Aphra-Cashflow Generation through Peg Stability

AphraFinance
Version 1.0

dao@aphra.finance

Abstract. Decentralized finance has emerged to be a relevant player in the crypto world. In this field, stablecoins are an important tool to avoid asset price fluctuations as best as possible thus generating stable yields for investors. Recently, especially decentralized algorithmic stablecoins have gained popularity in the community. However, their drawback is based on missing price stability due to the lack of asset liquidity. Such low liquidity rates could lead to market manipulation, long peg rebalancing times, and potential losses for the end-user. The APHRA engine tackles this problem by providing a programmable way to offer liquidity to stablecoin projects. This engine consists of a continuous integration platform facilitating workflow development that can be used to balance stablecoin pegs. Project-owned liquidity applied for peg equilibration is generated from cashflow-generating assets that are fed back into our ecosystem to ensure long-term liquidity. The engine is managed through a decentralized autonomous organisation and governance is obtained by ownership of the vote-escrowed APHRA governance token. Our engine provides a solution to an important problem within the decentralized finance space, enabling its sustainable upscaling, and thus greater adoption in the near future.

Keywords: Decentralized Finance · Stablecoin · Peg Stability.

1 Introduction

Since its appearance in late 2017, the total USD value locked (TVL) in decentralized finance (DeFi) protocols has seen an exponential growth[1] giving it the potential to rise to one of the most important cornerstones in the crypto world in the upcoming years (see Fig. 1). The high returns that can be achieved within the DeFi ecosystem attract institutional capital in addition to traditional investors.[3] Today, the boundaries of financial theories are being tested daily, and more and more decentralized applications are joining the ecosystem. This growing number of participants is accelerating the progression of concepts such as liquidity pools,[4] flash loans,[5] yield farming,[6] and stablecoins.[7] The latter are important components in DeFi as they enable investors to generate yield on their crypto assets while alleviating the potential adverse effect of market volatility.[8] Despite the steady increase in demand for stablecoins (six-fold growth in between 10/20 and 10/21),[9] lending rates remain high,[10] indicating that demand is in excess.

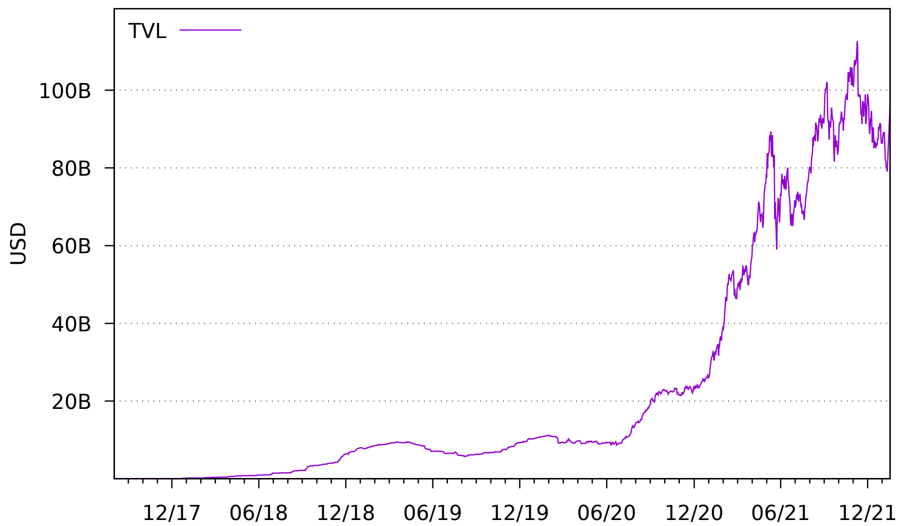

Fig. 1: The development of the total USD value locked in DeFi protocols since August 2017 (08/17) - data obtained from *DeFi Pulse*.[2]

Stablecoins can be classified into three major classes: First generation stablecoins are off-chain and supposed to be backed-up by bank deposits and regular auditing (*e.g.*, USDC,[11] TETHER[12], and WBTC[13]).[14] Second generation stablecoins are on-chain, associated with cryptocurrency collaterals, and thus embedding high-quality collaterals in a traceable sense (DAI[15]).[16] Third generation stablecoins are algorithm-based and function through a combination of endogenous and exogenous collateral ranging from totally endogenous (*e.g.*, UST[17]) to partially collateralised (*e.g.*, FRAX [18]).

The rules that define how algorithmic stablecoins work are defined in smart contracts that can only change by leveraging social consensus or *via* governance votes. Typical smart contract functions enable, *e.g.*, the minting and burning of tokens or the communication to services outside the blockchain through oracles.[19] Overall, the primary logic underpinning the functions of algorithm-based stablecoins relies on tokens being burned or minted when the price of the stable fluctuates from the predefined stable value - commonly referred to as its peg. Thus the algorithm would facilitate the minting of new tokens for cases where the price of the stablecoin falls below the peg, and would burn new tokens in cases where the price is over the peg. This mechanism is referred as maintaining the peg. The price stability of a stablecoin is strongly correlated to the project-owned liquidity. If there is only limited liquidity available, then it is easy to manipulate the market value of such an asset, which results in an unbalanced peg. The consequences can range from severe financial damages for investors to bankruptcy of the project.

Our goal is the creation of a suite of tools that enables the enforcement of stablecoin pegs by levering cashflow generating assets and fees from protocol-owned liquidity to funnel stability towards the peg. We are developing the APHRA engine (AE) a scriptable financial pipeline composed of chainable actions that allow traders and bots to interact with protocol-owned liquidity and help maintain our protocol state targets. This engine is governed by the vote-escrowed APHRA (veAPHRA) token holders (*vide infra*), who participate in governance decisions, elections, state targeting decisions, and asset management decisions through a decentralized autonomous organization (DAO).[20] In the following sections, we deep-dive into the role of AphraFinance, outline the APHRA token supply, introduce how the AE is set up, and present the cornerstones of the DAO ecosystem. We describe subsequently how peg stability can be achieved *via* project-owned liquidity by help of the AE peg stability module (AE-PSM) and share pseudo-implementations of several AE-PSM functions. This enables us to show how stablecoin pegs are equilibrated in a sustainable way.

