Astro: Over-collateralized stablecoin built on hyper parallel computer

Litepaper v1.0

By Astro Labs Research.
In collaboration with Community Labs.

Contributors: Kadar Abdi, Eric Crooks, Guilherme Lopes, Bithiah Koshy

July 2024

Abstract

Astro introduces USDA, an over-collateralized stablecoin developed on AO's hyper parallel computing environment. This litepaper presents an overview of the protocol's design - emphasizing stability, scalability, and security for digital currency transactions. It employs a robust collateralization mechanism to unlock and maintain liquidity while aiming to minimize volatility. The litepaper also briefly outlines the protocol's governance model, and the economic incentives designed to foster a decentralized ecosystem. The content aims to offer a foundational understanding of Astro Protocol's operational framework and security features, setting the stage for a comprehensive full whitepaper.

Motivation

Over the past decade, blockchain technology has transformed financial services, once dominated by traditional intermediaries like banks and other institutions. Platforms like Ethereum have enabled the development of Decentralized Finance (DeFi), providing open, transparent financial tooling that have reduced operational costs and complexity for users globally. Astro's introduction of the USDA stablecoin to the Arweave ecosystem is a major step forward. USDA aims to provide stability to the permaweb's economic environment, leveraging Arweave's decentralized storage and the innovative aoComputer (AO) for smart contract-like processes, enabling secure and efficient value exchange. The rapid growth of DeFi since 2020 underscores the need for stablecoins like USDA. Existing stablecoins like USDC and USDT, along with decentralized options like MakerDAO's DAI, have enhanced transactional stability and fostered a low-volatility store of value within the Ethereum ecosystem. However, the absence of a stablecoin can hinder ecosystem development by restricting liquidity and value movement. USDA addresses these issues by supporting economic activities on AO and fostering the growth of its financial ecosystem. Astro's USDA is designed to facilitate seamless transactions, enhance liquidity, and stabilize the Arweave ecosystem, encouraging broader adoption and innovation in DeFi applications.

Contents

1 The Astro Protocol

Astro Protocol is a blockchain-based framework that enables the minting of stablecoins and synthetic assets, backed by on-chain collateral, stored and managed by processes developed within the AO compute environment. Unlike existing platforms, Astro introduces dynamic liquidation processes and stability modules to enhance system resilience and user trust.

1.1 Basic Concepts

Astro Protocol utilizes the Vault Contract as its core, where users lock in collateral to mint synthetic stablecoins. The protocol's design includes unique mechanisms for liquidation and stability, supported by real-time data from integrated oracle services. We also introduce a Protocol Hosted Wallet (PHW) and Wrapped Arweave (wAR) tokens, extending functionality and usability, making the protocol adaptable to a wide range of blockchain environments.

Notice: In this document, the terms "contract" and "process" are used interchangeably. Within the AO compute environment, processes are analogous to contracts, and this terminology reflects their functional equivalence in the context of the Astro Protocol.

1.2 Formal Definitions

- **Vault Contract (VC):** Manages the deposits, withdrawals, and issuance of synthetic assets against locked collateral.

- **Oracle Module (OM):** Provides real-time pricing data by integrating feeds from sources like ChainLink, Pyth, and RedStone.

- **Liquidation Module (LM):** Activates to handle undercollateralized positions via direct user actions or systematic protocol-driven auctions.

- **Stability Module (SM):** Manages liquidity pools to mitigate systemic risks and ensure protocol stability.

- **Protocol Hosted Wallet (PHW):** A dedicated wallet system designed to hold and manage Arweave tokens securely within the protocol.

- **Wrapped Arweave (wAR):** A synthetic version of AR transferable within the aoComputer, designed for use within the Astro Protocol and other processes on the computer.

1.3 Astro Protocol Flow

Astro's Vault Contract is the entry point for users to interact with the protocol by depositing collateral and minting synthetic stablecoins. The Vault Contract holds the information needed to calculate the USD equivalent and USDA value and fees.

Let the following be defined:

- USD-equivalent value as V

- Quantity as q

- The price feed for the given currency identifier P

- Collateralization factor as c

- Calculated fees as F

- Stability fee percentage as s

- Asset loan as L

- Amount of currency as $amount$

The current USD equivalent value of a currency is:

$$V(\text{currency}, q) = q \times P(\text{currency})$$

The USDA loan value is:

$$L(\text{currency}, q, c) = \frac{V(\text{currency}, q)}{c}$$

The current fee calculation is:

$$F(s, \text{amount}) = s \times \text{amount}$$

1.3.1 Deposit and Mint

Users deposit collateral into the Vault Contract, which allows them to mint synthetic assets proportional to the value of their deposit, while maintaining a collateralization ratio deemed 'safe' by the protocol.

1.3.2 Liquidation Processes

In the event of market downturns affecting collateral values, the Liquidation Module is triggered to secure the protocol's assets and users' positions. The Contract is responsible for calculating collateralization ratios, liquidation bonuses, total redeemable collateral, and repayment amounts.

