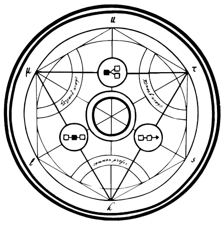
A comparable study of stablecoin protocols Liquity, Gyroscope, Maker, Frax, Curve (crvUSD), Aave (GHO)

April 29, 2023



Contents

1 Scope of the report

Common Prefix was commissioned to perform a study and prepare a report for Harmony, for the following six stablecoins:

- Liquity's LUSD
- Gyroscope's GYD
- Maker's DAI
- Frax protocol's FRAX
- Curve's crvUSD
- Aave's GHO

This report describes the design of each one of the above stablecoins, addresses and compares their strengths and weaknesses. More emphasis is given to the stablecoins LUSD, DAI and FRAX, which are three well-established stablecoin protocols with hundreds of millions of market cap. Special attention is also given to GYD, which is a relatively new project, with several interesting and novel aspects. crvUSD and GHO are only briefly discussed because they were released a few months ago and there are still several details pending in their design.

Usually, in order to compare two stablecoins or argue about the advantages of one project to another, one simply plots their prices for a certain time period and checks the deviations from the desired 1 USD price. This approach comes with certain caveats. First of all, note that It is not very informative to simply compare the prices if the stablecoins under comparison use different collateral assets. This is because it is not possible to distinguish if the stability/fluctuation of the stablecoin's market price is a result of its design or of the stability/volatility of the collateral asset. Also, a stablecoin's price history cannot ensure the same behavior for a future stablecoin protocol using a mostly similar design.

This report intends to assist Harmony regarding the main design of a new stablecoin, in accordance to an existing stablecoin design that seems to best suit Harmony's complete ecosystem. In the following sections of this report, we describe the main mechanisms of each protocol, explain the rationale of its design choices, explicitly express the assumptions underlying the design and compare them in terms of some general criteria as scalability/capital efficiency, stability, governance, complexity of the parametrization and fee policy. We also try to distinguish the core elements of each design from mainly arbitrary design choices.

2 Liquity [1]

2.1 Overview of the protocol

The stablecoin of the Liquity protocol is called LUSD. It is backed by an on-chain asset (ETH: Ethereum), so it can be characterized as an "on-chain collateralized stablecoin", following a broad classification of stablecoins by the European Central Bank [2]. ETH is an "exogenous collateral"[3] for LUSD, since it is not minted by the protocol and has many uses outside of it (as opposed to endogenous collateral, which is usually a secondary token used by algorithmic stablecoins to keep their peg, by adjusting the volume of this secondary asset following the volume of the stablecoin).

2.1.1 Borrowing LUSD

Anyone (to be more precise any Ethereum address) can borrow LUSD. To do so, he should open a debt position (called Trove), depositing ETH collateral and getting freshly minted LUSD by the protocol. The minimum collateral ratio (MCR) i.e. the minimum ratio of the value of the deposited ETH by the user into the trove, to the debt (LUSD minted for the user), should be at least 110% i.e. to borrow 1 LUSD he should deposit ETH of value at least 1.1 USD. As long as the collateral ratio (CR) of the Trove is at least 110%, the user can

[1] https://docs.liquity.org/

[2] Bullmann, Dirk and Klemm, Jonas and Pinna, Andrea, In Search for Stability in Crypto-Assets: Are Stablecoins the Solution?. European Central Bank, Occasional Paper Series (August, 2019).

[3] Klages-Mundt, A., Harz, D., Gudgeon, L., Liu, J.-Y., and Minca, A. (2020). Stablecoins 2.0: Economic Foundations and Risk-based Models. In Proceedings of the 2nd ACM Conference on Advances in Financial Technologies, pages 59–79.

adjust the Trove as he wants i.e. borrow more LUSD, increase or decrease the collateral. He can also return the LUSD (or part of them) he borrowed back to the protocol and get back his collateral (or a portion of it, if he does not repay all the loan). Users pay only a one-time fee. This fee is in the form of LUSD and equals a percentage, ranging from 0.5-5%, of the borrowed amount. The exact value of the fee rate is adjusted algorithmically by the protocol and depends on the redemption rate (we will talk later about redemptions). Borrowers also pay a fixed liquidation fee of 200 LUSD, which they can claim back if their Trove does not get liquidated. The fees are added to the debt of the Trove. For example if a user wants to borrow 2,000 LUSD and the current fee rate is 1%, his total debt will be 2,000+0,01×2,000+200=2,220 LUSD. If the ETH price is 2,000 USD , he should deposit at least 1.1×2,220/2,000=1.221 ETH. To avoid spamming, the protocol imposes a minimum debt for each Trove (2,000 LUSD).