2 AphraFinance

APHRA is a scriptable financial protocol designed to operate a peg stability module for algorithmic stablecoins. We use revenue from cashflow-generating assets and fees generated from peg arbitrage supported by protocol-owned liquidity (POL) to make the protocol functional.[21] Our main mission is to become a "black hole" for decentralized liquidity that is used to regulate stablecoin pegs. Furthermore, a positive market action is created as more and more assets are taken out of circulation. POL anchors those pegs by prohibiting market manipulation and economic attacks through adjustment of price fluctuations using automatized workflow actions. The APHRA engine implements automatized workflows that consist of economic actions each propagating the actual workflow-state to the next one. These actions are authorized contracts that live on-chain and are able to be executed in single calls using *multisig* procedures within the modified *weiroll* VM.[22] The protocol is bootstrapped as a continuous integration platform similar to, *e.g.*, Amazon Web Services, where experts are able to implement financial strategies in terms of directed acyclic graph[23] workflows. Authorization, feasibility, and ecosystem health are cross-checked by the APHRA scoring mechanism obtained through trusted participants that validate runs by providing trust scores in a similar way to, *e.g.*, oracles. Execution of workflows with high-enough trust scores will be performed while low trust-score workflows will not be executed. Next, we describe the structure of the APHRA engine and the underlying continuous integration platform as a combined and simplified ecosystem representation.

APHRA vaults allow the end-user to deposit liquidity within expert yield aggregator strategies – more details are given in section 2.2. Another stake vector is provided by means of white-listed crypto assets, where the end-user can provide liquidity through crypto assets that are used within yield farming strategies like peg arbitrage. The end-user obtains 20% of the generated revenue. and is entitled to obtain veAPHRA from weekly inflation. The usage is measured with gauges, which show how much an end-user is providing in liquidity. Each gauge is associated with a weight that determines how much of the inflation will be received by this liquidity gauge. All weights add up to unity and we calculate the inflation each week as discussed in section 2.1 until the unlock vote passes (see section 2.4).

Inflation is created by the APHRA minter and paid out to the liquidity gauges according to the pre-voted weights by the veDistributor. After the DAO activation, the inflation rate is dynamically defined with respect to ve-locked circulating supply (see section 2.1). veAPHRA holders decide through voting how the gauges inflation weights should be adjusted. Voting rights can also be acquired, which means that veAPHRA holders can pass on their voting rights to others by receiving financial incentives through voting bribes. Bribes thus allow the veAPHRA holder to build an additional passive revenue stream. After the distribution scheme is determined, inflation will be distributed to gauges liquidity providers coming with rolling locks of eight weeks. At this point it should also be said that there is a dilution protection for veAPHRA holders, which ensures that ve-locks increase based on the existing inflation.

Initial cashflow is generated by the remaining 80% revenue as obtained by APHRA yield farming strategies (see section 2.2). The integrated cashflow distributor gauge allocates liquidity to the different key areas of the ecosystem in order to maximize project-owned liquidity while helping our partner networks in the best possible way. Key areas of the ecosystem are: I) a protocol reserve as locked in XVADER tokens, II) peg liquidity through USDV 3CRV and a decentralised stablecoin pool consisting of three different algorithmic stablecoins (USDV ,[24]