The collateralization ratio calculation is:

$$\text{ratio} = \frac{\text{Collateral Value in USD}}{\text{USDA Debt}}$$

The liquidation bonus calculation is:

$$\text{Bonus} = \text{Liquidated Collateral} \times \frac{\text{Liquidation Bonus Percentage}}{100}$$

The total redeemable collateral calculation is:

$$\text{Total Redeemable} = \text{Liquidated Collateral} + \text{Bonus}$$

The repayment calculation is:

$$\text{Repayment} = \text{Debt} \times (1 + \text{Stability Fee})$$

2 Protocol Architecture

Astro Protocol's architecture is designed to support simple yet robust interactions among its components, optimizing for large amounts of liquidity while minimizing volatility.

2.1 Vault Contract

Central to the protocol, the Vault Contract enforces the deposits, withdrawals, and issuance of synthetic assets. It interacts directly with the Oracle Module to get real-time pricing, ensuring that the collateralization ratios are maintained within safe limits.

2.1.1 Key Functions and Role

- **Collateral Management**: The Vault Contract allows users to deposit collateral in exchange for synthetic assets or stablecoins (e.g., USDA).

- **Debt Issuance and Management**: Minting synthetic assets is enabled for users upon collateral deposit, following the protocol's determined ratios.

- **Real-Time Pricing Updates**: The Vault Contract integrates with the Oracle Module for real-time pricing updates on different collateral types. It enables accurate and fair vault management by maintaining current collateral values.

- **Liquidation Triggers**: The Vault Contract starts liquidation if collateral value drops below predefined thresholds. These can be handled directly through the Direct Liquidation Handler or, in more severe cases, passed to the Auction Module via the Protocol Liquidation Handler. Liquidation is discussed in more detail in the "Liquidation Module" section.

- **User Interaction Interfaces**: The contract offers action handlers for users to interact with their collateral and debts. It includes functions for depositing and withdrawing collateral, minting and burning synthetic assets, and managing debts.

- **Fee and Penalty Collection**: The Vault Contract calculates and collects stability fees and liquidation penalties during liquidations. These fees are crucial for compensating the protocol for the risks and maintaining overall economic stability.

2.1.2 Importance within Protocol's Architecture

The Vault Contract is vital for the operational efficiency and financial security of the Astro Protocol. It acts as the primary interface for users, facilitating all major interactions with the protocol. Its robust design ensures:

- **Security and Trust**: Users can trust the protocol with their assets, knowing that the Vault Contract enforces strict rules and transparent operations.

- **Efficiency**: The automated processes within the contract reduce the need for manual intervention, streamlining operations and minimizing errors or delays.

- **Flexibility**: By supporting various types of collateral and synthetic assets, the Vault Contract caters to a broad user base with diverse needs.

- **Stability**: Through the integration with the Stability and Oracle Modules, the contract contributes to the overall resilience of the protocol, adapting to market changes and user activities dynamically.

2.2 Liquidation Module

This module is triggered when collateral value falls below predefined thresholds, with two main components: the Direct Liquidation Handler and Protocol Liquidation Handler. It supports both immediate liquidations by users and systematic liquidations managed by the protocol itself.

2.2.1 Direct Liquidation Handler

The Direct Liquidation Handler is a specialized component of the Astro Protocol's Liquidation Module, crafted to facilitate the immediate liquidation of undercollateralized vaults when specific conditions are met. This handler enables rapid response to mitigate potential risks from fluctuating market values of collateral.

2.2.2 Key Functions and Role

- **Threshold-Based Liquidation Activation**: The Direct Liquidation Handler is triggered when a vault's collateralization ratio falls between predefined thresholds, such as less than 175% but more than 150%. For example, if a vault's collateralization ratio drops to 160%, the Direct Liquidation Handler will be activated. This trigger ensures swift liquidation to protect collateral value and system stability.

- **Execution of Liquidation**: Authorized users can directly liquidate a vault with this handler upon activation. To recover the collateral, the liquidator pays off the vault's debt, including fees and penalties.

- **Debt Settlement and Fee Calculation**: The handler calculates the repayment amount to close the vault in a direct liquidation event. This includes the debt principal (USDA Loan), stability fee (5%), and liquidation penalty (13%). These fees deter risky behavior and compensate for the associated risk.

- **Collateral Transfer and Vault Closure**: The Direct Liquidation Handler facilitates the collateral transfer upon receiving payment from the liquidator. Concurrently, it ensures that the original debt is marked as settled, and the vault is officially closed within the system's records.

- **Protocol Fee Distribution**: Collected fees will be managed by stewards via a protocol treasury until decentralized governance controls fee distribution.

- **Integration with Stability Measures**: While the Direct Liquidation Handler operates autonomously to address immediate liquidation needs, it is designed to work in harmony with other protocol components, such as the Stability Pool and the Oracle Module. This ensures actions are based on real-time market data and contribute to protocol stability and liquidity.

2.2.3 Protocol Liquidation Handler

The Protocol Liquidation Handler is an integral component of the Astro Protocol's Liquidation Module, specifically designed to manage the systematic liquidation of undercollateralized vaults when they fail to meet the required collateralization thresholds. This handler automates critical processes to maintain the system's stability and prevent potential financial crises within the protocol.

2.2.4 Key Functions and Role

- **Automated Liquidation Initiation**: The handler is activated when a vault's collateralization ratio falls significantly, specifically below the minimum threshold, such as less than 150%. For instance, if a vault's collateralization ratio drops to 130%, the Protocol Liquidation Handler will be triggered instead of the Direct Liquidation Handler. This automated trigger ensures timely intervention to mitigate risks associated with declining collateral values.