2.1.2 Redemptions

A second essential part of the Liquity protocol is the ability of any LUSD holder to redeem his LUSD at face value 1USD for ETH i.e. he can give an x amount of LUSD to the protocol, the protocol burns this amount and gives him an x/currentETHPrice of ETH minus fees. The fees are proportional to the redeemed amount, their rate is computed similarly as the borrowing fee rate, and the fees are paid in ETH and not LUSD i.e. if the current fee rate is 1% and the value of ETH 2,000USD, a user can redeem 2,000 LUSD for 2,000/2,000*(1-0,01)=0.99 ETH. Redemptions are something completely different compared to paying back the debt of a Trove. The ETH paid to the redeemer are not part of the ETH deposited as collateral to his Trove (the redeemer does not even necessarily need to hold a Trove, he could have just bought his LUSD in a secondary market). LUSD are redeemed against the Troves with the lower CRs i.e. the ETH paid to the redeemer are ETH deposited as collateral to the Trove with the lowest CR. The protocol manages to keep the Troves ordered (by their CR) in a very efficient way utilizing a clever computation of the rewards and debt distributed after a liquidation [4]. A redemption against a Trove decreases both the debt and the collateral of the Trove and increases its CR (if it was >100% before the redemption). But, since the Trove loses part of its collateral on every redemption, users are incentivized to keep a CR higher than the minimum 110%. This partially explains the much higher CR observed in practice. Redemptions is the primary stabilization mechanism of LUSD i.e. keeps the value of LUSD to 1 USD, since, as long as there is a sufficient amount of collateral into the Troves, anyone can exchange their LUSD for an amount of ETH of the same USD price. If the market price of LUSD is <1 USD LUSD holders are incentivized to redeem their LUSD at face value(which is higher than the market value in this case), therefore decreasing the total volume of circulating LUSD which will probably increase its value. If its market price is >1 LUSD users are incentivized to borrow LUSD from the Liquity protocol and sell them

[4] R. Pardoe, R, Laucko, B. Egizkitza, Efficient Order-Preserving Redistribution on Troves

to the market at this higher price. The result is an increased circulation of LUSD, which is expected to decrease the LUSD price back to around 1USD.

2.1.3 Liquidations

2.1.3.1 Stability Pool

As long as the total collateral ratio (TCR, the ratio of the total collateral to the total debt of the protocol) is high enough, the LUSD are backed by ETH of value in USD greater than the total amount of LUSD in circulation, therefore it is expected that LUSD will hold its peg. Users are incentivized to keep the CR of their Troves high enough, otherwise they are in danger of getting redeemed against, but the protocol cannot rely only on the behavior of the users to stabilize LUSD. If the collateral ratio of a Trove falls below 110% (the MCR) –this can happen if the ETH price drops and the user does not deposit extra collateral into his Trove-, the system enforces the Trove to be closed (liquidated) i.e. its debt is deleted and its collateral is absorbed. But in order to delete the debt an amount of LUSD equal to this debt should be burnt (it is not possible to enforce the holder of this undercollateralized Trove to burn his LUSD, since LUSD are just regular ERC20 tokens in the user address and the protocol has not any access on them, of course). The protocol does not rely on external actors for liquidations but has a Stability Pool, a pool with LUSD. Upon a liquidation of a Trove with debt xLUSD and collateral yETH, the protocol burns xLUSD from the Stability Pool (SP) and the yETH of collateral are transferred to the SP. If the liquidations happened near the 110% threshold, every liquidation is profitable for the SP. But where do the LUSD of the SP come from? Anyone can deposit LUSD in the SP. The incentives to do so are:

- Profit from liquidations (up to 10% in normal mode, up to 50% [5] in recovery mode) are distributed to the SP depositors proportionally to their deposits.

- SP depositors accumulate LQTY (the secondary token of the protocol) rewards proportional to their deposits and continuously[6]. LQTY holders can stake them and claim part of the minting and redemptions fees. In contrast to what happens with secondary tokens of other stablecoins, LQTY is not a governance token and has no direct impact on the LUSD.

Depositing in the SP is considered a relatively low risk investment. To avoid liquidations, while their LUSD are deposited in the SP, SP depositors are expected to keep their Troves at a higher CR. Since, as with every function of a smart contract, someone (a liquidator) has to trigger a liquidation, the protocol uses the 200 LUSD liquidation fee paid by the Trove owner when he opened the Trove, so the liquidator does not need to pay any gas and he also gets 0.5% of the collateral of the liquidated Trove.

[5] actually slightly smaller (9.95% and respectively 49.75%), since the liquidator (the address which triggered the liquidation) keeps 0.5% of the liquidated trove's collateral

[6] https://medium.com/liquity/liquity-launch-details-4537c5ffa9ea

2.1.3.2 Redistribution of the remaining debt and collateral

If the SP does not hold sufficient LUSD to complete a liquidation, the debt and the collateral of the liquidated Trove is distributed to the other Trovel proportional to their CR. This is not as effective as a liquidation against the SP, since redistribution does not increase the TCR (does not make the protocol healthier), but at least eliminates the risky Troves.

2.1.4 Normal and Recovery mode

A measure for the health of the protocol is the TCR (total collateral ratio). As long as TCR is greater than a threshold/critical value (CCR=150%) the protocol is in the Normal mode and has all the functionalities described above. If TCR falls below 150%, the protocol switches to the Recovery mode. Extra restrictions are imposed (minimum CR for opening a Trove is 150%) and also Troves with CR between 110% and 150% become subject to liquidation, but only against the SP and no redistribution to the other Troves is allowed (because the profit of liquidating a Trove with such high CR is significant, the protocol chooses to allow it only to the SP depositors, the most important players of the protocol). The borrowing fee is 0% during the recovery mode (TCR is less than 150% and during the Recovery mode the CR of a new Trove should be at least 150%, therefore this zero fee is an incentive to open new Troves, and therefore increase the TCR of the system). More details about the differences between the Normal and the Recovery mode can be found in the Liquity whitepaper [7].

