

Designing Autonomous Markets for Stablecoin Monetary Policy*

Ariah Klages-Mundt[†] Steffen Schuldenzucker[‡]

August 2023

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 an autonomous mechanism for 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 issuance and redemption mechanisms, 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. This means 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. Finally, we show how to implement the P-AMM efficiently on-chain.

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. The terminology here is borrowed from ETF market structure and contrasts “primary market”, where shares of a fund 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). A primary market for a stablecoin helps to maintain peg by allowing users to exchange stablecoins with the protocol near the peg price, providing a means to arbitrage other markets back toward the peg value,

*The design from this paper is implemented as part of the upcoming Gyroscope stablecoin system under the name *Dynamic Stability Mechanism (DSM)*. The source code will be made available later.

[†]Researcher at Superluminal Labs; in a separate capacity, a PhD student at Cornell University.

[‡]Researcher at Superluminal Labs

should they deviate. In a blockchain protocol, primary markets are automated; we call the mechanism that controls mint and redeem prices the *primary algorithmic market maker (P-AMM)* of the stablecoin. Every stablecoin design has a P-AMM, be it intentionally designed or not.

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 causes the price of Dai to increase as borrowers need to buy it to reduce exposure. This was shown to amplify collateral and liquidity drawdown and cause instability in Dai Klages-Mundt and Minca (2021, 2022). This demonstrated fundamental problems around deleveraging, liquidity, and scaling in stablecoins like Dai, in which supply depends on an underlying market for leverage as opposed to a primary market.¹

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.² 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). This arguably compromises the 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. Mostly, these designs have either no or dubious degrees of asset backing. These designs have almost universally experienced depegging events, as depicted in Figure 2 due to susceptibility to downwards spirals arising from the lack of asset backing and ad hoc primary market structure when under-reserved.

Algorithmic stablecoins are best understood in the context of currency peg models, such as Morris and Shin (1998). 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

¹In 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.

²Two other notable approaches are using negative rates to equilibrate supply and demand at the target (e.g., Rai) and using dedicated liquidity pools to smooth the effects of deleveraging (e.g., Liquity and the solution proposed in Klages-Mundt and Minca (2022)). 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 spirals.

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.

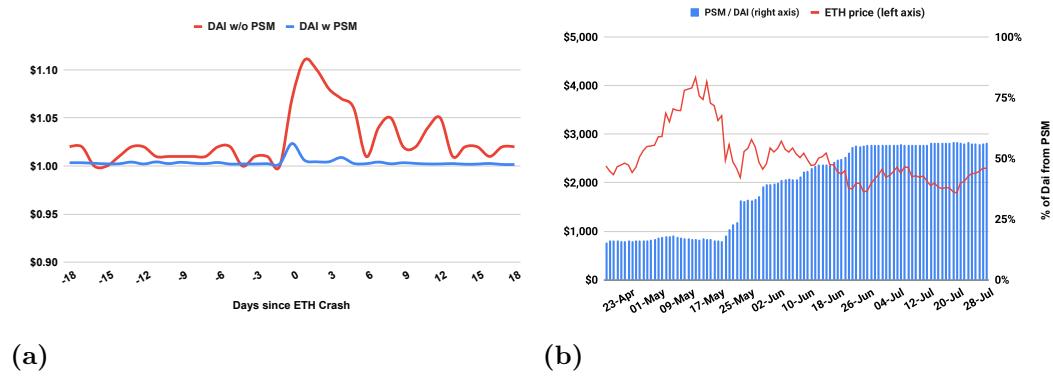
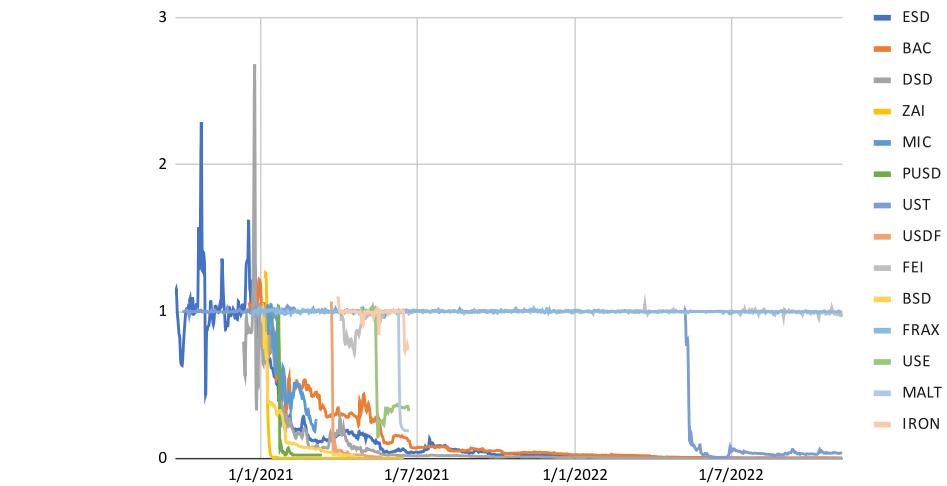


Figure 2 The recent churn of algorithmic stablecoins.



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.

Algorithmic stablecoins have encountered several fundamental problems, which contribute challenges to primary market design. Many are under-reserved by design while having no native economic usage, leading to many observed depeggings through downwards spirals, often exhausting the asset backing. 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 and can spiral to zero Klages-Mundt et al. (2020). A better equipped limit case is a stablecoin backed fully by a portfolio of exogenous, but risky and possibly illiquid, assets, which could enter an under-reserve state if assets experience shocks. Any design that could experience under-reserved states requires a good policy for how the protocol applies reserve assets to maintain liquidity near the peg in sustainable ways, factoring in the state of reserve backing. This challenge effectively becomes the problem of designing a primary market for the stablecoin.

1.1 This Paper

In this paper, we study 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. Such a formulation will require minimal intervention by governance, further limiting risks from governance extractable value Lee and Klages-Mundt (Apr. 23, 2021). We make the following contributions.

- We introduce our analysis framework of the *redemption curve* of a stablecoin and conduct a case study of different existing P-AMM designs (Section 2).
- We formulate the P-AMM desiderata (Section 3).
- We design a new P-AMM redemption curve implicitly (Section 4). The design is parameterized by a virtual *anchor point* that captures system health and redemption pressure. We specify the curve explicitly as a function of the anchor point (Section 5) and we show that the anchor point is uniquely determined by the current system state (Section 6), implying that the overall design is well-defined. We also establish that the shape of the redemption curve satisfies several of our desiderata directly. Furthermore, we formulate a simpler redemption curve that satisfies many, but not all, desiderata (Section 4.2 and Appendix B).
- We show that our P-AMM redemption curve is path independent and we prove several path deficiency properties in an extended setting with trading fees and minting. In particular, we show that system health weakly improves relative to the path independent setting along any trading curve and there is no incentive

to strategically subdivide redemptions (Section 7).

- Finally we show that our P-AMM can be implemented efficiently on-chain. Specifically, the implementation only requires a constant number of basic arithmetic operations and at most two square roots to evaluate. The implementation makes use of additional structural results (Section 8).

The result 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 reliance on governance intervention.

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.

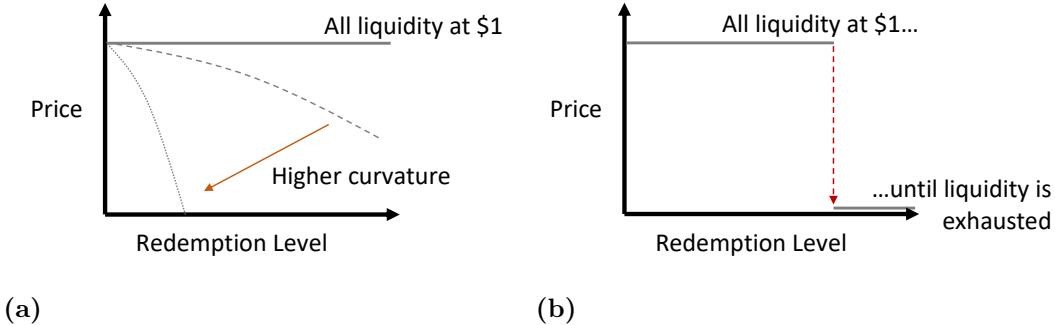
We make two important, but not contentious, assumptions in this work. First, we exclude endogenous/circularly priced collateral by assuming that reserve assets are exogenously priced. Second, we assume that the system has an accurate oracle that provides the price of reserve assets in USD. The need for 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., Werner et al. (2021)), it is important to incorporate other protective mechanisms; however, these are separate from the P-AMM mechanism itself.

1.2 Primary Markets: Related Work

Our work is most closely related to currency peg models in international economics (e.g., Morris and Shin (1998); Guimaraes and Morris (2007)) as well as models of pegged money market mutual funds (e.g., Parlatore (2016)). Although these types of models have been discussed and adapted recently in the context of stablecoins (e.g., Routledge and Zetlin-Jones (2021); Li et al. (2020)), 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. For further academic background on stablecoins, we refer to Klages-Mundt et al. (2020); Bullmann et al. (2019); Pernice et al. (2019) and references therein.

For an overview of theory work on AMMs, we refer to Angeris and Chitra (2020); Angeris et al. (2020); Capponi and Jia (2021). Further background and references are available in Werner et al. (2021). Current AMMs resemble Uniswap Adams et al. (2021) and Curve Egorov (2019), 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

Figure 3 Stylized primary market redemption curves.



analyzes such constructions for stablecoins.

A well-designed primary market for a stablecoin can be interpreted as an autonomous version of open market operations, comparing with how central banks interact with markets to shape monetary policy. See Appendix A for further discussion on this comparison. Designing an algorithmic primary market presents a challenge akin to designing a rules-based monetary policy (i.e., a *Taylor Rule*; see, e.g., Orphanides (2010)). However, rather than setting nominal interest rates in a quasi-algorithmic way, as in normal central bank monetary policy, an algorithmic primary market is setting prices in a programmatic way.

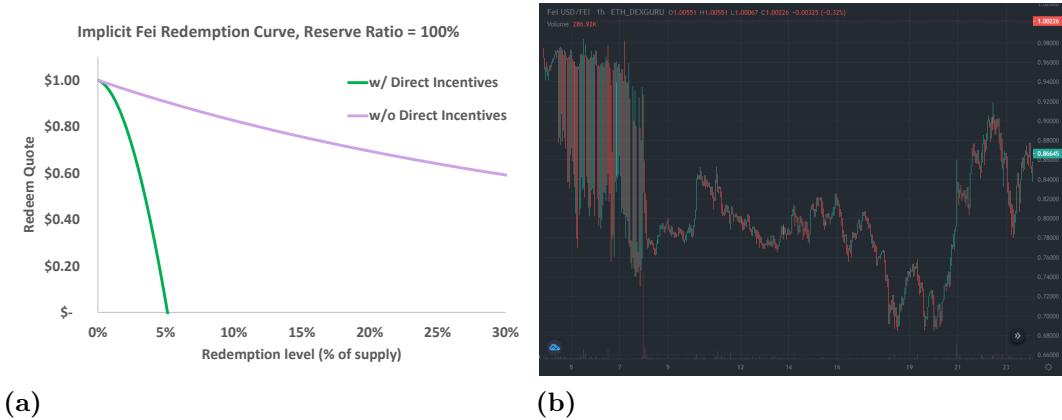
2 Primary Markets: Case Studies

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.³ 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.,

³For recent background on AMMs, see Angeris and Chitra (2020), which focuses on constant function market makers (CFMMs). However, primary markets will not fit this category in general.

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



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 $\sim \$1$. 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.

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 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. 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 akin to 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 (“direct incentives”). This has the effect of distorting the implicit Fei redemption curve into a poor shape (see 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. Following the Fei launch in April 2021 and despite an 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 (see Figure 4b).⁴

UST / Seigniorage Shares. The TerraUSD (UST) stablecoin was intended to be backed by a seigniorage shares-style token, LUNA. UST was redeemable for newly minted LUNA, inflating the supply of the latter. The redemption curve was intended to be flat at \$1. However, since LUNA was an endogenous/circularly priced asset, there was no guarantee that speculators' demand would be enough to support its UST backing. In Feb. 2022, a partial backing of Bitcoin was added. Despite this, in May 2022, a downwards spiral was triggered, in which UST saw mass redemptions, the Bitcoin reserve was exhausted, and the value of LUNA went to zero, removing essentially all support from UST and allowing it to crash to mere cents on the dollar (see Figure 5). This is a variation on the stylized redemption curve in Figure 3b.

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.

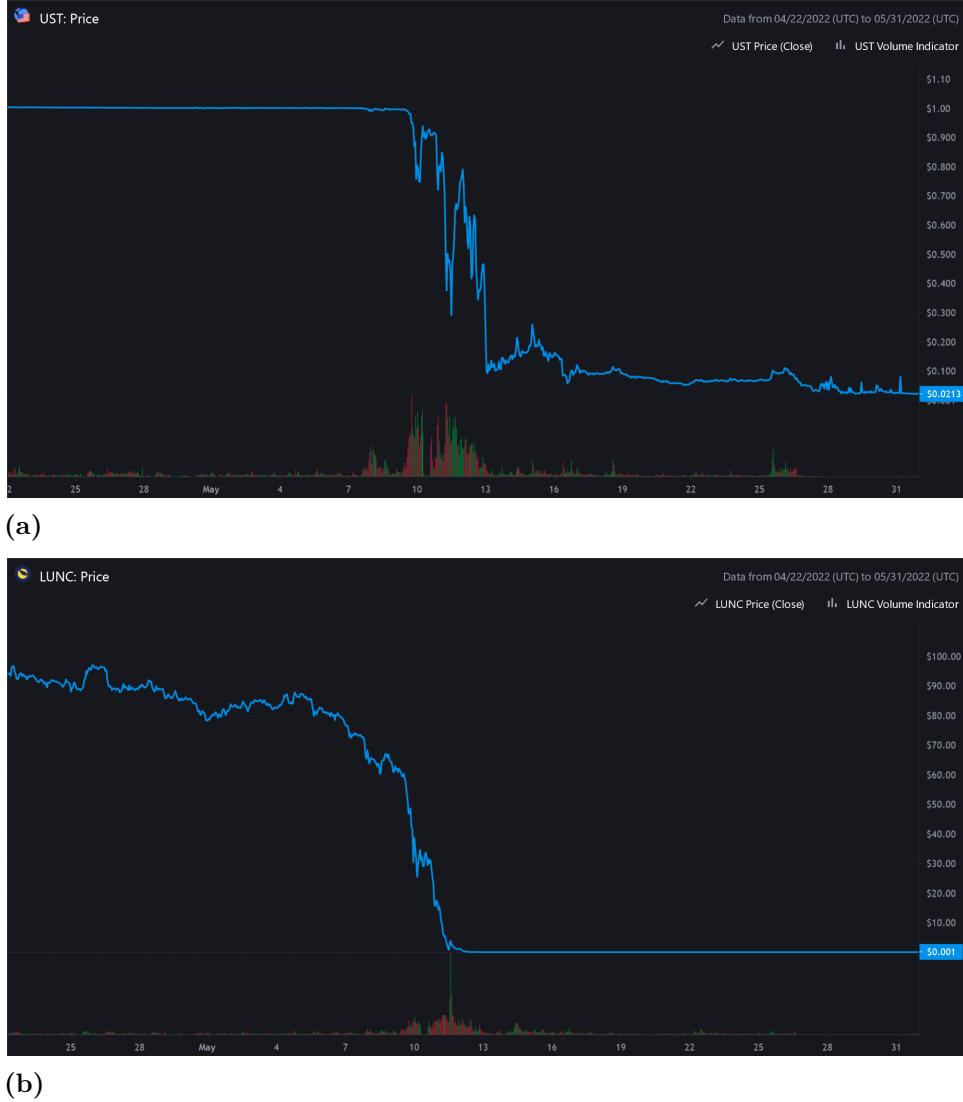
We strive for several desiderata in the design of a primary market mechanism that has good properties from stability and usability perspectives. We separate these into properties of the P-AMM within a block and more general properties.