- **Auction Process Management**: For severely undercollateralized vaults, the handler initiates an auction to liquidate the collateral efficiently. It interacts with the Auction Module, setting up the auction's parameters such as starting price, price decrement rates, and auction duration based on the prevailing market conditions and the vault's debt levels. Auctions are discussed in more detail in the "Auction Module" section.

- **Debt and Fee Handling**: The handler calculates the total amount due for the auction, including the principal debt, stability fees, and liquidation penalties. This total forms the recovery target for the auction, ensuring that the protocol recoups the necessary funds to cover the defaulted loan.

- **Vault Closure and Administration**: Post-triggering an auction, the handler is responsible for closing the defaulting vault. It transfers the collateral to the auction mechanism and, following the auction, manages the allocation of the recovered funds and finalizes the closure of the vault within the protocol's ledger.

- **Contribution to Systemic Stability**: The Protocol Liquidation Handler plays a crucial role in maintaining the overall health and stability of Astro Protocol by preventing losses that could escalate into broader systemic risks. This is achieved through efficient and orderly liquidation processes, even under adverse market conditions.

- **Integration with Other Protocol Modules**: Utilizing real-time data from the Oracle Module, the handler ensures that liquidation prices reflect current market values, enhancing the chances of successful debt recovery. It may also interact with the Stability Module to utilize or replenish protocol reserves, depending on the outcomes of the liquidation process.

2.3   Stability Module

The Stability Module is integral for maintaining the health of the protocol during market volatility. It includes a Stability Pool where users can deposit stablecoins to earn rewards and a Collateral Pool that enhances liquidity and supports the protocol's stability. It acts as a financial buffer against market volatility and systemic risks by managing liquidity pools and providing mechanisms to mitigate potential defaults and liquidations.

2.3.1   Key Functions and Role

- **Liquidity Management**: The Stability Module aggregates user deposits in the form of stablecoins (e.g., USDC). These deposits are used to support the protocol during periods of high demand for liquidation or when additional liquidity is necessary to maintain operations, ensuring that the protocol can cover its liabilities efficiently.

- **Risk Mitigation**: By pooling resources, the Stability Module can intervene in liquidation events to purchase undercollateralized assets at a discount. By preventing large-scale sell-offs, this intervention stabilizes the market and safeguards collateral values.

- **Reward Distribution**: Users who contribute to the Stability Pool will be rewarded with AST tokens or other incentives, proportionate to their share of the pool over time. These rewards compensate users for the temporary loss of liquidity during fund usage in stability operations.

- **Integration with Oracle Module**: The Stability Module interacts with the Oracle Module for accurate pricing updates on assets. Current market values are used to make decisions about liquidation or collateral purchases, optimizing results.

- **Automated Liquidation Participation**: The Stability Module automatically purchases distressed assets if a vault lacks collateral. This process minimizes default impact on the protocol's financial health by resolving them quickly.

- **Governance and Protocol Support**: Governance votes determine where to allocate funds from the Stability Module. This can include funding development, enhancing protocol security, or other activities that contribute to the long-term sustainability of the system.

2.3.2   Stability Pool

The Stability Pool in the Astro Protocol is designed to act as a financial buffer that enhances the system's resilience against defaults and helps maintain overall liquidity and stability. This component is critical for absorbing shocks from market volatility and managing undercollateralized loans in a decentralized finance environment.

The Stability Pool collects deposits in the form of stablecoins, such as USDA, from users who wish to support the protocol's stability and earn rewards. These funds are used to purchase collateral from liquidated vaults, effectively absorbing the debt from undercollateralized loans. When the Vault Contract or Auction Module processes liquidations, the Stability Pool is often the first line of defense. It uses its pooled resources to buy out distressed collateral at a discounted rate, helping to stabilize the protocol's economy and mitigate potential losses.

Stability Pool parameters, such as reward distribution rates, intervention thresholds, and other operational policies, are often governed by the protocol's DAO. This allows stakeholders to participate in decision-making processes, aligning the pool's strategies with the broader interests of the community.

2.3.3 Stability Pool Liquidation Scenario in Astro Protocol

1. **Assumption Setup:**

   - Stability Pool Total Deposit: 1,000,000 USDA.
   - Bob's Contribution: 100,000 USDA (Bob contributes to the Stability Pool, giving him a 10% share in the pool).
   - Alice's Vault Details: Alice's vault gets liquidated, which has a debt of 20,000 USDA and collateral of 400 wAR, with the price of wAR being \$75 per wAR.
   - The collateralization ratio for protocol liquidation to occur is 150

2. **Impact of Liquidation on Bob's Deposit:**

   (a) **Bob's Share in the Pool:**

   $$\text{Bob's Share} = \frac{\text{Bob's Contribution}}{\text{Total Pool Deposit}} = \frac{100,000 \text{ USDA}}{1,000,000 \text{ USDA}} = 10\%$$

   (b) **Debt from Alice's Liquidated Vault:**

   $$\text{Debt} = 20,000 \text{ USDA}$$

   (c) **Bob's Contribution to Repaying Debt:**

   $$\text{Bob's Contribution to Debt} = \text{Bob's Share} \times \text{Debt} = 10\% \times 20,000 = 2,000 \text{ USDA}$$