2.2 Advantages of the Liquity protocol

Capital efficiency: One possible way to compare two different stablecoin protocols is to check the amount of collateral needed from each one to issue the same amount of stablecoins. This criterion is not useful for stablecoins backed by fiat assets (for them 1 USD -in this report we deal with USD pegged stablecoins- should be deposited to mint 1 stablecoin) or for algorithmic stablecoins (these are not even fully backed by some type of asset), but it is a very useful criterion for the evaluation of stablecoins backed by on-chain collateral, as LUSD. Liquity requires a significantly lower minimum collateral ratio (110%), compared for example with DAI (150% if the deposited collateral is ETH) i.e. to mint x DAI someone needs 1.5*x/ETHprice ETH, but only 1.1*x/ETHprice ETH to mint x LUSD (26.7% less ETH). This considerable reduction of the required collateral with no compromises on the stability of the coin is made possible by the novel liquidation mechanism of Liquity. Liquidations in Liquity are much faster compared to auction based liquidations, since the debt of the liquidated Trove is absorbed by the SP.

Interest-free borrowing: Borrowing and redemptions are charged with a one-time fee, varying from 0.5%-5% for borrowing and 0%- for redemptions.

[7] https://docsend.com/view/bwiczmy

The borrowing fees are paid in LUSD upon creation of the Trove, therefore the borrowers do not have to worry about getting undercollateralized as time passes due to an increase of their debt as happens in protocols charging interest. This approach is preferable for users planning to keep the LUSD for a long period, before they repay their debt, but it is not suited for short term loans. The fee rate is not decided by governance, in contrast to DAI's interest rate, but it is adjusted algorithmically. The protocol defines the so called base rate and uses it to compute the borrowing and redemption fee rates. The base rate changes after every redemption following the formula:

$$b'(t) = b(t) + a\frac{m}{n}$$

where b' is the new base rate, b the old one, α a constant of the protocol (=0.5), m the amount of redeemed LUSD and n the current total supply of LUSD. The initial value of the base rate is 0. The base rate changes also over time since the last redemption:

$$b(t) = b \times \delta^t$$

where b(t) is the base rate at time t since the last redemption, b the base rate immediately after the last redemption (computed using the previous formula), δ a protocol constant (=0.94). The redemption fee rate equals the base fee rate, while the borrowing fee rate is max(0.005+base rate, 0.05) i.e. if base rate=1%, then users should pay to the protocol 1% of the redeemed collateral on every redemption and 1.5% of the LUSD they borrow on every borrowing operation.

Relatively simple parametrization: There are just a few parameters used in the protocol MCR, CCR, α, δ. The impact of each one is relatively simple and easily understood.

No governance: Liquity's contracts are non upgradeable and there is no owner. The design of the protocol makes governance redundant, since there are just a few parameters, and their value can be decided and set once before deployment. Although a fork of the protocol can add setter functions for some of these parameters, but with extra caution. For example an increase of the MCR after deployment would possibly lead to the instant liquidation of several Troves (troves with CR higher than the old MCR , but lower than the new one).

Hard price floor: LUSD are directly redeemable for ETH at face value (this is not true for many other stablecoins i.e. not possible with DAI except if the protocol is in the emergency shutdown mode, not possible of course with algorithmic stablecoins). This mechanism imposes a hard floor price of around 1 USD on LUSD and is the main stability mechanism of Liquity (along with the SP), but there are some caveats. First of all, redemptions are possible as long as there is enough collateral in the system. The

MCR=110% ensures that even if the price of ETH falls around 10% there will still be enough ETH in the system to back all the LUSD in circulation. In practice many Troves have a much higher CR. The current TCR is around 270%, therefore the LUSD holders should be able to redeem their LUSD even if the ETH price drops (270-100)/270=62.96%. We should also not forget that there is a redemption fee. If someone wants to redeem x LUSD the protocol will give him ETH of value x*(1-base rate) USD. Therefore the "hard price floor " is usually lower than 1 USD. It actually increases in cases of mass redemptions (since then the base rate increases). In practice we observe that the market price of LUSd is almost always above 1USD.

Non-gameable borrowing fees: The base rate changes only on redemptions, therefore even if the user splits a big loan into several smaller ones, he will pay the same total fee amount.

2.3 ...and some disadvantages and problems

Scalability: All stablecoins backed by on-chain assets are not scalable (at least compared to algorithmic or stablecoins backed by fiat-assets) in the sense that a supply of x amount of the stablecoin is only possible if and only if a higher amount of the collateral asset is locked. For Liquity this is not a huge problem, since the collateral asset it ETH, but for a fork of Liquity with a collateral asset of significantly lower price there is definitely a cap on the growth of the stablecoin.

Bank run resistance: If the TCR is >100%, even if all the LUSD holders decide to redeem their LUSD, the protocol can serve them. Of course this would empty all the Troves (except one, since there is restriction for technical reasons that at every moment there is at least one Trove), but all the users would be able to redeem their LUSD at face value. But if the TCR is less than 100% the protocol has failed and there isn't any mechanism to help the LUSD price increase or prevent it from going to zero.

