Gyroscope P-AMM: Designing Autonomous Markets for Stablecoin Monetary Policy

5 May 2022

—PATENT PENDING—

Ariah Klages-Mundt
Superluminal Labs

Steffen Schuldenzucker
Superluminal Labs

ABSTRACT

We develop a new type of automated market maker (AMM) that helps to maintain stability and long-term viability in a stablecoin. This primary market AMM (P-AMM) is a primary market issuance mechanism for autonomously pricing minting and redemption of stablecoins in all possible states and is designed to achieve several desirable properties. We first cover several case studies of current ad hoc stablecoin primary market designs, several of which have contributed to recent stablecoin de-peggings, and formulate desirable properties of a P-AMM that support stability and usability. We then design a P-AMM redemption curve and show that it satisfies these properties, including bounded loss for both the protocol and stablecoin holders. We further show that this redemption curve is path independent and has properties of path deficiency in extended settings involving trading fees and a separate minting curve. In particular, we show that system health weakly improves relative to the path independent setting along any trading curve and that there is no incentive to strategically subdivide redemptions. Our mechanism can be implemented efficiently on-chain.

KEYWORDS

Stablecoins, Automated Market Makers, Currency Peg, DeFi

1 INTRODUCTION

The design of non-custodial stablecoins has faced several recent turning points, both in the Black Thursday crisis in Dai and the recent churn of algorithmic stablecoins. These have both pointed toward the importance of designing good primary markets for stablecoins —i.e., mechanisms for pricing minting and redeeming of stablecoins.[1] Black Thursday in March 2020 saw a $\sim$ 50% crash in ETH in the day. This triggered a deleveraging spiral, a short squeeze effect that amplifies collateral and liquidity drawdown, in the stablecoin Dai [10, 11]. This demonstrated fundamental problems around deleveraging, liquidity, and scaling in leverage-based stablecoins, like Dai, in which supply depends on an underlying market for leverage.[2]

PSM: a primary market for Dai. Patching the deleveraging problem has been a major topic since Black Thursday. Several approaches have been pursued, the most prominent of which is the tethering of Dai to the custodial stablecoin USDC.[3] This takes the form of Maker's peg stability module (PSM), which maintains exchangeability of Dai with USDC via a protocol-held USDC reserve. The PSM in this way effectively becomes a primary market for minting and redeeming Dai, backed by USDC reserves. The PSM has greatly enhanced the liquidity around Dai's peg and its resilience to deleveraging spirals, as evidenced in Figure 1a, which plots Dai price for days t since the major ETH shocks of 12 March 2020 (w/o PSM) and 19 May 2021 (w/ PSM). However, this has further exposed the scaling problem of the original Dai mechanism: the leverage market doesn't necessarily scale with demand. Since the May 2021 crisis, Dai backed by USDC has grown from 17% to now over 60% of the Dai supply (Figure 1b), arguably compromising the effective decentralization of Dai by importing the custodial and regulatory risks of USDC.

Algorithmic Stablecoins. The problems with Dai, including its most recent USDC centralization issue, has also motivated a wave of algorithmic stablecoins, which aim to keep the stablecoin supply in line with demand algorithmically. While these designs can have varying (and sometimes dubious) degrees of asset backing, we use the term more generally to include 100% reserve backing as well. Most of the algorithmic stablecoins that have been launched have experienced depegging events, as depicted in Figure 2, often due to susceptibility to downwards spirals and ad hoc primary market structure.

These types of stablecoins are best understood in the context of currency peg models, such as [14]. In a simplified sense, these systems are backed by two sources of value: (i) asset backing in a currency reserve and (ii) economic usage, an intangible value that represents the demand to hold the currency as it unlocks access to an underlying economy. Supposing these two values are together great enough, a currency peg is maintainable; otherwise, it is susceptible to breaking. A peg break can also be triggered by a speculative attack that is profitable for the attacker, akin to the attack on the British pound on Black Wednesday.

[1] The terminology is borrowed from ETF market structure and contrasts "primary market", where shares are minted and redeemed for underlying assets, and "secondary market", where existing shares are traded for other assets (and where ordinary exchange trading takes place).

[2] In this market, a speculator can post collateral and borrow Dai against this collateral to achieve a risky leveraged position. As a result, the supply of Dai will depend on the demand for leverage, which can and does plummet in a crisis.

[3] Two other notable approaches are using negative rates to equilibrate supply and demand at the target value (e.g., Rai) and using dedicated liquidity pools to smooth the effects of deleveraging in crises (e.g., Liquity and the solution proposed in [11]). The former leads to questions of liquidity and equilibrium participation under negative rate regimes, and the latter is not a full fix as it smooths but postpones the potential spiral.

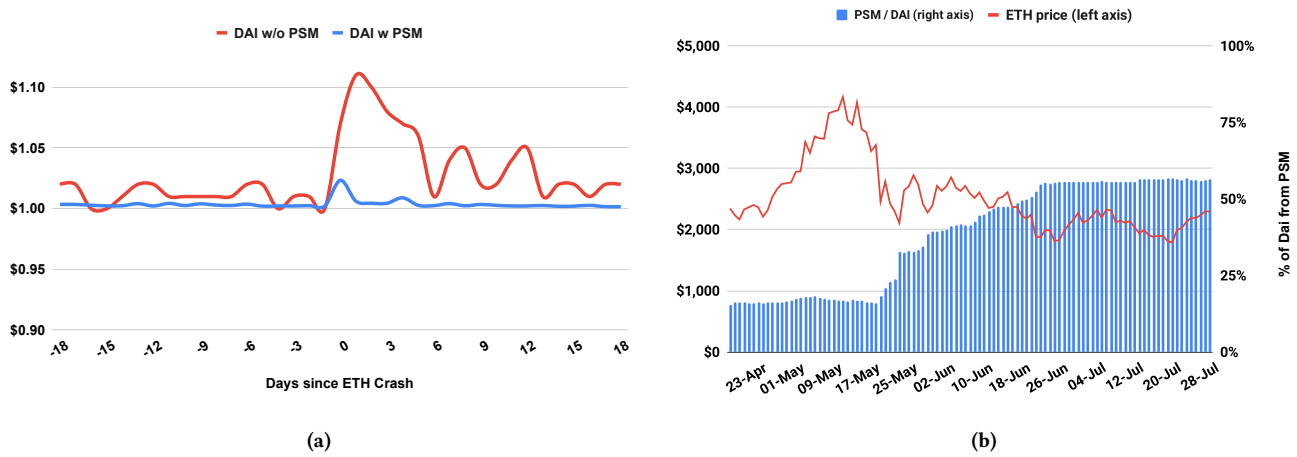


Figure 1: Effects of the Dai PSM. (a) Dai price for days t since major ETH shocks w/ and w/o the PSM, (b) The portion of Dai issued through the PSM has grown $> 3\times$ since the May 2021 ETH shock.

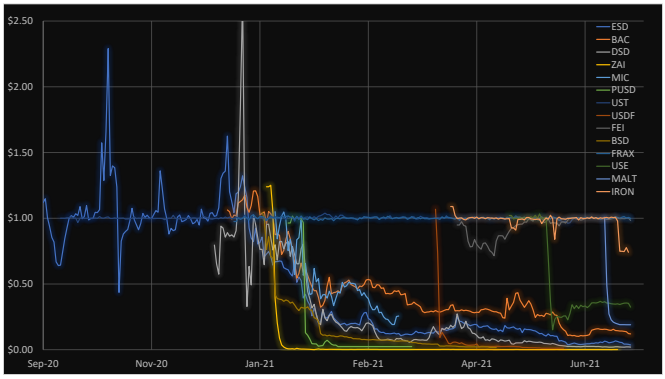


Figure 2: The recent churn of algorithmic stablecoins in 2021.

Algorithmic stablecoins have encountered several fundamental problems, which contribute challenges to strong primary market design. Many have tried to start out under-reserved while having no native economic usage, leading to many observed depeggings through downwards spirals, often exhausting the assets backing the system. Further, the composition of reserve assets that can be held on-chain are inherently risky. In some cases, these assets are non-existent (e.g., Basis). In seigniorage shares–style designs (e.g., Terra and Iron), the backing is effectively the value of "equity shares", which have an endogenous/circular price with the expected growth of the system [9]. A further type is backed by a portfolio of some mix of exogenous, but risky, assets. Both of these must factor in when formulating a good policy for how the protocol applies reserve assets to maintain liquidity near the peg in sustainable ways. This challenge effectively becomes the problem of designing a primary market for the stablecoin.

1.1 Primary Markets: Related Work

Our work is most closely related to currency peg models in international economics (e.g., [8, 14]) as well as models of pegged money market mutual funds (e.g., [16]). Although these types of models have been discussed and adapted recently in the context of stablecoins (e.g., [13, 18]), there is no prior work building a cryptocurrency mechanism that can adapt the lessons of good currency peg policies. Our work constructs such a mechanism from first principles that functions in a novel way as an autonomous primary market for stablecoin issuance. This can be thought of as a passive, pre-programmed version of open market operations embedded in a stablecoin protocol. For further academic background on stablecoins, we refer to [4, 9, 17] and references therein.

For an overview of theory work on AMMs, we refer to [2, 3, 5]. Further background and references are available in [20]. Current AMMs resemble Uniswap [1] and Curve [7], in which liquidity providers add pairs of assets to a pool that quotes trading prices algorithmically depending on the state of the pool. Such AMMs are *secondary markets* in which assets that already exist are traded. In contrast, we develop a new type of AMM that plays the role of a *primary market*, in which assets are minted and redeemed against the protocol itself. No existing work analyzes such constructions for stablecoins.

A well-designed primary market for a stablecoin can be interpreted as a mechanism for open market operations of a central bank (in this case, often a decentralized central bank). When new stablecoins are sold on the primary market, the balance sheet is expanded, and when stablecoins are redeemed, the balance sheet is contracted. The primary market design determines how much the balance sheet changes, supposing all proceeds of the market go onto the balance sheet.[4] Notice here that the primary market mechanism essentially solves the scaling issues that arise in leverage-based stablecoins, like Dai: the stablecoin is always able to meet excess demand by

[4]Notably, many algorithmic stablecoins divert a share of primary market cash flow to holders of "equity" tokens —we consider such systems *insolvent-by-design* as they give away part of the "seigniorage" income from purchases of newly minted stablecoins (typically via buybacks of "equity" tokens), unlike a bank that maintains full asset-backing of deposits. This structure has contributed to many experienced crises for these coins.

expanding the balance sheet (it does not need to match the demand of other agents in doing so).

In some ways, designing a truly algorithmic primary market presents a challenge akin to designing a Taylor rule (see, e.g., [15]) for monetary policy. However, rather than setting nominal interest rates in a quasi-algorithmic way, an algorithmic primary market is setting prices in a programmatic way. As this is not reliant on an assessment of the output gap and GDP, among other things that can't be measured accurately, we might expect this to be easier and more robust (it is notoriously difficult to formulate traditional Taylor rules that are robust to wide arrays of settings).

In this paper, we consider the wider problem of designing good primary market mechanisms for minting and redeeming stablecoins. We first cover several case studies that illustrate the consequences of different primary market shapes. These help to explain the issues these stablecoins have faced and illustrate that existing primary markets —which are often not directly recognized as primary markets— are ad hoc in design, both in the shapes chosen and the ability to adapt shape to changing circumstances. One general consequence of this ad hoc structure is that existing systems are left to rely on protocol governance to make quick fixes to primary market shape in a crisis, which further introduces vectors for governance abuse (e.g., governance extractable value [12]). This can cause significant problems in decentralized and pseudonymous systems.

1.2 Primary Markets: Case Studies

In contrasting the shapes of primary market mechanisms, it will be useful to interpret these as automated market makers (AMMs), which price the exchange of assets algorithmically along a curve as a function of reserves and possibly other state variables.[5] Sometimes these are explicit AMM curves implemented by the protocol, while other times we must factor in the effects of several mechanisms to find an implicit AMM curve that describes the primary market. This AMM structure will depend on the assets backing the system. In some cases, these assets are *implicitly* backing the system, such as in seigniorage shares systems. Other times, they are a portfolio of assets more explicitly. We will refer to this asset backing as the *reserve assets*.

A primary market can be separated into two curves (possibly coinciding): a minting curve and a redemption curve. These curves price the stablecoin in terms of underlying reserve assets as a function of system state (e.g., level of redemptions and reserve health). To illustrate, Figure 3a shows some stylized possible redemption curves, plotted as a function of redemption level. An advanced redemption curve might shift the curvature of the 2-d curve as other variables in the state change (e.g., reserve health). Note that, should the reserve assets backing the system be exhausted, the redemption curve becomes flat at \$0, as depicted in Figure 3b.