   (d) **Remaining USDA in Bob's Deposit Post-Liquidation:**

   $$\begin{aligned}\text{Remaining USDA} &= \text{Bob's Contribution} - \text{Bob's Contribution to Debt} \\ &= 100,000 \text{ USDA} - 2,000 \text{ USDA} \\ &= 98,000 \text{ USDA}\end{aligned}$$

   (e) **Calculating Bob's Gain in Collateral:**
   - **Collateral from Liquidated Vault:**

   $$\text{Collateral} = 400 \text{ wAR}$$

   - **Bob's Share of Collateral:**

   $$\begin{aligned}\text{Bob's Share of Collateral} &= \text{Bob's Share} \times \text{Collateral} \\ &= 10\% \times 400 \\ &= 40 \text{ wAR}\end{aligned}$$

   - **Financial Evaluation of the Transaction:**

– **Value of wAR Received:**

$$\text{Value of wAR Received} = \text{Bob's Share of Collateral}$$
$$\times \text{Price per wAR}$$
$$= 40 \times \$75$$
$$= \$3,000$$

– **Net Gain:**

$$\text{Net Gain} = \text{Value of wAR Received}$$
$$- \text{Bob's Contribution to Debt}$$
$$= \$3,000 - \$2,000$$
$$= \$1,000$$

3. **Post-Liquidation Scenario:**

- Bob's remaining deposit in the Stability Pool is 98,000 USDA.
- Bob additionally acquires 40 wAR, valued at $3,000.
- Bob realizes a net gain of $1,000 from this single liquidation event.

2.4 Peg Stability Handler

The Peg Stability Handler is a critical component designed to maintain the stability of the USDA peg within the Astro Protocol. It targets vaults with a Collateral Ratio (CR) <175%. If there are no such vaults, the handler includes the lowest loan-to-value (LTV) vaults. The dual criteria approach enhances the protocol's stability by ensuring flexibility in selecting vaults for redemption.

Users or automated agents can redeem USDA for wAR using the Peg Stability Handler. The process includes identifying vaults, processing redemption requests, and executing adjustments. This section outlines the detailed steps and benefits of the Peg Stability Handler.

2.4.1 Identifying Eligible Vaults

The first step in the Peg Stability Handler's operation is to identify vaults eligible for redemption. This involves the following criteria and steps:

Criteria:

- **Primary:** Vaults with a Collateral Ratio (CR) of less than 175%.

- **Secondary:** If no vaults meet the primary criteria, select vaults based on the lowest Loan-to-Value (LTV) ratios.

2.4.2 Key Functions and Role:

1. **Data Collection:** Retrieve current data on each vault's collateral value and the amount of USDA issued.

2. **Calculate CR and LTV:**

$$\text{CR} = \left(\frac{\text{Value of Collateral}}{\text{Value of USDA Issued}} \right) \times 100\%$$

$$\text{LTV} = \left(\frac{\text{Amount of USDA Issued}}{\text{Value of Collateral}} \right) \times 100\%$$

3. **Filter Vaults:** Initially filter for vaults where CR <175%. If no vaults meet this criterion, select vaults with the lowest LTV.

2.4.3   Redemption Requests

Once eligible vaults are identified, the Peg Stability Handler facilitates the redemption of USDA at par value for wAR. This process includes the following steps:

1. **Interaction:** Users or automated agents interact with the protocol to request the redemption of USDA at its par value for wAR from the selected vaults.

2. **Steps:**

   (a) **Request Initiation:** Users or agents submit a redemption request. Validate the request to ensure the vault meets the specified criteria (CR <175% or lowest LTV).

   (b) **Redemption Execution:** Transfer the equivalent amount of wAR from the vault to the user and reduce the debt by the amount of USDA redeemed, thereby increasing the vault's CR.

2.4.4   Collect & Adjust Mechanism

The collect and adjust mechanism ensures that the collateral ratio is impacted positively by the redemption of wAR, thereby pushing the CR higher and reducing the debt-to-collateral ratio of the affected vaults. The process involves:

1. **Collect wAR:** The protocol collects wAR from the selected vaults.

2. **Adjust CR:** The USDA used for redemption is removed from the vault's debt, which increases the CR by reducing the debt relative to the collateral.

2.4.5   Benefits

The Peg Stability Handler provides several key benefits. Users can profit and stabilize the USDA peg through arbitrage within Astro Protocol. It aids in vault liquidations, improving their health by adjusting CR and debt-to-collateral ratio. This dual action enhances the overall stability of the protocol.

2.4.6   Process Flow & Scenario

The following flow illustrates the operation of the Peg Stability Handler:

1. **User Initiates Redemption:** A user or automated agent initiates a redemption request through the protocol interface.

2. **Identify Eligible Vaults:** The protocol checks for vaults with CR <175%. If none are found, it looks for the vaults with the lowest LTV.

   - **Example:** If Vault A has a CR of 160% and Vault B has an LTV of 40%, Vault A is prioritized for redemption.

3. **Validate and Process Redemption:** The request is validated to ensure the vault meets the criteria. The user's USDA is accepted, and the equivalent value in wAR is transferred from the vault to the user.

4. **Adjust CR:** The USDA used in the redemption is removed from the vault's debt, increasing the CR and improving the vault's stability.