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 $\sim \$1$.
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.

⁴The 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.

Figure 5 UST case study. (a) following a downwards spiral, UST price near \$0. (b) LUNA price going to zero at the same time.



These desiderata are informed by results about currency peg models, in which the shape of optimal monetary policies involve peg support up to a threshold and reserve preservation past that. 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 property reduces risk for traders and incentives for potential speculative attacks. Supposing the peg is not maintainable, the system can't know what the equilibrium price of the stablecoin will be. It only knows upper and lower bounds on it, considering the target and the level of reserves. A continuous P-AMM enables the new equilibrium price to be found along the curve and helps smooth flows around it.

The fourth and fifth properties are also 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. 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).

4 Redemption Curve Design

We now discuss our P-AMM design. We first introduce the dynamical system framework within which our design will take place. We then describe a greatly simplified redemption curve design that satisfies all desiderata but one: its redemption curve is not continuous but has a steep discontinuity. Finally, we introduce our actual, more sophisticated continuous redemption curve design.

4.1 Dynamical System, Anchor Point

For the purpose of designing the P-AMM, we model the stablecoin 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.⁵ Observe that $y(x) = y_a - x$ and $b(x) = b_a - \int_0^x p(x')dx'$, where $p(x')$ is the marginal redemption price offered by the P-AMM at redemption level x' .

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 ($y_0 = y(x_0)$)

Note that we will generlaly 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

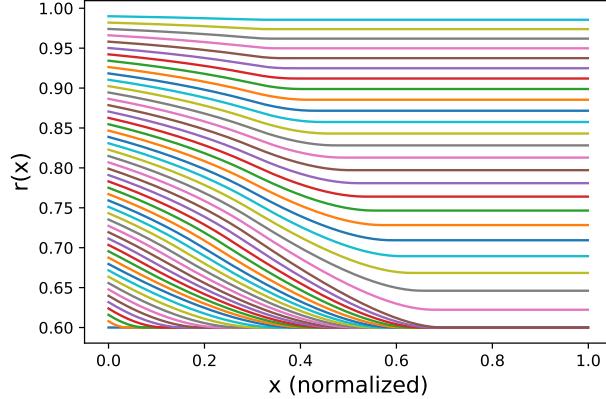
$$(0, b_a, y_a),$$

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.

The pricing curve p is, in general, a function of b_a and y_a . We will see later 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 $b/y \geq 1$, we set $\rho(x, b, y) = 1$. The dynamical

⁵We 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 $y_a = 1$.



system is then described by the following system of ordinary differential equations:

$$\begin{aligned} \frac{db(x)}{dx} &= -\rho(x, b(x), y(x)) \\ \frac{dy(x)}{dx} &= -1. \end{aligned} \tag{1}$$

Our P-AMM, conceptually speaking, solves the initial value problem defined by (x_0, b_0, y_0) and the system (1). 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 $b(x_0 + X) - b_0$.

4.2 Simplified, Discontinuous Redemption Curve Design

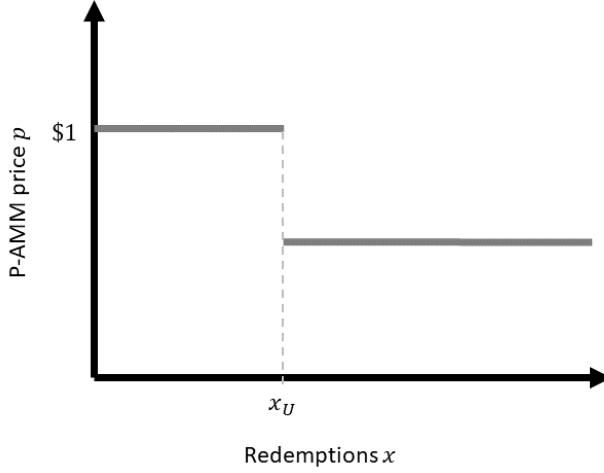
We now discuss a simplified P-AMM redemption curve as a pedagogical starting point. This simplified curve has discrete price decay (i.e., the curve is discontinuous: a portion of the curve is at \$1 and another portion maintains a sustainable reserve ratio) and is very simple to reason about. This will fulfill many desirable properties except for continuity. We provide a semi-formal treatment here; see Appendix B for the formal details.

To define the redemption curve, we assume that the anchor point (b_a, y_a) is fixed and given. We will discuss in Sections 6 and 8 how the anchor point can be chosen based on the current state of the system. Assume WLOG $b_a < y_a$ (i.e., $r_a < 1$) since otherwise, we always use the trivial redemption curve $p(x) = 1$. For simplicity of analysis, we will for now disregard any trading fees that may be added to the P-AMM.

Our simplified redemption curve is illustrated in Figure 7 and defined by the following function:

$$p(x) := \begin{cases} 1 & \text{if } x \leq x_U \\ r_U := r(x_U) & \text{if } x > x_U, \end{cases}$$

Figure 7 Simplified redemption curve with discrete price decay.



Observe that $r(x_U)$ can be computed from only b_a , y_a , and x_U , so that $p(x)$ is a well-defined function.

This redemption curve maintains a redemption price of 1 up until some redemption pressure value $x_U \in [0, y_a]$ and then drops the redemption price to the reserve ratio below that value. From this point onwards, the reserve ratio will stay constant (this is easy to see) and in particular, we will be able to provide redemptions at price r_U , potentially until the whole SC supply has been redeemed.

The parameter x_U is a *dynamic parameter*. Concretely, this means that, given a specific value of this parameter, the shape of the redemption curve is fixed. However, the dynamic parameters itself depends on the state of the system. More in detail, it is a function of the anchor point (b_a, y_a) .

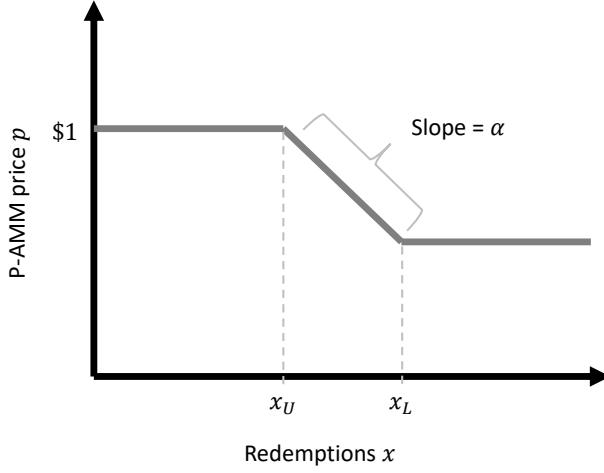
The choice of the parameter x_U introduces a trade-off: when it is high, we maintain a price of 1 for a long time (in terms of redemption pressure). This allows the stablecoin to maintain the peg for longer, but the eventual redemption price r_U will be low. Lower x_U values enable a higher eventual redemption price but weaken the peg more quickly. To weigh this trade-off, we assume that two *static parameters* are set externally (e.g., by the protocol's governance system):

Parameter	Definition
\bar{x}_U	$\in [0, \infty]$ upper bound on x_U ($x_U \leq \bar{x}_U$)
$\bar{\theta}$	$\in [0, 1]$ target reserve ratio floor

x_U is then chosen such that the following conditions hold:

1. At any point x of the redemption curve, $r(x) \geq \bar{\theta}$, if this is possible, and $r(x)$ maximal otherwise. Equivalently, we want $r_U \geq \bar{\theta}$ if possible and r_U maximal otherwise.
2. $x_U \leq \bar{x}_U$.
3. Among the x_U values that satisfy these conditions, x_U is chosen maximal.

Figure 8 Our redemption curve design with piecewise-linear price decay.



One can show that this is the case iff

$$x_U = \min\left(\bar{x}_U, \max\left(0, y_a \frac{r_a - \bar{\theta}}{1 - \bar{\theta}}\right)\right)$$

The static parameter \bar{x}_U is optional and can be set to ∞ to turn off this feature. In this case, the choice of x_U will always create a situation where $r_U = \min(r_a, \bar{\theta})$, i.e., we always choose the lowest acceptable eventual reserve ratio to maximize x_U . Setting $\bar{x}_U < \infty$ makes the trade-off less extreme and allows $r_U > \bar{\theta}$ when b_a is large.

It is easy to see that the redemption curve design from this section satisfies our desiderata 1.–3. from Section 3, but it obviously violates desideratum 4 (continuity). This is undesirable for traders and it creates a potential target for speculative attacks on the stablecoin price. This is why in the following, we discuss a continuous redemption curve design.

4.3 Continuous Redemption Curve

To maintain continuity, we alter the design from the previous sub-section to receive a three-piece-wise curve design. This requires some more sophisticated machinery. Again, we assume in this section that an anchor point (b_a, y_a) is given.

We now parameterize the curve in terms of *three* dynamic parameters. Conceptually, the three dynamic parameters describe three regions of the P-AMM pricing curve p as a function of x , as visualized in Figure 8. For a small redemption level x , the P-AMM provides redemptions at \$1 up until a redemption level x_U is reached. In a second region, the P-AMM pricing decays linearly with slope α as more redemptions occur up until a redemption level x_L . Then, in a third region, the P-AMM provides redemptions at the new reserve ratio (reserve value per outstanding stablecoin), which is fully sustainable for the entire remaining stablecoin supply. The dynamic parameters are summarized in the following table.

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 $b_a < y_a$,

$$p(x; b_a, y_a) = \begin{cases} 1, & x \leq x_U \\ 1 - \alpha(x - x_U), & x_U \leq x \leq x_L \\ r_L, & x \geq x_L \end{cases}, \quad (2)$$

where $r_L = r(x_L)$. In the other case that $b_a \geq y_a$, 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 parameters are chosen in Section 5.

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 $\bar{\theta}$, 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 ($\alpha \geq \bar{\alpha}$)
\bar{x}_U	$\in [0, \infty]$ upper bound on x_U ($x_U \leq \bar{x}_U$)
$\bar{\theta}$	$\in [0, 1]$ 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 is 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. We explore this option further in Section 8.

5 Calculation of Dynamic Parameters for a given anchor point

We first establish how to calculate the dynamic parameters of the redemption curve when the anchor point (b_a, y_a) is given. Recall that this anchor point is a mathematical

modeling tool and is not known as a real quantity at any point in time. Instead, it will be ‘‘reconstructed’’ from the current market state (see Section 6 below). Assume for non-triviality that $1 > b_a/y_a > \bar{\theta}$. Then the dynamic parameters are chosen as follows.

- x_L is chosen such that $p(x_L) = r(x_L)$, i.e., the computed redemption price (in the linear segment) equals the reserve ratio at this point. If x_L is chosen like this, all remaining stablecoin units could be redeemed at this price without running out of reserves. x_L is a function of (b_a, y_a) , x_U , and α . Note that $r(x_L)$ is the lowest reserve ratio on the curve.⁶
- α and x_U are chosen to guarantee that $r(x_L) \geq \bar{\theta}$ while minimizing price decay.
- Among the (α, x_U) pairs satisfying the previous condition, we prioritize making α as small as possible (but at least $\bar{\alpha}$), i.e., making price decay as mild as possible in the linear part. If $\alpha = \bar{\alpha}$, we then choose x_U as large as possible (but at most \bar{x}_U) while always ensuring $r(x_L) \geq \bar{\theta}$.

This leads to the following equations (see Appendix C for details; let $\Delta_a := y_a - b_a$):

$$\alpha = \max(\bar{\alpha}, \hat{\alpha}) \text{ where}$$

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

$$x_U = \min(\bar{x}_U, \hat{x}_U) \text{ where}$$

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

$$x_L = y_a - \sqrt{(y_a - x_U)^2 - \frac{2}{\alpha} \Delta_a}$$

$$r_L = 1 - \alpha(x_L - x_U)$$

6 Uniqueness of Reconstruction

We now move on to show that we can construct the anchor point (b_a, y_a) uniquely from the current state (x, b, y) , which proves that our dynamical system (1) is in fact well-defined. Recall that, in that dynamical system, 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) .

Our proof in this section is indirect: we show that each state (x, b, y) can only have arisen from one specific anchor point (see Section 8 for an explicit reconstruction technique). Uniqueness of y_a is trivial because $y = y_a - x$, so $y_a = y + x$; it remains

⁶One can show that $r(x_L)$ increases when α is increased (i.e., the reserve is protected when redemption prices decay more steeply) and when x_U is decreased (i.e., the reserve is protected when the redemption price starts to decay earlier).

to show that b_a is unique. We show that this is the case because, for fixed x , the reserve value

$$b(x; b_a, y_a) = \int_0^x p(x'; b_a, y_a) dx'$$

is a strictly monotonic function of b_a , whenever that state is non-trivial.⁷

Theorem 1. Fix values y_a , $\bar{\theta}$, $\bar{\alpha}$, \bar{x}_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 $1 > r(x; b_a)$, $r(x; b'_a) > \bar{\theta}$ (and in particular $1 > b_a/y_a$, $b'_a/y_a > \bar{\theta}$). Then $b(x; b_a) < b(x; b'_a)$.

The result is less immediate than it may seem at first. While it is easy to see 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 propositions 4 and 5 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.