USDC/USDT. Custodial stablecoins like USDC and USDT have flat redemption curves at ~ \$1. Note that this primary market has a large off-chain component, where dollars are actually exchanged for stablecoins. Because of this off-chain component, users must trust the issuer to maintain the primary market. There are various reasons why this may not happen or may not be possible, including custodial and regulatory risks as well as potential loss on risky reserve assets. Note that Dai's PSM discussed above essentially borrows USDC's primary market by wrapping USDC, and so the PSM redemption curve is similar.

In traditional finance, e-money, money market mutual funds with pegged redemptions, and exchange traded funds (ETFs) also bear resemblance to this type of primary market structure.

Basis. In Basis-type designs, including basis Cash and Empty Set Dollar, there is an implicit redemption curve for "coupons", which promise to be redeemable for a multiple of new stablecoins in the event that new stablecoins are minted if new demand enters the system later. Often, these coupons also expire a certain time after creation. However, since there is no asset backing of the system (all income from selling newly minted stablecoins is disbursed to various stakeholders), there is no redemption available for exogenous assets. In the event that stablecoin demand and willingness to speculate on growth of the system deteriorates, the value of these coupons circularly goes to zero, and the redemption curve becomes flat at \$0.[6] As seen in Figure 2, these systems did not maintain a peg both because of this solely circular value structure and the lack of a supporting primary market mechanism.

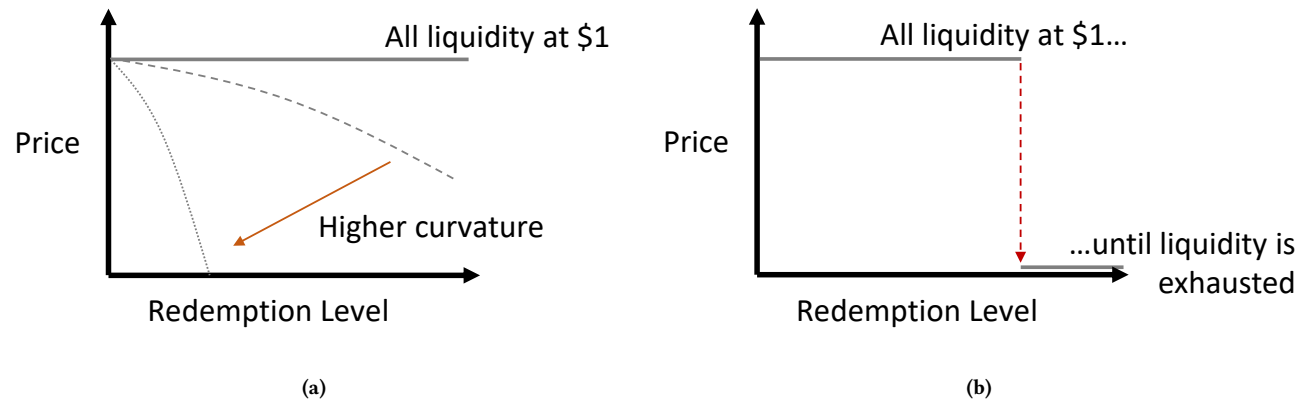
Fei. The Fei stablecoin places reserve assets in a constant product AMM pool. The action that can be interpreted as redemption is to sell Fei for ETH in this pool. At launch, this pool was designed with a fee that grows quadratically in the amount of redemptions (what was called "direct incentives"). This has the effect of distorting the implicit Fei redemption curve into a poor shape, as visualized in Figure 4a that essentially guarantees low primary market liquidity during a supply contraction, leaving Fei holders entrapped once secondary market liquidity dries up, even under good reserve health.

This is precisely what happened following the Fei launch in April 2021. Although initially intending to be under-reserved at launch, the system actually started over-reserved because of appreciation in the ETH reserve asset. As the initial Fei supply was much higher than demand, many holders sought to exit the system. Despite the effectively high reserve ratio, the implicit redemption curve was unable to handle the size of sought redemptions, leading the stablecoin to deviate erratically from the peg, as seen in Figure 4b. The direct incentive mechanism was later removed, shifting the implicit redemption curve to the constant product curve visualized in Figure 4a. Later, Fei governance chose to forgo this implicit redemption curve by offering direct redemptions at \$0.95.

Iron/Seigniorage Shares. The Iron stablecoin was intended to be ~ 74% backed by USDC and the remaining portion backed by the seigniorage shares-style token, Titan. It was redeemable proportionally for a basket of both, inflating the Titan supply to fulfill the Titan portion of redemptions. The redemption curve was intended to be flat at \$1. However, since Titan was a volatile and endogenous/circularly priced asset, there was no guarantee that its market cap would be enough to support its share of the Iron backing. In fact, a downwards spiral was triggered, in which Iron would see mass redemptions, and the value of Titan would go to zero, leaving

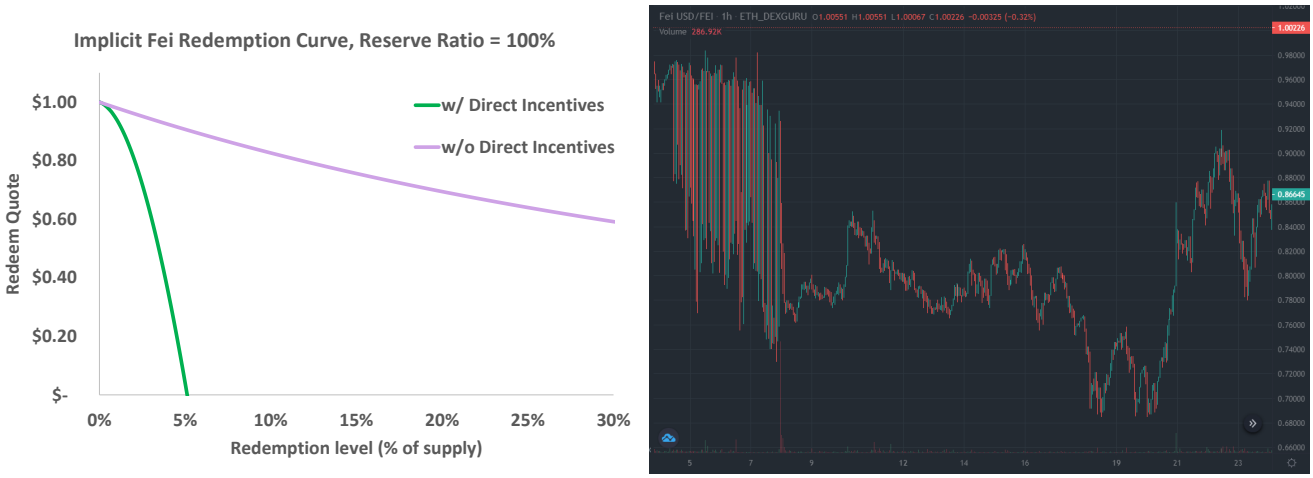
[5] For recent background on AMMs, see [2], which focuses on constant function market makers (CFMMs). However, primary markets will not fit this category in general.

[6] Note that while these coins may be sold for > \$0, such a trade occurs on secondary markets as opposed to primary markets.



(a) (b)

Figure 3: Stylized primary market redemption curves.



(a) (b)

Figure 4: Fei case study. (a) implicit redemption curve shape w/ and w/o direct incentives. (b) depegging following large redemptions at launch.

the redemption price of Iron at the ~ $0.74 worth of USDC. This is a variation on the stylized redemption curve in Figure 3b and is precisely what happened in June 2021 as shown in Figure 5.

1.3 Desiderata for P-AMM Design

A major missing piece in the current space is the rigorous design of stablecoin primary markets developed from first principles. As we've seen in the previous case studies, the primary market design plays a large role in the stability of these systems. Up until this paper, it is not well-specified what the desirable properties are in designing these primary markets. We first tackle this issue before continuing on the design of our primary market automated market maker (P-AMM) redemption curves in the remainder of this paper.

We strive for several desiderata in the design of a primary market mechanism that has good properties from stability and usability perspectives. We separate these into properties of the P-AMM within a block and more general properties.

Within a block, the following properties are desirable.

(1) The relative collateralization (i.e., reserve ratio) of the protocol is guaranteed to stay above a lower bound (unless this is impossible because of an exogenous shock to reserve assets).
(2) The P-AMM normally maintains a region of open market operations in which the stablecoin price is ~ $1.
(3) The worst-case P-AMM redemption rate is lower bounded.
(4) The P-AMM redemption curve is continuous and not too steep, unless this would violate the other desiderata.
(5) There is no incentive for redeemers to strategically subdivide redemptions.

(a) (b)

Figure 5: Iron case study. (a) following a downwards spiral, Iron redeemable at $0.74. (b) Titan market cap going to zero during the attack.

The first property means that the loss for the protocol is bounded, as the reserve is never exhausted in the operation of the P-AMM unless all reserve asset prices exogenously go to zero. The second property means that the stablecoin can support a possible equilibrium price at the dollar target. The third property means that the loss for stablecoin holders who redeem is bounded. The fourth and fifth properties are motivated by usability: it is simpler for traders to use when the pricing is continuous and predictable and strategy in optimal order reporting is simple and minimized. Property four further reduces risk for traders and incentives for potential speculative attacks. As we will see, the fifth property is related to notions of path independence and path deficiency.

More generally, and across blocks, we desire the following properties.

(6) Over many blocks, the reserve can only be exhausted over a long time period.
(7) Over many blocks, a de-pegged stablecoin has a path toward regaining peg.
(8) The P-AMM mechanism can be efficiently implemented and computed on-chain.

The sixth property ensures that the stablecoin's asset backing persists well into the future (e.g., speculative attacks on the system cannot exhaust the reserve). The seventh property means that there are credible reasons why speculators could decide to bet on re-pegging of the stablecoin during a crisis. The eighth property ensures that the mechanism could be used under the severe computational restrictions of real world smart contract systems (e.g., is not prohibitive in terms of gas fees on Ethereum).

1.4 This Paper

We now turn our attention to the rigorous design of stablecoin primary markets with these desirable properties. In particular, a well-designed curve will be able to adapt shape/pricing autonomously to achieve these properties. Aside from the value of the properties themselves, which enhance the survival and usability prospects of the stablecoin, such a formulation will require minimal intervention by governance, further limiting risks from governance extractable value. In the remainder of this paper, we confront this challenge in designing our P-AMM.

We make the following contributions in this paper.

- We formulated the desirable P-AMM properties as desiderata in Section 1.3 and covered several case studies of current ad hoc designs in Section 1.2.
- We design the P-AMM redemption curve implicitly in Section 2. We prove that this curve is well-defined in Sections 3-4, culminating in Theorem 1, as well as establishing that its shape satisfies several desiderata directly (Prop. 2, Lemma 1, Prop. 4). we also formulate a simpler redemption curve that satisfies many, but not all, desiderata in Appendix A.
- We show that the P-AMM redemption curve is path independent in Section 5 (Theorem 2) and further consider an extended setting with trading fees and minting, which we show has properties of path deficiency. In particular, we show that system health weakly improves relative to the path independent setting along any trading curve (Theroem 3) and that there is no incentive to strategically subdivide redemptions (Theorem 4).

Our mechanism can be implemented efficiently on-chain. The results in Section 4 imply that it is mathematically well-defined how to transition from one state to the next when a redemption takes place, but the proof of this result is not constructive. The mechanism can be described in an equivalent way that *is* constructive and efficiently implementable. However, this requires multiple optimization techniques and further structural results that are beyond the scope of the present paper.[7]

The output of this paper is an autonomously adapting P-AMM that satisfies the desired properties throughout the possible state space. The P-AMM formulation contains a few select hyperparameters, which can in principle be tuned by governance; however, the desired properties stand over the entire parameter space. In particular, if parameters are tuned, it does not need to happen on-the-fly, thus still minimizing the reliance on governance intervention.

[7] This work is not yet publicly available.

Note that the stablecoin peg target is implicitly \$1. However, the mechanics remain fully functional under any arbitrary target within a block. Through adapting this implicit parameter, the system could also implement much more arbitrary monetary policy while retaining desirable properties.

We make two important, but not contentious, assumptions in this work. First, we exclude endogenous/circularly priced collateral by assuming that reserve assets are exogenously priced. Second, we assume that the system has an accurate oracle that provides the price of reserve assets in USD. The need for an oracle is inescapable in a stablecoin that pegs to outside assets, so this is not an unusual assumption. Since oracles can provide manipulation surfaces (see, e.g., [20]), it is important to incorporate other protective mechanisms; however, these are separate from the P-AMM mechanism itself.

2 REDEMPTION CURVE DESIGN

For the purpose of designing the P-AMM, we model the system along three dimensions: an outstanding stablecoin (SC) supply y, a total reserve value backing the stablecoin b, and a level of stablecoin redemptions from the reserve x. These state variables are summarized in the following table.