5. **Update Vault Status:** The vault's records are updated to reflect the new amounts of USDA issued and wAR collateral. The CR of the vault is recalculated and monitored.

   The Peg Stability Handler is an essential mechanism for maintaining the stability of USDA within the Astro Protocol. Targeting vaults based on CR and LTV criteria improves redemption efficiency. This mechanism facilitates arbitrage and supports partial liquidations, improving protocol health and stability. Positively impacting the collateral ratio supports protocol resilience and USDA's stable value.

2.5   Auction Module

The Auction Module is an essential component of the Astro Protocol, designed to manage the auctioning of collateral from undercollateralized vaults. This module facilitates efficient asset liquidation, promoting debt recovery and financial stability. It implements Dutch-style auctions to enable broader market participation in liquidations, promoting fair market prices and efficient collateral redistribution.

2.5.1   Key Functions and Role

- **Auction Initiation and Management**: The Auction Module is activated for vaults with severely undercollateralized collateral. It oversees the entire auction process, ensuring adherence to rules and protocols.

- **Dynamic Pricing Strategy**: The module implements a dynamic pricing mechanism where the starting price is set above the current market value (typically 20-30% higher) to maximize debt recovery. The price decreases based on a predefined decrement percentage until the auction ends.

- **Debt Recovery and Fee Handling**: Auctions address debts of the liquidated vault, including principal, stability fees, and liquidation penalties. The module guarantees payment of financial obligations from auction proceeds.

- **Transparent and Fair Bidding Process**: Bidders participate by submitting bids aligned with the Auction Module's price. The process promotes transparency and fair participation. The module uses a decremental pricing strategy to update bid prices at regular intervals.

- **Integration with Oracle Module**: To ensure that auctions start at a reasonable price relative to the market, the Auction Module integrates closely with the Oracle Module for accurate and timely asset valuations. This integration sets and adjusts auction prices.

- **Handling Auction Outcomes**: At the conclusion of an auction, the module handles the transfer of collateral to the highest bidder and ensures the distribution of funds to cover the debts associated with the liquidated vault. Surplus funds are either returned or redirected as per rules.

2.5.2   Auction Mechanism

Below are variables and formulas used to calculate auction parameters and execute auctions.

Let the following be defined:

- Quantity of collateral (e.g., number of wAR tokens) as q

- Price feed for the collateral currency as P

- Collateral value in USDA as V

- Collateralization factor (a multiplier based on risk assessment) as c

- Stability fee percentage as s

- USDA Loan (debt) as d

- Total fees calculated as F

- Debt including fees as d_f

- Time as t

- Adjusted value of the collateral as V_{adj}

1. **Collateral Value Calculation:**
$$V = q \times P$$

   Here, V represents the current market value of the collateral in USDA, calculated as the product of the quantity of collateral q and its current market price per unit P.

2. **USDA Value Calculation Adjusted for Collateralization:**

$$V_{\text{adj}} = c \times V$$

   The adjusted value of the collateral V_{adj} considers the collateralization factor c, which adjusts the raw market value to account for risk factors associated with the collateral type.

3. **Fees Calculation:**
$$F = \left(\frac{s}{100}\right) \times d$$

   The total fees F are calculated as a percentage s of the debt d. This includes the stability fee and potentially other fees like liquidation penalties.

4. **Debt Including Fees Calculation:**
$$d_f = d + F$$

   The total amount needed to clear the debt, d_f, includes the original debt d plus the calculated fees F.

Auction Execution Process

1. **Auction Start Price Calculation:**

$$\text{start\_price} = P \times (\text{markup})$$

   The auction's start price is set higher than the current market price P by a certain markup percentage (e.g., 20 to 30%) to maximize the potential recovery amount.

2. **Price Decrement Over Time:**

$$\text{current\_price} = \text{start\_price} - (\text{decay\_factor} \times t)$$

   The current price current_price is decremented over time based on a decay factor that is calculated as a percentage reduction every set interval until it reaches or is still sufficient to cover d_f.

3. **Determine the Auction Closure Condition:**

$$d_f \leq \text{current\_price} \times q$$

   When a bidder pays the current_price $\times q$ and this amount covers at least d_f, the auction is considered successful. The bidder receives the collateral, and the debt d is considered settled.

4. **Auction Closure:**
$$(\text{start\_price} \times (1 - \text{decay\_factor})^t \times q) \geq d_f$$

   The auction closes successfully when the amount paid by the bidder, which is the current price of the asset multiplied by the quantity, is greater than or equal to the total debt including fees.

2.6 Oracle Module & Service

The Oracle Module is a pivotal component of the Astro Protocol, tasked with providing accurate and timely market data to various other parts of the system. This module ensures that all financial operations within the protocol are based on the most current and reliable asset valuations.

2.6.1 Key Functions and Role

- **Real-Time Data Feeds**: The Oracle Module collects price data from multiple sources to minimize manipulation and errors. This data is crucial for the accurate valuation of collateral across the protocol.

- **Integration with Vault Contract**: Real-time pricing updates are provided to the Vault Contract by the module, allowing for dynamic assessment of collateral values. This integration ensures proper collateralization and triggers liquidation if values drop.