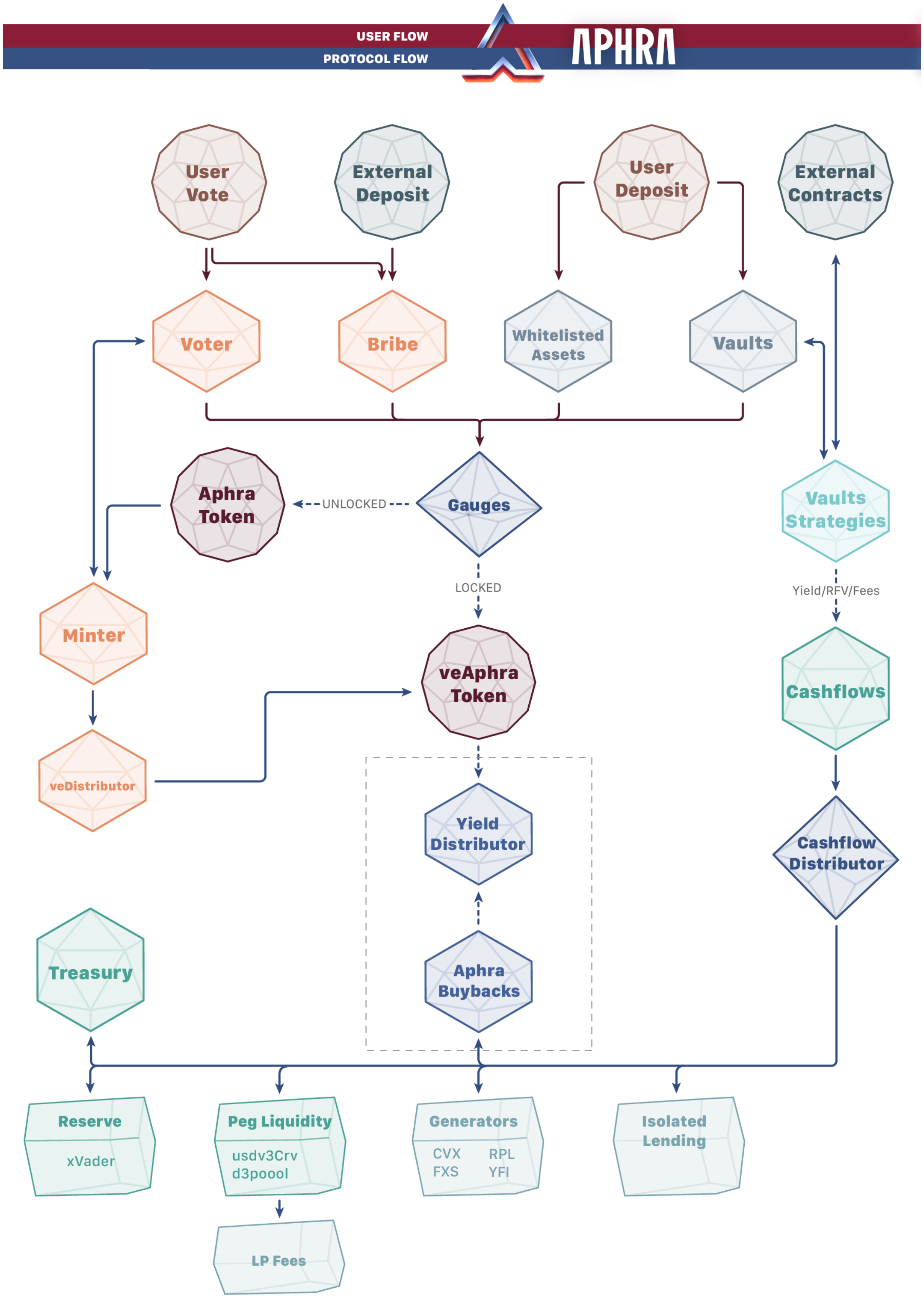

Fig. 2: Flowchart diagram of the APHRA ecosystem from the perspective of end-users, who provide liquidity and can help shape the DAO through voting rights as obtained *via* vote-escrowed APHRA tokens.

BEAN ,[25] and FRAX [18]), III) cashflow generating assets (*e.g.*, CRV ,[26] FXS ,[18] RPL ,[27] or YFI [28]), and IV) an isolated lending market. Initial priority is the development of project-owned reserves and the setup of peg liquidity since we see those points as base pillars of the ecosystem. Once a reliable source of cash-flow has established through stablecoin peg arbitrage, the future health of the APHRA DAO is consolidated. As soon as we reach a reasonable reserve of POL (45–50 million), another key area of the protocol gets activated – an isolated lending market. This will enable the development of new strategies by means of the recently published YieldBox.[29,30] More details about the isolated lending market follow in an upcoming version.

2.1 Vote-escrowed mechanism

Standard vote-escrowed (ve) rules enables the end-user to lock a base token into the ve-contract for a period of one week to up to four years. Those locks are, however, not transferable and thus bound to one address. Holder of ve-tokens vote on the destribution of inflation and hence which liquidity pools should be incentivized. Three changes to this standard procedure have been suggested[31] and implemented within the veAPHRA model: First, inflation is dynamically determined with respect to the amount of ve-locked circulating supply, which will be the active mechanism after the DAO activation. Before that the inflation rate θ is set to a value of 625,000.

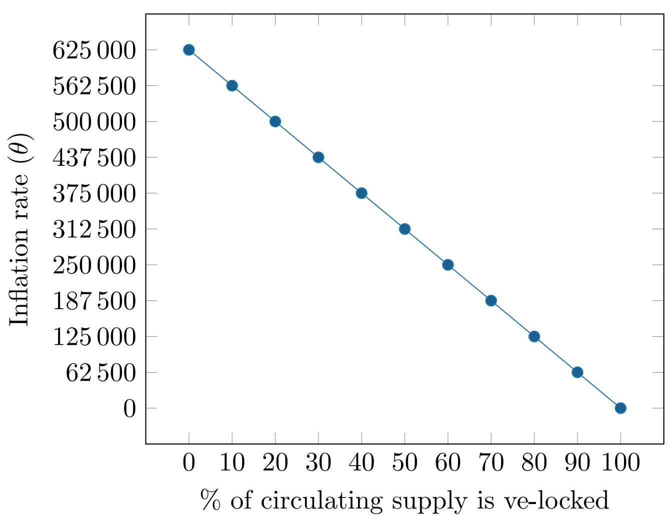

Fig. 3: Inflation rate is depending on ve-locked circulating supply.

The inflation is calculated according to equation 1, where we use the inflation rate θ, the weekly emission α_w, the circulating supply (CS), and the total supply (TS). One month after the DAO activation, the weekly emission starts to decay at a rate of two percent per week. An example clarifies how we calculate the inflation: Starting with an inflation constant of 625,000, a weekly emission constant of 98, a CS of 8,000,000, and a TS of 29,500,000 we obtain the following inflation

$$\text{Inflation} = \frac{\theta\, \alpha_{\mathrm{w}}\, \mathrm{CS}}{100\, \mathrm{TS}} = \frac{625,000 \times 98 \times 8,000,000}{100 \times 29,500,000} = 166,101\, \frac{41}{59}. \tag{1}$$

Second, all ve-lockers increase their holdings proportional to the inflation. Following the example given above the weekly inflation rate is 0.54%. Our modification will ensure that ve-lockers will never be diluted, as such, their holdings increase by 0.54%. Last, ve-lockers are represented as non-fungible token[32,33] (NFT), which allows a single address to have multiple locks with different locking periods at the same time. This further allows ve-locks to be traded on secondary markets, which solves the capital inefficiency problem of standard ve-tokens. The maximum locking time is shortened from four years to two years (see section 2.4). We present next how APHRA yield farming strategies help the end-user to generate revenue and the protocol to build up a healthy DAO ecosystem.