Liquidation cascades: As long as the SP absorbs liquidations, there is no impact on the remaining Troves. But if a liquidation with redistribution of the collateral and the debt to the other Troves happens, then the CR of all the Troves drops (the TCR does not change though). If the liquidated Trove had a huge debt, the result of the redistribution could be that the CR of some other Troves drops below MCr and therefore they will be also liquidated.

Redemption fees are gameable: Let b the current base rate, n the total supply of LUSD, $m = m_1 + m_2$ the redeemed amount of LUSD. If the user redeems all m LUSd at once and if he first redeems m_1 and in a second tx m_2 (we assume that the delay between the two redemptions is practically zero, so no exponential decay is applied), the redemption fees in each cae are respectively:

$$
\begin{aligned}
f &= (b+\alpha\frac{m}{n})\frac{m}{ETHprice}\\
f' &= (b+\alpha\frac{m_1}{n})\frac{m_1}{ETHprice}+(b+\alpha\frac{m_1}{n}+\alpha\frac{m_2}{n-m_1})\frac{m_2}{ETHprice}\\
f-f' &= \alpha\cdot\frac{m_2}{ETHprice}(\frac{m_1+m_2}{n}-\frac{m_2}{n-m_1})>0
\end{aligned}
$$

i.e. splitting the redemption tx the user managed to pay less in fees. The difference is minor -at least as long as m is relatively small compared to n, which is a reasonable assumption- and also the base rate at the end is the same, therefore there is no impact on the future behavior of the protocol. As a result, this is not a worrisome issue.

Liquidations-by-redistribution part: The SP of Liquity has absorbed the debt of all the liquidations till now and no liquidation has hit the other Troves (via redistribution), therefore this part of the protocol has been never used. There are some possible problems with this part, which had arisen for example in a fork of Liquity [8], but they can only arise if the protocol had already failed from an economic point of view.

Tellor oracle issue [9]: Liquidity uses the secondary oracle (Tellor) in an unsafe way. If a fork plans to use the same oracle, the part of the code related to the Tellor call should be altered [10].

3 Gyroscope [11]

3.1 Overview of the protocol

The name of the stablecoin of the Gyroscope protocol is GYD (Gyroscope dollar). It is a stablecoin fully backed by a variety of on-chain collateral assets, but, since it is not overcollateralized, it also incorporates algorithmic aspects in order to keep the peg if the price of the collateral drops. Everyone can mint GYD, if he deposits an amount of equal USD value into the reserves of the protocol. The deposited amount can be in the form of any of the approved by governance assets (it can also be a combination of these assets). At the moment (the protocol is only deployed on a testnet) the allowed collateral assets are some stablecoins (USDC, USDT, TUSD, DAI) and WETH. The reserves are implemented as a series of vaults and each vault holds a different collateral asset or a combination of assets. For example, there is a WETH vault, a USDC/DAI

[8] A.Klages-Mundt, S.Schuldenzucker, Gyroscope P-AMM: Designing Autonomous Markets for Stablecoin Monetary Policy

[9] https://www.liquity.org/blog/tellor-issue-and-fix

[10] https://github.com/tellor-io/tellor-caller-liquity/blob/main/contracts/TellorCaller.sol

[11] https://docs.gyro.finance/gyroscope-protocol/readme

vault. The deposits of a vault are either just kept there or invested following strategies decided by governance. At the moment the only strategy which is implemented is depositing the assets of the vault as liquidity to an AMM and hence accumulating profits from the swap fees. The yield from these investments increases the collateralization of the stablecoin. Each vault has an ideal weight (percentage of the total reserves which are held in the vault) decided by governance. Minting and redemptions on this vault are only allowed if the percentage deviation of the actual weight from the ideal one does not exceed a max value (decided also by governance).

3.1.1 Primary market

The primary market, also called P-AMM (primary AMM) or DSM (Dynamic Stability Mechanism) in the docs[12], is the place where the stablecoin is minted and can be redeemed for collateral. While, as we said, the minting is possible at a 1-1 ratio using the current price of the collateral asset (not overcollateralization required), a more sophisticated approach is needed on redemptions, to deal with the case that, due to a drop of the price of the collateral assets, there is not enough collateral to redeem all the available GYD at a face value of 1 USD. The redemption price of the GYD follows a piecewise-linear curve as a function of the total amount of redemptions. The details of this curve (x_U, x_L, α) are decided by governance and also depend on the current total value of the reserves. The idea of this redemption curve is that initially GYD can be redeemed at face value. If the total reserves can cover all the GYD supply, then the redemption price should be a straight line (α=0), since there is plenty of collateral to redeem all the GYD supply at face value. But, if the reserve ratio (same as toal collateral ratio of Liquity i.e. sum of reserves in USD to total GYD supply) is $<$ 1 and users keep asking for redemptions, it is not possible to redeem all these GYD at face value. Instead of just blocking the redemptions when there are not sufficient reserves, the protocol just decreases the redemption price at such a level that the reserves can support it. Users are therefore incentivized to keep their GYD, instead of getting this decreased price and waiting till the redemption price recovers.

3.1.2 Secondary markets

The protocol also creates secondary markets where GYD can be exchanged. These are AMMs with concentrated liquidity (CLP: concentrated liquidity pools) around the redemption price of the P-AMM. There are 3 types of such markets:

- Uniswap3-like pools with 2 assets, but the liquidity is concentrated in a single tick [13].