- **Support for Liquidation and Auction Modules**: The Oracle Module safeguards the protocol's financial integrity by ensuring fair valuation of assets during liquidation and auctions.

- **Price Update Mechanisms**: Utilizing advanced algorithms and time-weighted averages, the Oracle Module updates prices at predefined intervals or in response to significant market movements. It helps maintain stability and predictability for protocol participants.

- **Security and Reliability Enhancements**: The module incorporates features to detect and mitigate potential threats such as flash loan attacks or unusual market activity. This proactive security approach preserves the resilience and trustworthiness of the protocol.

- **Governance and Updates**: The protocol's decentralized governance framework governs decisions on price feed additions or adjustments. Token holders shape the Oracle Module's evolution in line with community interests and market environment.

2.6.2 Oracle Module Price Update Mechanism

The Oracle Module operates by maintaining a consistent update cycle governed by predefined intervals. This ensures that all dependent contracts within the Astro Protocol receive timely and accurate market data. The Oracle Module holds the necessary information to feed accurate prices of collateral to the protocol.

Let the following be defined:

- **TimeDelay**: The fixed interval between price updates (typically one hour).

- **LastUpdateTime**: The timestamp when the price was last updated.

- **CurrentPrice**: The most recent price of the collateral.

- **NextPrice**: The upcoming price of the collateral, set to be published after the TimeDelay.

- **Whitelists**: A list of contract addresses that are authorized to receive updated prices after each interval.

Price Update Process The price update process can be described using the following steps and formulas:

1. **Initiating Price Updates:** The Oracle Module is triggered by a regular call to an action handler (e.g., Poke). This can be automated through a cron job or similar scheduling mechanism to occur at LastUpdateTime + TimeDelay.

2. **Updating Current and Next Prices:** When the Poke function is called, the Oracle Module performs the following operations:

   (a) **Set Current Price:**
   $$CurrentPrice = NextPrice$$

(b) **Fetch New Price:** The new price is obtained from an aggregated feed of external sources or directly from a trusted oracle service.

(c) **Set Next Price:**
$$\text{NextPrice} = \text{newly obtained price}$$

3. **Broadcasting the Price Update:** After updating the prices, the Oracle Module sends the new CurrentPrice to all contracts listed in the Whitelists. This ensures that all relevant parts of the Astro Protocol, such as the Vault Contract, are operating with the most recent price data.

2.7 Protocol Hosted Wallet (PHW)

The Protocol Hosted Wallet (PHW) is an essential component of the Astro Protocol, designed to streamline user interactions with Arweave and AO layers by managing assets directly within the protocol itself. This dedicated wallet system simplifies the user experience and enhances security by maintaining a controlled environment for asset transactions and management.

The PHW serves a critical role in the Astro Protocol by managing deposited Arweave tokens (AR) securely. Given the importance of the PHW in the ecosystem, strategic decisions regarding its governance and legal framework are paramount to ensure sustainability, security, and legal compliance.

In the early days, a community-driven model will be used so development and maintenance will be as a public good, supported by a consortium of teams from within the ecosystem, such as the Astro Labs team and other core members. Operational and maintenance responsibilities would fall to the collective comprising core community members and affiliate service providers. This structure would allow for shared responsibility, ensuring that the wallet's management remains transparent, decentralized, and aligned with the community's interests.

The PHW serves as a gateway to assets into AO, taking charge of managing users' AR deposits. It secures these assets through predefined wallets, enhancing security and simplifying operations for users within the ecosystem. Similar to the Wrapped Bitcoin (WBTC) model with BitGo as the primary custodian, consideration is being given to appointing a third-party custodial partner to oversee the development of new wallets. This partnership would improve transparency and efficiency, particularly in wrapping AR tokens for use on AO compute environments.

2.7.1 Legal and Governance Structure

The PHW may be governed by two legal entities: a foundation and a trustee. The foundation would manage overarching governance, while the trustee would oversee daily operations and legal responsibilities. This dual-entity approach facilitates structured management of the PHW, with the foundation acting as a non-profit steward for the community in commercial dealings with service providers.

2.7.2 Bankruptcy Remote Vehicle

Incorporating the PHW within a trust's legal framework would make it bankruptcy remote, safeguarding it against the insolvency of associated entities. This setup provides a robust legal buffer, enhancing asset security for users.

Noting that as the protocol matures and grows, the needs will change for both the community at large and Astro itself, thus these considerations and approaches may differ and be adjusted as the landscape changes.

3 Risk Factors and Mitigation

3.1 Liquidation Risk

Liquidation risk occurs when the value of the collateral backing USDA drops significantly, making it insufficient to cover the issued stablecoins. This could lead to forced liquidation of collateral assets, causing instability in the protocol.

Mitigation Strategies:

- **Over-Collateralization**: Astro ensures that all USDA stablecoins are over-collateralized. The value of the collateral always exceeds the stablecoins issued, providing a buffer against market volatility.

- **Automated Liquidation Mechanisms**: Astro employs automated systems to monitor collateral levels and initiate liquidations when values fall below a threshold. This maintains stablecoin stability by ensuring adequate backing.

- **Direct Liquidation Handler**: It enables immediate liquidation of undercollateralized vaults under specific conditions. A vault is liquidated if its collateralization ratio drops below set thresholds, and users can do so by paying off the debt, including fees and penalties. The handler then transfers the collateral to the liquidator's account and closes the vault, ensuring stability.

