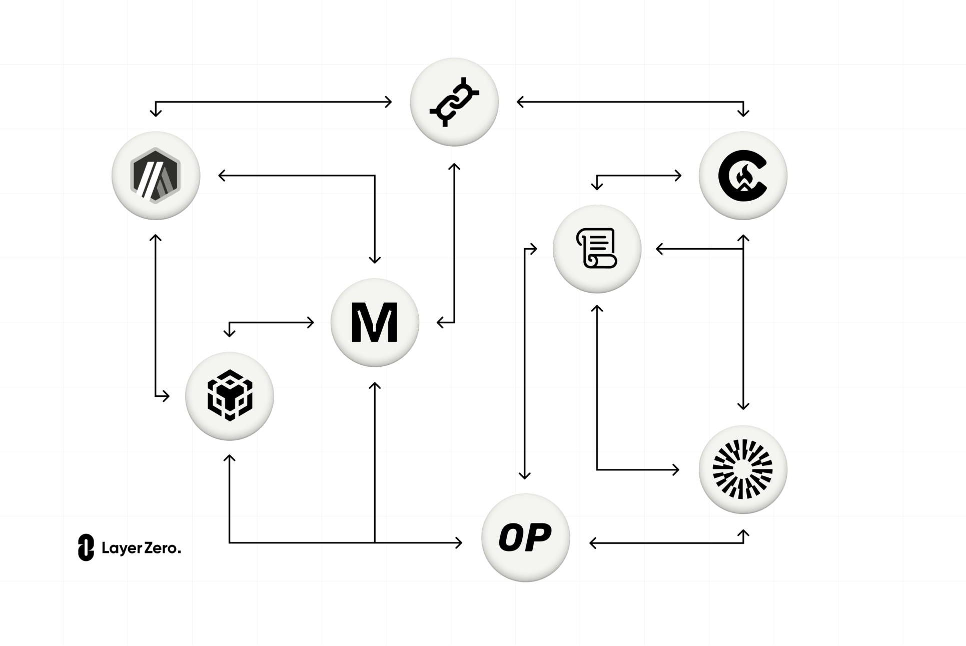


Figure 5: LayerZero multi-chain representation.

This is mitigated by limiting the supply that can be bridged, depending on conditions. Users would remain free to bridge collateral and mint asUSD on other chains, however will not be able to bridge large quantities of asUSD cross-chain. This should not impact the majority of users, and as liquidity deepens on more chains, the limit can be adjusted.

6.2.2 Exploit Contagion

Exploit Contagion refers to any potential exploit of a protocol or bridge that might result in unbacked asUSD in circulation. The effects of such an exploit are mitigated by an hourly bridging limit, containing unbacked asUSD supply on other chains.

Additional risk mitigation measures such as bridge pausing and bridge fees funding a treasury insurance fund have been developed, and their implementation may be considered in the future.

6.3 Bridge Limit Implementation

asUSD LayerZero OFT implementation allows the Astera DAO to set a maximum outflow limit 'to' a specific chain. For example, if there is a transfer from chain A to chain B, the change in balances is updated on both chains. If the transfer limit is reached, the transfer will revert on the debited chain (Figure 6).

Given a transfer of asUSD from chain A to chain B, the OFT implementation adheres to Equations 3 and 4:

$$R_{txn} = amt - amt * fee, \tag{3}$$

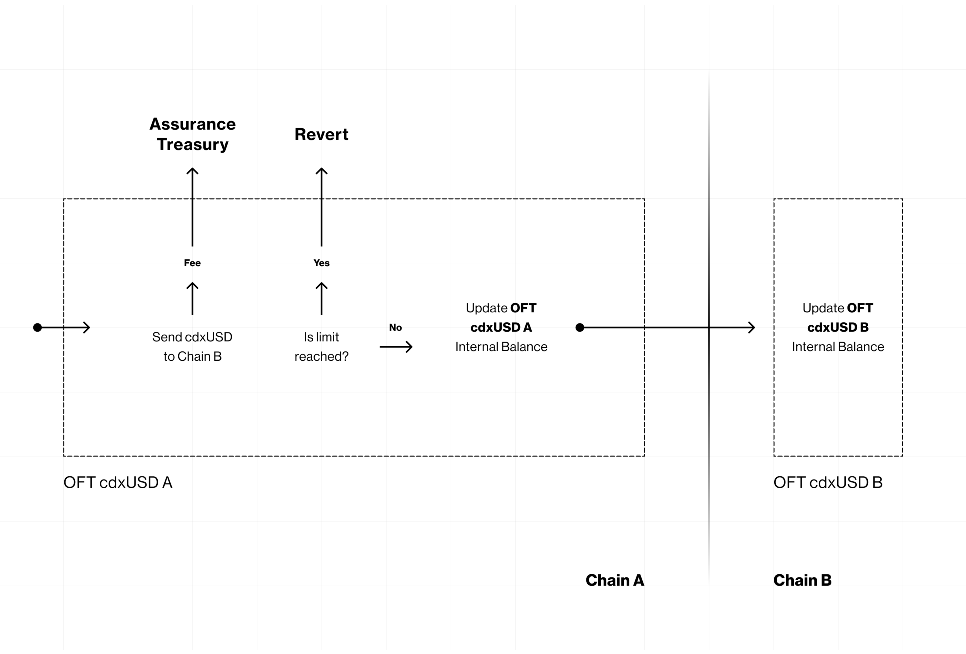


Figure 6: Bridge limit implementation.

$$L_{A,txn} = L_{A,txn-1} - R_{txn}, \tag{4}$$

on the debited chain (chain A), and Equation 5:

$$L_{B,txn} = L_{B,txn-1} + R_{txn}, \tag{5}$$

on the credited chain (chain B), where:

- R_{txn} is amount of asUSD sent to chain B at transaction txn
- amt is the amount of asUSD sent by the user
- fee is the bridge fee, taken on the debited chain
- $L_{A,txn}$ is the asUSD on chain A that is allowed to be transferred out at transaction txn
- $L_{B,txn}$ is the asUSD on that is allowed to be transferred to chain B at transaction txn.