State Variable	Definition
b	total reserve value (in USD)
y	outstanding SC supply
x	level of SC redemptions

We model the system as a dynamical system, in which x is the independent variable that drives the system. Put another way, x will represent the "current point along the trading path" of the P-AMM. We will also be interested in the *reserve ratio* $r(x) := b(x)/y(x)$, which describes the reserve value per outstanding stablecoin.[8]

The dynamical system models P-AMM trades that occur within a single block. At the beginning of the block, we will have initial conditions (x_0, b_0, y_0). Here, x_0 represents a measure of redemption history in previous blocks. Net redemptions within the modeled block will increase x from x_0. The final P-AMM will evolve over many blocks using this same intra-block model; however, x_0 at the start of each block will be computed as an exponentially time-discounted sum over all past SC redemptions in previous blocks. For our analysis in this paper, we restrict ourselves to the context of a single block, in which x_0 is a fixed initial condition. The initial conditions are summarized in the following table.

Init. Condition	Definition
x_0	level of SC redemptions at block start
b_0	reserve value at block start ($b_0 = b(x_0)$)
y_0	SC supply at block start ($y_0 = y(x_0)$)

Since, in the final P-AMM, x_0 in a given block will be computed as an exponential time-discounted sum of redemptions in past blocks, we will generally not have $x_0 = 0$ in practice. However, it will be useful to reference a fictitious initial condition that would describe a starting point of 0. We call this the *anchor point*, which is formally the triplet

$$(0, b_a, y_a),$$

[8]We will write b, y, x and r referring to the "current' state of these variables. In contrast, we will write $b(x)$ etc for the value at some point of the driving variable x and based on other system parameters.

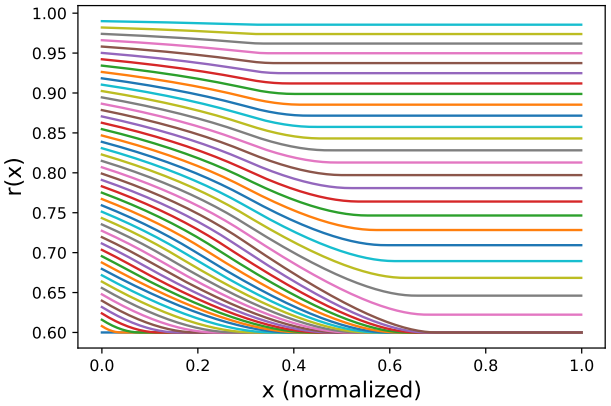


Figure 6: Reserve ratio curves as a function of x for different values of r_a (starting points) in the "normalized" case where $y_a = 1$.

where $b_a = b(0)$ and $y_a = y(0)$. Many times, we will be interested in the reserve ratio at the anchor point $r_a = b_a/y_a$. Figure 6 visualizes what the reserve ratio curves will look like as a function of x for various values of r_a. As we will see, each curve will have a unique anchor point r_a, which corresponds to the starting point of the curve.

We introduce a simplified P-AMM redemption curve in Appendix A as a pedagogical starting point. This simplified curve has discrete price decay (i.e., the curve is discontinuous: a portion of the curve is at \$1 and another portion maintains a sustainable reserve ratio) and is very simple to reason about. This fulfills many desirable properties except for continuity. To maintain continuity, we instead develop a three-piece-wise curve design, which requires some more sophisticated machinery.

We now move on to constructing the P-AMM redemption curve. We parameterize this curve in terms of *dynamic parameters*. Concretely, this means that, given specific values of these parameters, the shape of the redemption curve is fixed. However, these dynamic parameters themselves depend on the state of the system (more in detail, they are functions of the anchor point). Conceptually, the three dynamic parameters describe three regions of the P-AMM pricing curve p as a function of x, as visualized in Figure 7. For simplicity of analysis, we will for now disregard any trading fees that may be added to the P-AMM. The first region provides redemptions at \$1 up until the redemption level x_U is reached. In the second region, the P-AMM pricing decays linearly with slope α as more redemptions occur up until redemption level x_L. The third region provides redemptions at the new reserve ratio (reserve value per outstanding stablecoin), which is fully sustainable for the entire stablecoin supply. The dynamic parameters are summarized in the following table.

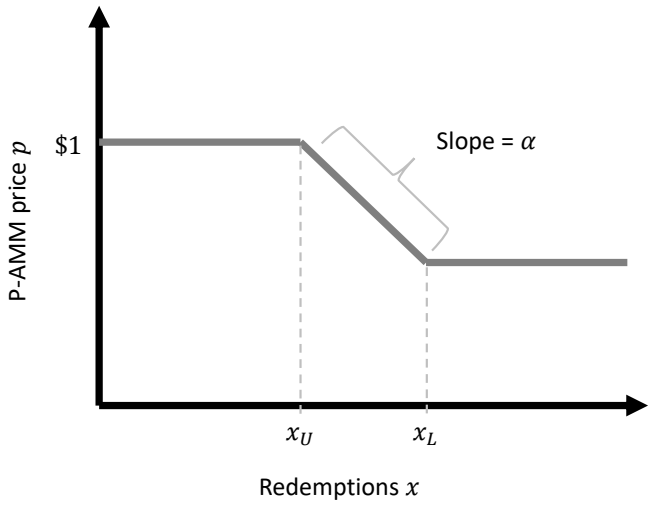


Figure 7

Dynamic Params	Definition
α	decay slope of redemption curve
x_U	point at which redemption deviates from \$1
x_L	point at which redemption stops decaying at new reserve ratio

The resulting P-AMM pricing curve, as a function of x and parameterized by the anchor point, is, in the case that $b_a < y_a$,

$$p(x; b_a, y_a) = \begin{cases} 1, & x \le x_U \\ 1 - \alpha(x - x_U), & x_U \le x \le x_L \\ r_L, & x \ge x_L \end{cases}, \tag{1}$$

where $r_L = r(x_L)$. In the other case that $b_a \ge y_a$, we will simply set $p(x) = 1$. Notice that the dynamic parameters α, x_U, x_L are, in fact, functions of the anchor point (b_a, y_a). We discuss the rules by which the dynamic paramters are chosen in Section 3.

We define three *static parameters* that constrain the shape of the curve and inform the choice of the dynamic parameters. These are the only parameters that are set externally. We define a lower bound $\bar{\alpha}$ to the linear decay slope α, an upper bound $\bar{x}_U$ to x_U, and a target reserve ratio floor $\bar{\theta}$. The target reserve ratio floor is the minimum reserve ratio that the P-AMM curve can decay to, and it is the value of the reserve ratio in the third region. In case that the initial reserve ratio b_0/y_0 is smaller than $\overline{\theta}$, the P-AMM only offers redemptions at the initial reserve ratio (i.e., $x_L = 0$). These parameters are summarized in the following table.

Parameter	Definition
$\bar{\alpha}$	$\in (0, \infty)$ lower bound on decay slope ($\alpha \ge \bar{\alpha}$)
$\bar{x}_U$	$\in [0, \infty]$ upper bound on x_U ($x_U \le \bar{x}_U$)
$\bar{\theta}$	$\in [0, 1]$ target reserve ratio floor

Note that an implicit fourth static parameter is the target for the stablecoin price, thus far assumed to be \$1. In general, this could take different values (and could be changed over time by governance) to adjust monetary policy. The underlying mechanics and our essential results would stay the same.

In this paper, we are agnostic to how the static parameters were set and consider them fixed, but arbitrary. One particularly useful choice would be to set them proportional to the anchored outstanding SC supply y_a, which we believe would minimize the need for governance interaction as the outstanding amount changes.

Recall that the pricing curve p above is parameterized by the anchor point and is, in general, a function of b_a and y_a. We will see that the anchor point can be expressed in terms of the current state alone. With this in mind, it will be analytically useful to define the evolution of the dynamical system in terms of the current state (x, b, y) directly. Toward this, we will construct an abstract pricing function $\rho(x, b, y)$ that we will show is equivalent to the function p in case $b/y < 1$; in the (trivial) case where $b/y \ge 1$, we set $\rho(x, b, y) = 1$. The dynamical system is then described by the following system of ordinary differential equations:

$$\begin{aligned} \frac{\mathrm{d}b(x)}{\mathrm{d}x} &= -\rho\big(x, b(x), y(x)\big) \\ \frac{\mathrm{d}y(x)}{\mathrm{d}x} &= -1. \end{aligned} \tag{2}$$

3 CALCULATING DYNAMIC PARAMETERS

We first establish how to calculate the dynamic parameters of the redemption curve from the anchor point (b_a, y_a). We do this as a series of technical lemmas that will be used in our later results. We start by showing how to calculate $b(x)$ in the simplified context in which the dynamic parameters are known/fixed. Recall though that, in general, the dynamic parameters are functions of the current state (more precisely, of the anchor point) and the static parameters. We then move on to derive results about how to calculate the dynamic parameters in their general form. We prove additional technical guarantees, which are not required for the purpose of this exposition, but may be useful when implementing our methods, in Appendix **??**.

We now consider how the current state is connected to the anchor point. For $y(x)$, we simply have $y(x) = y_a - x$. When α, x_U, and x_L are known and fixed, it is simple to calculate the function $b(x)$. The next proposition specifies how to do this. To state the proposition, observe that the reserve ratio at x is $r(x) = b(x)/y(x) = b(x)/(y_a - x)$. Observe that $r(0) = r_a = b_a/y_a$. Note that $r(y_a)$ would be ill-defined in this sense since the denominator would be 0. We extend the definition continuously by $r(y_a) := \lim_{x \to y_a} r(x)$. This will be well-defined for all relevant cases below.

Prop. 1. *For fixed α, x_U, x_L with $x_U \le x_L$ we have*

$$b(x) = b_a - \int_0^x p(x')\mathrm{d}x' = \begin{cases} b_a - x, & x \le x_U \\ b_a - x + \frac{\alpha}{2}(x - x_U)^2, & x_U \le x \le x_L \\ r_L(y_a - x), & x_L \le x, \end{cases}$$

where $r_L = r(x_L)$. r_L can be computed using the second case in the case distinction alone.

[Link to Proof]

Recall that we have three static parameters $\overline{\alpha} \in (0, \infty), \bar{x}_U \in [0, \infty]$, and $\overline{\theta} \in [0, 1]$. $\overline{\theta}$ defines a floor on the reserve ratio, if achievable, and $\overline{\alpha}$ and $\bar{x}_U$ are bounds on the respective parameter: we always have $\alpha \ge \overline{\alpha}$ and $x_U \le \bar{x}_U$. Depending on the anchor point (b_a, y_a) and constrained by these parameters, we choose values for

the dynamic parameters that determine the curve shape. Define an auxiliary function

$$p^U(x) := \begin{cases} 1, & x \le x_U \\ 1 - \alpha(x - x_U), & x \ge x_U. \end{cases} \tag{3}$$

Then the dynamic parameters x_U, α, and x_L are chosen according to the following rule.

- For given x_U and α, x_L is chosen such that $x_L \in (x_U, y_a]$ and $p(x_L; b_a, y_a) = r(x_L; b_a, y_a)$, where both sides of this equation can be computed based on p^U. The values of the remaining parameters x_U and α will be chosen such that such a point exists (see Proposition 2 below). Note that the case $x_L = y_a$ is not pathological, but, as we will see, it occurs regularly. It is easy to see that, by choice of x_L, we have $r(x) = p(x) = r_L$ for all $x \ge x_L$, i.e., we redeem at the reserve ratio beyond x_L, and this is sustainable.
- x_U and α are chosen such that $0 \le x_U \le \bar{x}_U$, $\alpha \ge \overline{\alpha}$, x_L exists, and $r_L \ge \overline{\theta}$, if possible. It is easy to see that this is possible iff $r_a > \overline{\theta}$ (one possible choice is $x_U = 0$ and $\alpha \to \infty$ as $r_a \searrow \overline{\theta}$). In the trivial case where this does not hold, we set the marginal redemption price to constant r_a.
- Among the admissible combinations of x_U and α, the parameter values are chosen such that first, α is minimized among all possible α values and, second, x_U is maximized given this α. This implies that, if there are admissible solutions and $\alpha < \overline{\alpha}$, then we must have $x_U = 0$. This follows from the fact that r_L increases if we reduce x_U.

The rule by which x_u and α are chosen in the third step encodes that, when confronted with a trade-off between a not-too-steep price decay and a prolonged support of the exact peg of \$1, our mechanism prioritizes the former over the latter. We argue that this is the appropriate trade-off in the interest of market stability for the reasons outlined in Section 1.3. Note that the mechanism only applies trade-off only applies within the limits set by the $\overline{\alpha}$ and $\bar{x}_U$ static parameters.

Going forward, we will focus on the non-trivial case where $b_a < y_a$ (otherwise $b > y$ at any point and the marginal price is constant at 1), $r_a > \overline{\theta}$ (otherwise the marginal price is constant at $r_a = r(x)\ \forall x$), and, where x_U occurs as a parameter, we assume $y_a \ge x_U$ (otherwise the system would be configured to redeem at price 1 for all x and in particular will run out of reserves at some point since $b_a < y_a$).

The following proposition shows how to calculate x_L based on x_U and α and in what settings such a point exists. This result also shows that a key tenet of the primary market design will be choosing parameters such that x_L exists as otherwise the reserve can be exhausted. To make our formulas more compact, define the following shorthands: let $\Delta_a = y_a - b_a$ and $y_U = y_a - x_U$; let $b_L = b(x_L)$.