[12] https://github.com/gyrostable/technical-papers/blob/main/P-AMM/P-AMM%20technical%20paper.pdf

[13] Quadradic Concentrated Liquidity Pool (2-CLP): Technical Overview

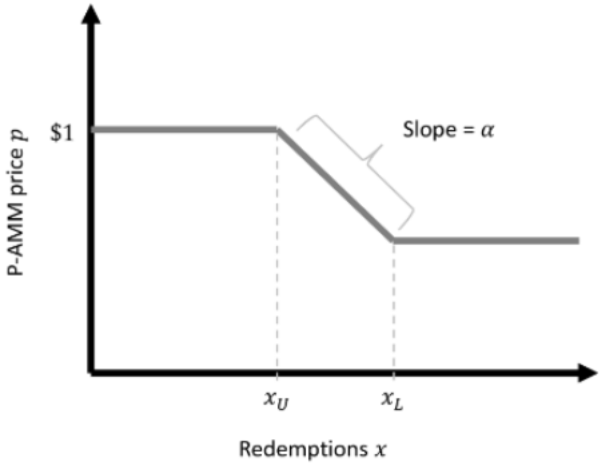


Figure 1: The piecewise-linear curve of the redemption price

- Uniswasp3-like pools with 3 assets and again liquidity concentrated into a single tick [14].
- A novel type of AMM, called by the Gyroscope team elliptic AMM (the curve of the AMM is part of an ellipse). Since the liquidity in these secondary markets is concentrated around the redemption price on the P-AMM, only exchanges of GYD around the redemption price are possible to these markets, therefore the protocol does not create arbitrage opportunities (this is the reason the protocol uses AMMs with concentrated liquidity) [15].

3.1.3 Consolidated Price Feed (CPF)

Gyroscope needs oracles to get the prices for the collateral assets when it needs them. It uses Chainlink and also TWAPs from AMMs and there is nothing new to it. What is really nice is that the protocol takes extra care to check the validity of the prices from the oracles and if it is not it can also pause some functionalities.

3.2 Advantages and disadvantages

+Scalability: The existence of many possible collateral assets and the only 100% collateralization makes Gyroscope more scalable, compared to Liquity and other overcollateralized stablecoins, in the sense that the protocol can mint huge amounts of GYD locking many different assets in the reserves and therefore it does not depend on the availability of a single asset.

[14] Cubic Concentrated Liquidity Pool (3-CLP): Technical Overview

[15] Elliptic Concentrated Liquidity Pool (E-CLP): Technical Overview

Of course, it is less scalable compared to purely algorithmic stablecoins, not fully backed by collateral.

+Capital efficiency: Minting GYD requires to deposit just an equal value of collateral assets, therefore the required "collateral ratio" is just 100%, the minimum possible for a fully backed by collateral stablecoin. Of course this comes at the cost that any drop of the price of any of the collateral assets will immediately put the protocol in an undercollateralized position.

+Non manipulable redemption price: There is no incentive for a redeemer to either split the redemption into smaller ones or merge several redemptions into a larger one, because the collateral he will get in all the cases is the same. This is a consequence of the path independence property of the P-AMM (Theorem 2 of the P-AMM paper [16]).

+-Bank run resistance (?): The Gyroscope team claims that the protocol is bank run resistant. In mass redemptions events, if the total reserves cannot support all the redemptions, the P-AMM decreases the redemption price (<1 USD), therefore GYD holders are incentivized to hold their GYD otherwise -if they still try to redeem them- they will suffer a loss. But this mechanism (adapting the redemption price when there are not sufficient reserves) could lead the GYD holders to try to redeem their GYD immediately after even a slight drop of the value of the total reserves to be sure they will get the value price for their GYD.

-Governance has to make important and complicated decisions: There are several decisions to be made:

- Which assets should be used as collateral? A large list improves the scalability of the protocol, but it also increases the risk, since it exposes it to more assets.
- Weights of the vaults. These parameters determine the desired exposure on each asset.
- Values of the parameters of the redemption curves.
- Strategies on the vaults. At the moment vaults can only deposit their reserves into CLPs. But the docs claim that there will be possible other strategies related to investing the reserves of the vaults and these should be decided by governanceas well.

These are complicated issues and the optimal choices are not obvious.

-Not sufficient real-world data: At the moment there is only a restricted, with a capped supply of GYD -the total supply till now is 13,304 GYD [17]-. It would be necessary if someone wants to fork Gyroscope to have

[16] A.Klages-Mundt, S.Schuldenzucker, Gyroscope P-AMM: Designing Autonomous Markets for Stablecoin Monetary Policy

[17] https://app.gyro.finance/

sufficient data since these would be necessary for example in the complex parametrization of the protocol.

-Stability: The protocol has many mechanisms to support the peg of the stablecoin (P-AMM, secondary markets for GYD) and also some mechanisms to help it recover (yield generated by the reserves of the vaults, potential revenue from protocol fees -if governance decided so-), but even if the aim of the system is the stablecoin to be 100% covered by the reserves, the protocol cannot promise a hard floor price on redemptions all the time. This could harm the trust of the market in the protocol.