- **Protocol Liquidation Handler**: This component automates the liquidation of undercollateralized vaults to maintain system stability. It initiates auctions, calculates the total due (including fees and penalties), and recovers funds for the protocol. The handler's integration with the Auction Module ensures efficient liquidation under adverse market conditions.

- **Stability Module and Stability Pool**: The Stability Module, including the Stability Pool, acts as a financial buffer during market volatility. Stablecoin deposits are used to support the protocol during high liquidation demand or liquidity needs. The Stability Pool stabilizes the market and prevents sell-offs by purchasing undercollateralized assets at a discount during liquidation events. This intervention ensures quick resolution of potential defaults, minimizing financial health.

- **Auction Model**: The Auction Module manages the auctioning of collateral from undercollateralized vaults through Dutch-style auctions, ensuring efficient liquidation and fair market prices for collateral.

3.2 Custodial & Distributed Wallets Risk (Protocol Hosted Wallet)

Custodial risk involves potential loss or mismanagement of collateral assets. If custodians fail or act maliciously, it could jeopardize asset security.

Mitigation Strategies:

- **Protocol Hosted Wallet (PHW)**: Astro uses a Protocol Hosted Wallet (PHW) to manage assets directly within the protocol. This dedicated wallet system enhances security and simplifies user interactions by maintaining a controlled environment for asset transactions.

- **Trusted Custodians**: In cases where third-party custodial services are used, Astro collaborates with reputable custodial service providers known for robust security measures. Similar to the Wrapped Bitcoin (WBTC) model with BitGo, a third-party custodial partner may oversee new wallet development, enhancing transparency and efficiency.

- **Community-Driven Governance**: The PHW is supported by a consortium of ecosystem teams, such as the Astro Labs team and core members, ensuring that the wallet's management remains transparent, decentralized, and aligned with the community's interests.

- **Legal and Governance Structure**: The PHW may be governed by a foundation and a trustee to manage overarching governance and daily operations, respectively. This dual-entity approach facilitates structured management and legal compliance, ensuring sustainability and security.

- **Bankruptcy Remote Vehicle**: Incorporating the PHW and custodial wallets within a trust's legal framework makes it bankruptcy remote, safeguarding it against the insolvency of associated entities, thus enhancing asset security.

3.3 Oracle Risk

Oracle risk involves the potential for inaccurate or delayed market data from oracles, which could lead to improper valuations of collateral and subsequent financial instability within the protocol.

Mitigation Strategies:

- **Real-Time Data Feeds**: The Oracle Module aggregates price data from multiple external sources, ensuring a robust and diversified feed that reduces the risk of manipulation or errors.

- **Price Update Mechanisms**: Utilizing advanced algorithms and time-weighted averages, the Oracle Module updates prices at predefined intervals or in response to significant market movements, maintaining a stable and predictable environment.

- **Security and Reliability Enhancements**: The module incorporates features to detect and mitigate potential threats such as incorrect prices from malicious actor feeds or unusual market activity, preserving the protocol's resilience. Moreover, the Oracle Module and its dependent contracts verify each other's identity before price data is updated and used. The use of battle-tested oracle services and feeds will be critical in maintaining accurate and reliable data.

4 Governance of the Protocol

Astro Protocol's governance model will be designed to evolve from being initially stewarded to fully decentralized, mirroring successful frameworks like MakerDAO's. Astro Labs will have a major role as a contributor, overseen by the Astro Foundation. The protocol's development will introduce the Astro Token (AST) for governance, with a clear roadmap towards decentralization.

Executive Voting and Governance Polling empower AST holders to participate in key decision-making processes for protocol upgrades, risk management, and other critical decisions. This approach strives for stability, transparency, and resilience in the Astro Protocol with an inclusive governance structure.

5 Conclusion

The Astro Protocol uses an innovative compute environment to introduce the USDA stablecoin, which is crafted to enhance liquidity and ensure stability across the ecosystem. The protocol's architecture prioritizes adaptability, considering potential changes in use-cases, community dynamics, and technology. Astro's modular approach ensures continuous support for stable transactions, evolving with the ecosystem's growth.

Astro brings two significant innovations to enhance the DeFi ecosystem:

- **Stable Value Preservation**: USDA provides a stable value against volatile market conditions, aiding in financial planning and risk management for users across the network.

- **Enhanced Liquidity Solutions**: By integrating with the aoComputer (AO), Astro allows for efficient and secure smart contract executions, bolstering the liquidity and usability of USDA within various financial applications.

Following its deployment, Astro will continue to advance its commitment to decentralization with the introduction of additional features. A Governance Model will be implemented, allowing users to participate actively in the evolution of the protocol:

- **Protocol Level**: An introduction of AST (Astro Token) for overarching updates and strategic decisions, enhancing user involvement and transparency.

- **Customizable Modules**: Enabling users to adapt and deploy tailored solutions based on Astro's core smart contracts, fostering innovation and diversification within the ecosystem.

Through these measures, Astro aims to establish a resilient and adaptive framework that not only supports the growth of aoComputer (AO) but also sets a new standard for stability and user empowerment in the DeFi sector.