We segment the space of (x, b_a) pairs along all case distinctions we have made so far. Specifically, we distinguish cases along the following dimensions. Note that these cases define closed regions and overlap at their boundaries and that within the intersection of any selection of these regions, the function $b(\cdot)$ is smooth. Recall that $r_a = y_a/b_a$ is the reserve ratio at the anchor point.

- **Case I–III** depending on the values of α and x_U . Specifically, let $\alpha = \max(\hat{\alpha}, \bar{\alpha})$, write short $\hat{x}_U := \hat{x}_U(\alpha)$, and let $x_U = \min(\hat{x}_U, \bar{x}_U)$, and define:

I $\hat{\alpha} \geq \bar{\alpha}$ and $\hat{x}_U \geq \bar{x}_U$, so that $\alpha = \bar{\alpha}$ and $x_U = \bar{x}_U$.

II $\hat{\alpha} \geq \bar{\alpha}$ and $\hat{x}_U \leq \bar{x}_U$, so that $\alpha = \bar{\alpha}$ and $x_U < \bar{x}_U$ except in the equality case.

III $\hat{\alpha} \leq \bar{\alpha}$, so that $\alpha < \bar{\alpha}$ except in the equality case and (in any case) $x_U = 0$.

- Within case II, **case II h**, where $\alpha\Delta_a \leq \frac{1}{2}\theta^2$ and thus $\hat{x}_U = \hat{x}_{U,h}$ and **case II l**, where $\alpha\Delta_a \geq \frac{1}{2}\theta^2$ and thus $\hat{x}_U = \hat{x}_{U,l}$.
- Within case III, **case III H**, where $r_a \geq \frac{1+\bar{\theta}}{2}$ and thus $\hat{\alpha} = \hat{\alpha}_H$ and **case III L**, where $r_a \leq \frac{1+\bar{\theta}}{2}$ and thus $\hat{\alpha} = \hat{\alpha}_L$.
- **Case i–iii** depending on the value of x relative to x_U and x_L . Specifically, define:

⁷Equivalently, 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 $\bar{\theta}$, $\bar{\alpha}$, \bar{x}_U fixed while the dynamic parameters α and x_U take on values dependent on the anchor point as discussed in Section 5.

- i** $x \leq x_U$
- ii** $x_U \leq x \leq x_L$
- iii** $x_L \leq x$

Note that only the distinction between case i–iii depends on x . In the following, we will address cases by a sequence of letters, such as case II h ii. Note that not all 36 potential combinations of these cases need to be addressed one-by-one. Many of these cases are irrelevant or easy to handle. For instance, in case I, the values of the parameters are known to be the constants $(\bar{\alpha}, \bar{x}_U)$ and thus we do not have to distinguish the H/L or h/l cases. The following proposition helps us when distinguishing the H/L and h/l cases. This will be useful for the proof of Theorem 1. Recall that all dynamic parameters we have defined so far, like x_L , are functions of b_a .

Prop. 1. *In case II h and III H, $x_L = y_a$. In case II l and III L, $r_L = \bar{\theta}$.*

[[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.

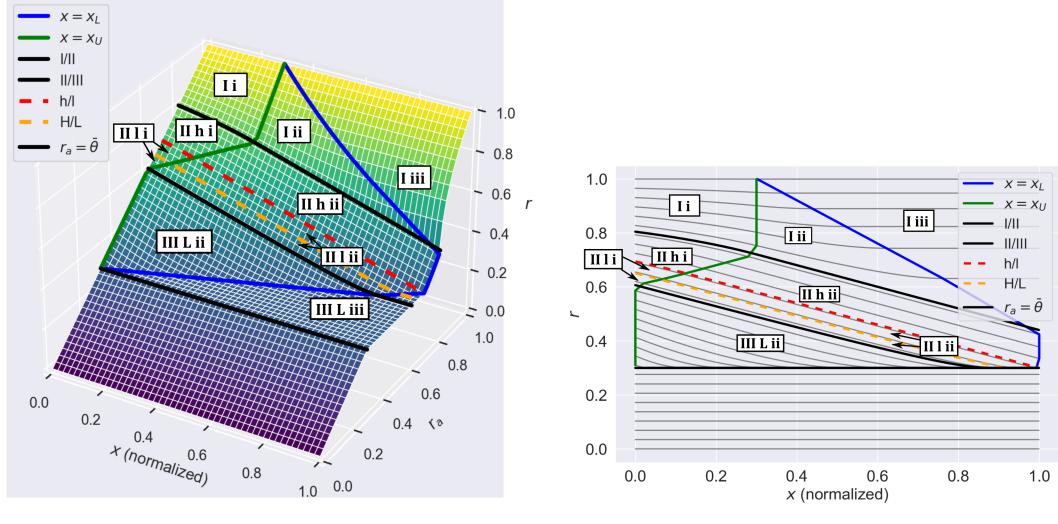
The result immediately implies that we do not need to consider cases II iii or III iii because the recovery rate is at most our defined floor and thus the mechanism defines that redemption must happen at the reserve ratio.

Corollary 1. *In case II iii and III iii, $r(x) \leq \bar{\theta}$.*

[[Link to Proof](#)]

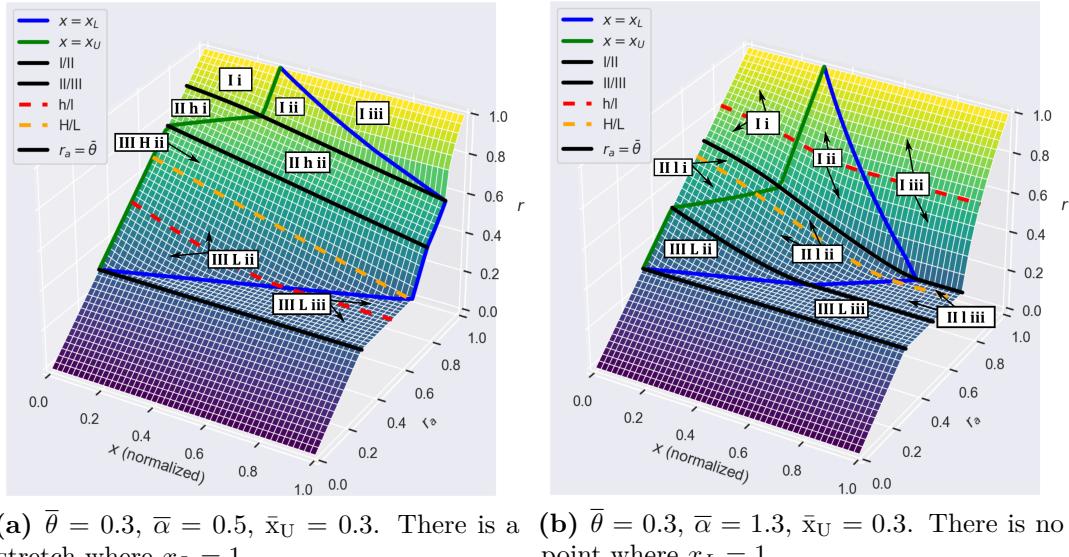
Conceptually, we can visualize the function $b(x; b_a)$, with which Theorem 1 is concerned, as a 3d surface. Figure 9a shows the surface of the reserve ratio as a function of x and b_a , where the different regions partition the (x, b_a) space.⁸ We have chosen $y_a = 1$ so that $b_a = r_a$ (but in general $b \neq r$). Notice that, as mentioned above, several of the regions can be essentially ignored. This is for two reasons: first, some of the lines separating different cases fall into a part of the (x, r_a) space where the respective case is not relevant. For instance, in this example, the line separating the H and L cases itself falls into region II, so that only case III L is present. In contrast, the line separating cases h and l falls into region II, so that both cases II h and II l are present. The second reason why distinctions between regions can be ignored is that 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 9b, in which many r curves are plotted (in gray) for differing values of r_a , which are the starting points of these curves. In this space, the region

Figure 9 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 $\bar{\theta} = 0.3$, $\bar{\alpha} = 0.8$, 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) 3d curve. (b) 2d projection to the (x, r) plane.

Figure 10 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.



(a) $\bar{\theta} = 0.3$, $\bar{\alpha} = 0.5$, $\bar{x}_U = 0.3$. There is a stretch where $x_L = 1$. (b) $\bar{\theta} = 0.3$, $\bar{\alpha} = 1.3$, $\bar{x}_U = 0.3$. There is no point where $x_L = 1$.

boundaries are given by particular cases of r curves, as shown. Notice that the flat section of the 3-d surface mentioned above disappears in the 2d-projection.

In Figure 9, region III H does not exist and 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 10.

Using the region partition, we can prove Theorem 1. Our proof is by case distinction over the different regions. Observe that the function $b(x, b_a)$ is smooth across any given region and we can compute the partial derivative of $b(x, b_a)$ with respect to b_a explicitly. The main challenge is to handle the adjustment in the dynamic parameters that takes place as b_a is varied.

[\[Link to Proof of Theorem 1\]](#)

As a simple corollary, we receive:

Corollary 2. *Fix values y_a , $\bar{\theta}$, $\bar{\alpha}$, \bar{x}_U , and $x \in [0, y_a]$, if $\bar{\theta} y_a < b_a < b'_a < 1$, then (a) $b(x; b_a) < b(x; b'_a)$ or (b) $r(x; b_a) = r(x; b'_a) = \bar{\theta}$. In particular, the functions $b(x; \cdot)$ and $r(x; \cdot)$ are weakly monotonic.*

[\[Link to Proof\]](#)

7 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.

7.1 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.

⁸Note 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.

Theorem 2. (*Path independence*) Let $S_0 := (x_0, b_0, y_0)$ be a state and let $X, Y > 0$ such that $X + Y \leq y_0$. Let the state 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](#)]

The theorem holds because the right-hand sides of (1) only depend on the current state of the system and not, for instance, on the initial conditions or the specific trading path that led to the current state. In the dynamical systems literature, this property is also known as invariance under horizontal translations.

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.

7.2 Path Deficiency Properties with Minting and Fees

We next discuss two properties analogous to path deficiency in CFMMs (see Angeris and Chitra, 2020) that holds in an extended setting with fees and the possibility of minting tokens in addition to redemption (where minting occurs at the same or a higher price than redemption). In this section, we provide an informal discussion of these results. For a formal treatment, see Appendix D.

Our first result is that, for any non-negative fee, trading along any *trading path* (i.e., any sequence of mint and redeem operations) can only improve system health compared to the net of the path. This property is important because it implies that the system is robust even under (and, in fact, benefits from) combinations of mint and redeem operations, which may result from market volatility. We capture “system health” by the reserve ratio $r(x)$ at a given redemption level x . This is a function of the anchor point (b_a, y_a) and the static parameters $\bar{x}_U, \bar{\alpha}, \bar{\theta}$. We assume in the following that these values are held fixed.

Theorem 3 (*Path Deficiency Vs. Netting, Informal*). *Consider any trading path ending in redemption level x . Let r_1 be the reserve ratio of the system after following the trading path through its mint and redeem operations and let $r_0 := r(x)$ be the reserve ratio at the net minting or redemption amount. Then $r_1 \geq r_0$.*

Our second result states 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. Note that, clearly, this may not be true when fees are non-linear in the size of a trade.

Theorem 4 (Path Deficiency Vs. Subdivision, Informal). *Assume that a non-negative fee is taken proportional to the redemption amount. Then the following hold:*

1. *The system is path independent with respect to combinations of only redemption (but not minting) operations even in the presence of fees.*
2. *An individual trader has no incentive to subdivide a net redemption within a block into a combination of minting and redemption operations.*

For traders, the previous theorem means that interacting with the mechanism is straightforward. For the mechanism, it means that the mechanism cannot be exploited by forming complex trading paths.

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 .

8 Efficient Implementation

We now discuss how to implement our mechanism on-chain. This section provides a high-level overview. The formal details are presented in Appendix E. Appendix B.2 discusses the implementation of the simplified redemption curve with discrete price decay.

The P-AMM can be operationalized as follows: we are given the current state of the system (x, b, y) , a redemption amount X , and we need to compute a redemption amount B that the trader should receive in exchange for X units of the stablecoin. To do this, the system constructs the anchor point (b_a, y_a) consistent with the current state, constructs the redemption curve from this, and then integrates over the redemption curve to compute the redemption amount.

Most of the implementation operates in a space normalized to $y_a = 1$. This is convenient because it allows the system to be configured in a way that is invariant under scaling of the stablecoin supply. We therefore assume that the static parameters refer to the *normalized* space. Specifically, we assume that the following static parameters are given:

Parameter	Definition
$\bar{\alpha}_1$	$\in (0, \infty)$ lower bound on decay slope in normalized space
$\bar{x}_{U,1}$	$\in [0, 1]$ upper bound on x_U in normalized space
θ	$\in [0, 1]$ target reserve ratio floor

Note that under the normalization, we assume that the *anchor* stablecoin supply y_a is 1, not the *current* supply y . Note also that the target reserve ratio floor is not affected by normalization. In Appendix E, we discuss the conversion between normalized and non-normalized space in detail.

The implementation of the algorithm now proceeds as follows (see Algorithm 4 in Appendix E). Assume WLOG that $b/y \in (\bar{\theta}, 1)$ since otherwise, the behavior of the P-AMM is trivial.

First, we can easily reconstruct $y_a = y + x$. The algorithm then normalizes all values to $y_a = 1$; specifically, we consider the *normalized state* $(x/y_a, b/y_a, y/y_a)$ and at the end of the algorithm, we will undo the normalization by scaling the computed normalized redemption amount by y_a . To simplify the exposition, assume in this section WLOG that $y_a = 1$ so that the original state and the normalized state are the same and we don't need to introduce any additional variables.

The algorithm now reconstructs the anchor reserve value b_a consistent with the current state. This is the most complex step of the algorithm. Recall that (b_a, y_a) together with the static parameters determine the dynamic parameters and thus the full redemption curve. We are looking for a b_a such that

$$b = b(x; b_a, y_a = 1).$$

It follows from continuity that such a b_a must exist and Theorem 1 implies that it is unique, but the theorem provides no way of computing it efficiently. To do this, we proceed in two steps:

1. First, we determine the *region* of (x, b, y) among the regions introduced in Section 6. Recall that these regions depend on b_a because they depend on the dynamic parameters x_U and α . The main insight that enables this step is that the region of a state can still be determined efficiently even if b_a is not known. To enable this, the algorithm (pre-)computes certain b_a values that separate different regions. We also show that (b_a, y_a) can be replaced by (b, y) when computing certain specific thresholds.
2. Second, given the region, we determine b_a . This is now relatively straightforward by replacing the definitions of α and x_U from propositions 4 and 5 as functions of b_a into the definition. Note that the region determines all case distinctions in the definitions, so that the equation $b = b(x; b_a, y_a)$ is smooth. In fact, it turns out that this can be written as a polynomial equation of degree at most 2 in b_a and thus solved easily for each individual region.