2.2 Aphra yield farming

In the DeFi space, there are many projects that give out rewards to their end-users for interacting with their platforms. One example is staking tokens on a platform, which in turn can increase the total value locked for that project. Typically, liquidity pool tokens are used for this purpose, as many projects issue rewards in return for users providing the liquidity needed to run the platform, which is commonly referred to as yield farming. For end-users with limited means, yield farming can be prohibitively expensive due to the high transaction costs of claiming rewards. To address this problem, so-called yield aggregator contracts have been developed to pool the funds used and allow users to optimise their return.[6]

A yield aggregator is a set of smart contracts that pools invested funds, and reinvests them in an array of yield-producing products or services through interacting with their respective protocols. The level of aggregation offered by yield aggregators usually has a number of advantages. First, investors do not have to actively put together their own strategy, but can use developed expert strategies and transform their investment strategy from an active to a passive approach without requiring extensive knowledge of the underlying protocols and infrastructures. Secondly, since cross-protocol transactions take place *via* a smart contract, capital shifts are performed automatic, removing the need for the investor to transfer funds manually between protocols. Finally, because funds are pooled in a strategy contract, the gas costs are socialized, resulting generally in fewer and thus lower interaction costs.

AphraFinance offers the end-user to participate in yield aggregator strategies. Locked provided liquidity is allocated to be used in strategies to, *e.g.*, peg arbitrage algorithmic stablecoins (see section 3). This allows both the stablecoin community and the end-user to benefit from AE strategies. Beneath obtaining veAPHRA inflation as reward, 20% of the yield farming aggregator revenue is entitled to the liquidity provider, while 80% are retained as fees by the protocol.

2.3 Tokenomics

The total supply of the APHRA token is set at 100 million tokens and we show its total distribution in the pie chart below.

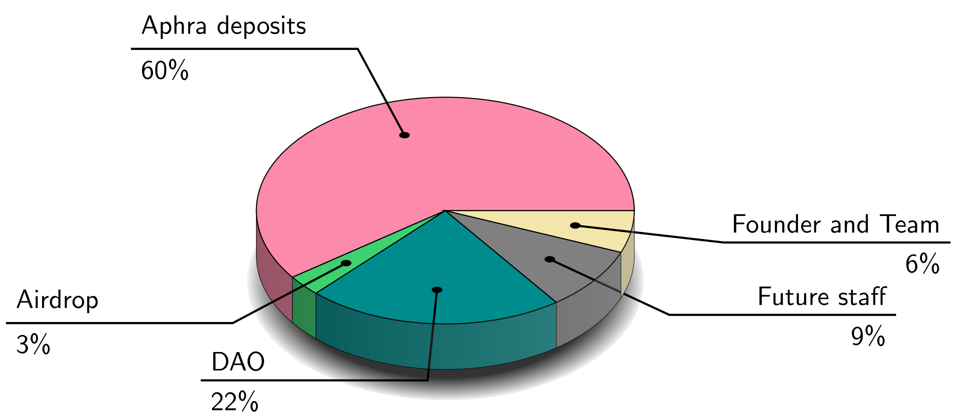

Fig. 4: Total APHRA token distribution.

15 million tokens or 15% of APHRA's token supply is allocated to the AphraFinance team with 6% getting allocated towards the existing team and 9% being reserved for future team members. The existing team receives 6% of the APHRA token supply with 2% being reserved for the founder and 1% being reserved for every other team member, where allocation is given to 100% in

veAPHRA . The allocations for future team members will be decided on a case by case basis as the project and the value of the token evolve. Current and future AphraFinance team members receive half of their allocation in veAPHRA with a 2 year locking period and the other half of their allocation in the form of APHRA base tokens. There exist a technical council that is responsible for hiring new team members (see section 2.5).

3% of the total supply which equates to 3 million tokens will be reserved for the airdrop recipients and will be emitted in the form of veAPHRA . Once claimed the tokens are locked for two years. Eligible airdrop participants have staked VADER tokens before the snapshot Ethereum block 13925000, tokens in a BeanstalkFarms SILO, SOW'ed[25], or FXS tokens before the snapshot Ethereum block 14005000.[18] All 6,566 airdrop addresses are shared separately.[34] Airdrop recipients can claim their airdrop whenever they want having the mentioned locking period of two years.

60% of the token supply which equates to 60 million tokens is scheduled to be emitted into APHRA depositors as incentives, where a certain amount is reserved for vaults. The purpose of this is to incentivise market actors to take actions that lead to the growth of AphraFinance over the long term. In a future update, token emissions can be adjusted in real time between different stablecoin vaults in case of a peg dislocation with the aim of attracting market actions that can restore the peg of a specific stablecoin if needed. In the future, vault deposits can be represented with yield bearing ERC20 tokens that can be used as collateral into different DeFi protocols. Below is the schedule of emissions towards APHRA deposits:

By having a long term emissions schedule, AphraFinance attracts capital flows in order to establish itself with the aim of keeping that capital by benefiting all participants of its ecosystem through the results of its actions. After the endpoint of AphraFinance's emission schedule, the DAO can arrive to the decision of directing part of AphraFinance profits into the buyback of APHRA tokens on the open market in order to distribute them to depositors as rewards.

22% of the APHRA supply which equates to 22 million tokens is reserved for the DAO treasury and is granted through a 14 year emissions schedule that follows the issuance rate decrease that is established by the deposits emission schedule as described above. The DAO emission scheme is presented below:

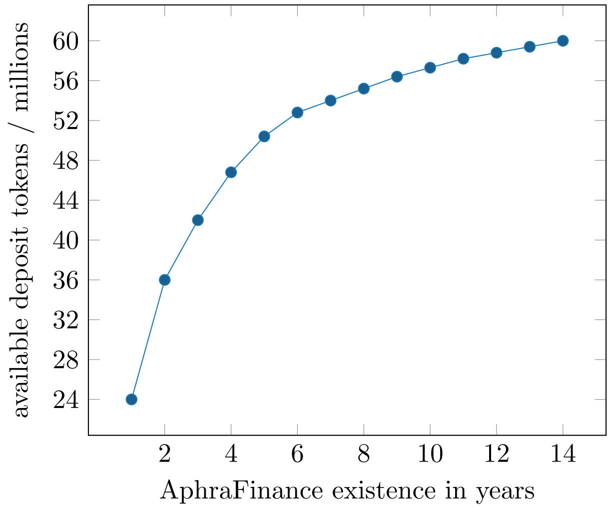

Fig. 5: Emission of APHRA deposit tokens within the upcoming 14 years.