4 Maker [18]

4.1 Overview of the protocol

The stablecoin of the Maker protocol is called DAI. As a protocol that issues a stablecoin backed by on-chain assets as collateral, it has many similarities with Liquity, but also important differences. Maker protocol uses also a secondary token called MKR, which has a double role in the system: it is both a governance token and also plays a role in some stabilizations mechanisms of the DAI. Borrowing DAI Anyone can borrow DAI from the protocol by depositing the required amount of collateral. The protocol accepts a variety of assets as collateral decided by governance. The user has to open a Vault (collateralized debt position, same thing as Liquity's Trove), deposit there a collateral amount, and then the protocol will mint for him the requested amount of DAI, as long as the collateral ratio is greater than a minimum (this value is also decided by governance). Each vault should hold only one type of collateral (therefore if the user wants to borrow using a variety of collateral assets, he must open several Vaults) and the minimum CR depends on the type of the collateral. The user can claim his collateral (or part of it) if he pays back his debt plus a Stability fee (both in DAI). Each Vault type (Vaults can categorized by their collateral asser) is assigned an interest rate and the stability fee equals (interest rate)*(duration of the loan)*(debt in DAI) (of course this is a simplified formula since the interest rate is not necessarily constant).

4.1.1 Liquidations

Governance sets a Liquidation ratio for every Vault type (same as the MCR of Liquity). If the CR of a Vault falls below its Liquidation ratio the Vault gets liquidated. The liquidation procedure here is more complicated compared to Liquity and also much slower since it uses auctions.

4.1.2 Auctions

There are three types of auctions:

[18] https://makerdao.com/whitepaper/

Collateral Auction: If a vault is liquidated, the protocol initiates an auction to sell the collateral of the vault and get in return DAI to cover the debt of the liquidated vault. The first bidder offers an amount of DAI for the collateral of the vault. Then others can increase the bid, offering more DAI for the same amount of collateral. If there is a bid for the whole debt of the vault, a reverse auction starts: for this fixed amount of DAI, bidders offer this amount to get a decreased amount of collateral. In this case, the remaining collateral can be claimed by the owner of the vault. If the first part of the auction does not reach an offer equal to the whole debt of the vault, this extra debt is added to the total debt of the system and can be covered by a Debt auction.

Debt Auction: If the debt of the protocol surpasses a limit, the protocol starts a Debt auction. This is a reverse option. Users bid on how little MKR they are willing to accept for a fixed amount of debt (DAI). If the auction is successful the protocol gets the DAI from the winner, burns them, and gives him freshly minted MKR in return.

Surplus Auction: The protocol uses this auction to sell a fixed surplus (these extra DAI come from stability fees paid by the borrowers) amount of DAI for MKR. The protocol burns these MKR.

4.1.3 DAI Savings Rate (DSR)

DAI holders can stake their DAI into the DSR contract and earn extra DAI from the protocol's stability fees at a variable savings rate determined by governance. Generally, if the market price of DAI is >1 USD this rate will decrease and it will increase if the market price is <1 USD. Therefore DSR is not only a zero-risk investment for the users (they can get their DAI back any time) but also acts as a stabilization mechanism i.e. higher rates will incentivize users to mint more DAI and increase the supply (and therefore probably decrease the price), lower rates will lead DAI holders to repay their debt and therefore decrease the DAI supply and increase the value.

4.1.4 Emergency Shutdown

Under several circumstances e.g. non-responsive oracles, long-term market irrationality, hacks, the protocol governors can trigger the Emergency Shutdown. Many functionalities are limited then, but we are mainly interested in the fact that during an emergency shutdown, DAI holders can redeem their DAI and get collateral assets. Under normal circumstances, DAI are not redeemable. Users can only pay back their debt and get their collateral, but if someone just buys DAI in the market, he cannot redeem them for collateral using the protocol. This is an important difference with Liquity and a weakness of the Maker protocol.

4.2 Advantages and disadvantages

+Decentralized governance: Maker uses a decentralized governance model, which has the advantages of central governance i.e. the intervention to the protocol when it is needed e.g. after a hack, while allowing the users to participate in the governance of the system.

+Many stabilization mechanisms: The protocol does not rely only on the overcollateralization to keep the peg of the stablecoin, but it has many supplementary stabilization mechanisms: DSR, emergency shutdown, debt auctions.

+DSR: DSR allows DAI holders to earn extra DAI risk-free. It acts as a use case for DAI (someone can just borrow DAI, deposit them into the DSR contract for some time and then repay his debt, get back his collateral and sell the extra DAI from the DSR) and also as a stabilization mechanism.

+Careful use of oracles: Maker does not just read the prices of the collateral assets, when the protocol needs them, from the external oracles. The oracle prices have to go through the Oracle Security Module (OSM). OSM delays the propagation of the prices into the system and in the meanwhile it checks if they are reasonable, it can reject them if not, use emergency oracles and remove oracles if turned out to be adversarial.

-No hard price floor: The protocol does not support redemptions, therefore cannot impose a hard floor price (in contrast to Liquity), even if the total collateral ratio is >100% i.e. if a DAI holder bought his DAI at the market and does not have a Vault in the protocol, he cannot exchange his DAI for collateral into the protocol and he should find another place to sell them and hope that he gets a price of at least 1 USD (which is probably usually true). Redemptions are only possible during Emergency Shutdown, but this is a rare case when the protocol is in really "bad health" economically and serves as a last resort.