With b_a determined, we can compute α and x_U and from this we compute

$$B = b - b(x + X; b_a, y_a).$$

Note that the involved integral can be computed easily because p is piecewise-linear in x . We finally undo the normalization by returning $y_a \cdot B$.

Regarding computational cost, the algorithm can be implemented using only a constant number of arithmetic operations (no loops) and at most two square roots.

While techniques like pre-computation and caching could be used to further speed up the region detection step, their utility would have to be carefully traded off against the cost of storage; our current implementation does not use these techniques.

9 Concluding Remarks

We have designed a desirable P-AMM redemption curve based on an anchored state that codifies how a stablecoin can sustainably adapt monetary policy to respond to crisis events without external input. This can work to mitigate currency runs if the stablecoin becomes under-reserved or, with some modification to consider the liquid reserve ratio, to mitigate bank run-like risks if the reserve contains illiquid assets. We showed how this design satisfies desiderata 1–5 and 8 introduced in Section 3.

Desiderata 6 and 7 can be 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 and 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.

The desiderata properties that the P-AMM achieves were informed by results about optimal monetary policies in currency peg models and redemption policies in bank run models. A natural follow-up question is how to optimally parameterize the P-AMM. A first step in this direction would be to adapt currency peg models to a stablecoin setting with the general P-AMM shape defining the monetary policy and optimize the outcomes of the resulting game.

A remaining question is how one should optimally calibrate the P-AMM. This would be best carried out using formal game-theoretic models of speculative attacks on the P-AMM. An example of this type of attack involves an attacker who can take an outside short position and try to profit by triggering a de-peg of the stablecoin. Models of these attacks would integrate the P-AMM, a secondary market, and a shorting market, and is outside the scope of this paper. Models of speculative attacks on fiat currencies, which informed the P-AMM desiderata in the first place, may serve as a good starting point; we discuss these in Appendix A.

Another avenue for future work is to explore alternative P-AMM designs that may 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

- H. Adams, N. Zinsmeister, M. Salem, R. Keefer, and D. Robinson. Uniswap v3 core. Technical report, Technical report, 2021.

- G. Angeris and T. Chitra. Improved price oracles: Constant function market makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, page 80–91, 2020.
- G. Angeris, A. Evans, and T. Chitra. When does the tail wag the dog? curvature and market making. *arXiv preprint arXiv:2012.08040*, 2020.
- D. Bullmann, J. Klemm, and A. Pinna. In search for stability in crypto-assets: are stablecoins the solution? *ECB Occasional Paper*, (230), 2019.
- A. Capponi and R. Jia. The adoption of blockchain-based decentralized exchanges: A market microstructure analysis of the automated market maker. *Available at SSRN 3805095*, 2021.
- D. W. Diamond and P. H. Dybvig. Bank runs, deposit insurance, and liquidity. *Journal of political economy*, 91(3):401–419, 1983.
- M. Egorov. Stableswap-efficient mechanism for stablecoin liquidity. *Retrieved Feb, 24: 2021, 2019.*
- B. Guimaraes and S. Morris. Risk and wealth in a model of self-fulfilling currency attacks. *Journal of Monetary Economics*, 54(8):2205–2230, 2007.
- A. Klages-Mundt and A. Minca. (in) stability for the blockchain: Deleveraging spirals and stablecoin attacks. *Cryptoeconomic Systems*, 2021.
- A. Klages-Mundt and A. Minca. While stability lasts: A stochastic model of noncustodial stablecoins. *Mathematical Finance*, 2022.
- A. Klages-Mundt, D. Harz, L. Gudgeon, J.-Y. Liu, and A. Minca. Stablecoins 2.0: Economic foundations and risk-based models. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies*, pages 59–79, 2020.
- L. Lee and A. Klages-Mundt. Governance extractable value, Apr. 23, 2021. URL <https://ournetwork.substack.com/p/our-network-deep-dive-2>.
- Y. Li, S. Mayer, et al. *Managing Stablecoins: Optimal Strategies, Regulation, and Transaction Data as Productive Capital*. Ohio State University, Fisher College of Business, Charles A. Dice Center . . . , 2020.
- S. Morris and H. S. Shin. Unique equilibrium in a model of self-fulfilling currency attacks. *American Economic Review*, pages 587–597, 1998.
- A. Orphanides. Taylor rules. In *Monetary Economics*, pages 362–369. Springer, 2010.
- C. Parlatore. Fragility in money market funds: Sponsor support and regulation. *Journal of Financial Economics*, 121(3):595–623, 2016.
- I. G. Pernice, S. Henningsen, R. Proskalovich, M. Florian, H. Elendner, and B. Scheuermann. Monetary stabilization in cryptocurrencies—design approaches and open questions. In *2019 Crypto Valley Conference on Blockchain Technology (CVCBT)*, pages 47–59. IEEE, 2019.
- B. Routledge and A. Zetlin-Jones. Currency stability using blockchain technology. *Journal of Economic Dynamics and Control*, page 104155, 2021.
- G. Selgin. 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/>, 2020.
- S. M. Werner, D. Perez, L. Gudgeon, A. Klages-Mundt, D. Harz, and W. J. Knottenbelt. Sok: Decentralized finance (defi). *arXiv preprint arXiv:2101.08778*, 2021.

Appendix

A Parallels with the monetary economics literature.

A well-designed primary market for a stablecoin can be interpreted as an autonomous version of open market operations, comparing with how central banks interact with markets to shape monetary policy. 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.⁹ 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 expanding the balance sheet (it does not need to match the demand of other agents in doing so).

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., Morris and Shin (1998)). 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 Morris and Shin (1998), 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.¹⁰ Compared to a

⁹Notably, 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.

¹⁰While certain uncollateralized (or “implicit collateral”, see Klages-Mundt et al. (2020)) stablecoins

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 Diamond and Dybvig (1983). 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 Selgin (2020) 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.¹¹

Some qualitative results from the literature on speculative attacks on currencies can be applied directly to the P-AMM setting. In particular, Routledge and Zetlin-Jones (2021) 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 Routledge and Zetlin-Jones (2021) 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.

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.

¹¹Similarly, 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.

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 Routledge and Zetlin-Jones (2021). 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.

B Simplified, Discrete Redemption Curve

In this section, we provide the formal details for the simplified price decay function from Section 4.2 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.

We first describe the general design and the computation of dynamic parameters (similar to Section 5) and we then discuss the implementation of the mechanism (similar to Section 8).

B.1 Design and Dynamic Parameters

Recall that here, we use

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

where x_U is a dynamic parameter and r_U is chosen such that $r_U = r(x_U)$ 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.

Lemma 1. *Let $b_a < y_a$. Then the following hold:*

1. *We have*

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

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

3. *In this case, we have $r_U \geq \bar{\theta}$ iff $b_a/y_a \geq \bar{\theta}$ and $x_U \leq \frac{b_a - \bar{\theta} y_a}{\bar{\theta}}$, where $\theta = 1 - \bar{\theta}$.*

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 $r_U = r(x_U) = b(x_U)/y(x_U)$. By assumption, $r_U \in (0, 1)$ 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, $r_U \geq \bar{\theta}$ iff $x_U \leq \frac{b_a - \bar{\theta} y_a}{\bar{\theta}}$. This is only possible if $b_a/y_a \geq \bar{\theta}$ since otherwise, the right-hand side is negative. \square

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

$$\hat{x}_U := \max \left(0, y_a \frac{r_a - \bar{\theta}}{1 - \bar{\theta}} \right) \quad (3)$$

where we recall that $r_a := b_a/y_a$. Note that we choose $x_U = 0$ if $r_a < \bar{\theta}$, so that in this case, we redeem at the reserve ratio from the very beginning.

B.2 Implementation

To implement our mechanism (i.e., to define $\rho(x, b, y)$), we can perform a distinction into different regions like in sections 6 and 8, though the operation is much simpler here. We only consider two dimensions with two cases each.

- Case I, where $\hat{x}_U \geq \bar{x}_U$, and case II, where $\hat{x}_U \leq \bar{x}_U$.
- Case i, where $x \leq x_U$ and case iii, where $x \geq x_U$. There is no case ii.

For the implementation, we proceed analogously to Section 8. Reconstruction of b_a is greatly simplified in the discrete case because the range of possible values is much restricted and, importantly, all relevant equations are linear and do not involve either a square root or a square. First note that, as always, we can easily obtain $y_a = y + x$, so it only remains to reconstruct b_a . Also recall that we only need to do this when $1 > r = b/y > \bar{\theta}$ since we otherwise always redeem at 1 or r , respectively. It is easy to see that, like in Theorem 1, $b(x)$ (and equivalently $r(x)$) for a fixed x is strictly monotonic in b_a whenever $r > \bar{\theta}$ and thus, any such point has a unique b_a associated. Reconstruction of b_a can now be done using a “trial and error” approach as follows:

- (Case i) Let $b'_a = b + x$ and test if $x \leq x_U(b'_a, y_a)$. In this case, $b_a = b'_a$.
- (Case I iii) Otherwise, $b_a = b + \bar{x}_U + r \cdot (x - \bar{x}_U)$.¹²

Correctness of the above reconstruction follows from uniqueness of b_a and the fact that the respective conditions hold in the respective cases. Correctness in case I

¹²This value is unimportant to calculate redemption amounts, though, and would not have to be computed. This is because, since we’re in case iii, the redemption price will always be $r = b/y$ for all $x' \geq x$.

iii follows by solving the equation for $b(x)$ from Lemma 1 for b_a . Note that case II iii does not need to be checked because, by choice of x_U , we must have $r_U = \bar{\theta}$ in this case. To compute a redemption amount, in case i, we have to now compute the dynamic parameter x_U using Equation 3 and then integrate over the redemption curve, just like in the case with linear price decay. In case I iii, this is trivial and we can simply compute $X \cdot r$, where X is the amount of redeemed stablecoins. It is obvious that the mechanism can be implemented using a constant number of basic arithmetic operations.

C Detailed Calculation of 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 G.

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 $r(y_a) := \lim_{x \rightarrow y_a} r(x)$. This will be well-defined for all relevant cases below.

Prop. 2. *For fixed α, x_U, x_L with $x_U \leq x_L$ we have*

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

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 $\bar{\alpha} \in (0, \infty)$, $\bar{x}_U \in [0, \infty]$, and $\bar{\theta} \in [0, 1]$. $\bar{\theta}$ defines a floor on the reserve ratio, if achievable, and $\bar{\alpha}$ and \bar{x}_U are bounds on the respective parameter: we always have $\alpha \geq \bar{\alpha}$ and $x_U \leq \bar{x}_U$. 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

$$p^U(x) := \begin{cases} 1, & x \leq x_U \\ 1 - \alpha(x - x_U), & x \geq x_U. \end{cases} \quad (4)$$

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 3 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 $x \geq x_L$, i.e., we redeem at the reserve ratio beyond x_L , and this is sustainable.
- x_U and α are chosen such that $0 \leq x_U \leq \bar{x}_U$, $\alpha \geq \bar{\alpha}$, x_L exists, and $r_L \geq \bar{\theta}$, if possible. It is easy to see that this is possible iff $r_a > \bar{\theta}$ (one possible choice is $x_U = 0$ and $\alpha \rightarrow \infty$ as $r_a \searrow \bar{\theta}$). 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 $\alpha < \bar{\alpha}$, 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 3. Note that the mechanism only applies trade-off only applies within the limits set by the $\bar{\alpha}$ 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), $r_a > \bar{\theta}$ (otherwise the marginal price is constant at $r_a = r(x) \forall x$), and, where x_U occurs as a parameter, we assume $y_a \geq x_U$ (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. 3. *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*

$$\alpha \geq 2 \frac{y_a - b_a}{(y_a - x_U)^2}. \quad (5)$$

2. *If (5) 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 (5) holds, then x_L is unique and

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

[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 $x \geq x_L$, 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 $\bar{\theta}$. We call a pair (α, x_U) *admissible* if x_L exists and $r_L \geq \bar{\theta}$. 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 (5), the fact that r_L is monotonically decreasing in x_U (as can be seen from the formulas in Proposition 3), 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 $\bar{\alpha}$, 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 3 we can see that $\hat{\alpha}$ always exists (if $b_a/y_a > \bar{\theta}$) and is positive and for $\alpha \geq \hat{\alpha}$, $\hat{x}_U(\alpha)$ always exists.

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

1. First let $\alpha = \max(\hat{\alpha}, \bar{\alpha})$.
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 $\bar{\theta}$ bound on the reserve ratio is not binding.¹³ The lower bound $\bar{\alpha}$ is also optional and can be deactivated by setting $\bar{\alpha} = 0$. Note, however, that for $\bar{\alpha} = 0$, 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 3). The following lemma will help us in our construction. Let $\theta = 1 - \bar{\theta}$.

Lemma 2. *If (5) holds, then $r_L \geq \bar{\theta}$ iff*

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

$$\text{or } \alpha(b_a - \bar{\theta} y_a) - \alpha \theta x_U - \frac{1}{2} \theta^2 \geq 0. \tag{TL}$$

[Link to Proof]

¹³This will be captured formally as cases II h and III H below.

We can interpret the distinction between the conditions (TH) and (TL) in terms of whether or not the reserve ratio floor $\bar{\theta}$ is binding. Observe first that (TH) is equivalent to $1 - \alpha(y_a - x_U) \geq \bar{\theta}$, and this implies that $p(x) \geq \bar{\theta}$ for all x and independently of x_L , including for the case $x_L = y_a$, where the redemption curve p has no final constant segment. In this case we say that $\bar{\theta}$ 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 $\bar{\theta}$; we say that $\bar{\theta}$ 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 2, we can now construct the values $\hat{\alpha}$ and $\hat{x}_U(\alpha)$ for any α . We begin with $\hat{\alpha}$. Recall that $\theta = 1 - \bar{\theta}$.

Prop. 4. *We have*

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

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

[Link to Proof]

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

Prop. 5. *We have*

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

and $\hat{x}_U(\alpha)$ 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.

D A Formal Treatment of Path Deficiency under Minting and Fees

D.1 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 (1):

$$\begin{aligned} \frac{db(x)}{dx} &= -\rho(x, b(x), y(x)) + \gamma(x, b(x), y(x)) \\ \frac{dy(x)}{dx} &= -1. \end{aligned} \tag{6}$$

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

$$\begin{aligned} \frac{db(x)}{dx} &= -\varphi(x, b(x), y(x)) \\ \frac{dy(x)}{dx} &= -1. \end{aligned} \tag{7}$$

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.