Prop. 2. *For given fixed parameters x_U, α, the following hold.*

(1) There exists a point $x_L \in [0, y_a]$ where $p(x_L) = r(x_L)$ iff

$$\alpha \ge 2\frac{y_a - b_a}{(y_a - x_U)^2}. \tag{4}$$

(2) If (4) does not hold and $x_L := \infty$ in the definition of p, then the reserve is exhausted before all tokens have been redeemed. Formally, in this case, there is $x \in [0, y_a)$ such that $b(x) = 0$.

(3) If (4) holds, then x_L is unique and

$$x_L = y_a - \sqrt{(y_a - x_U)^2 - \frac{2}{\alpha}(y_a - b_a)}$$
$$r_L = 1 - \alpha(x_L - x_U)$$
$$b_L = (1 - \alpha(x_L - x_U))(y_a - x_L)$$

[Link to Proof]

Remark 1. From the previous proposition, we easily receive an analytical expression for $r(x) = b(x)/y(x) = b(x)/(y_a - x)$. Observe that $b(x)$ and $r(x)$ are continuous functions of x. Observe in particular that, for $x \ge x_L$, we have $r(x) = r_L(y_a - x)/(y_a - x) = r_L = p(x)$. Thus, after x_L, the reserve ratio remains constant and the marginal redemption price is the reserve ratio.

We now formalize the rule by which α and x_U are chosen. Fix y_a, b_a, and $\overline{\theta}$. We call a pair (α, x_U) *admissible* if x_L exists and $r_L \ge \overline{\theta}$. We call x_U *admissible for* α if (α, x_U) is admissible and we call α *admissible* if there exists some x_U such that (α, x_U) is admissible. Note that the set of x_U admissible for α always form a closed interval $[0, \hat{x}_U(\alpha)]$ and the set of admissible α is also a closed interval $[0, \hat{\alpha}]$. This follows from monotonicity in (4), the fact that r_L is monotonically decreasing in x_U (as can be seen from the formulas in Proposition 2), and closedness. Define $\hat{\alpha}$ and $\hat{x}_U(\alpha)$ as the interval bounds indicated above. In words, $\hat{\alpha}$ is the minimum α, disregarding $\overline{\alpha}$, such that $(\alpha, x_U = 0)$ is admissible and $\hat{x}_U(\alpha)$ is the maximum x_U, disregarding $\bar{x}_U$, such that (α, x_U) is admissible. By Proposition 2 we can see that $\hat{\alpha}$ always exists (if $b_a/y_a > \overline{\theta}$) and is positive and for $\alpha \ge \hat{\alpha}$, $\hat{x}_U(\alpha)$ always exists.

We now choose the dynamic parameters α and x_U as follows:

(1) First let $\alpha = \max(\hat{\alpha}, \overline{\alpha})$.
(2) Then let $x_U = \min(\hat{x}_U(\alpha), \bar{x}_U)$.

Note that the upper bound $\bar{x}_U$ is essentially optional for our construction; we can choose $\bar{x}_U = \infty$ (or $\bar{x}_U = y_a$) to deactivate it. In this case, we always have $x_L = y_a$ if the $\overline{\theta}$ bound on the reserve ratio is not binding.[9] The lower bound $\overline{\alpha}$ is also optional and can be deactivated by setting $\overline{\alpha} = 0$. Note, however, that for $\overline{\alpha} = 0$, we will *always* receive $x_U = 0$. This is because then $\alpha = \hat{\alpha}$ and it is easy to see that $\hat{x}_U(\hat{\alpha}) = 0$ (otherwise, we could have chosen $\hat{\alpha}$ smaller by strict monotonicity; see Proposition 2). The following lemma will help us in our construction. Let $\theta = 1 - \overline{\theta}$.

Lemma 1. *If (4) holds, then $r_L \ge \overline{\theta}$ iff*

$$\alpha(y_a - x_U) \le \theta \tag{TH}$$

$$\text{or} \qquad \alpha(b_a - \overline{\theta}\, y_a) - \alpha\, \theta\, x_U - \frac{1}{2}\theta^2 \ge 0. \tag{TL}$$

[Link to Proof]

We can interpret the distinction between the conditions (TH) and (TL) in terms of whether or not the reserve ratio floor $\overline{\theta}$ is binding. Observe first that (TH) is equivalent to $1 - \alpha(y_a - x_U) \ge \overline{\theta}$, and this implies that $p(x) \ge \overline{\theta}$ for all x and independently of x_L,

[9] This will be captured formally as cases II h and III H below.

including for the case $x_L = y_a$, where the redemption curve p has no final constant segment. In this case we say that $\overline{\theta}$ is not binding. If (TH) does not hold, then we need to choose $x_L < y_a$ since otherwise the reserve ratio would fall short of the floor $\overline{\theta}$; we say that $\overline{\theta}$ is binding. Conceptually, if at least one of (TH) or (TL) holds, the redemption price will always be at least $\bar{\theta}$, conditional on the assumptions at the beginning of this section (in particular, the system starts with enough reserve capitalization). This is desirable as anyone can understand this bounding (as well as other PAMM mechanics) ahead-of-time.

Armed with Lemma 1, we can now construct the values $\hat{\alpha}$ and $\hat{\mathrm{x}}_{\mathrm{U}}(\alpha)$ for any α. We begin with $\hat{\alpha}$. Recall that $\theta = 1 - \overline{\theta}$.

Prop. 3. *We have*

$$\hat{\alpha} = \begin{cases} \hat{\alpha}_H := 2\frac{1-r_a}{y_a}, & r_a \geq \frac{1+\overline{\theta}}{2} \\ \hat{\alpha}_L := \frac{1}{2}\frac{\theta^2}{b_a - \overline{\theta}\, y_a}, & r_a \leq \frac{1+\overline{\theta}}{2} \end{cases}$$

and $\hat{\alpha}$ is continuous in the other parameters.

[Link to Proof]

We continue with an explicit formula for $\hat{\mathrm{x}}_{\mathrm{U}}(\alpha)$. Note that, due to the way in which we choose our parameters, we only need to consider $\hat{\mathrm{x}}_{\mathrm{U}}(\overline{\alpha})$. However, no additional effort is required to obtain a formula for general α.

Prop. 4. *We have*

$$\hat{\mathrm{x}}_{\mathrm{U}}(\alpha) = \begin{cases} \hat{\mathrm{x}}_{\mathrm{U,h}} := y_a - \sqrt{2\frac{\Delta_a}{\alpha}}, & \alpha\Delta_a \leq \frac{1}{2}\theta^2 \\ \hat{\mathrm{x}}_{\mathrm{U,l}} := y_a - \frac{\Delta_a}{\theta} - \frac{1}{2\alpha}\theta & \alpha\Delta_a \geq \frac{1}{2}\theta^2 \,. \end{cases}$$

and $\hat{\mathrm{x}}_{\mathrm{U}}(\alpha)$ is continuous in α and in the other parameters.

[Link to Proof]

The technical results in this section show how the dynamic parameters α, x_U, and x_L can be calculated from the current state using the anchor point. In the following sections, we will proceed with our analysis with these rules for choosing dynamic parameters as given.

4 UNIQUENESS OF RECONSTRUCTION

We now move on to show that we can construct ρ uniquely from the current state (x, b, y), which proves that our dynamical system (2) is in fact well-defined. Recall that ρ, which is a function solely of the current state, 'reconstructs' p, which is also a function of the anchor point (b_a, y_a). We show that it is in principle possible to 'reconstruct' p from the current state by showing that each state (x, b, y) can only have arisen from one specific anchor point. We show that this is the case because the reserve value $b(x)$ at some fixed x is strictly monotonic in b_a, whenever that state is non-trivial.[10]

Theorem 1. *Fix values y_a, $\overline{\theta}$, $\overline{\alpha}$, $\bar{\mathrm{x}}_{\mathrm{U}}$ and fix some $x \in [0, y_a)$. Assume that x_U and α are chosen dependent on b_a according to the rule described above. Let b_a and b'_a be such that $b_a < b'_a$ and $1 > r(x; b_a)$, $r(x; b'_a) > \overline{\theta}$ (and in particular $1 > b_a/y_a$, $b'_a/y_a > \overline{\theta}$). Then $b(x; b_a) < b(x; b'_a)$.*

[10] Equivalently, the reserve ratio $r(x)$ is strictly monotonic in b_a, since it is a strictly monotonic transformation of $b(x)$ for fixed x. In this section, we consider the static parameters $\overline{\theta}$, $\overline{\alpha}$, $\bar{\mathrm{x}}_{\mathrm{U}}$ fixed while the dynamic parameters α and x_U take on values dependent on the anchor point as discussed above.

The result is less immediate than it may seem at first. While it is clear that a lower b_a leads to a lower value of $b(x)$ *when leaving the parameters α, x_U fixed*, the situation we consider here is different. In particular, as we reduce b_a, the parameters α and x_U will adjust according to proposition 3 and 4 to ensure our desiderata. A priori, it might be the case that, through this adjustment, a lower value of b_a leads to a lower value of $b(x)$ at some point x, but to a *higher* or the same value of $b(x')$ at some other point x'. Theorem 1 proves that this is not the case: the whole reserve value curve $b(\,\cdot\,)$ is strictly monotonic in the anchor reserve value b_a at all non-trivial points.

The following proposition provides conditions under which the ultimate constant segment is degenerate because it either does not exist or it lies at the reserve ratio floor. This will be useful for the proof of Theorem 1.

Prop. 5.

(1) *Assume that one of the following holds: (a) $\hat{\alpha} \geq \overline{\alpha}$, $\hat{\mathrm{x}}_{\mathrm{U}} \leq \bar{\mathrm{x}}_{\mathrm{U}}$, and $\alpha\Delta_a \leq \frac{1}{2}\theta^2$; or (b) $\hat{\alpha} \leq \overline{\alpha}$ and $r_a \geq \frac{1+\overline{\theta}}{2}$. Then $x_L = y_a$.*
(2) *Assume that one of the following holds: (a) $\hat{\alpha} \geq \overline{\alpha}$, $\hat{\mathrm{x}}_{\mathrm{U}} \leq \bar{\mathrm{x}}_{\mathrm{U}}$, and $\alpha\Delta_a \geq \frac{1}{2}\theta^2$; or (b) $\hat{\alpha} \leq \overline{\alpha}$ and $r_a \leq \frac{1+\overline{\theta}}{2}$. Then $r_L = \overline{\theta}$.*

[Link to Proof]

The result allows us to exclude certain parts of the state space from the analysis because there, the recovery rate is at most our defined floor and thus the mechanism defines that redemption must happen at the reserve ratio.

Corollary 1. *If any of the conditions from Proposition 5 hold and furthermore $x \geq x_L$, then $r(x) \leq \overline{\theta}$.*

[Link to Proof]

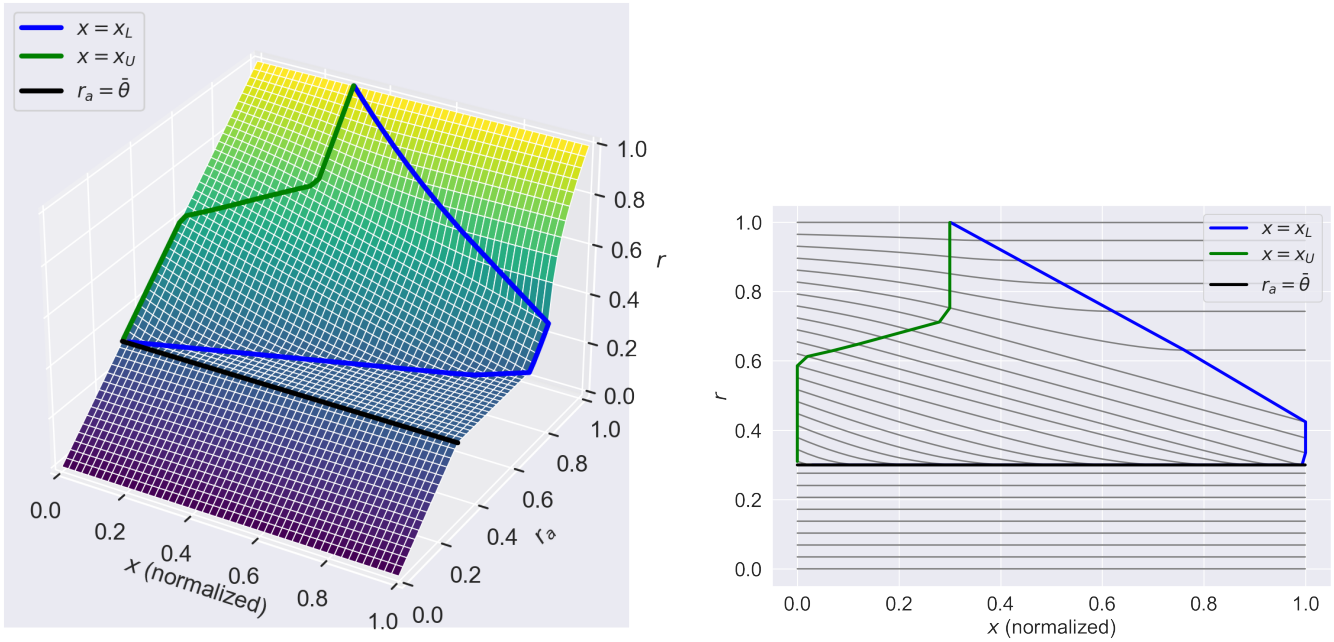
Conceptually, we can visualize the function $b(x; b_a)$, with which Theorem 1 is concerned, as a 3d surface. Figure 8a shows the surface of the reserve ratio as a function of x and b_a.[11] We have chosen $y_a = 1$ so that $b_a = r_a$ (but in general $b \neq r$). Notice that, as mentioned above, part of the (x, b_a) space can be essentially ignored because they fall along a certain flat region of the surface that has zero area in a projection of interest. This projection of interest is the 2-d (x, r) space. This is visualized in Figure 8b, in which many r curves are plotted (in gray) for differing values of r_a, which are the starting points of these curves. Notice that the flat section of the 3-d surface mentioned above disappears in the 2d-projection.