-Capital efficiency: The slow liquidation procedure (using auctions) forces Maker to have a much higher minimum required collateral ratio. The exact value of the minimum collateral depends on the collateral type of the vault. For example, there are Vaults with ETH as collateral and the minimum required CR ranges from 120%-170%, while on Liquity it is just 110%.

-Complex governance: Governance plays a serious role in the Maker protocol. MKR holders can vote about:

- Adding new collateral assets
- Defining/changing the Risk parameters (Liquidation Ratio, maximum cap) of a Vault type
- Trigger the Emergency Shutdown

- Update the DSR

Maker managed to build a large and active community that seems, till now, to be able to complete all these tasks. It would be a serious challenge for a fork of Maker to build such a community. If you replace voting via governance tokens, with a centralized governance model, then all these decisions should be made by the chosen governors, therefore they should be really sophisticated. Another problem of the governance model of Maker is that MKR is used both as a governance token (for voting) and also at some stabilization mechanisms of the stablecoin (surplus and debt auctions). The problem is that this double use of MKR builds a strong correlation between the MKR and DAI price i.e. a drop in the MKR price, would affect the stabilization mechanisms and therefore the DAI price and, if the DAI price decreases, this certainly makes the governance token less attractive and further decreases its price.

-Interest: The users of the protocol should pay interest (called Stability fees) for the DAI they are borrowing. This seems less appealing compared to Liquity's one-time fee, especially for long-term borrowers.

5 Frax [19]

5.1 Overview of the protocol

FRAX is a partially collateralized algorithmic stablecoin. The Frax protocol issues also a secondary token (FXS: Frax Share), which plays a dual role as a governance token and a supporting mechanism for FRAX.

The idea of the protocol is that of a stablecoin backed by other on-chain assets, but not only exogenous collateral but also FXS i.e. to mint n FRAX the user should deposit collateral asset and FXS of total value n USD. Initially, the stablecoin is fully backed by collateral [20]i.e. the user deposits collateral of value x USD, and the protocol mints for him x FRAX. This is the 100% collateralization phase. An x% collateralization phase means that the user has to deposit only x% of the required value as a collateral asset and the rest (1-x)% as FXS. The case x=100 corresponds to a fully backed by collateral stablecoin and the x=0 to a purely algorithmic stablecoin. More precisely if

- F is the amount of the requested FRAX

- X collateral asset amount deposited by the user

[19] https://docs.frax.finance/

[20] Currently, the protocol allows only stablecoins as collateral (mainly USDC), but the DAO can vote to add other collateral assets.

- Y amount of FXS deposited by the user

- p_X, p_Y USD prices of the collateral asset and the FXS token respectively

at the x% collateralization phase, all these quantities are related by the equations:

$$F = p_X \cdot X + p_Y \cdot Y$$
$$x = \frac{p_X \cdot X}{F} \cdot 100$$

Given , we can solve these equations and find the collateral and FXS amounts the user should deposit. For example, if the collateralization is 80% and the user wants to mint 100 FRAX, he should deposit 80 USD of collateral and 20 USD of FXS tokens. The protocol keeps the deposited collateral and burns the FXS amount. On redemptions, the protocol burns the redeemed FRAX tokens and the user gets collateral and freshly minted FXS.

Once per hour, anyone can call an update-the-collateralization-x function. If the market price of FRAX is >1 USD x increases by 0.25% and if it is <1 USD it decreases by 0.25%. The protocol uses TWAPs from AMMs to get the price of the FRAX and FXS tokens.

If there is an excess of collateral in the system i.e. if the x% drops, the protocol invests this extra collateral. Either deposits it as liquidity to Uniswap or Curve pools, or to other yield-generating protocols (Aave, Compound, Yearn).

5.2 Advantages and disadvantages

+Low minting and redemption fees: The protocol does not use the fees as a stabilization mechanism, therefore it can keep them low.

+Scalabity: This is the main advantage of all algorithmic stablecoins.

+Stable compared to algorithmic stablecoins: The use of exogenous collateral makes the FRAX stablecoin more stable compared to purely algorithmic stablecoins.

]item [-Possible fast changes of the collateralization:] The protocol allows updates of the collateral ratio once per hour. There are no other restrictions. This fast varying collateralization can harm the trust of the market in the protocol since it is not possible to predict the long-term percentage of FRAX which is actually backed by collateral.

-Strong interdependence of the FRAX and FXS prices (possible death spirals): An increased market price for FRAX will decrease the collateralization and increase the demand for FRAX (users want to mint FRAX from the protocol at face value and sell them in the market where the price is higher). Users will burn FXS to mint FRAX, decreasing the supply and increasing the price of FXS. On the contrary, if the market price of FRAX is low, users will redeem FRAX for collateral and FXS, and the price of FXS will also decrease. Since part of the FRAX is “backed” by FXS, a low FXS price will probably harm the trust of the market which could lead to bank runs and further decrease of the prices.