If $L_{A,txn} \leq 0$, the transaction reverts on chain A,

6.4 Hourly Limit Rate Implementation

To limit the impact of a hack on LayerZero, a chain, or a asUSD Facilitator, a sliding hourly limit rate has been implemented in Astera asUSD LayerZero OFT. Astera DAO can set a maximum hourly transfer limit to a specific chain. The credited chain is blind to this mechanism; only the debited chain is responsible for this check. For example, if there is a transfer between chain A and chain B, the hourly transfer balance is updated on chain A. The transfer reverts if the hourly limit is reached (Figure 7).

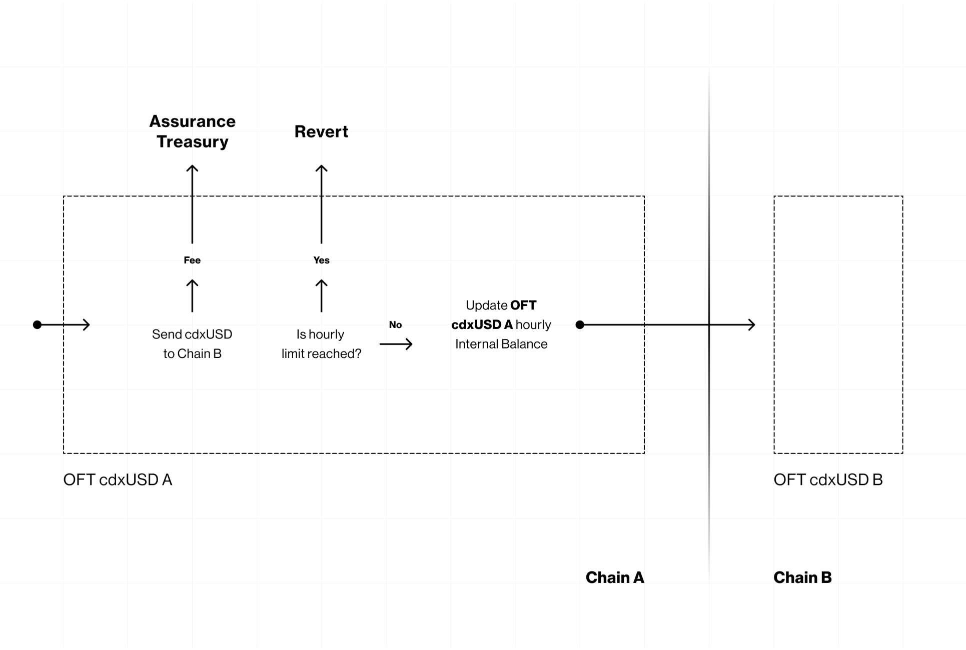


Figure 7: Hourly limit implementation.

Given a transfer of *amt* from chain A to chain B, the OFT implementation adheres to Equation 3 above, as well as Equations 6, 7, and 8:

$$\Delta T = t_{now} - T_{n-1}, \tag{6}$$

$$D(A)_{txn} = \frac{\Delta T * HL(A)}{1hour}, \tag{7}$$

$$HU(A)_{txn} = HU(A)_{txn-1} - min(D(A)_{txn}, HU(A)_{txn-1} + R_{txn}), \tag{8}$$

where:

- ΔT is the time elapsed between now and the last bridging transaction
- T_{now} is the current timestamp
- T_{n-1} is the timestamp at the last bridging transaction
- $D(A)_{txn}$ is the chain A hourly utilization proportional decrease at transaction txn.
- $HL(A)$ is the chain A sliding Hourly Limit
- $HU(A)_{txn}$ is the chain A Hourly Utilization at transaction txn.

If $HU(A)_{txn} \geq HL(A)$, the transaction reverts on chain A.

7. Conclusion

Stablecoin providers currently focus on reactive architectures in order to reduce the perceived risk of their platforms, hindering user experience. asUSD is designed to address perceived shortfalls in decentralized stablecoins by integrating new use-cases and architectures to promote yield and growth in a secure and autonomous fashion. Facilitators like Astera Lend give users more options and control over their risk, while decreasing overall systemic risk.

The hierarchical approach of prioritizing security to achieve yield and scalability, while still offering quality of life features that do not compromise the stablecoin, sets Astera apart as an industry leader in stablecoin technology.

References

Boneh, Y. (2024). Autonomous money supply strategy utilizing control theory. *SSRN Electronic Journal*. https://doi.org/10.2139/ssrn.4844212

Cod3x Labs. (2024a). Cod3x-labs/cod3x-vault. https://github.com/Cod3x-Labs/Cod3x-vault

Cod3x Labs. (2024b). Cod3x-labs/reliquary. https://github.com/Cod3x-Labs/Reliquary

Curve. (2024). Pegkeepers: Stabilizing the crvusd peg. https://docs.curve.fi/crvUSD/pegkeepers/overview/

LayerZero Labs. (2024). Layerzero whitepaper. https://layerzero.network/publications/LayerZero_Whitepaper_V2.1.0.pdf