D.2 Path Deficiency Properties

We next show two properties analogous to path deficiency in CFMMs (see Angeris and Chitra (2020)). 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 (1) that map x to a reserve ratio $r(x)$ parameterized by an anchor point $r_a = b_a/y_a$, where we assume \bar{x}_U , $\bar{\alpha}$, and $\bar{\theta}$ 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,

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

Notice that $r_{f,\tau}$ sweeps away the details of (6) and (7) but is easy to see is well-defined for a given $f \in \mathcal{C}$.

Paths in the set \mathcal{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 3. *Let $\tau \in \mathcal{R}$ such that $\tau \leq 1$ and $f \in \mathcal{C}$. Then $r_a(f(t), r_{f,\tau}(t))$ —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.¹⁴

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

[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.

¹⁴These results parallel those of path deficiency in CFMMs (see Angeris and Chitra (2020)). 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* $S(\tau) = \left\{ \psi \in \mathcal{R} \mid (f(t), r_{f,\tau}(t)) \in \psi \text{ for some } t \in [0, 1] \text{ and for some } f \in \mathcal{C} \right\}$ that weakly contract along a path. To illustrate, Lemma 3 would express that functions in this reachable set are point-wise lower bounded by τ , 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.

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

1. The redemption system described in (6) is path independent within a block.
2. An individual trader in the extended system described in Section D.1 has no incentive to subdivide a net redemption within a block.

[Link to Proof]

E Details on Efficient Implementation

In this section, we discuss how to implement our mechanism on-chain. To execute a redemption using our mechanism, we are given the current state $(x, b(x), y(x))$ and we need to find b_a and y_a such that $b(x; b_a, y_a) = b(x)$. We can then simply integrate the curve of marginal redemption rates, starting at x , to execute a redemption; note that integration can easily be done analytically using Proposition 2. Recall from Section 6 that finding y_a is trivial because $y(x) = y_a - x$, so $y_a = y(x) + x$. The main challenge is therefore to find the appropriate b_a . By strict monotonicity (Theorem 1), b_a is unique. The proofs for this section can be found in Appendix F.3. 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 G.

In this section, we assume that the parameters $\bar{\alpha}$ and \bar{x}_U scale in the anchored amount of outstanding stablecoins y_a (see also Section 4). More in detail, we assume that $\bar{x}_U = \bar{x}_{U,1} \cdot y_a$ and $\bar{\alpha} = \bar{\alpha}_1/y_a$, where $\bar{x}_{U,1}$ and $\bar{\alpha}_1$ are parameters that can be chosen arbitrarily and that correspond to the value of \bar{x}_U and $\bar{\alpha}$ for $y_a = 1$. Choosing the parameters like this is intuitive and economically meaningful because $\bar{x}_{U,1}$ is now the *share* of “initial” (anchored) outstanding stablecoins that can be redeemed at dollar value and $\bar{\alpha}_1$ is minimum decay in reserve ratio relative to the *share* of “initial” outstanding stablecoins that have been redeemed. Note that the minimum reserve ratio $\bar{\theta}$ remains an absolute number and is *not* relative to y_a . As these parameters $\bar{x}_{U,1}$ and $\bar{\alpha}_1$ are economically meaningful, we expect that they only need to be adjusted rarely, so that governance interventions are minimized.

If we were working under the mild computational constraints of a regular machine, our mechanism could be implemented in a straightforward way using bipartition. Using this method, we can find a $b_a \in [0, y_a]$ such that $b(x; b_a, y_a) = b(x) \pm \varepsilon$, where ε is a chosen precision. This would require $\log(y_a/\varepsilon)$ evaluations of $b(x; b_a, y_a)$ in the worst case. While this is computationally unproblematic for a regular machine, this method is far too computationally expensive to be implemented on-chain: each evaluation of $b(x; b_a, y_a)$ (for a changing value of b_a) requires the re-computation of the dynamic parameters x_U and α , and it requires computing up to two square roots (for x_L and potentially for x_U). Square roots can of course only be computed using an iterative process, which is also computationally relatively expensive. The whole computation then has to be repeated several times until the interval of possible b_a values is small enough.

Fortunately, we can implement our mechanism in a much more computationally efficient way that is amenable to implementation on-chain. Our method makes use of precomputed data that only depends on the normalized parameters. More in detail, we will show the following theorem. We can limit our view to states where the reserve ratio r lies in the interval $(\bar{\theta}, 1)$ as our mechanism otherwise simply yields a redemption rate of r or 1, respectively.

Theorem 7. *Given is a state (x, b, y) such that $1 > b/y > \bar{\theta}$. Let $y_a = y + x$. We can find the unique b_a such that $b = b(x; b_a, y_a)$ using a constant number of basic arithmetic operations and at most one square root, together with precomputed data that only depends on the parameters $\bar{x}_{U,1}$, $\bar{\alpha}_1$, and $\bar{\theta}$ and is independent of the state (x, b, y) . Our precomputation can be performed using a constant number of basic arithmetic operations and one square root, and it can be verified using a constant number of arithmetic operations and without taking any square root.*

Our method proceeds in three steps: in the precomputation step, we compute the curves of form $x \mapsto b(x; b_a, y_a = 1)$ that mark the threshold between the different cases defined in Section 6: the threshold between case I and II, case II and III, and the thresholds between cases h and l and H and L, respectively. Note that these computations in principle only need to do once as long as the parameters $\bar{x}_{U,1}$, $\bar{\alpha}_1$, $\bar{\theta}$ are kept the same.

In the second step and given a state (x, b, y) , we use this precomputed information to detect the region (such as II h i) into which this state falls. Since most of the work has already been done in the precomputation step, this step only requires a constant number of arithmetic operations and no square roots. Finally, once we know the region, we solve an equation of degree 1 or 2 to compute the value of b_a that leads to b . This third step may involve a square root, depending on the region.

E.1 Normalization

Recall that the precomputed information only applies to the $y_a = 1$ case. To use it in the region detection step, we normalize all values to $y_a = 1$. We then run all further computations on this normalized version and scale the resulting b_a back to the original value of y_a . Formally, we exploit the following scaling property. Throughout this section, we denote the dynamic parameters as functions of the values on which they depend. For example, we write $\alpha(b_a, y_a)$ for the value that the dynamic parameter α would take according to Proposition 4 at a certain (b_a, y_a) combination.

Lemma 4. *Assume that \bar{x}_U and $\bar{\alpha}$ are chosen relative to y_a as described above. Let $\zeta > 0$. Then*

$$b(\zeta x; \zeta b_a, \zeta y_a) = \zeta b(x; b_a, y_a).$$

[Link to Proof]

The lemma immediately implies that it is enough to be able to determine b_a in the *normalized* case where $y_a = 1$.

Theorem 8. Assume that \bar{x}_U and $\bar{\alpha}$ are chosen relative to y_a as described above. For some given x , b , and y_a , let $b_{a,1}$ be such that $b(x/y_a; b_{a,1}, 1) = b/y_a$. Let $b_a = b_{a,1}y_a$. Then $b(x; b_a, y_a) = b$.

Proof. This follows immediately from Lemma 4 for $\zeta = 1/y_a$. \square

By Theorem 8, it is enough to consider the case $y_a = 1$. Otherwise, given some state (x, b, y) we can consider the scaled state $(x/y_a, b/y_a, y/y_a)$ (where $y_a := y + x$), consider the resulting b_a , and return $y_a \cdot b_a$. Despite our normalization, in the following, we will usually use an explicit variable for y_a in the interest of clarity of the exposition.

E.2 Precomputation Step

We now discuss our precomputation step. We use the following lemma to distinguish between cases I, II, and III.

Lemma 5. Let $z \leq y_a$. Let $y_z := y_a - z$. Then $\hat{x}_U = z$ iff

$$b_a = \begin{cases} y_a - \frac{\alpha}{2} \cdot y_z^2 & \text{if } 1 - \alpha y_z \geq \bar{\theta} \\ y_a - \theta y_z + \theta^2 \cdot \frac{1}{2\alpha} & \text{otherwise.} \end{cases}$$

[Link to Proof]

Algorithm 1 Precomputation step

Input: $\bar{\alpha}, \bar{x}_U, \bar{\theta}$

Output: $P := (b_a^{I/II}, x_L^{I/II}, b_a^{II/III}, x_L^{II/III}, b_a^{h/l}, x_U^{h/l}, b_a^{H/L})$

- 1: Calculate $b_a^{I/II}$ via Lemma 5 such that $\hat{x}_U = \bar{x}_U$ for $y_a = 1$ and $\alpha = \bar{\alpha}$.
- 2: Calculate $x_L^{I/II}$ via Proposition 3 for $b_a^{I/II}$, $y_a = 1$, $\alpha = \bar{\alpha}$, and $x_U = \bar{x}_U$.
- 3: Calculate $b_a^{II/III}$ via Lemma 5 such that $\hat{x}_U = 0$ for $y_a = 1$ and $\alpha = \bar{\alpha}$.
- 4: Calculate $x_L^{II/III}$ via Proposition 3 for $b_a^{II/III}$, $y_a = 1$, $\alpha = \bar{\alpha}$, and $x_U = 0$.
- 5: Let $b_a^{h/l} := y_a - \theta^2 \cdot \frac{1}{2\bar{\alpha}}$.
- 6: Calculate $x_U^{h/l}$ via Proposition 5 for $b_a^{h/l}$, $y_a = 1$, and $\alpha = \bar{\alpha}$.
- 7: Let $b_a^{H/L} := y_a \cdot \frac{1+\bar{\theta}}{2}$

Our precomputation step is depicted in Algorithm 1. It exploits Lemma 5 as well as other relationships to calculate all relevant thresholds between cases I / II / III as well as those between cases h / l and H / L. Each of these thresholds is determined by a specific b_a value. We also compute the dynamic parameters for each of these b_a values as far as it is necessary, so that any point along the respective threshold curve for $b(x)$ can be quickly evaluated. The following lemma tells us that these threshold values can be used to determine in which of the different regions we are. As discussed above, we only need to consider the normalized case $y_a = 1$.

Recall from Section 6 that not all regions need to exist. Specifically, it may be the case that only one of region II h or II l exists and it may be the case that only

one of region III H or III L exist.¹⁵ The following lemma also describes how to check for existence of these sub-regions based on the precomputed values. Note that, while the thresholds $b_a^{h/l}$ and $b_a^{H/L}$ can always be computed, they are meaningless if the respected sub-region does not exist.

Lemma 6. *Fix $y_a = 1$ and let $b_a \in [0, y_a]$ be arbitrary. Let $x \in [0, y_a]$ and assume that $1 > b(x; b_a)/y(x) > \bar{\theta}$. Consider the precomputed values chosen like in Algorithm 1. Then the following hold:*

1. (a) We are in case I iff $b_a \geq b_a^{I/II}$. (b) For $b_a^{I/II}$ we have $\alpha = \bar{\alpha}$, $x_U = \bar{x}_U$, and $x_L = x_L^{I/II}$. (c) We are in case I iff $b(x; b_a) \geq b(x; b_a^{I/II})$.
2. (a) We are in case III iff $b_a \leq b_a^{II/III}$. (b) For $b_a = b_a^{II/III}$ we have $\alpha = \bar{\alpha}$, $x_U = 0$, and $x_L = x_L^{II/III}$. (c) We are in case III iff $b(x; b_a) \leq b(x; b_a^{II/III})$.
3. Assume that we are in case II. (a) We are in case h iff $b_a \geq b_a^{h/l}$. (b) If $b_a^{h/l} \in [b_a^{II/III}, b_a^{I/II}]$, then for $b_a = b_a^{h/l}$ we have $\alpha = \bar{\alpha}$, $x_U = x_U^{h/l}$, and $x_L = 1$. (c) We are in case h iff $b_a^{h/l} \leq b_a^{II/III} \vee (b_a^{h/l} \leq b_a^{I/II} \wedge b(x; b_a) \geq b(x; b_a^{h/l}))$.
4. Assume that we are in case III. (a) We have $b_a \geq b_a^{H/L}$ iff we are in case H. (b) If $b_a^{H/L} \leq b_a^{II/III}$, then for $b_a = b_a^{H/L}$ we have $\alpha = \theta = 1 - \bar{\theta}$, $x_U = 0$, and $x_L = 1$. (c) We are in case H iff $b_a^{H/L} \leq b_a^{II/III} \wedge b(x; b_a) \geq b(x; b_a^{H/L})$.

In part 3. (c) and 4. (c), the inequalities for $b_a^{h/l}$ and $b_a^{H/L}$ ensure that both regions exist (otherwise the question regarding the sub-region is trivial) and the inequality for $b(x; b_a)$ checks where the current state is compared to the respective state that would be attained based on the threshold anchor value.

[\[Link to Proof\]](#)

Regarding the runtime properties of the precomputation step, we receive:

Prop. 6. *Algorithm 1 only requires a constant number of basic arithmetic operations and the computation of at most one square root. Furthermore, correctness of the values computed by algorithm 1 can be verified using a constant number of basic arithmetic operations and no square root.*

[\[Link to Proof\]](#)

¹⁵For each of region II or III, at least one of the two sub-cases need to exist, though, so that region II and region III always exist. To see this, consider the continuous evolution of α and x_U as functions of b_a . When not both region II h and II l exist, $x_U^{h/l}$ may be negative. In these situations, $x_U^{h/l}$ won't be used (see below), but some implementations may want to avoid computation of $x_U^{h/l}$ altogether in this case.

Algorithm 2 Region detection. We use “emit” as a shorthand to denote that the algorithm outputs that we are in a particular case without stopping execution of the function.