6 Curve [21]

crvUSD is a new stablecoin designed by Michael Egorov, the creator of the Curve protocol. It is a stablecoin based on CBDs (collateralized debt positions), similar to Liquity, but with a novel liquidation mechanism. Instead of a tight threshold for liquidations, it supports gradual/partial liquidations using an AMM-like mechanism called LLAMMA (lending-liquidating automatic market maker algorithm). To fully understand the design of crvUSD, someone has to be familiar with the idea of concentrated liquidity and Uniswap v3, but we will briefly describe the main idea without many technicalities. As with all CBD-based stablecoins, the user deposits collateral and borrows freshly minted stablecoins. The protocol does not keep this collateral in a vault but deposits it as liquidity in a Uniswap v3 AMM. The protocol decides the ticks/price-bands where this liquidity should be placed, based on the current price of the stablecoin and other factors. For example, let’s assume that ETH is the collateral asset, the current price of the ETH is 2.1k and the user deposits 4 ETH as collateral. The protocol could deposits these 4 ETH as liquidity in the following ticks (These numbers are not realistic and we just use them to keep the example simple)

- 1 ETH in the band 1.7k-1.8k
- 1 ETH in the band 1.8k-1.9k
- 1 ETH in the band 1.9k-2k
- 1 ETH in the band 2k-2.1k

If at some point the market price of ETH decreases to 1.9k, the last two ticks are crossed and the user now holds 2 ETH, distributed in the first 2 bands, and the other 2 ETH of the 3rd and 4th bands were exchanged (using uniswap v3 rule) for a number of stablecoins. If the price increases again,the stablecoins are exchanged for ETH again (this is what the word ”deliquidation” in the whitepaper means). If the price is in a band, the user will hold simultaneously ETH and stablecoins in a ratio computed using the uniswap v3 rule.

There are two types of liquidations:

The classical one: the protocol uses a measure, similar to CR, called the health factor of the position. If this drops below 0, anyone can repay the debt of the position in crvUSD, the protocol will burn these tokens, remove the liquidity corresponding to the collateral of the liquidated position and give it to the liquidator.

[21] https://github.com/curvefi/curve-stablecoin/blob/master/doc/curve-stablecoin.pdf

A novel type of partial and reversible liquidation: the protocol uses also an external oracle to determine the spot price on the AMM (this is completely different compared to classical uniswap-like AMMs). If the price of the collateral token falls, the price in the amm will become even lower (this is achieved by a proper choice of parameters in the design of the LLAMMA). Therefore arbitrageurs will use the amm to buy collateral tokens from the AMM to sell it to the market. They have to swap crvUSD for this collateral. The result is that part of the collateral of the depositors is transformed into stablecoins. But this is reversible, since if the market price of the collateral token increases, arbitrageurs will sell collateral tokens to the amm, restoring the collateral of the users.

The partial liquidation mechanism is the main advantage of crvUSD compared to other collateralized products. Its disadvantages are the complex parametrization (even the specifics of LLAMMA are not optimally chosen) and the delicate interaction between the special purpose AMM and the market which is the main stabilization mechanism. The design we briefly described could change since the smart contracts are constantly updated. You couldn't find any details about the launch date, any testnet deployment or simulations about this coin.

7 Aave [22]

A couple of months ago the Aave protocol launched the protocol's native stablecoin (GHO) on testnet. There are no new ideas in the design of this stablecoin, but it has some advantages related to the role of GHO in the Aave ecosystem -therefore non-applicable if someone builds a fork of GHO-. GHO is a stablecoin following the idea of CBDs (collateralized debt positions) as LUSD and DAI. A variety of assets can be used as collateral. The user can back the GHO he borrows by any combination of collateral assets from a list of approved ones (he does not need to open a new position for each collateral asset and this is an improvement compared to DAI). The CR of the position should be higher than a minimum value, otherwise, the position can be liquidated i.e. someone can repay the debt of the position and will get the collateral supporting it (since the positions are overcollateralized, the liquidator is expected to have some net profit). As long as the position is not yet liquidated, the user can repay his debt plus the interest and get back his collateral. The collateral assets supported initially will be assets already used in the Aaave protocol. The Aave protocol is a lending protocol. While deposited as collateral, the protocol can lend the collateral assets. Therefore the deposited collateral on a position accrues interest, which belongs to the owner of the position (the user you deposited his collateral to borrow GHO). This interest paid to the user for his deposited collateral can be seen as a discount on the interest he has to pay for the GHO. There is also an explicit discount on the interest rate of GHO for users depositing stkAAVE tokens as collateral (these users have staked their AAVE token to support the

[22] https://docs-gho.vercel.app/concepts/faq

Aave protocol and this is the reason they are rewarded with this reduced interest rate). The protocol uses also another mechanism called FlashMinter to support the peg of the stablecoin, which can mint and burn GHO without anyone needing to deposit collateral. The Aave governance plays an important role in the stablecoin protocol as it has to decide the minimum collateral ratio, the interest and discount rates, the strategy of the FlashMinter.

About Common Prefix

Common Prefix is a blockchain research, development, and consulting company consisting of a small number of scientists and engineers specializing in many aspects of blockchain science. We work with industry partners who are looking to advance the state-of-the-art in our field to help them analyze and design simple but rigorous protocols from first principles, with provable security in mind. Our consulting and audits pertain to theoretical cryptographic protocol analyses as well as the pragmatic auditing of implementations in both core consensus technologies and application layer smart contracts.