In Figure 8, there is a stretch of r_a values where $x_L = 1$. This, however, is not universally the case and depends on the parameters. We illustrate two 3d curves $r(x; r_a)$ where this is and is not the case, respectively, in Figure 9.

We are now armed with the tools to prove Theorem 1. Our proof is by case distinction and explicit calculation of the partial deriviatives for each of the cases. The main challenge is to handle the adjustment in the dynamic parameters that takes place as b_a is varied.

[Link to Proof of Theorem 1]

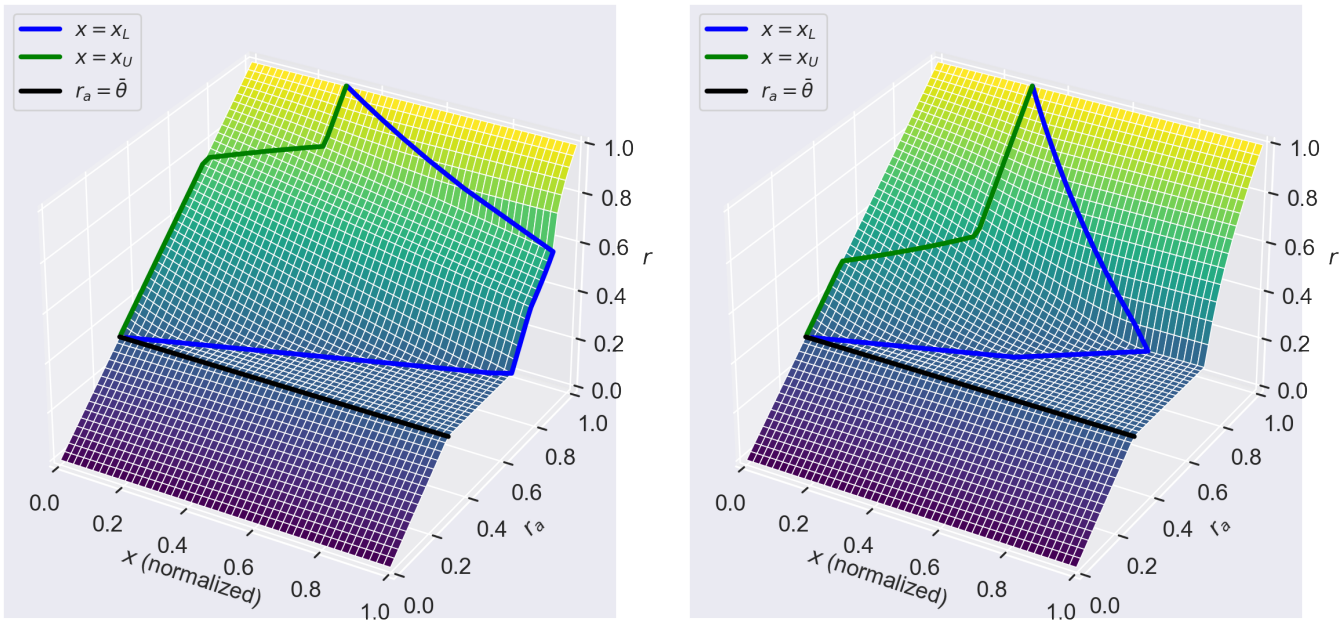
[11] Note that $b(x; b_a) = r(x; b_a) \cdot (y_a - x)$, so that there is a simple 1:1 relationship between the reserve value and the reserve ratio. We present the reserve ratio because we find it more illustrative of the different phenomena.



(a) 3d curve.

(b) 2d projection to the (x, r) plane.

Figure 8: Reserve ratio r as a function of the current redemption amount x and the initial reserve ratio r_a for the normalized case $y_a = 1$. Due to normalization, we have $r_a = b_a$. The parameters $\overline{\theta} = 0.3$, $\overline{\alpha} = 0.8$, and $\bar{x}_U = 0.3$ were used. The figures also depict x_L and x_U on the X axis as functions of r_a



(a) $\overline{\theta} = 0.3$, $\overline{\alpha} = 0.5$, $\bar{x}_U = 0.3$. There is a stretch where $x_L = 1$.

(b) $\overline{\theta} = 0.3$, $\overline{\alpha} = 1.3$, $\bar{x}_U = 0.3$. There is no point where $x_L = 1$.

Figure 9: Reserve ratio r as a function of the current redemption amount x and the initial reserve ratio r_a for $y_a = 1$ and two choices of parameters.

5 PATH PROPERTIES

Now that we've established that the P-AMM design is well-defined and robust in shape, we move on to show that it obeys many useful trading properties, including in settings involving trading fees and a separate minting curve. We characterize these in terms of path independence and path deficiency, which will lead us to two main useful properties:

- There is no incentive for redeemers to strategically subdivide redemptions, including in some settings with trading fees.
- In a wide array of settings involving a P-AMM with minting, redeeming, and trading fees, the protocol itself is only better off in terms of the reserve ratio curve no matter which trading path is realized.

5.1 Path Independence

We first show that the P-AMM redemption curve, as developed thus far without trading fees, is path independent within a block. This means that the end result of any path of redemptions is the same for any given starting and ending point. On the ground, this is useful for traders as they do not need to worry about how exactly they use the P-AMM within a block: there is no incentive to split up redemptions into smaller chunks or to merge many small redemptions into bigger units.

Given an initial state (x_0, b_0, y_0) and a desired amount of redemptions $X \in [0, y_0]$, our P-AMM, conceptually speaking, solves the initial value problem defined by (x_0, b_0, y_0) and the system of differential equations (2). We then transition to the new state $(x_0 + X, b(x_0 + X), y(x_0 + X)) = (x_0 + X, b(x_0 + X), y_0 - X)$ and the redemption amount (which is paid out to the redeemer) is $b(x_0 + X) - b_0$.

Notice that the right-hand sides of (2) only depend on the current state of the system and not, for instance, on the initial conditions or the context of which trading path (i.e., sequence of redemptions) has been followed to arrive at the current state. This immediately implies that P-AMM pricing is independent of the trading path taken, which is our desired path independence property. In the dynamical systems literature, this property is also known as invariance under horizontal translations. We formalize this property in the following theorem.

Theorem 2. *(Path independence) Let (x_0, b_0, y_0) be a state and let $X, Y > 0$ such that $X + Y \leq y_0$. Then the total redeemed amount and the resulting state from redeeming $X + Y$ at $S_0 := (x_0, b_0, y_0)$ are the same as the amount and state resulting from first redeeming X, and then redeeming Y. Formally, let S_X result from redeeming X at S_0, $S_{X,Y}$ from redeeming Y at S_X, and S_{X+Y} from redeeming $X + Y$ at S_0. Let the paid-out amounts be $P_X, P_{X,Y}$, and P_{X+Y} respectively. Then the following hold.*

(1) $P_X + P_{X,Y} = P_{X+Y}$
(2) $S_{X,Y} = S_{X+Y}$

[Link to Proof]

Note that the theorem only holds for redemptions immediately following each other within the same block –the context of our model in this paper– as otherwise we need to consider the time decay of the initial condition x_0 across blocks as well as exogenous changes to b and minting operations happening between two redemptions. Additionally, if there are many traders using the P-AMM to redeem, there will at times be an incentive to be earlier in the redemption queue.

5.2 Extension to Fees and Minting

The P-AMM in reality will take an extended form of the setup developed thus far. In this extended form, the redemption curve will incorporate a trading fee and there will be a separate minting curve for x that moves in the reverse direction. We will now show how the desired properties –but not path independence directly– can be retained in this extended form.

This extended form can no longer be modeled by a single dynamical system. Instead, different differential equations describe the effects of increasing x (redemptions) as opposed to decreasing x (minting). Let $\gamma(x, b, y) \geq 0$ be the trading fee that is imposed on redemptions. And let $\varphi(x, b, y) \geq 1$ be a function describing the marginal price of minting a new stablecoin. Notice that $\varphi(x, b, y) = 1+\varepsilon$ is such a function for any $\varepsilon > 0$.

In the extended form, redemption actions are described by the following slightly altered form of (2):

$$\begin{aligned} \frac{\mathrm{d}b(x)}{\mathrm{d}x} &= -\rho\big(x, b(x), y(x)\big) + \gamma\big(x, b(x), y(x)\big) \\ \frac{\mathrm{d}y(x)}{\mathrm{d}x} &= -1. \end{aligned} \tag{5}$$

And minting actions are described by the different set of differential equations:

$$\begin{aligned} \frac{\mathrm{d}b(x)}{\mathrm{d}x} &= -\varphi\big(x, b(x), y(x)\big) \\ \frac{\mathrm{d}y(x)}{\mathrm{d}x} &= -1. \end{aligned} \tag{6}$$

As the extended system evolves differently for different directions of change in x, we no longer have path independence. To see this, simply consider a closed path in x, which returns to the same starting point in x-space, but will often not return to the same starting point in (x, b, y)-space. However, there a generalization of path independence, called *path deficiency*, which retains many of the useful properties we desire.

5.3 Path Deficiency Properties

We next show two properties analogous to path deficiency in CFMMs (see [2]). As the P-AMM is not a CFMM, we approach this slightly differently. For our purposes, we will characterize path deficiency-like results in terms of *reserve ratio curves* that can be encountered along a trading path. These reserve ratio curves are defined in previous sections and visualized in Figure 6. In particular, these reserve ratio curves are functions arising from our original system (2) that map x to a reserve ratio $r(x)$ parameterized by an anchor point $r_a = b_a/y_a$, where we assume $\bar{\mathrm{x}}_{\mathrm{U}}$, $\overline{\alpha}$, and $\overline{\theta}$ are fixed. Without loss of generality, we will take $y_a = 1$ so that $r_a = b_a$.

Recall that each current state is associated with a single such reserve ratio curve. While in the case of redemptions without fees, we always remain on this reserve ratio curve, when we add in fees and a separate minting curve, we instead may shift reserve ratio curves as we move along a path in x.

We start with the following definitions:

- $\mathcal{R}$ is the set of all reserve ratio curves,
- $\mathfrak{r} \in \mathcal{R}$ is some initial reserve ratio curve,
- C is the set of paths in $[0,1]$, i.e., $C = \{f : [0,1] \to [0,1] \mid f \text{ is continuous}\}$,
- $r_{f,\mathfrak{r}} : [0,1] \to [0,\infty)$ is the function returning the reserve ratio at points along the path $f \in C$ starting at the initial point $\big(f(0), \mathfrak{r}(f(0))\big)$ in (x,r)-space.

Notice that $r_{f,\mathfrak{r}}$ sweeps away the details of (5) and (6) but is easy to see is well-defined for a given $f \in C$.

Paths in the set C are interpreted as paths for the variable x. Note that we consider paths for x within $[0,1]$. The upper bound comes from the maximum amount that can be redeemed. It is inherently possible for more supply to be minted than y_a, and so the lower bound could conceptually be passed in reality. It is possible to extend the results by renormalizing the system to $y_a = 1$.

The following lemma establishes that the anchor point r_a is weakly increasing along any trading path.