Input: $\bar{\alpha}, \bar{x}_U, \bar{\theta}, (x, b, y)$ such that $\bar{\theta} < b/y < 1$ and $y_a := y + x = 1$; P precomputed using Algorithm 1

Output: The region in which (x, b) lies.

```

1: if  $b \geq b(x; b_a^{I/II}, y_a = 1, \alpha = \bar{\alpha}, x_U = \bar{x}_U, x_L = x_L^{I/II})$  then
2:   Emit case I
3:   if  $x \leq \bar{x}_U$  then
4:     Emit case i
5:   else if  $b/y \leq 1 - \bar{\alpha}(x - \bar{x}_U)$  then
6:     Emit case ii
7:   else
8:     Emit case iii
9:   end if
10:  else if  $b \geq b(x; b_a^{II/III}, y_a = 1, \alpha = \bar{\alpha}, x_U = 0, x_L = x_L^{II/III})$  then
11:    Emit case II
12:    if  $b_a^{h/l} \leq b_a^{II/III} \vee (b_a^{h/l} \leq b_a^{I/II} \wedge b \geq b(x; b_a^{h/l}, y_a = 1, \alpha = \bar{\alpha}, x_U = x_U^{h/l}, x_L = 1))$ 
13:      then
14:        Emit case h
15:        if  $y - b \leq \frac{\bar{\alpha}}{2} \cdot y^2$  then
16:          Emit case i
17:        else
18:          Emit case ii
19:        end if
20:      else
21:        Emit case l
22:        if  $b - \bar{\theta}y \geq \frac{\theta^2}{2\bar{\alpha}}$  then
23:          Emit case i
24:        else
25:          Emit case ii
26:        end if
27:      end if
28:    else
29:      if  $b_a^{H/L} \leq b_a^{II/III} \wedge b \geq b(x; b_a^{H/L}, y_a = 1, \alpha = \theta, x_U = 0, x_L = 1)$  then
30:        Emit case H
31:      else
32:        Emit case L
33:      end if
34:    end if
```

E.3 Region Detection

Lemma 6 provides a way to use the precomputed values to detect in which region we are along the I-III and h/l and H/L dimension. This can be done based on only the current state (x, b, y) and without any knowledge of b_a . For example, to tell case I and II apart, by part (1c) of the lemma, we only need to compare the value $b(x)$ (which we know) to the value $b(x; b_a^{I/II})$. This latter value can be easily computed because we also know the values of x_U , α , and x_L corresponding to $b_a^{I/II}$ by part (1b) of the lemma. The same reasoning applies to the other items. Algorithm 2 formalizes this idea and adds an additional method that allows us to also tell case i–iii apart. In effect, Algorithm 2 allows us to fully reconstruct the region of a given point (x, b, y) without knowledge of b_a and only with a constant number of basic arithmetic operations (and in particular without computing a square root).

Theorem 9. *Algorithm 2 is correct and only requires basic arithmetic operations, and only a constant number of them.*

[[Link to Proof](#)]

E.4 Reconstructing the value of b_a

Given sufficient knowledge about the region, it is now conceptually straightforward (though mathematically somewhat inconvenient) to reconstruct the precise value of b_a by solving a linear or quadratic equation. This is captured in Algorithm 3.

Theorem 10. *Algorithm 3 is correct and only requires a constant number of basic arithmetic operations together with at most one square root.*

[[Link to Proof](#)]

E.5 Full Implementation

Algorithm 4 shows the full implementation of our redemption mechanism and illustrates how our reconstruction algorithm is applied. We receive the following consistency result, which states that going to some state and then performing redemption over some amount using Algorithm 4 is the same as going to the state corresponding to the overall redemption amount directly. This is because Algorithm 4 correctly reconstructs the original anchor point (b_a, y_a) and then simply continues on the corresponding curve of marginal redemption prices. This is another form of path independence (see also Section 7). The proof is immediate by the preceding theorems and is omitted.

Corollary 3. *Fix values for $\bar{\alpha}_1$, $\bar{x}_{U,1}$, $\bar{\theta}$. Let b_a, y_a be such that $1 > b_a/y_a > \bar{\theta}$. Let $x \in [0, y_a]$ and let $X \in [0, y_a - x]$. Let (x', b', y') be the new state as of Algorithm 4 when applied to the parameters, the state $(x, b(x; b_a, y_a), y(x; b_a, y_a))$, and the collection of precomputed values as of Algorithm 1 for the parameters. Then $x' = x + X$, $b' = b(x + X; b_a, y_a)$, and $y' = y(x + X; b_a, y_a)$.*

Algorithm 3 Reconstruction of b_a

Input: $\bar{\alpha}, \bar{x}_U, \bar{\theta}, (x, b, y)$ such that $\bar{\theta} < b/y < 1$ and $y_a := y + x = 1$; the region of (x, b)

Output: b_a such that $b(x, b_a, y_a = 1) = b$

- 1: Let $r = b/y$.
- 2: **if** case i applies **then**
- 3: $b_a = b + x$
- 4: **else if** case I applies **then**
- 5: **if** case ii applies **then**
- 6: $b_a = b + x - \frac{\bar{\alpha}}{2}(x - \bar{x}_U)^2$
- 7: **else** ▷ Now case iii applies.
- 8: $b_a = y_a - (y_a - \bar{x}_U)(1 - r) + \frac{1}{2\bar{\alpha}}(1 - r)^2$
- 9: **end if**
- 10: **else if** case II applies **then** ▷ Now case ii applies.
- 11: **if** case h applies **then**
- 12: Let $\Delta_a := \frac{\bar{\alpha}}{2} \cdot \left(\frac{1}{\alpha} \cdot (1 - r) + \frac{1}{2} \cdot y\right)^2$
- 13: $b_a = y_a - \Delta_a$
- 14: **else** ▷ Now case l applies
- 15: Let $p' := \theta \cdot \left(\frac{\theta}{2\bar{\alpha}} + y\right)$
- 16: Let $d := \theta^2 \cdot \frac{2}{\alpha} \cdot (b - \bar{\theta}y)$
- 17: Let $\Delta_a := p' - \sqrt{d}$
- 18: $b_a = y_a - \Delta_a$
- 19: **end if**
- 20: **else** ▷ Now case III ii applies.
- 21: **if** case H applies **then**
- 22: Let $\Delta_a := \frac{y-b}{1-\frac{x^2}{y_a^2}}$.
- 23: $b_a = y_a - \Delta_a$
- 24: **else** ▷ Now case L applies.
- 25: Let $p' := \frac{1}{2}(y - b + \theta y_a)$
- 26: Let $q := (y - b)\theta y_a + \frac{1}{4}\theta^2 x^2$
- 27: Let $\Delta_a := p' - \sqrt{p'^2 - q}$
- 28: $b_a = y_a - \Delta_a$
- 29: **end if**
- 30: **end if**

Algorithm 4 Full implementation of the redemption mechanism

Input: $\bar{\alpha}_1, \bar{x}_{U,1}, \bar{\theta}$, the current state (x, b, y) , and a desired amount of redemptions $X \leq y$; the collection of precomputed values P calculated by Algorithm 1 for the given parameters.

Output: A new state (x', b', y') after the amount of X has been redeemed. The difference $b' - b$ is paid out as the redemption amount.

- 1: $x' := x + X; y' := y - X$
 - 2: **if** $X = 0$ **then**
 - 3: $b' := b$
 - 4: **else if** $b/y \geq 1$ **then**
 - 5: $b' := b - X$
 - 6: **else if** $b/y \leq \bar{\theta}$ **then**
 - 7: $b' := b - b/y \cdot X$
 - 8: **else**
 - 9: Let $y_a := y + x$. Let $x_N := x/y_a, b_N := b/y_a, y_N := y/y_a$.
 - 10: Apply Algorithm 2 to (x_N, b_N, y_N) and P to determine the region of this point.
 - 11: Apply Algorithm 3 to (x_N, b_N, y_N) and the region information computed in the previous step to determine $b_{a,N}$ such that $b(x_N; b_{a,N}, y_a = 1) = b_N$.
 - 12: Let $b_a := b_{a,N} \cdot y_a$.
 - 13: $b' := b(x + X; b_a, y_a)$
 - 14: **end if**
-

F Proofs

F.1 Technical Lemmas

Prop. 2.

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

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

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

$$b(x) = b(x_L) - \int_0^{x-x_L} r_L dx' = r_L(y_a - x_L) - r_L(x - x_L) = r_L(y_a - x). \quad \square$$

Prop. 3.

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

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

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 the “-” solution. Obviously, this exists iff (5) holds. Assuming that (5) does hold, we obviously have $x \leq y_a$ and furthermore

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

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

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

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 (5) does not hold and where we choose $x_L := \infty$ to define p . Then by applying Prop. 2 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 (5) does not hold. By continuity of b , there exists $x < y_a$ such that $b(x) = 0$. \square

Lemma 2.

Proof. By Proposition 3 we have that $r_L \geq \bar{\theta}$ iff

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

The conclusion now follows via another simple algebraic transformation. \square

Prop. 4.

Proof. It is easy to see that the transition is continuous and thus well-defined; more in detail, in the edge case $r_a = \frac{1+\bar{\theta}}{2}$, 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 (5) holds and one of (TL) or (TH) hold (with $x_U = 0$). Note that (5) alone puts a bound on α and the right-hand side of (5) 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

$$\begin{aligned} & 2 \frac{1 - r_a}{y_a} \cdot y_a \leq \theta \\ \Leftrightarrow & r_a \geq \frac{1 + \bar{\theta}}{2}. \end{aligned}$$

The equivalence immediately follows from the definition of $\theta = 1 - \bar{\theta}$. If this inequality does not hold, then there is no α that satisfies both (5) and (TH). (observe that the two limit α in different directions!)

Assume next that $r_a \leq \frac{1+\bar{\theta}}{2}$. Then α must be chosen minimal such as to satisfy (5) and (TL). The minimal α satisfying (TL) with $x_U = 0$ is obviously $\hat{\alpha}_L$. It remains to show that this also satisfies (5), i.e., that

$$\begin{aligned} & \frac{1}{2} \frac{\theta^2}{b_a - \bar{\theta} y_a} \geq 2 \frac{y_a - b_a}{y_a^2} \\ \Leftrightarrow & \frac{1}{2} \frac{\theta^2}{r_a - \bar{\theta}} \geq 2(1 - r_a) \\ \Leftrightarrow & \frac{1}{4} \theta^2 \geq (1 - r_a)(r_a - \bar{\theta}). \end{aligned}$$

The equivalences are by definition of $r_a = b_a/y_a$ and straightforward transformation.

Let $\zeta = \frac{1+\bar{\theta}}{2} - r_a$. By assumption, $\zeta \geq 0$ and we have $1 - r_a = \theta/2 + \zeta$ and $r_a - \bar{\theta} = \theta/2 - \zeta$. Thus, the above inequality is equivalent to

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

which is obviously true. \square

Prop. 5.

Proof. We proceed similarly to Proposition 4. 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 (5) and one of (TH) or (TL), this time without assuming $x_U = 0$ of course. (5) is equivalent to

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

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

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

If this does not hold, no x_U satisfies both (5) and (TH).

Assume now that $\alpha\Delta_a \geq \frac{1}{2}\theta^2$. We need to satisfy ((5) and) (TL). Clearly, (TL) holds iff

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

It remains to check that $x_U = \hat{x}_{U,1}$ satisfies (5). 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 $2\frac{\Delta_a}{\alpha} = 2 \cdot 2 \cdot \frac{\Delta_a}{\theta} \cdot \frac{1}{2\alpha}\theta$. \square

Corollary 2.

Proof. Note that, by construction, we always have $r(x; b_a), r(x; b'_a) \in [\bar{\theta}, 1)$. We now distinguish three cases:

- If $r(x; b_a), r(x; b'_a) > \bar{\theta}$, then $b(x; b_a) < b(x; b'_a)$ by Theorem 1.
- If $r(x; b_a) = \bar{\theta} < r(x; b'_a)$ then also $b(x; b_a) = r(x; b_a) \cdot (y_a - x) < r(x; b'_a) \cdot (y_a - x) = b(x; b'_a)$.
- If $r(x; b_a) > \bar{\theta} = r(x; b'_a)$, then this leads to a contraction. Specifically, Theorem 1 implies that

$$\forall b''_a \in [b_a, b'_a] : r(x; b''_a) > \bar{\theta} \Rightarrow r(x; b''_a) \geq r(x; b_a).$$

Now, considering continuity of $r(x; \cdot)$, since the conclusion of the above implication is topologically closed, the implication also holds when we replace the premise with its topological closure, which is simply the statement $b''_a \in [b_a, b'_a]$. In particular, $r(x; b'_a) \geq r(x; b_a)$. \square

F.2 Main Results

Proposition 1.

Proof. In case II h, we have $x_U = \hat{x}_U = \hat{x}_{U,h}$ and thus (by the proof of Proposition 5) Inequality (5) holds with equality. It follows immediately from Proposition 3 that this implies $x_L = y_a$. Likewise in case III H. In case II l, $x_U = \hat{x}_U = \hat{x}_{U,l}$ and thus (by the proof of Proposition 5) (TL) holds with equality. By the proof of Lemma 2, this immediately implies $r_L = \bar{\theta}$. Likewise for case III L. \square

Corollary 1.

Proof. By Proposition 1, since we're in case II or III we have $x_L = y_a$ or $r_L = \bar{\theta}$. Since we're in case iii, $x_L \leq x < y_a$ and thus $x_L = y_a$ is not possible. We must therefore have $r_L = \bar{\theta}$. And, again since $x \geq x_L$, $r(x) = r_L$. \square

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 $r(x; b_a) > \bar{\theta}$, then we have

$$\frac{db(x; b_a)}{db_a} > 0.$$

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

Case i: This case is trivial because here, $b(x; b_a) = b_a - x$ and so $\frac{db(x; b_a)}{db_a} = 1 > 0$.

Case I ii and I iii: Here the statement follows immediately from Prop. 2 and Prop. 3 Part 3. Note that whenever we are in case I, the parameters $\alpha = \bar{\alpha}$ and $x_U = \bar{x}_U$ are constant.

Case II iii and III iii: By Corollary 1, we do not need to discuss these cases.

It remains to show that the statement holds for case II ii and III ii, which requires some calculation. We distinguish four cases: II h ii, II l ii, III H ii, and III L ii. We combine Prop. 2 with Propositions 5 and 4, respectively, to compute the partial derivatives.

Case II h ii: Here we have $x_U = \hat{x}_{U,h}$ and

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

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.

Case II l ii: Here we have $x_U = \hat{x}_{U,l}$ and

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

Thus,

$$\begin{aligned}
\frac{db(x; b_a)}{db_a} &= 1 - \bar{\alpha}(x - \hat{x}_{U,h}(b_a)) \frac{1}{\theta} > 0 \\
\Leftrightarrow p(x; b_a) &= 1 - \bar{\alpha}(x - \hat{x}_{U,h}(b_a)) > \bar{\theta}
\end{aligned}$$

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

Case III H ii: In this case we have $x_U = 0$ and $\alpha = \hat{\alpha}_H(b_a)$ and we have

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

since $x < y_a$.