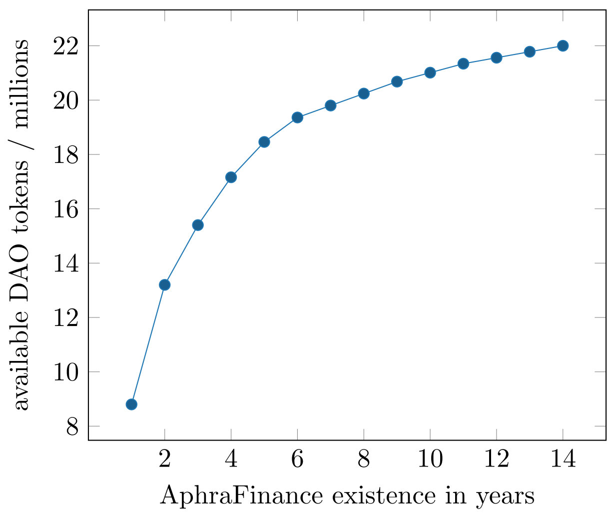

Fig. 6: Emission of APHRA DAO tokens within the upcoming 14 years.

The DAO is tasked with making decisions in regards to the optimal use of treasury funds with the end goal of advancing AphraFinance and its ecosystem partners forward.

Treasury funds can be used for the following purposes:

1 Grants for research and development that can lead to the further development of AphraFinance and its ecosystem.

2 Execution of treasury swaps with other entities for strategic purposes.

3 Funding the seed and investment rounds of projects that can further advance AphraFinance and its ecosystem partners through innovative offerings.
4 Investing into assets that can be beneficial to AphraFinance and its ecosystem from a strategic perspective.
5 Offering of APHRA tokens into the market through the sale of bonds.
6 Security audits of smart contracts.
7 Continuous funding of the community reward program in order to ramp up productive engagement from the AphraFinance community.
8 Any other expense that is deemed to be essential or worthwhile for the advancement or operations of AphraFinance.

2.4 DAO: Activation

In order for the AphraFinance DAO to be activated and the APHRA token to become tradeable, a vote with a duration of 7 days will be enacted requiring 15,000,000 tokens in favor. In case of failing the proposal to pass, the vote can be reenacted every 200,000 blocks until there is agreement within the community. With the activation of the DAO, an additional vault for APHRA /USDV liquidity pools will be introduced with the aim of incentivising market actors for the provision of liquidity into decentralised exchanges. For the first 6 months of the emission schedule all rewards will be provided in the form of veAPHRA . After the DAO activation, all the rewards will be provided in the form of the base APHRA token with the option of locking laying in the hands of each individual participant.

APHRA token holders can lock their tokens for up to two years in order to participate in the DAO and the value it generates. The exact APHRA to veAPHRA exchange rate is dependent on the locking period as seen below:

For a locking period of 6 months, one APHRA token will be exchanged to 0.25 veAPHRA . An increase of locking time will increase the exchange rate for veAPHRA . The maximum amount is obtained for a locking period of 24 months, where one APHRA tokens is exchanged to one veAPHRA token. Vote locked APHRA can be represented as NFT giving APHRA vote lockers the ability of having multiple locks inside a wallet for different quantities and time horizons. The representation of vote locked positions as NFTs also creates the capability of enabling a vote market inside AphraFinance itself thus creating another source of yield for

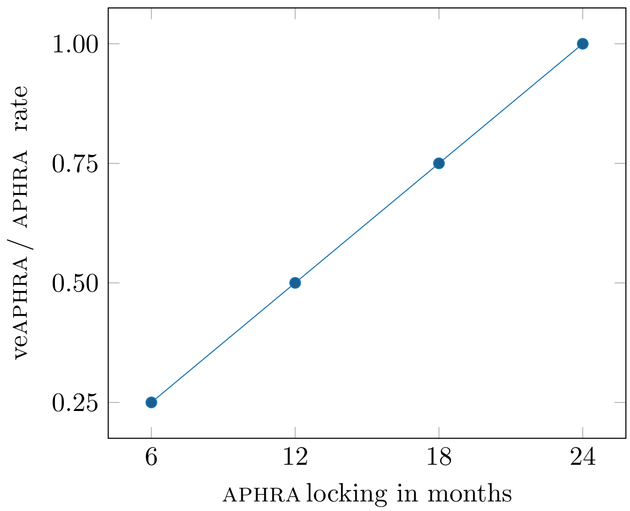

Fig. 7: Exchange rate of veAPHRA for APHRA depends on chosen locking period.

veAPHRA positions. Furthermore, veAPHRA holders will be able to participate in the DAO decision making process regardless of the size of their holdings. For the submission of proposals to the DAO, a minimum of 2500 veAPHRA tokens will be required. Submissions will be published on the Snapshot[35] platform (see section 2.5).

As AphraFinance produces cashflow those assets will be used as follows: First, we provide another source of funding for the DAO treasury outside of the emissions of our native token. Second, we accumulate strategic cashflow producing assets with voting rights (*e.g.*, CVX ,[36] VADER ,[24] or FXS [18]) and compound these positions while a percentage of the profits can be directed towards veAPHRA holders. Lastly, direct part of protocol profits is redirected towards veAPHRA holders through the buyback and distribution of native tokens or in other ways that can be voted on by the DAO. The DAO furthermore adjusts the ratios of the allocations towards each one of the specified strategies however it sees fit. Once credibility has been established, AphraFinance can take on higher risk activities like providing credit lines to other DAOs.

2.5 DAO: Governance

One of the most immediate challenges for decentralized communities is how to address governance. Managing collective decision making to optimize resources and operations plays a critical role. Governance, however, requires a significant coordination effort stemming from the need to involve network participants in voting on every decision. This coordination effort can be radically reduced in decentralized networks where smart contracts enable participants to govern co-operatively. DAOs run almost entirely by code and refer to collections of people that come together with aligned incentives and interests.