Lemma 2. *Let $\mathfrak{r} \in \mathcal{R}$ such that $\mathfrak{r} \leq 1$ and $f \in C$. Then $r_a\big(f(t), r_{f,\mathfrak{r}}(t)\big)$ —the anchor point for each state (x,r) along the path— is non-decreasing in t.*

[Link to Proof]

This enables our first path deficiency-like result in the next theorem. Consider that we start on an initial reserve ratio curve. Moving along this curve describes the behavior of the original path independent system along a trading path, which we proved various desirable properties about in the previous sections. The reserve ratio curve that we are on –independent of where we are on it– is one good measure for the health of the system as being on a higher curve is point-wise weakly better than being on a lower curve. The following theorem establishes that the protocol health is weakly increasing in this way along any trading path.[12]

Theorem 3. *Let $\mathfrak{r} \in \mathcal{R}$ such that $\mathfrak{r} \leq 1$. Then for all $f \in C$ and for all $t \in [0,1]$, we have $\mathfrak{r}\big(f(t)\big) \leq r_{f,\mathfrak{r}}(t)$.*

[Link to Proof]

We now turn to our second path deficiency-like result. The following theorem shows that, in settings with a proportional fee, there is no incentive for a trader to strategically subdivide a net redemption trade into a sequence of different trades.

Theorem 4. *Let $\gamma(\cdot) = \varepsilon\rho(\cdot)$ for some $0 \leq \varepsilon < 1$ and let $\mathfrak{r} \leq 1$ be the initial reserve ratio curve. Then:*

(1) The redemption system described in (5) is path independent within a block.

(2) An individual trader in the extended system described in Section 5.2 has no incentive to subdivide a net redemption within a block.

[Link to Proof]

Note that there may still be strategic interaction between many traders, but these considerations are limited and fairly simple (and can in fact be avoided with a batch settlement of trades in the block, which is fundamentally possible if more difficult to implement). There can be an incentive for a given trader to get a redemption trade in earlier than other redemption trades. There can also be an incentive for a given trader to get a redemption trade in after any minting trades are settled. Note that in many circumstances where this would matter, we are not likely to see mint and redemption transactions in the same block, however, as a trader would likely get a better price for one or the other on a secondary market. A further concern is whether arbitrage trades, in which the net redemption is zero, are profitable (e.g., a sandwich attack around other trades). This is not endogenously profitable from the P-AMM structure alone since redemption prices are ≤ 1 while minting prices are ≥ 1.

Speculative Attacks. Another possibility worthy of reflection is that of a speculative attack, in which an attacker takes an outside short position on the stablecoin and attempts to trigger the outflows necessary to derive profit from the short position. Should the system be under-reserved, this is a valid concern. Modeling this fully requires composing the P-AMM, a secondary market, and a shorting market and is outside the scope of this paper.

Models of speculative attacks in currencies serve as a good starting point (e.g., [14]). We discuss these in more detail in Appendix B. Some qualitative results from these models can be applied directly to the P-AMM setting. In particular, [18] analyzes a game theoretic model that is implicitly similar to the P-AMM setting, in which a government or currency issuer tries to maintain an optimal exchange rate peg while under-reserved. In this model, the optimal strategy involves the central bank demonstrating commitment to devalue the currency if too many traders demand redemption from reserves, which eliminates the speculative attack equilibrium and stabilizes the exchange rate.

Although [18] is written in the context of cryptocurrency stabilization, the model is most descriptive of traditional currency models, in which the exchange rate is pegged to another currency that is held by the central bank in reserves. The cryptocurrency setting is a little different: (1) reserve assets may not be the currency target, and (2) exchange rate policy needs to be encoded on-chain in smart contracts as opposed to determined on-the-fly by central bank governors. However, after translating reserve asset values into the appropriate numeraire for the peg and adjusting for the fact that these values follow a stochastic process, the P-AMM setting can be adapted to the underlying model in [18]. In this case, the P-AMM shape when under-reserved provides the means of committing to stablecoin devaluation in the event of speculative attacks, which can eliminate the speculative attack equilibrium.

6 CONCLUDING REMARKS

We have designed a desirable P-AMM redemption curve based on an anchored state that codifies how a stablecoin can sustainbly adapt monetary policy to respond to crisis events without external input. This can work even if the stablecoin becomes under-reserved

[12] These results parallel those of path deficiency in CFMMs (see [2]). To draw the parallel further, these and potentially further path deficiency results for P-AMMs may be expressed in terms of *reachable sets of reserve ratio curves* $S(\mathfrak{r}) = \Big\{ \psi \in \mathcal{R} \mid \big(f(t), r_{f,\mathfrak{r}}(t)\big) \in \psi \text{ for some } t \in [0,1] \text{ and for some } f \in C \Big\}$ that weakly contract along a path. To illustrate, Lemma 2 would express that functions in this reachable set are point-wise lower bounded by $\mathfrak{r}$, and that reachable sets do not expand along a path. This may be useful in expanded contexts, such as involving discrete trades, in which it is not obvious that two valid paths can be concatenated into a single valid path, or settings in which reserve ratio curves are not nicely represented by anchor points.

We showed how this design satisfies desiderata 1–5. Desideratum 8 is shown to be satisfied in a dedicated implementation paper.[13].

Desiderata 6–7 can be easily reasoned about considering how the anchored state changes over time according to an exponentially time-discounted sum and using desiderata 1–5. It is possible to show that desiderata 6–7 are satisfied formally. We leave this as the starting point for a wider study of time evolution. In particular, future work should also study how the P-AMM behaves under wider market reactions and other stabilization mechanisms, including a model of exogenous random shocks to reserve value.

Alternative P-AMM designs may also be possible that satisfy the desiderata. For instance, a P-AMM with a sigmoidal shape would have further smoothness. However, such designs would likely present computational issues on-chain, including both the raw number of computational steps required (i.e., gas requirements for on-chain execution) and amplification of rounding errors arising from fixed point arithmetic.

REFERENCES

[1] Hayden Adams, Noah Zinsmeister, Moody Salem, River Keefer, and Dan Robinson. 2021. *Uniswap v3 core.* Technical Report. Technical report.

[2] Guillermo Angeris and Tarun Chitra. 2020. Improved Price Oracles: Constant Function Market Makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 80–91.

[3] Guillermo Angeris, Alex Evans, and Tarun Chitra. 2020. When does the tail wag the dog? Curvature and market making. *arXiv preprint arXiv:2012.08040* (2020).

[4] Dirk Bullmann, Jonas Klemm, and Andrea Pinna. 2019. In search for stability in crypto-assets: are stablecoins the solution? *ECB Occasional Paper* 230 (2019).

[5] Agostino Capponi and Ruizhe Jia. 2021. The Adoption of Blockchain-based Decentralized Exchanges: A Market Microstructure Analysis of the Automated Market Maker. *Available at SSRN 3805095* (2021).

[6] Douglas W Diamond and Philip H Dybvig. 1983. Bank runs, deposit insurance, and liquidity. *Journal of political economy* 91, 3 (1983), 401–419.

[7] Michael Egorov. 2019. StableSwap-efficient mechanism for Stablecoin liquidity. *Retrieved Feb* 24 (2019), 2021.

[8] Bernardo Guimaraes and Stephen Morris. 2007. Risk and wealth in a model of self-fulfilling currency attacks. *Journal of Monetary Economics* 54, 8 (2007), 2205–2230.

[9] Ariah Klages-Mundt, Dominik Harz, Lewis Gudgeon, Jun-You Liu, and Andreea Minca. 2020. Stablecoins 2.0: Economic Foundations and Risk-based Models. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*. 59–79.

[10] Ariah Klages-Mundt and Andreea Minca. 2019. (In) Stability for the Blockchain: Deleveraging Spirals and Stablecoin Attacks. *To appear in Cryptoeconomic Systems 2021, MIT Press* (2019).

[11] Ariah Klages-Mundt and Andreea Minca. 2020. While Stability Lasts: A Stochastic Model of Stablecoins. *arXiv preprint arXiv:2004.01304* (2020).

[12] Leland Lee and Ariah Klages-Mundt. Apr. 23, 2021. Governance Extractable Value. https://ournetwork.substack.com/p/our-network-deep-dive-2

[13] Ye Li, Simon Mayer, et al. 2020. *Managing Stablecoins: Optimal Strategies, Regulation, and Transaction Data as Productive Capital.* Ohio State University, Fisher College of Business, Charles A. Dice Center ….

[14] Stephen Morris and Hyun Song Shin. 1998. Unique equilibrium in a model of self-fulfilling currency attacks. *American Economic Review* (1998), 587–597.

[15] Athanasios Orphanides. 2010. Taylor Rules. In *Monetary Economics*. Springer, 362–369.

[16] Cecilia Parlatore. 2016. Fragility in money market funds: Sponsor support and regulation. *Journal of Financial Economics* 121, 3 (2016), 595–623.

[17] Ingolf GA Pernice, Sebastian Henningsen, Roman Proskalovich, Martin Florian, Hermann Elendner, and Björn Scheuermann. 2019. Monetary stabilization in cryptocurrencies–design approaches and open questions. In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*. IEEE, 47–59.

[18] Bryan Routledge and Ariel Zetlin-Jones. 2021. Currency stability using blockchain technology. *Journal of Economic Dynamics and Control* (2021), 104155.

[19] George Selgin. 2020. Modeling the legend, or, the trouble with Diamond and Dybvig: Parts I and II. https://www.alt-m.org/2020/12/18/modeling-the-legend-or-the-trouble-with-diamond-and-dybvig-part-ii/.

[20] Sam M Werner, Daniel Perez, Lewis Gudgeon, Ariah Klages-Mundt, Dominik Harz, and William J Knottenbelt. 2021. Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778* (2021).

[13] This will be released soon and is available upon request.

A DISCRETE PRICE DECAY

In this section, we discuss an alternative price decay function, where prices decay discretely from 1 to the reserve ratio. This discrete price decay form leads to much simpler calculations than the linear one outlined in the main text of this paper. However, it has the disadvantage that price decay happens abruptly, which creates risk for arbitrageurs and may also create an opportunity for speculative attacks.

Let

$$p(x; b_a, y_a) := \begin{cases} 1 & \text{if } x \geq x_U \\ r_L & \text{if } x < x_U, \end{cases}$$

where x_U is a dynamic parameter and r_L is chosen such that $r_L = r(x_U)$ based on the other parameters. The parameters fulfill the same role as in our linear price decay mechanism where, however, the linear segment (and its parameter α) as well as the lower cut-off point x_L are missing. Note that, in contrast to the case with linear price decay, p is not continuous.

Lemma 3. *Let $b_a < y_a$. Then the following hold:*

(1) We have

$$b(x) = \begin{cases} b_a - x & \text{if } x \geq x_U \\ b_a - x_U - r_L \cdot (x - x_U) & \text{if } x \leq x_U \end{cases}$$

(2) If $x_U < b_a$, then $r_L = \frac{b_a - x_U}{y_a - x_U}$ and the reserve is never exhausted. Otherwise, the reserve is exhausted at a point $x < y_a$.

(3) In this case, we have $r_L \geq \overline{\theta}$ iff $b_a/y_a \geq \overline{\theta}$ and $x_U \leq \frac{b_a - \overline{\theta}\, y_a}{\theta}$, where $\theta = 1 - \overline{\theta}$.

Proof.

(1) This follows immediately by integration over p.

(2) First assume $x_U < b_a$. By part 1 we have $b(x_U) = b_a - x_U$ and further $y(x_U) = y_a - x_U$, and $r_L = r(x_U) = b(x_U)/y(x_U)$. By assumption, $r_L \in (0, 1)$ and, since we redeem at the reserve ratio after the point x_U, the reserve is never exhausted. Now assume $x_U \geq b_a$. Then, by part 1, we have $b(b_a) = 0$ and by assumption, $b_a < y_a$.

(3) By part 2 and simple algebraic transformation, $r_L \geq \overline{\theta}$ iff $x_U \leq \frac{b_a - \overline{\theta}\, y_a}{\theta}$. This is only possible if $b_a/y_a \geq \overline{\theta}$ since otherwise, the right-hand side is negative. □

Let $\bar{x}_U$ be an (optional) ceiling value for x_U. Then by the previous lemma the maximal $x_U \leq \bar{x}_U$ that ensures $r_L \geq \overline{\theta}$ is $x_U = \min(\bar{x}_U, \hat{x}_U)$, where

$$\hat{x}_U = \max\left(0,\ \frac{b_a - \overline{\theta}\, y_a}{\theta}\right).$$

Note that we choose $x_U = 0$ if $b_a/y_a < \overline{\theta}$, so that in this case, we redeem at the reserve ratio from the very beginning. It is easy to see that if $\hat{x}_U \leq \bar{x}_U$, then $r_L \leq \overline{\theta}$.

B PARALLELS WITH THE MONETARY ECONOMICS LITERATURE.

The P-AMM can be compared to a variant on a crawling or managed float system for a currency peg. The monetary economics literature on these topics provides a starting point to understand this design.

International monetary economics is concerned with balance of payments crises (i.e., sudden changes in capital flows). With a stablecoin as opposed to a national currency, we're less concerned with money flows in/out of a country's economy. The analog for a stablecoin is with flows in/out of the reserve and the level of economic demand for use of the stablecoin as opposed to demand to speculate on the stablecoin. Further, stablecoin monetary policy is simplified to targeting stability relative to the target as opposed to further targeting growth of a national economy.