Case III L ii: Here we have

$$\frac{d}{db_a} \hat{\alpha}_L(b_a) = \frac{1}{2} \cdot \theta^2 \cdot (-1) \cdot \frac{1}{(b_a - \bar{\theta} y_a)^2} = -\frac{1}{2} \frac{\theta^2}{(b_a - \bar{\theta} y_a)^2} = -\hat{\alpha}_L(b_a) \frac{1}{b_a - \bar{\theta} y_a},$$

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)

$$\begin{aligned}\frac{db(x; b_a)}{db_a} &= 1 + \frac{1}{2}x^2 \cdot \left(-\alpha \frac{1}{b_a - \bar{\theta}y_a}\right) \\ &= 1 - \alpha \cdot \frac{1}{2}x^2 \frac{1}{b_a - \bar{\theta}y_a}.\end{aligned}$$

To see that this is positive, first note that, by Proposition 1 and Proposition 3, $\bar{\theta} = r_L = 1 - \alpha x_L$ and thus $x_L = \theta/\alpha$. Since we're in case ii and we have $r(x) > \bar{\theta} = r_L$, we must have $x < x_L = \theta/\alpha$ and thus

$$\begin{aligned}1 - \alpha \cdot \frac{1}{2}x^2 \frac{1}{b_a - \bar{\theta}y_a} &> 1 - \alpha \cdot \frac{1}{2} \frac{\theta^2}{\alpha^2} \frac{1}{b_a - \bar{\theta}y_a} \\ &= 1 - \frac{1}{\alpha} \cdot \frac{1}{2} \frac{\theta^2}{b_a - \bar{\theta}y_a} = 1 - \frac{1}{\alpha} \cdot \alpha = 0\end{aligned}$$

as required. This concludes the proof. \square

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 $P_X + P_{X,Y} = (b_0 - b_X) + (b_X - b_{X,Y}) = b_0 - b_{X,Y} = b_0 - b_{X+Y} = P_{X+Y}$. \square

Lemma 3.

Proof. Separate into two cases: (i) when $\frac{df}{dt} \geq 0$, and (ii) when $\frac{df}{dt} < 0$. These correspond to the x value increasing or decreasing respectively along the path f . Suppose we are at the current state $(f(t), r_{f,r}(t))$ and that this point is on the reserve ratio curve $\hat{r} \in \mathcal{R}$. In (i), x is increasing (redemption operation), and so (6) applies. Taking derivative of $r(x)$,

$$\begin{aligned}\frac{dr}{dx} &= \frac{\frac{db}{dx}y(x) + b(x)}{y^2(x)} \\ &= \frac{r(x) - \rho(x, b(x), y(x)) + \gamma(x, b(x), y(x))}{y(x)}.\end{aligned}$$

The derivative is greater (in this case less negative) when $\gamma > 0$. When $\gamma = 0$, we have the system (1), and the reserve ratio follows $\hat{t}(x)$.

In (ii), x is decreasing (minting operation), and so (7) applies. Taking derivative of $r(x)$,

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

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

In both cases, the path does not bring us to a region below \hat{t} 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. \square

Theorem 3 (formal).

Proof. From Lemma 3, 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. \square

Theorem 4 (formal).

Proof. This setup is equivalent to changing the RHS of (1) 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,
- $\bar{\alpha} \mapsto (1 - \varepsilon)\bar{\alpha}$,
- $\bar{\theta} \mapsto (1 - \varepsilon)\bar{\theta}$.

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 (6).

To show the second result of the theorem, we need to add in the minting process as described in Section D.1. 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. \square

F.3 Proofs regarding Implementation (Appendix E)

Lemma 4.

Proof. The lemma follows from the fact that all dynamic parameters and the input and output of the function p scale in ζ . More in detail, the statement follows from the following observations.

- We have $\alpha(\zeta b_a, \zeta y_a) = 1/\zeta \cdot \alpha(b_a, y_a)$. To see this, note that $r_a(\zeta b_a, \zeta y_a) = r_a(b_a, y_a)$ and consider Proposition 4 to see that $\hat{\alpha}(\zeta b_a, \zeta y_a) = 1/\zeta \cdot \hat{\alpha}(b_a, y_a)$. Note further that $\bar{\alpha}(\zeta y_a) = \bar{\alpha}_1 \cdot 1/(\zeta y_a) = 1/\zeta \cdot \bar{\alpha}(y_a)$ by choice of $\bar{\alpha}$.
- Similarly, we have $x_U(\zeta b_a, \zeta y_a) = \zeta x_U(b_a, y_a)$. To see this, note that $\Delta_a(\zeta b_a, \zeta y_a) = \zeta \Delta_a(b_a, y_a)$ and apply the preceding statement on α to Proposition 5 to receive that $\hat{x}_U(\zeta b_a, \zeta y_a) = \zeta \hat{x}_U(b_a, y_a)$. Also note that $\bar{x}_U(\zeta y_a) = \bar{x}_{U,1} \zeta y_a = \zeta \bar{x}_U(y_a)$ by choice of \bar{x}_U .
- It is now easy to see that $x_L(\zeta b_a, \zeta y_a) = \zeta x_L(b_a, y_a)$ and $r_L(\zeta b_a, \zeta y_a) = r_L(b_a, y_a)$ using Proposition 3 and then one can directly verify the statement of the lemma using Proposition 2. \square

Lemma 5.

Proof. We distinguish cases h and l. It is easy to see that

$$\begin{aligned}\hat{x}_{U,h} = z &\Leftrightarrow b_a = y_a - \frac{\alpha}{2} y_z^2 \\ \hat{x}_{U,l} = z &\Leftrightarrow b_a = y_a - \theta y_z + \theta^2 \cdot \frac{1}{2\alpha}.\end{aligned}$$

By plugging the above formulas for b_a into the condition $\alpha \Delta_a \leq \frac{1}{2} \theta^2$ (which defines cases h and l), we receive by simple algebraic transformations:

$$\begin{aligned}\text{Case h applies } \wedge \hat{x}_{U,h} = z &\Rightarrow 1 - \alpha y_z \geq \bar{\theta} \\ \text{Case l applies } \wedge \hat{x}_{U,l} = z &\Rightarrow 1 - \alpha y_z \leq \bar{\theta}.\end{aligned}$$

This implies the statement because exactly one of the cases on the right-hand side (or both in case of equality) must be satisfied. \square

Lemma 6.

Proof. 1. First note that $b_a^{I/II}$ always exists and is $> \bar{\theta}$ because for $b_a \rightarrow 1$, we will eventually arrive in case I and for $b_a \rightarrow \bar{\theta}$ from above we will eventually arrive at case III. By construction, both case I and II hold at $b_a^{I/II}$. Statement (a) now follows by monotonicity of α and x_U in b_a . Statement (b) follows by construction noting that case I applies at $b_a^{I/II}$. Statement (c) follows from statement (a) by strict monotonicity of $b(x; \cdot)$ (Corollary 2). Note here that we can exclude the case $r(x; b_a) = r(x; b_a^{I/II}) = \bar{\theta}$ by assumption.

2. This is analogous to part 1.

3. Towards statement (a), note that the equation for $b_a^{h/l}$ results from Proposition 5 as the solution to the edge case of the case distinction, and then consider monotonicity of the condition of the case distinction in b_a . Statement (b) follows because, by part 2., case II applies to $b_a^{h/l}$ and we have $x_L = 1$ by Proposition 1 because case II h applies. Towards statement (c), this follows from part (a), now also taking care of the fact that not both sub-regions need to exist. We distinguish three cases:

- If $b_a^{h/l} \leq b_a^{II/III}$, we are always in sub-region h.
- If $b_a^{h/l} > b_a^{I/II}$, we are never in sub-region h.
- Otherwise, we have $b_a^{h/l} \in [b_a^{II/III}, b_a^{I/II}]$ and the statement follows like part 1 (c). Since part (b) applies, we can use the parameters from there to compute $b(x; b_a^{h/l})$.

4. This is analogous to part 3, except for the value of α . To see that $\alpha = \theta$, note that $r_a = \frac{1+\bar{\theta}}{2}$ if $b_a = b_a^{H/L}$ by construction. Since we are both in sub-regions H and L, we have

$$\hat{\alpha} = \hat{\alpha}_H = 2 \frac{1 - r_a}{y_a} = 2 \frac{\frac{1-\bar{\theta}}{2}}{y_a} = \frac{\theta}{y_a} = \theta,$$

and since we are in case III, $\hat{\alpha} \leq \bar{\alpha}$ so that $\alpha = \hat{\alpha}$. \square

Prop. 6.

Proof. The statement regarding operations is obvious. The algorithm requires the computation of one square root, in line 2. Note that no square root is required for the computation of $x_U^{h/l}$ because the calculation of \hat{x}_U for case l can be applied by choice of $b_a^{h/l}$. Candidate values for these numbers can be easily verified without taking a square root. To verify the only non-trivial value $x_L^{I/II}$, it is sufficient to check whether $p(x; b_a^{I/II}, y_a = 1, \alpha = \bar{\alpha}, x_U = \bar{x}_U) = r(x; b_a^{I/II}, y_a = 1, \alpha = \bar{\alpha}, x_U = \bar{x}_U)$, which does not require a square root. \square

Theorem 9.

Proof. The statement regarding operations is obvious. Note in particular that output values of the function b are only ever calculated while providing fixed values for the dynamic parameters α , x_U , x_L . Correctness of detection of cases I–III and h/l and H/L immediately follows from Lemma 6.

It remains to show that cases i–iii are detected correctly. We go through the different cases one-by-one.

First assume that (x, b, y) lies in case I. Obviously we're in case i iff $x \leq x_U = \bar{x}_U$. Assume now that we are in case I but not in case I i. By choice of x_L and definition of the regions ii and iii, we are in region ii iff $r \leq p^U(x)$, where $p^U(x)$ is defined in (4). The expression $p^U(x)$ implicitly depends b_a via the choice of α and x_U . However, since we are in region I, we know that $\alpha = \bar{\alpha}$ and $x_U = \bar{x}_U$. Furthermore, $x \geq x_U$ and thus $p^U(x) = 1 - \bar{\alpha}(x - \bar{x}_U)$. Therefore, line 5 appropriately checks the condition $r \leq p^U(x)$.

Assume now that (x, b, y) does not lie in case I. Case iii is impossible in case II or III by Corollary 1. Case i is further trivial in case III because $x_U = 0$ in this case. Thus, these cases do not have to be checked. It remains to correctly distinguish case i and ii given that we are in case II.

Now assume that (x, b, y) lies in case II h. It lies in case i iff $x \leq x_U = \hat{x}_{U,h} = y_a - \sqrt{2\frac{\Delta_a}{\bar{\alpha}}}$, where the last equality follows from Proposition 5 and the fact that we are in case II h. It is easy to see that this is equivalent to

$$\Delta_a \leq \frac{\bar{\alpha}}{2}y^2. \quad (8)$$

Line 14 checks this condition, but with $\Delta_a = y_a - b_a$ replaced by $\Delta := y - b$. We show that the two conditions are equivalent, given that we are in case II h. First, note that

$$\Delta_a - \Delta = b - (b_a - x) = \begin{cases} 0 & \text{in case i} \\ \frac{\bar{\alpha}}{2}(x - x_U)^2 & \text{in case ii.} \end{cases}$$

In any case, $\Delta_a - \Delta \geq 0$ and thus $\Delta \leq \Delta_a$. Therefore, (8) implies line 14.

For the other direction, assume that (8) does not hold, so that $\Delta_a > \frac{\bar{\alpha}}{2}y^2$ and we are in case ii. We have, via the above, that

$$\begin{aligned} \Delta &= \Delta_a - \frac{\bar{\alpha}}{2}(x - x_U)^2 = \Delta_a - \frac{\bar{\alpha}}{2} \left(\sqrt{\frac{2}{\bar{\alpha}}\Delta_a} - y \right)^2 \\ &= \Delta_a - \left(\Delta_a - \bar{\alpha}\sqrt{\frac{2}{\bar{\alpha}}\Delta_a}y + \frac{\bar{\alpha}}{2}y^2 \right) = \bar{\alpha}\sqrt{\frac{2}{\bar{\alpha}}\Delta_a}y - \frac{\bar{\alpha}}{2}y^2 \\ &> \bar{\alpha}y^2 - \frac{\bar{\alpha}}{2}y^2 = \frac{\bar{\alpha}}{2}y^2, \end{aligned}$$

where the last line follows by assumption.

Assume finally that (x, b, y) lies in case II l. It lies in case i iff $x \leq x_U = \hat{x}_{U,l} = y_a - \frac{\Delta_a}{\theta} - \frac{\theta}{2\alpha}$, where the last equality again follows from Proposition 5 and the fact

that we are in case II 1. This is equivalent to

$$\Gamma_a := b_a - x - \bar{\theta}y \geq \frac{\theta^2}{2\alpha}. \quad (9)$$

This follows by simple transformation, noting that $\theta y - \Delta_a = \Gamma_a$. Line 21 checks this condition, but with Γ_a replaced by $\Gamma := b - \bar{\theta}y$. Again, we show that the two conditions are equivalent, given that we are in case II 1. For the first direction of the equivalence, note that $\Gamma_a - \Gamma = \Delta - \Delta_a \leq 0$ and thus $\Gamma_a \leq \Gamma$ and (9) implies line 21.

For the other direction, assume that (9) does not hold, so that $\Gamma_a < \frac{\theta^2}{2\alpha}$ and we are in case ii. Observe that

$$\begin{aligned} x - x_U &= x - y_a + \frac{\Delta_a}{\theta} + \frac{\theta}{2\alpha} = \frac{1}{\theta} \left(\frac{\theta^2}{2\alpha} + \Delta_a - \theta y \right) \\ &= \frac{1}{\theta} \left(\frac{\theta^2}{2\alpha} - \Gamma_a \right). \end{aligned}$$

We thus have

$$\begin{aligned} \Gamma &= \Gamma_a + \Delta_a - \Delta = \Gamma_a + \frac{\bar{\alpha}}{2}(x - x_U)^2 = \Gamma_a + \frac{\bar{\alpha}}{2\theta^2} \left(\frac{\theta^2}{2\alpha} - \Gamma_a \right)^2 \\ &= \Gamma_a + \frac{\theta^2}{8\bar{\alpha}} - \frac{1}{2}\Gamma_a + \frac{\bar{\alpha}}{2\theta^2}\Gamma_a^2 = \frac{1}{2}\Gamma_a + \frac{\theta^2}{8\bar{\alpha}} + \frac{\bar{\alpha}}{2\theta^2}\Gamma_a^2 \\ &< \frac{1}{2} \cdot \frac{\theta^2}{2\bar{\alpha}} + \frac{1}{4} \cdot \frac{\theta^2}{2\bar{\alpha}} + \frac{1}{4} \cdot \frac{\theta^2}{2\bar{\alpha}} = \frac{\theta^2}{2\bar{\alpha}}. \end{aligned} \quad \square$$

Theorem 10.