Within the DAO, we have two councils: First, a technical council that will come up with suggestions on improving the ecosystem on a technical level and the hiring process of new personal (see “Hire staff” below). Second, a treasury council that will come up with suggestions on asset management and asset curation (see “Risk management” and “Asset curation” below). All suggestions will be released in transparent proposals that have to go through a community election where we decide collectively on important changes by using voting power that has been transferred to holders of the veAPHRA governance token. All proposals will be published on the Snapshot[35] platform.

Incentives are critical to governance because otherwise there is little reason for community members to invest time, money, or energy in managing or improving the ecosystem. Therefore, we established a reward system to acknowledge active members in the community for their contributions (see “Community rewards” below). Note that we actively reward good ideas and suggestions that will lead to the improvement of the ecosystem. We list in the following essential subjects that are crucial to the success of the DAO:

Collective asset management Initial capital is provided in the form of governance tokens held by the DAO smart contract and assets used to purchase governance tokens. For example, if the DAO begins minting 1,000 governance tokens and sells 500 of them to genesis members for 100 ETH, then the initial treasury consists of 500 governance tokens and 100 ETH. However, as the DAO grows in terms of user base or accumulated cash-flows, it becomes important for the DAO to manage this capital similar to a business.

Risk management The balance sheet of the DAO can consist of risky assets. Therefore, managing currency risk is very important to ensure that future operations can be funded. These assets are intended to be used to fund development, audits, insurance, and for spending on user growth and acquisition. To achieve these goals, we must manage the treasury to meet specific metrics or key performance indicators (KPIs). Quantitative tools are useful in enabling the community to visualize and make DAO members understand the risk of the DAO in relation to market conditions. This creates more transparency on the risk level of a DAO treasury and allows the community to update the treasury composition to meet specific KPIs.

Asset curation The DAO governance token is used for voting on adding or removing assets. This is because a number of parameters must be chosen for each asset - margin requirements, yield curves, insurance costs - and the decisions are critical to the security of the ecosystem.

Hire staff Once the DAO has a large enough community and sufficient assets, it is important to hire people who can take care of maintenance, communication, and administrative tasks full time. The DAO must, however, be careful not to create "active participants" that token holders could rely on to increase the value of the underlying token. Therefore, decentralization must be kept in mind when adding service providers.

Community rewards Community grants, internal salaries and special projects can be stimulated and rewarded by the community itself. Instead of cumbersome voting or black box committees, contributors themselves can quickly and transparently reward the value they believe has been created. For this purpose, we create a community reward program, which enables active members to be rewarded based on their contributions. At the moment this reward program is available within a Coordinape circle, however, the scheme can change in the foreseeable time.[37] Within the circle, each member has an amount of 100 GIVE tokens that can be distributed to other members in the circle. After each epoch (1 month), a certain amount of veAPHRA tokens will be allocated based on the amount of GIVE tokens distributed. New members can be elected by existing circle members to also participate in the distribution of rewards. Three votes of active circle members are necessary to become a member of the AphraFinance-Coordinape circle. Note that the amount of distributed APHRA tokens can be adjusted in the future through DAO governance.

3 Peg maintenance

End-users rely on the maintenance of the peg for predictable value transfer. Hence the maintenance of the peg should be used as the primary indicator of value. However, in the case of algorithmic stablecoins, there are a number of other relevant parties from whose perspective the value of the stablecoin ecosystem can be assessed. There is a significant profit opportunity for arbitrageurs and speculators exposed to the stablecoin and its stabilizing asset. The theoretical loss of value due to the divergence of the peg is at least partially offset by the resulting opportunities for these parties to earn relatively low-risk returns by participating in the rebalancing process, which could optimistically be viewed as a benefit shift rather than a net loss. Here, the end-user only suffers a loss of value from a peg deviation if he sells the stablecoin before the successful rebalancing. Thus, the time required for rebalancing is a metric that can be used to measure the value of the stablecoin.

The concept of time value of money states that assets that can be spent in the present are worth more than assets that can be spent in the future. Assuming that a rational end-user whose stablecoins have fallen below their peg waits until the peg is restored to spend them, and that the peg is indeed restored at some point in the future, the net present value of the stablecoins to the user decreases only as the expected time to restore equilibrium increases. In this scenario, the magnitude of a given deviation ultimately determines value only to the extent that it affects the time required to restore equilibrium, making the latter the primary indicator of value. It should be noted, however, that this logic is not the only relevant factor, because the longer the expected rebalancing time of a stablecoin, the greater the risk that its holder will incur opportunity costs or other unavoidable costs while waiting for the peg to be restored. There are scenarios in which opportunity costs become so large or other costs become so immediate that the end user must liquidate before rebalancing, in which case the magnitude of the deviation is likely to be as important or more important than the rebalancing time.

In the following, we present our solution to minimize the rebalancing time and thus offer the end-user the possibility to cash out his value whenever it might be convenient. We use POL, together with automated processes, to ensure that the rebalance time is kept as short as possible. The automated processes are stored as code in the AE peg stability module (AE-PSM) and ensure that an algorithmic stablecoin maintains its peg in the long term. At the same time, arbitrage opportunities arise, which allow us to add another source of income and thus a positive cashflow to maintain the DAO ecosystem. In the following section, we exemplify the AE-PSM by presenting its effect on the peg of the USDV stablecoin as released recently by the developers of the VADER protocol.