Speculative attacks on currency pegs are characterized in the global games literature (e.g., [14]). In these models, speculators can coordinate to attack the currency while profiting from bets on currency devaluation. High levels of coordination can force the government to abandon the peg. There is a unique equilibrium in such games, shown in [14], given uncertainty in common knowledge of fundamentals (e.g., faith in government policy, economic demand, and health of reserves), which can lead to speculative attacks even when fundamentals are strong.

The curvature of the P-AMM serves to deter speculative attacks by increasing their cost in several ways. In large outflow settings, the curvature of f can allow short-term (though not necessarily long-term) depreciation from the peg. This can be interpreted as raising interest rates for new stablecoin holders. Akin to zero coupon bonds bought at a discount, buyers expect to redeem for a higher price later. This is supported by the fundamental value of the reserve, which, when healthy, tends to shift the coordination equilibrium to \$1 as outflows equilibrate.[14] Compared to a typical currency peg, the curvature of the P-AMM forces an attacking speculator to redeem at deteriorating prices throughout the attack, after which the redemption rate can bounce back. As a consequence, the crisis has to be stretched over long periods of time, during which speculators incur the spread loss, to have a permanent effect on the peg and reserve health. Additionally, the funding rate for a short bet on the stablecoin–a prime profit source for a speculative attack–ought to take into account the transparent shape of the P-AMM and state of the reserve. In settings that are otherwise prime for speculative peg attacks (e.g., when reserve value per stablecoin is much less than \$1), the short funding rate ought to be very high to account for the ease of causing short-term devaluations via the P-AMM shape, which serves to further raise the costs of attack.

Lastly, we contrast with the bank run model in [6]. In that model, the bank serves as insurance for two types of agents: one type who will need to withdraw early and another type who will not, but without knowing which is which ahead-of-time. Given the setup of the model, the bank is often prone to bank runs that depletes the bank's liquid assets. Speculative attacks on a stablecoin can often be viewed in a similar way to a bank run. In this context, the stablecoin design effectively alters the assumptions of the Diamond-Dybvig model to deter the undesirable bank run equilibrium (see [19] for further discussion of the following points). First, the curvature of the P-AMM reduces the redemption rate of large withdrawals. One cause of fragility in the Diamond-Dybvig model is requiring absolute liquidity out of bank deposits. Altering this structure can increase robustness at relatively small costs in terms of stablecoin liquidity. Second, since a liquid stablecoin is tradeable on secondary markets there is often no need to directly redeem it in the primary market.[15]

[14] While certain uncollateralized (or "implicit collateral", see [9]) stablecoins also propose similar narratives as here, they do so without a fundamental force, such as from a reserve, pushing coordination toward the \$1 equilibrium. Accordingly, one may question whether the stable equilibrium may really be \$0 price in such cases.

C PROOFS

C.1 Technical Lemmas

Prop. 1.

Proof. The first equality is just the definition. For the second equality, first assume that $x \le x_U$. Then $p(x') = 1 \, \forall x' \le x$ and thus the equality holds. For the second case, we have

$$\begin{aligned} b_a - \int_0^x p(x')\mathrm{d}x' &= b_a - x_U - \int_{x_U}^x 1 - \alpha(x' - x_U)\mathrm{d}x' \\ &= b_a - x_U - \int_0^{x-x_U} 1 - \alpha x' \, \mathrm{d}x' \\ &= b_a - x_U - (x - x_U) + \frac{\alpha}{2}(x - x_U)^2 \\ &= b_a - x + \frac{\alpha}{2}(x - x_U)^2 \end{aligned}$$

Finally, if $x_L \le x$, we have

$$b(x) = b(x_L) - \int_0^{x-x_L} r_L \, \mathrm{d}x' = r_L(y_a - x_L) - r_L(x - x_L) = r_L(y_a - x).$$

□

Prop. 2.

Proof. Consider the definition of $p^U(x)$, and the implied value for $b(x)$, for the case $x_U \le x \le y_a$. Let $x' = x - x_U$ and assume first that $x < y_a$. We have

$$\begin{aligned} & p^U(x) = r(x) \\ \Leftrightarrow \quad & 1 - \alpha x' = \frac{b_a - (x_U + x') + \alpha/2 x'^2}{y_U - x'} \\ \Leftrightarrow \quad & (y_U - x')(1 - \alpha x') = b_a - x_U - x' + \frac{\alpha}{2}x'^2 \\ \Leftrightarrow \quad & \frac{\alpha}{2}x'^2 - \alpha y_U x' + y_a - b_a = 0 \\ \Leftrightarrow \quad & x' = y_U \pm \sqrt{y_U^2 - 2/\alpha(y_a - b_a)} \\ \Leftrightarrow \quad & x = y_a \pm \sqrt{y_U^2 - 2/\alpha(y_a - b_a)}. \end{aligned}$$

Note that, if the discriminant is positive, then the "+" solution is $> y_a$ and thus not acceptable for x_L, so we only need to consider

[15] Similarly, digital commercial bank money does not need to be redeemed from the bank to use but can be used as a means of payment directly. A stablecoin on a public interoperable blockchain could be even more flexibly used without requiring redemption.

the "-" solution. Obviously, this exists iff (4) holds. Assuming that (4) *does* hold, we obviously have $x \le y_a$ and furthermore

$$\begin{aligned} & x = y_a - \sqrt{y_U^2 - 2/\alpha\Delta_a} > x_U \\ \Leftrightarrow \quad & y_U - \sqrt{y_U^2 - 2/\alpha\Delta_a} > 0, \end{aligned}$$

which is true because the radicand is $< y_U^2$ because $\Delta_a > 0$ by our basic assumptions. Thus, this x serves the role of $x_L := x$, and it is unique by the above.

If for the above choice of x_L we have $x_L < y_a$, then the identity $p(x_L) = r(x_L)$ follows by construction. Consider now the case where $x_L = y_a$. This is the case iff the above discriminant is 0, i.e., iff $\alpha = 2\frac{y_a - b_a}{(y_a - x_U)^2}$. In this case, it is easy to see that $b(x_L) = y(x_L) = 0$ and we can use L'Hospital's rule to compute

$$r_L = \lim_{x \to y_a} \frac{b(x)}{y(x)} = \lim_{x \to y_a} \frac{b_a - x + \alpha/2(x - x_U)^2}{y_a - x} = \frac{-1 + \alpha(x - x_U)}{-1} = 1 - \alpha(y_a - x_U) = p(x_L),$$

so the identity $r_L = p(x_L)$ still holds.

The formulas for r_L and b_L now simply follow from the fact that $r_L = p(x_L)$ and $b_L = r_L \cdot y(x_L)$.

Finally, consider the case where (4) does not hold and where we choose $x_L := \infty$ to define p. Then by applying Prop. 1 to $x := y_a$ we receive

$$b(y_a) = b_a - y_a + \frac{\alpha}{2}(y_a - x_U)^2 < 0,$$

where the inequality is by the assumption that (4) does not hold. By continuity of b, there exists $x < y_a$ such that $b(x) = 0$. □

Lemma 1.

Proof. By Proposition 2 we have that $r_L \ge \overline{\theta}$ iff

$$\begin{aligned} & 1 - \alpha(x_L - x_U) \ge \overline{\theta} \\ \Leftrightarrow \quad & 1 - \alpha\left(y_U - \sqrt{y_U^2 - 2/\alpha\Delta_a}\right) \ge \overline{\theta} \\ \Leftrightarrow \quad & \alpha\sqrt{y_U^2 - 2/\alpha\Delta_a} \ge \alpha y_U - \theta \\ \Leftrightarrow \quad & \alpha y_U - \theta \le 0 \\ \text{or} \quad & \alpha^2\left(y_U^2 - 2/\alpha\Delta_a\right) \ge (\alpha y_U - \theta)^2 . \end{aligned}$$

The conclusion now follows via another simple algebraic transformation. □

Prop. 3.

Proof. It is easy to see that the transition is continuous and thus well-defined; more in detail, in the edge case $r_a = \frac{1+\overline{\theta}}{2}$, we have $\hat{\alpha}_H = \hat{\alpha}_L = \theta/y_a$.

By the discussion at the beginning of this section, we only need to consider $x_U = 0$. $\hat{\alpha}$ is the maximal α such that (4) holds and one of (TL) or (TH) hold (with $x_U = 0$). Note that (4) alone puts a bound on α and the right-hand side of (4) is equal to $\hat{\alpha}_H$ for $x_U = 0$. Thus, whenever it is possible to choose $\alpha = \hat{\alpha}_H$, this is minimal. We can choose $\alpha = \hat{\alpha}_H$ if (TH) holds for $\hat{\alpha}$, i.e., if

$$\begin{aligned} & 2\frac{1 - r_a}{y_a} \cdot y_a \le \theta \\ \Leftrightarrow \quad & r_a \ge \frac{1 + \overline{\theta}}{2}. \end{aligned}$$

The equivalence immediately follows from the definition of $\theta = 1 - \overline{\theta}$. If this inequality does not hold, then there is no α that satisfies both (4) and (TH). (observe that the two limit α in different directions!)

Assume next that $r_a \le \frac{1+\overline{\theta}}{2}$. Then α must be chosen minimal such as to satisfy (4) and (TL). The minimal α satisfying (TL) with $x_U = 0$ is obviously $\hat{\alpha}_L$. It remains to show that this also satisfies (4), i.e., that

$$\begin{aligned} & \frac{1}{2}\frac{\theta^2}{b_a - \overline{\theta}\, y_a} \ge 2\frac{y_a - b_a}{y_a^2} \\ \Leftrightarrow \quad & \frac{1}{2}\frac{\theta^2}{r_a - \overline{\theta}} \ge 2(1 - r_a) \\ \Leftrightarrow \quad & \frac{1}{4}\theta^2 \ge (1 - r_a)(r_a - \overline{\theta}). \end{aligned}$$

The equivalences are by definition of $r_a = b_a/y_a$ and straightforward transformation. Let $\zeta = \frac{1+\overline{\theta}}{2} - r_a$. By assumption, $\zeta \ge 0$ and we have $1 - r_a = \theta/2 + \zeta$ and $r_a - \overline{\theta} = \theta/2 - \zeta$. Thus, the above inequality is equivalent to

$$\frac{1}{4}\theta^2 \ge (\theta/2 + \zeta)(\theta/2 - \zeta) = \frac{\theta^2}{4} - \zeta^2,$$

which is obviously true. □

Prop. 4.

Proof. We proceed similarly to Proposition 3. Again, it is easy to see that in the edge case $\alpha\Delta_a = \frac{1}{2}\theta^2$ we have $\hat{x}_{U,h} = \hat{x}_{U,l} = y_a - \frac{\theta}{\alpha}$. We need to choose x_U such as to satisfy (4) and one of (TH) or (TL), this time without assuming $x_U = 0$ of course. (4) is equivalent to

$$x_U \le y_a - \sqrt{2\frac{\Delta_a}{\alpha}}.$$

If we can choose x_U equal to the right-hand side such that (TH) is satisfied for this choice, then this is optimal. This is the case if

$$\begin{aligned} & \alpha \cdot \sqrt{2\frac{\Delta_a}{\alpha}} \le \theta \\ \Leftrightarrow \quad & \alpha\Delta_a \le \frac{1}{2}\theta^2 . \end{aligned}$$

If this does not hold, no x_U satisfies both (4) and (TH).

Assume now that $\alpha\Delta_a \ge \frac{1}{2}\theta^2$. We need to satisfy ((4) and) (TL). Clearly, (TL) holds iff

$$x_U \ge \frac{b_a - \overline{\theta}\, y_a}{\theta} - \frac{1}{2\alpha}\theta^2 = y_a - \frac{\Delta_a}{\theta} - \frac{1}{2\alpha}\theta = \hat{x}_{U,l} .$$

It remains to check that $x_U = \hat{x}_{U,l}$ satisfies (4). This is the case iff

$$\begin{aligned} y_U^2 &\geq 2\frac{\Delta_a}{\alpha} \\ \left(y_a - \left(y_a - \frac{\Delta_a}{\theta} - \frac{1}{2\alpha}\,\theta\right)\right)^2 &\geq 2\frac{\Delta_a}{\alpha} \\ \left(\frac{\Delta_a}{\theta} + \frac{1}{2\alpha}\,\theta\right)^2 - 2\frac{\Delta_a}{\alpha} &\geq 0 \\ \left(\frac{\Delta_a}{\theta} - \frac{1}{2\alpha}\,\theta\right)^2 &\geq 0, \end{aligned}$$

which is obviously true. The last line follows using the binomial formulae since $2\frac{\Delta_a}{\alpha} = 2 \cdot 2 \cdot \frac{\Delta_a}{\theta} \cdot \frac{1}{2\alpha}\,\theta$. □

C.2 Main Results

Proposition 5.