Proof. The statement regarding operations is obvious. Towards correctness, all calculations result from Propositions 2, 3, 4, and 5, by replacing the value of α and x_U (and x_L in case of case I iii) into the equation for $b(x)$ from Proposition 2. Within each region, this yields a smooth equation (i.e., without a case distinction or a maximum/minimum) that has degree 1 or 2 in b_a can therefore be solved for b_a easily.

The only part that requires further discussion are the equations for Δ_a in cases II 1 ii and III L ii. These calculations result from a quadratic equation each, which has two solutions (unless the radicand is zero). We show why the equation always has a solution and only the respective chosen solution is possible as a choice of Δ_a .

First consider case II 1 ii. Here we have $\alpha = \bar{\alpha}$, $x_U = \hat{x}_{U,1} = y_a - \frac{\Delta_a}{\theta} - \frac{1}{2\alpha}\theta$, and $\alpha\Delta_a \geq \frac{1}{2}\theta^2$. Replacing this into the equation for $b(x)$ in Proposition 2 for case ii yields the following.

$$\begin{aligned} b &= b_a - x + \frac{\alpha}{2} \left(x - y_a + \frac{\Delta_a}{\theta} + \frac{1}{2\alpha}\theta \right)^2 \\ \Leftrightarrow 0 &= \Delta_a^2 - 2\theta\bar{\gamma}\Delta_a + \frac{2\theta^2}{\alpha}(y - b) + \theta^2\gamma^2, \end{aligned}$$

where $\gamma := \frac{\theta}{2\alpha} - y$ and $\bar{\gamma} := \frac{\theta}{2\alpha} + y$. The second line follows by straightforward algebraic transformation. Let $p' = \theta\bar{\gamma}$ and $q = \frac{2\theta^2}{\alpha}(y - b) + \theta^2\gamma^2$. By the quadratic formula, the solutions to this equation are

$$\Delta_a = p' \pm \sqrt{p'^2 - q} = p' \pm \sqrt{d},$$

where $d = \theta^2 \frac{2}{\alpha}(b - \bar{\theta}y)$ and the second equality again follows by simple algebraic transformation. Note that $d > 0$ since, by assumption, $b/y > \bar{\theta}$, so the equation has two distinct solutions. Algorithm 3 chooses the “−” solution. We show that the “+” solution to the equation is not a feasible value of Δ_a . To see this, assume towards a contradiction that $\Delta_a = p' + \sqrt{d} = \theta \left(\gamma + \sqrt{2/\alpha(b - \bar{\theta}y)} \right) =: \theta(\gamma + \delta)$. Note that $\delta > 0$ because $d > 0$. Then

$$\begin{aligned} x_U &= y_a - \frac{\Delta_a}{\theta} - \frac{\theta}{2\alpha} \\ &= y_a - \gamma - \delta - \frac{\theta}{2\alpha} \\ &= y_a - \frac{\theta}{2\alpha} + y - \delta - \frac{\theta}{2\alpha} = x - \frac{\theta}{\alpha} - \delta. \end{aligned}$$

Therefore,

$$\begin{aligned} \rho(x) &= 1 - \alpha(x - x_U) = 1 - \alpha\left(\frac{\theta}{\alpha} + \delta\right) \\ &= 1 - \theta - \alpha\delta = \bar{\theta} - \alpha\delta < \bar{\theta}. \end{aligned}$$

Contradiction to case ii and choice of x_L .

Next consider case III L ii. We have $\alpha = \frac{1}{2} \frac{\theta^2}{b_a - \bar{\theta}y_a}$ and $x_U = 0$, and $r_a \leq \frac{1+\bar{\theta}}{2}$. Again, replacing this into the equation from Proposition 2 yields:

$$\begin{aligned} b &= b_a - x + \frac{1}{2} \cdot \frac{1}{2} \frac{\theta^2}{b_a - \bar{\theta}y_a} x^2 \\ \Leftrightarrow 0 &= \Delta_a^2 - (y - b + \theta y_a)\Delta_a + (y - b)\theta y_a + \frac{1}{4}x^2\theta^2 \end{aligned}$$

Let $p' = \frac{1}{2}(y - b + \theta y_a)$ and $q = (y - b)\theta y_a + \frac{1}{4}x^2\theta^2$. Then

$$\Delta_a = p' \pm \sqrt{d},$$

where $d := p'^2 - q = \frac{1}{4} \left((b + x - \bar{\theta}y_a)^2 + \theta^2x^2 \right)$. We trivially have $d > 0$.¹⁶ Assume

¹⁶Note that we trivially always have $d \geq 0$. If $d = 0$, then $x = 0$ and we must have $0 = b + x - \theta y_a = b - \theta y$ and thus $b/y = \theta$; contradiction to the assumption of the algorithm.

towards a contradiction that $\Delta_a = p' + \sqrt{d}$. Then

$$\begin{aligned}\Delta_a &\geq p' + \sqrt{\frac{1}{4}(b+x-\bar{\theta}y_a)^2} \\ &= p' + \frac{1}{2}(b+x-\bar{\theta}y_a) \\ &= \frac{1}{2}(y-b+\theta y_a + b+x-\bar{\theta}y_a) \\ &= \frac{1}{2}(y_a + \theta y_a - \bar{\theta}y_a) = \frac{1}{2} \cdot 2\theta y_a = \theta y_a.\end{aligned}$$

For the first equality, note that by assumption $b_a \geq \bar{\theta}y_a$ and $b \geq b_a - x$ (since b arises from b_a by redeeming at a rate ≤ 1), so $b+x \geq b_a \geq \bar{\theta}y_a$, and thus the operand of the square is non-negative.

Now, since $y_a - b_a = \Delta_a \geq \theta y_a$, we equivalently have $b_a \leq \bar{\theta}y_a$, i.e., $r_a \leq \bar{\theta}$. Contradiction to non-triviality. \square

G Additional Technical Guarantees

The following technical guarantees may be useful for implementation, e.g., to understand error conditions or the data types required to store certain values. They are essentially redundant but stated explicitly here for additional clarity. Note that numerical errors in any implementation can lead to slight violations of these properties in practice even though they are mathematically guaranteed.

The following lemma shows that Proposition 3 can be safely used to store x_L in an unsigned integer of bounded width.

Lemma 7. *Assume that $b_a < y_a$, $r_a > \bar{\theta}$, and let $x_U \leq y_a$ and $\alpha > 0$ be arbitrary. Assume that Inequality (5) holds. Then the formula for x_L in Proposition 3 is well-defined and $0 \leq x_L \leq y_a$. Specifically, we have:*

$$\begin{aligned}(y_a - x_U)^2 - \frac{2}{\alpha}(y_a - b_a) &\geq 0 \\ y_a - \sqrt{(y_a - x_U)^2 - \frac{2}{\alpha}(y_a - b_a)} &\in [0, y_a]\end{aligned}$$

Proof. The first inequality immediately follows from (5). Towards the second inequality, the expression is obviously $\leq y_a$. To see that it is ≥ 0 , note that this is equivalent to

$$\begin{aligned}y_a &\geq \sqrt{(y_a - x_U)^2 - \frac{2}{\alpha}(y_a - b_a)} \\ \Leftrightarrow y_a^2 &\geq (y_a - x_U)^2 - \frac{2}{\alpha}(y_a - b_a)\end{aligned}$$

and this inequality obviously holds since $y_a^2 \geq (y_a - x_U)^2$. \square

The following lemma shows that Proposition 5 can be safely used to store x_U in an unsigned integer of bounded width if α is chosen appropriately. We do not consider the caps \bar{x}_U and $\bar{\alpha}$ explicitly here; these only make the bounds on x_U tighter.

Lemma 8. *Assume that $b_a < y_a$ and $r_a > \bar{\theta}$ and let $\alpha \geq \hat{\alpha}$ be arbitrary where $\hat{\alpha}$ is like in Proposition 4. Then for the formula for \hat{x}_U in Proposition 5 we have $0 \leq \hat{x}_U(\alpha) \leq y_a$.*

Proof. It follows immediately from the formulas that $\hat{x}_{U,h}(\alpha) < y_a \forall \alpha > 0$.

It remains to show that $\bar{x}_U(\alpha) \geq 0$. By construction (see the proof of Proposition 4), $\hat{x}_U(\hat{\alpha}) = 0$. Furthermore, $\hat{x}_U(\alpha)$ is monotonically increasing in α . To see this, note that the expressions $\hat{x}_{U,h}$ and $\hat{x}_{U,l}$ are both monotonically increasing as functions of α . Continuity of $\hat{x}_U(\alpha)$ (see Proposition 5) implies that $\hat{x}_U(\alpha)$ as a whole must be monotonically increasing. \square

Remark 2. In general (if α is not chosen according to Proposition 4 but is arbitrary), we can have $\hat{x}_U(\alpha) < 0$. To see this, consider the limit $\alpha \rightarrow 0$. Then $\alpha\Delta_a \leq \frac{1}{2}\theta^2$, so $\hat{x}_U(\alpha) = \hat{x}_{U,h} = y_a - \sqrt{2\frac{\Delta_a}{\alpha}} \rightarrow -\infty$.

The following lemma shows that, to ensure that the boundary conditions of our method hold, it is enough to check the reserve ratio b/y at the beginning of any redemption.

Lemma 9. *Consider Algorithm 4 and assume that $\bar{\theta} < b/y < 1$. Consider the values b_a and y_a computed by the algorithm. Then also $\bar{\theta} < b_a/y_a < 1$.*

Proof. By construction, if there is a b_a with $\bar{\theta} < b_a/y_a < 1$ such that $b(x; b_a, y_a) = b$, then the algorithm determines this b_a and in particular it lies in the interval $(\bar{\theta}, 1)$ as required.

Existence (and, in fact, uniqueness) of this b_a can be seen explicitly as follows. Fix x and y and note that this fixes $y_a = y + x$. Consider the function $f(b_a) := b(x; b_a, y_a)$. We need to show that there is a unique $b_a \in (\bar{\theta} y_a, y_a)$ such that $f(b_a) = b$. This is implied by the following facts: f is strictly monotonic in b_a in the region of those b_a values where $f(b_a)/y \in (\bar{\theta}, 1)$ (see Theorem 1); f is continuous (see the propositions in Appendix C); $f(b_a) \rightarrow y$ for $b_a \rightarrow y_a$; and $f(b_a) \rightarrow \bar{\theta} y$ for $b_a \rightarrow \bar{\theta} y_a$. We explicitly prove the last two statements.

For $b_a \rightarrow y_a$, first note that we eventually have $\alpha = \bar{\alpha}$ and $x_U = \bar{x}_U$ constant (propositions 4 and 3) and furthermore $x_L \rightarrow x_U$ and $r_L \rightarrow 1$ (Proposition 3). Now, via Proposition 2, it is easy to see that $f(b_a) \rightarrow y_a - x = y$.

For $b_a \rightarrow \bar{\theta} y_a$, the statement is trivial for $x = 0$, so assume $x > 0$. Observe that $\alpha = \hat{\alpha}_L$ eventually and $\hat{\alpha}_L \rightarrow \infty$ (Proposition 4), and furthermore $x_U = 0$ eventually (by choice of α or via Proposition 3) and these statements imply that $x_L \rightarrow 0$ (see Proposition 3). Consider a b_a sufficiently close to $\bar{\theta} y_a$ such that all of the eventual statements hold, $\alpha \geq \theta$, and $x_L \leq x$, so that $f(b_a) = r_L y$. We show that¹⁷ $r_L = \bar{\theta}$.

¹⁷This does not contradict Theorem 1 because that theorem only stated strict monotonicity of f in the region of b_a where $f(b_a)/y \in (\bar{\theta}, 1)$. We do not usually have *strict* monotonicity in the larger region of b_a where $b_a/y_a \in (\bar{\theta}, 1)$.

This can be seen by explicit calculation as follows. To simplify notation, assume WLOG $y_a = 1$. By Proposition 3 and $x_U = 0$ we have $r_L = 1 - \alpha x_L$, so the statement is equivalent to showing $\alpha x_L = \theta$. This statement is equivalent to

$$\begin{aligned} & \alpha \left(1 - \sqrt{1 - \frac{2}{\alpha} (1 - b_a)} \right) = \theta \\ \Leftrightarrow & \alpha - \theta = \alpha \sqrt{1 - \frac{2}{\alpha} (1 - b_a)} \\ \Leftrightarrow & (\alpha - \theta)^2 = \alpha^2 - 2\alpha(1 - b_a) \\ \Leftrightarrow & \theta^2 - 2\alpha(\theta - (1 - b_a)) = 0 \\ \Leftrightarrow & \theta^2 - 2\alpha(b_a - \bar{\theta}) = 0. \end{aligned}$$

Recall now that $\alpha = \hat{\alpha}_L = \frac{1}{2} \frac{\theta^2}{b_a - \bar{\theta}}$. The statement now clearly holds. \square

The following lemma shows that Lemma 5 can be safely applied in unsigned integers.

Lemma 10. *For any arbitrary α and $z \leq y_a$, let $y_z = y_a - z$. Then the following hold:*

1. If $1 - \alpha y_z \geq \bar{\theta}$, then $y_a - \frac{\alpha}{2} \cdot y_z^2 \geq 0$.
2. In any case, $y_a - \theta y_z + \theta^2 \cdot \frac{1}{2\alpha} \geq 0$.

Proof. 1. The assumption in particular implies $1 - \alpha y_z \geq 0$, i.e., $y_z \geq 1/\alpha$. Now, since $y_z \leq y_a$,

$$y_a - \frac{\alpha}{2} y_z^2 \geq y_a - \frac{\alpha}{2} y_z y_a \geq y_a - \frac{\alpha}{2} \frac{1}{\alpha} y_a = y_a/2 \geq 0$$

2. Since $y_a \leq y_a$,

$$y_a - \theta y_z + \theta^2 \cdot \frac{1}{2\alpha} \geq y_a - \theta y_a + \theta^2 \cdot \frac{1}{2\alpha} = \bar{\theta} y_a + \theta^2 \cdot \frac{1}{2\alpha} \geq 0 \quad \square$$

Note that the expression $1 - \alpha y_z$ may *not* always yield a non-negative number, but we can re-write the condition as $1 \geq \bar{\theta} + \alpha y_z$.

Disclaimer. *This paper is for general information purposes only. It does not constitute investment advice or a recommendation or solicitation to buy or sell any investment and should not be used in the evaluation of the merits of making any investment decision. It should not be relied upon for accounting, legal or tax advice or investment recommendations. This paper may contain experimental code and technical designs that may not be ready for general use. This paper reflects the current opinions of the authors and is not made on behalf of Superluminal Labs or its affiliates and does not necessarily reflect the opinions of Superluminal Labs, its affiliates or individuals associated with Superluminal Labs. The opinions reflected herein are subject to change without being updated.*