3.1 Peg stability module: USDV example

VADER is a liquidity protocol that combines a hybrid algorithmic-collateralized stablecoin with liquidity pools enhanced via synthetic assets.[24] The stablecoin, USDV , is issued by burning VADER tokens and liquidity pools use USDV as the settlement asset. Therefore, it is of utmost interest to the end-user that the USDV peg is kept stable. The AE-PSM has an API entry point (*hit* function) which can be used to call methods within the module. Pseudocode for the *hit* method is given below:

```
// Get actual price, check for events,
// and payout reward in case that event happened.
function hit(uint256 amount) internal {

    // Get price information
    uint256 price = feed.getPrice();
    uint256 delta = uint256(0);

    // Check for possible events
    if (price >= high) {
        delta = pegDown(amount);
    } else if (price <= low) {
        delta = pegUp(amount);
    }

    // Payout reward
    if (delta > actionableDelta) {
        aphra.safeTransferFrom(
            address(this), address(msg.sender));
    }
}
```

Listing 1.1: *hit* defines the entry point to the PSM.

If there is too much USDV in circulation and its price is trading below the peg, then the “pegUp” PSM-method automatically mines VADER from existing USDV such that there is less amount in circulation and thus the price is rebalancing back to its peg. Pseudocode for the *pegUp* method is given below:

```
// Mints Vader from USDV and stakes Vader to
// increase xVader to bring the ratio back in line.
// Amount represents how much USDV is to be removed.
```

```
function pegUp(uint256 amount) internal {

    // USDV position in metapool, coin 0
    int128 usdv = 0;

    // How much USDV to remove from the pool
    uint withdraw = right.calc_withdraw(amount, usdv);

    // remove USDV
    right.remove_liquidity(withdraw, usdv);

    // Partner burn the USDV to mint Vader
    uint256 vader = vaderMinter.partnerBurn(withdraw);

    // Stake the Vader to increase xVader
    left.enter(vader);
}
```

Listing 1.2: *pegUp* gets xVader from USDV.

On the other hand, if the price is above the peg, the *pegDown* method is used. This method burns existing VADER and USDV is minted. As a result, the amount of USDV that is in circulation is increased leading to a reduction in price achieving peg stability. Pseudocode for the *pegDown* method is given below:

```
// Redeem Vader for xVader, partner mints, and then
// deposit into the pool to bring the ratio back in line.
// Amount represents how much xVader is to be removed.
function pegDown(uint256 amount) internal {

    // Hits the leave method
    left.leave(amount);

    // Burn all of our Vader on the PSM
    uint256 usdv = vaderMinter.partnerMinter(
        vader.balanceOf(address(this)));

    // Define minimum amount to stake
    uint256 min = right.calc_token_amount(
        rightPool, [usdv, 0, 0, 0], true);

```

```
    // Setup enforcement checks
    right.add_liquidity(rightPool, [usdv, 0, 0, 0], min);
}
```

Listing 1.3: *pegDown* gets USDV from xVader.

A simplified USDV peg rebalancing can be seen in Fig. 8.

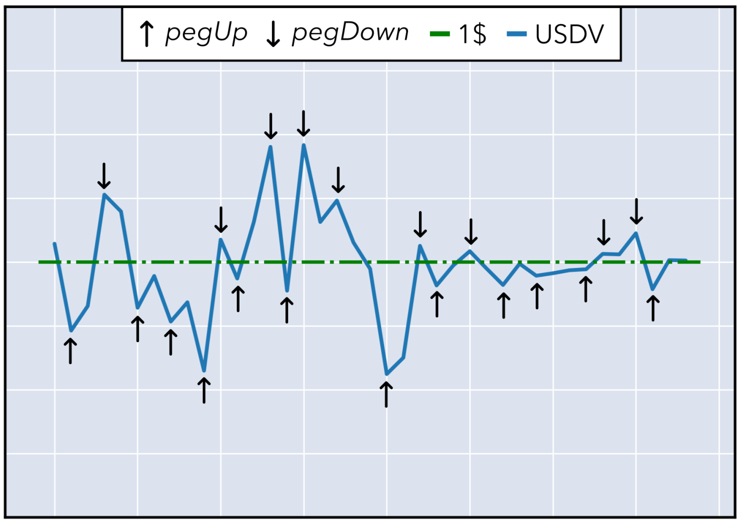

Fig. 8: USDV market scenario where its price (blue) is influenced by *pegUp* (↑) and *pegDown* (↓) events in order to stabilize the peg (green).

The *pegUp* method is represented by an arrow up (↑) and the *pegDown* method is represented by an arrow down (↓). After an initiation phase, the USDV peg can be successfully brought to balance by AE-PSM method calls. The entire AE-PSM can furthermore be represented in a flow diagram as exemplified in Fig. 9. Here, a potential node runner or bot hits the entry point of the AE-PSM and obtains access to the *pegUp* or *pegDown* methods, that initiate either a burn process of USDV (*pegUp*) or a burn process of VADER (*pegDown*) thus rebalancing the USDV peg.

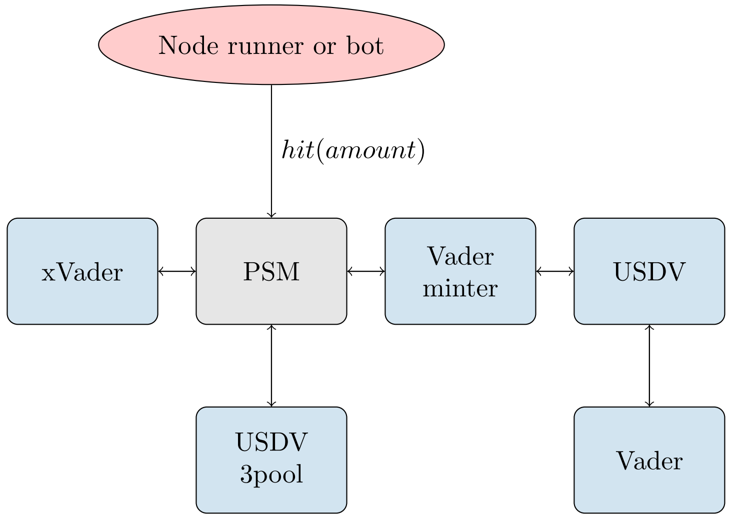

Fig. 9: The AE-PSM is accessible through the *hit* entry function that enables a bot or a node runner to interact with the module. If the USDV peg is out of balance two events are available that decrease (*pegDown*) or increase (*pegUp*) the value of the USDV stablecoin.