Proof. If the condition in part 1.a holds, we have $x_U = \hat{x}_U = \hat{x}_{U,h}$ and thus (by the proof of Proposition 4) (XM) holds with equality. It follows immediately from Proposition 2 that this implies $x_L = y_a$. Likewise if the condition in part 1.b holds. If the condition in part 2.a holds, then $x_U = \hat{x}_U = \hat{x}_{U,l}$ and thus (by the proof of Proposition 4) (TL) holds with equality. By the proof of Lemma 1, this immediately implies $r_L = \overline{\theta}$. Likewise for the condition in 2.b. □

Corollary 1.

Proof. By Proposition 5, we have $x_L = y_a$ or $r_L = \overline{\theta}$. By assumption, $x_L \leq x < y_a$ and thus $x_L = y_a$ is not possible. We must therefore have $r_L = \overline{\theta}$. And, again since $x \geq x_L$, $r(x) = r_L$. □

Theorem 1.

Proof. If $S \subseteq [0, y_a] \times [0, y_a]$ is a set of (b_a, x) pairs, define the *b_a-interior* of S as the set $\{(b_a, x) \in S \mid \exists \varepsilon > 0 : (b_a + \varepsilon, x), (b_a - \varepsilon, x) \in S\}$. It suffices to show the following: for any point (b_a, x) that lies within the b_a-interior of any of the sets of pairs (b_a, x) defined by the following (topologically closed) conditions, if $r(x; b_a) > \overline{\theta}$, then we have

$$\frac{\mathrm{d}b(x; b_a)}{\mathrm{d}b_a} > 0.$$

We will perform case distinction in such a way that this derivative always exists. Assume that $r(x; b_a) > \overline{\theta}$. The statement is easy to see in the following cases:

If $x \geq x_U$, the statement is trivial because here, $b(x; b_a) = b_a - x$ and so $\frac{\mathrm{d}b(x;b_a)}{\mathrm{d}b_a} = 1 > 0$. If $x_U = \bar{x}_U \leq x \leq x_L$, the statement follows immediately from Prop. 1 and Prop. 2 Part 3. Note that whenever $x_U = \bar{x}_U$, the parameters $\alpha = \overline{\alpha}$ and $x_U = \bar{x}_U$ are constant. If any of the conditions of Proposition 5 holds, then by Corollary 1, we do not need to discuss these cases.

For the remainder of the (b_a, x) space, we perform further case distinction and we combine Prop. 1 with Propositions 4 and 3, respectively, to explicitly compute the partial derivatives.

Assume first that $\hat{\alpha} \geq \overline{\alpha}$, $\hat{x}_U \leq \bar{x}_U$, $\alpha\Delta_a \leq \frac{1}{2}\,\theta^2$, and $x_U \leq x \leq x_L$. This implies that $x_U = \hat{x}_{U,h}$. In a neighborhood of (x, b_a) we have

$$\begin{aligned} \frac{\mathrm{d}b(x; b_a)}{\mathrm{d}b_a} &= \frac{\mathrm{d}}{\mathrm{d}b_a}\left[b_a - x + \frac{\overline{\alpha}}{2}(x - \hat{x}_{U,h}(b_a))^2\right] \\ &= 1 + \frac{\overline{\alpha}}{2} \cdot 2(x - \hat{x}_{U,h}(b_a)) \cdot (-1) \cdot \frac{\mathrm{d}}{\mathrm{d}b_a}\,\hat{x}_{U,h}(b_a) \\ &= 1 - \overline{\alpha}(x - \hat{x}_{U,h}(b_a)) \cdot \frac{\mathrm{d}}{\mathrm{d}b_a}\left[y_a - \sqrt{2\frac{y_a - b_a}{\overline{\alpha}}}\right] \\ &= 1 - \overline{\alpha}(x - \hat{x}_{U,h}(b_a)) \cdot (-1) \cdot \frac{1}{2}\frac{1}{\sqrt{2\frac{y_a - b_a}{\overline{\alpha}}}} \cdot (-\frac{2}{\overline{\alpha}}) \\ &= 1 - \frac{x - \hat{x}_{U,h}(b_a)}{y_a - \hat{x}_{U,h}(b_a)} > 0. \end{aligned}$$

The last equality is by definition of $\hat{x}_{U,h}(b_a)$ and the inequality is because $x < y_a$ and $x, y_a > \hat{x}_{U,h}(b_a)$ by assumption. If we instead have $\alpha\Delta_a \geq \frac{1}{2}\,\theta^2$, then $x_U = \hat{x}_{U,l}$ and

$$\frac{\mathrm{d}}{\mathrm{d}b_a}\,\hat{x}_{U,l}(b_a) = \frac{\mathrm{d}}{\mathrm{d}b_a}\left[y_a - \frac{\Delta_a}{\theta} - \frac{1}{2\overline{\alpha}}\,\theta\right] = \frac{1}{\theta}.$$

Thus,

$$\begin{aligned} & \frac{\mathrm{d}b(x; b_a)}{\mathrm{d}b_a} = 1 - \overline{\alpha}(x - \hat{x}_{U,h}(b_a))\frac{1}{\theta} > 0 \\ \Leftrightarrow \quad & p(x; b_a) = 1 - \overline{\alpha}(x - \hat{x}_{U,h}(b_a)) > \overline{\theta} \end{aligned}$$

This is true because $x \leq x_L$ by assumption and thus $p(x) \geq r(x)$ and we have $r(x) > \overline{\theta}$ by assumption.

Assume now that $\hat{\alpha} \leq \overline{\alpha}$, $r_a \geq \frac{1+\overline{\theta}}{2}$, and $x_U \leq x \leq x_L$. In this case we have $x_U = 0$ and $\alpha = \hat{\alpha}_H(b_a)$ and we have

$$\begin{aligned} \frac{\mathrm{d}b(x; b_a)}{\mathrm{d}b_a} &= \frac{\mathrm{d}}{\mathrm{d}b_a}\left[b_a - x + \frac{\hat{\alpha}_H(b_a)}{2}x^2\right] \\ &= 1 + \frac{1}{2}x^2\frac{\mathrm{d}}{\mathrm{d}b_a}\,\hat{\alpha}_H(b_a) \\ &= 1 + \frac{1}{2}x^2 \cdot 2 \cdot \left(-\frac{1}{y_a^2}\right) \\ &= 1 - \left(\frac{x}{y_a}\right)^2 > 0 \end{aligned}$$

since $x < y_a$. If instead $r_a \leq \frac{1+\overline{\theta}}{2}$, then

$$\frac{\mathrm{d}}{\mathrm{d}b_a}\,\hat{\alpha}_L(b_a) = \frac{1}{2} \cdot \theta^2 \cdot (-1) \cdot \frac{1}{\left(b_a - \overline{\theta}\,y_a\right)^2} = -\frac{1}{2}\frac{\theta^2}{\left(b_a - \overline{\theta}\,y_a\right)^2} = -\,\hat{\alpha}_L(b_a)\frac{1}{b_a - \overline{\theta}\,y_a},$$

where the last equality is by definition of $\hat{\alpha}_L(b_a)$. Therefore, we have (writing just α for $\hat{\alpha}_L(b_a)$ in the interest of brevity)

$$\begin{aligned} \frac{\mathrm{d}b(x; b_a)}{\mathrm{d}b_a} &= 1 + \frac{1}{2}x^2 \cdot \left(-\alpha\frac{1}{b_a - \overline{\theta}\,y_a}\right) \\ &= 1 - \alpha \cdot \frac{1}{2}x^2\frac{1}{b_a - \overline{\theta}\,y_a}. \end{aligned}$$

To see that this is positive, first note that, by Proposition 5 and Proposition 2, $\overline{\theta} = r_L = 1 - \alpha x_L$ and thus $x_L = \theta/\alpha$. Since $x_U \leq x \leq$

x_L and we have $r(x) > \overline{\theta} = r_L$, we must have $x < x_L = \theta/\alpha$ and thus

$$1 - \alpha \cdot \frac{1}{2} x^2 \frac{1}{b_a - \overline{\theta}\, y_a} > 1 - \alpha \cdot \frac{1}{2} \frac{\theta^2}{\alpha^2} \frac{1}{b_a - \overline{\theta}\, y_a}$$
$$= 1 - \frac{1}{\alpha} \cdot \frac{1}{2} \frac{\theta^2}{b_a - \overline{\theta}\, y_a} = 1 - \frac{1}{\alpha} \cdot \alpha = 0$$

as required.

One easily checks that our case distinction is complete. This concludes the proof. □

Theorem 2.

Proof. Let (x^0, b^0, y^0) be a solution to the initial value problem at S_0. Note that x^0, b^0, y^0 are functions of x. Then the functions $b^X(x) := b^0(X + x)$ (and analogously for y) form the solution to the IVP at S_X. To see this, note that they satisfy the differential equations (because (x^0, b^0, y^0) do and translation by X does not affect the derivatives) and they satisfy the initial values by choice of S_X. We now have $b_{X,Y} = b^X(Y) = b^0(X + Y) = b_{X+Y}$, and likewise for the other two. This is easy to see for y because it is simply x plus a constant; however our argument does not depend on this fact. Overall, $S_{X,Y} = S_{X+Y}$. For the redemption amounts, we now have $P_X + P_{X,Y} = (b_0 - b_X) + (b_X - b_{X,Y}) = b_0 - b_{X,Y} = b_0 - b_{X+Y} = P_{X+Y}$. □

Lemma 2.

Proof. Separate into two cases: (i) when $\frac{\mathrm{d}f}{\mathrm{d}t} \geq 0$, and (ii) when $\frac{\mathrm{d}f}{\mathrm{d}t} < 0$. These correspond to the x value increasing or decreasing respectively along the path f. Suppose we are at the current state $(f(t), r_{f,\mathfrak{r}}(t))$ and that this point is on the reserve ratio curve $\hat{\mathfrak{r}} \in \mathcal{R}$. In (i), x is increasing (redemption operation), and so (5) applies. Taking derivative of $r(x)$,

$$\frac{\mathrm{d}r}{\mathrm{d}x} = \frac{\frac{\mathrm{d}b}{\mathrm{d}x} y(x) + b(x)}{y^2(x)}$$
$$= \frac{r(x) - \rho(x, b(x), y(x)) + \gamma(x, b(x), y(x))}{y(x)}.$$

The derivative is greater (in this case less negative) when $\gamma > 0$. When $\gamma = 0$, we have the system (2), and the reserve ratio follows $\hat{\mathfrak{r}}(x)$.

In (ii), x is decreasing (minting operation), and so (6) applies. Taking derivative of $r(x)$,

$$\frac{\mathrm{d}r}{\mathrm{d}x} = \frac{r(x) - \varphi(x, b(x), y(x))}{y(x)}.$$

Since $\varphi \geq 1$, we have $\varphi \geq \rho$. And so the derivative is greater than the corresponding derivative in (2), which would keep us on the reserve ratio curve $\hat{\mathfrak{r}}$.

In both cases, the path does not bring us to a region below $\hat{\mathfrak{r}}$ in (x, r) space. Since Theorem 1 gives us that r_a (via b_a) is monotonic in r, it must be non-decreasing along this path. □

Theorem 3.

Proof. From Lemma 2, we know that r_a is weakly increasing along the path. Since reserve ratio curves are point-wise non-decreasing in their parameter r_a, the result follows immediately. □

Theorem 4.

Proof. This setup is equivalent to changing the RHS of (2) to $(1-\varepsilon)\rho(\cdot)$, which is a constant scaling. From linearity of integration, the only thing that changes structurally about the system is the hyperparameters (static parameters), which can be thought of as mapping in the following ways:

- a thus far implicit parameter specifying the \$1 target $\mapsto$ $(1 - \varepsilon)$ target,
- $\overline{\alpha} \mapsto (1 - \varepsilon)\overline{\alpha}$,
- $\overline{\theta} \mapsto (1 - \varepsilon)\,\overline{\theta}$.

A useful interpretation is that this scaling can be effectively 'reversed' by normalizing the system (in this case the redemption system in isolation) back to a \$1 target. The underlying hyperparameters effectively shift slightly from the reverse scaling, but we are left with the same underlying structure and machinery. Since we proved the above results for all hyperparameter values –and it is simple to add in the thus far implicit hyperparameter specifying the target through this normalization argument– the results still stand even though the hyperparameters shift. In particular, we have retained path independence for the redemption system in (5).

To show the second result of the theorem, we need to add in the minting process as described in Section 5.2. Consider a sole trader interacting with the system. If they desire a net redemption from the protocol, then by the path independence of the redemption curve, there is no incentive to subdivide the redemptions into several smaller redemptions. The remaining possibility is that the trader subdivides the net redemption into a sequence of redemptions and minting that nets to the desired redemption. It is simple to see that this is not profitable for two consecutive mint and redeem trades since the integrands $(1 - \varepsilon)\rho(\cdot) \leq \varphi(\cdot)$ in this region (reserve ratio ≤ 1). In words, this is not profitable because the trader must pay a non-negative spread between minting and redeeming in backtracking in a path in x, and so it is more profitable not to backtrack (it is always better to cancel out a mint with a redemption). From a simple induction then, the best option for the trader is to choose the net redemption desired in aggregate. □