6 Acknowledgements

- MakerDAO SAI Whitepaper. `https://makerdao.com/en/whitepaper/sai`

- MakerDAO DAI Whitepaper. `https://makerdao.com/pt-BR/whitepaper`

- Liquity Whitepaper. `https://docsend.com/view/mk99y5abnr8yqxws`

7 Legal Disclaimer

BEFORE DOWNLOADING, PRINTING OR VIEWING LITEPAPER AND/OR ANCILLARY INFORMATION CONTAINED HEREIN, PLEASE CAREFULLY READ THIS DISCLAIMER. BY ACCESSING THE INFORMATION, YOU AGREE TO AND ACKNOWLEDGE THAT YOU HAVE READ AND ACCEPT THESE TERMS AND CONDITIONS OF ACCESS. IF YOU DO NOT UNDERSTAND THE INFORMATION CONTAINED IN THIS LITEPAPER, YOU SHOULD CONSULT YOUR PROFESSIONAL ADVISER WITHOUT DELAY.

7.1 Information purposes only

This Litepaper is for general information purposes only and may be subject to change without prior notice. Astro Labs Research Ltd ("Astro Labs") and any current or future affiliated entities, their managers, directors, officers, employees, advisors, consultants, agents, or any other person (the "Astro Team") do not make or purport to make, and hereby disclaim, any representation, undertaking or warranty in any form whatsoever to any person or entity, including any representation, undertaking or warranty concerning the accuracy and completeness of any of the information set out in this Litepaper, which is issued by Astro Labs in good faith and is provided for reference purposes only. Nothing contained in this Litepaper is or may be relied upon as a promise, representation, or undertaking as to the future performance of the Astro Token. By continuing to use the information contained in this Litepaper, you agree to the exclusion by Astro Labs, to the extent permitted by applicable law and regulation, of any and all liability for any direct, indirect, punitive, consequential, incidental, special or other damages, including, without limitation, loss of profits, revenue or data arising out of or relating to your use of and our provision of this Litepaper.

Astro Labs does not guarantee the accuracy of any information and disclaims all representations and warranties, whether express or implied, to the extent permitted by applicable law and regulation. Further, circumstances may change, and this Litepaper may become outdated. Astro Labs is under no obligation to update or correct this Litepaper in connection therewith.

This Litepaper may be translated into a language other than English for information purposes only. In such case, the English language version shall always prevail over the translated versions of this Litepaper.

7.2 No contractual relationship

The information herein does not imply any elements of a contractual relationship nor form the basis of or be relied upon in connection with, any investment decision. The information set out in this Litepaper is not legally binding and is for community discussion only. It provides an initial overview of certain business and technical essentials underlying the Astro Protocol. It does not constitute advice or personal recommendation for which Astro Labs would owe a duty of suitability. If you are unsure about the meaning of any information provided in this Litepaper, please consult your financial or other professional adviser. Any offering or sale

of Astro Tokens shall be governed by separate terms and conditions. In the event of a conflict between this Litepaper and the applicable terms and conditions, the terms and conditions shall prevail.

7.3 Third-party information

Astro Labs accepts no liability for damages, whether indirect or consequential, of any kind arising from the use, reference, or reliance on the contents of this Litepaper. This Litepaper may contain references to data, industry publications, and/or third-party research. No warranty is given to the accuracy and completeness of such third-party information. Neither the third-party information, its inferences nor its assumptions have been independently verified.

7.4 No offer of securities

This Litepaper does not constitute a prospectus, an offer of any sort including securities, a solicitation for investment in securities in any jurisdiction, or any offer to sell any product, item, or asset, whether digital or otherwise. No information in this Litepaper should be considered as business, legal, financial, or tax advice regarding the Astro Protocol or the Astro Token. Please consult your own legal, financial, tax, or another professional adviser regarding this project and the Astro Token. Astro Tokens do not in any way represent any shareholding, participation, right, title, or interest in any entity including Astro Labs or its affiliates, undertaking, or enterprise. Astro Tokens do not entitle anyone to any promise of dividends, revenue, fees, profits, or investment returns.

7.5 Risk associated with the purchase of Astro Tokens

Prospective purchasers of Astro Tokens should evaluate all risks and uncertainties associated with the purchase of Astro Tokens. This Litepaper does not constitute advice nor a recommendation by the Astro Team or Astro Labs on the merits of purchasing or holding Astro Tokens or any other token or cryptocurrency. Such purchase and holding carry substantial risks that could lead to a loss of part, or all, of the funds invested. As of the date hereof, the Astro Token has no known potential uses outside of the Astro Protocol. No promises of future performance, value, or utility are or will be made concerning the Astro Token, including no promise that the Astro Protocol will be launched and no guarantee that the Astro Tokens will have any intrinsic value. Astro Tokens are designed and intended for future use on public Astro Protocol, for governance to allow Astro Token holders to participate in key decision-making processes for protocol upgrades, risk management and other critical decisions. The Astro Team may decide to amend the intended functionality of Astro Tokens for any reason, including to ensure compliance with any legal or regulatory requirements to which it is subject, which may affect the utility or any other properties of the Astro Tokens. Any Astro Token could be impacted by regulatory action, including potential restrictions on the ownership, use, or possession of such tokens. Regulators or other competent authorities may demand that the mechanics of the Astro Tokens be altered, entirely or in part.