References

1. L. Fang, B. Hor, E. Azmi, and K. W. Win, *How to DeFi: Advanced*. Coingecko, 2021.
2. "Defi pulse: The decentralized finace leaderboard." `https://defipulse.com/`. Accessed: 2022-01-18.
3. "Defi report: An analysis of ethereum's decentralized finance ecosystem in q2 2021.." `https://consensys.net/reports/defi-report-q2-2021`. Accessed: 2022-01-18.
4. F. Schär, "Decentralized finance: On blockchain-and smart contract-based financial markets," *FRB of St. Louis Review*, 2021.
5. D. Wang, S. Wu, Z. Lin, L. Wu, X. Yuan, Y. Zhou, H. Wang, and K. Ren, "Towards a first step to understand flash loan and its applications in defi ecosystem," in *Proceedings of the Ninth International Workshop on Security in Blockchain and Cloud Computing*, pp. 23–28, 2021.
6. S. Cousaert, J. Xu, and T. Matsui, "Sok: Yield aggregators in defi," 2021.
7. W. Zhao, H. Li, and Y. Yuan, "Understand volatility of algorithmic stablecoin: Modeling, verification and empirical analysis," *arXiv preprint arXiv:2101.08423*, 2021.
8. L. Kristoufek, "On the role of stablecoins in cryptoasset pricing dynamics," *Available at SSRN*, 2020.

9. "Report on stablecoins." https://home.treasury.gov/system/files/136/StableCoinReport_Nov1_508.pdf. Accessed: 2022-01-19.
10. "Aave: Open source liquidity protocol." https://app.aave.com/#/markets. Accessed: 2022-01-17.
11. "Centre: Whitepaper." https://f.hubspotusercontent30.net/hubfs/9304636/PDF/centre-whitepaper.pdf. Accessed: 2022-01-18.
12. "Tether: Fiat currencies on the bitcoin blockchain." https://tether.to/wp-content/uploads/2016/06/TetherWhitePaper.pdf. Accessed: 2022-01-16.
13. "Wrapped tokens: A multi-institutional framework for tokenizing any asset." https://wbtc.network/assets/wrapped-tokens-whitepaper.pdf. Accessed: 2022-01-18.
14. J. M. Griffin and A. Shams, "Is bitcoin really untethered?," *The Journal of Finance*, vol. 75, pp. 1913–1964, 2020.
15. "The maker protocol: Makerdao's multi-collateral dai (mcd) system." https://makerdao.com/en/whitepaper. Accessed: 2022-01-16.
16. A. Fatás, *The Economics of fintech and digital currencies*. CEPR Press London, 2019.
17. "Terra money: Stability and adoption." https://assets.website-files.com/611153e7af981472d8da199c/618b02d13e938ae1f8ad1e45_Terra_White_paper.pdf. Accessed: 2022-01-17.
18. "Frax: Fractional-algorithmic stablecoin protocol." https://docs.frax.finance/. Accessed: 2022-01-17.
19. L. Breidenbach, C. Cachin, B. Chan, A. Coventry, S. Ellis, A. Juels, F. Koushanfar, A. Miller, B. Magauran, D. Moroz, S. Nazarov, A. Topliceanu, F. Tramèr, and F. Zhang, "Chainlink 2.0: Next steps in the evolution of decentralized oracle networks." https://research.chain.link/whitepaper-v2.pdf?_ga=2.241199361.280044258.1642587746-736256315.1641144110, 2021. Accessed: 2022-01-19.
20. C. Jentzsch, "Decentralized autonomous organization to automate governance," *White paper, November*, 2016.
21. "Aphra: Cashflow engine for the empire." https://www.aphra.finance/. Accessed: 2022-01-28.
22. "Weiroll: A simple and efficient operation-chaining/scripting language for the evm.." https://github.com/weiroll/weiroll. Accessed: 2022-01-26.
23. K. Thulasiraman and M. N. Swamy, *Graphs: theory and algorithms*. John Wiley & Sons, 2011.
24. "Vader protocol: Stablecoin anchored automated market maker with protocol owned liquidity." https://www.vaderprotocol.io/whitepaper. Accessed: 2022-01-16.
25. "Beanstalk: A decentralized credit based stablecoin protocol." https://bean.money/docs/beanstalk.pdf. Accessed: 2022-01-16.

26. “Curve finance.” https://curve.readthedocs.io/. Accessed: 2022-02-19.
27. “Rocket pool: Decentralized ethereum staking protocol.” https://rocketpool.net/. Accessed: 2022-02-19.
28. “Yearn finance.” https://docs.yearn.finance/getting-started/intro. Accessed: 2022-02-19.
29. BoringCrypto, “Yieldbox.” https://github.com/boringcrypto/YieldBox, 2022.
30. BoringCrypto. https://github.com/boringcrypto, 2022.
31. A. Cronje, “ve(3,3).” https://andrecronje.medium.com/ve-3-3-44466eaa088b. Accessed: 2022-02-19.
32. Q. Wang, R. Li, Q. Wang, and S. Chen, “Non-fungible token (nft): Overview, evaluation, opportunities and challenges,” *arXiv preprint arXiv:2105.07447*, 2021.
33. L. Ante, “The non-fungible token (nft) market and its relationship with bitcoin and ethereum,” *Available at SSRN 3861106*, 2021.
34. “Aphradrop: Dune analytics.” https://dune.xyz/androolloyd/AphraFinance. Accessed: 2022-02-23.
35. “Aphra finance proposals.” https://snapshot.org/#/aphrafinance.eth. Accessed: 2022-01-28.
36. “Convex finance.” https://docs.convexfinance.com/convexfinance/. Accessed: 2022-01-27.
37. “Coordinape: Tools for daos that do.” https://docs.coordinape.com/. Accessed: 2022-01-22.