Gyroscopic Stablecoins

Ariah Klages-Mundt Lewis Gudgeon Daniel Perez

December 2020

Abstract

Here we introduce a new class of stablecoin design: gyroscopic stablecoins. Analogous to a gyroscope, gyroscopic stablecoins use automated market maker (AMM) mechanisms in combination with a gyroscopic reserve to maintain stability. The reserve accretes a store of 'angular momentum' in the gyroscope, which serves as a rainy day fund that is used by a specially designed AMM to stabilize stablecoin markets. The reserve deploys assets in ways that stratify risk across tail risk groups while accreting value to the system. Gyroscopic stablecoins contrast with existing stablecoins, which are largely based on leverage mechanisms. We suggest that gyroscopic stablecoin mechanisms can align incentives of participants toward stability over a wider range of scenarios, leading to more flexible and robust systems that probabilistically survive large failure events. Gyroscopic stablecoins seek to provide the nearest feasible neighbour to a risk-free asset for the cryptocurrency ecosystem.

1 Introduction

All stablecoins come with significant failure risks, as we characterize in [12]. These range from traditional counterparty/censorship risks in custodial stablecoins to complex market structure, governance/oracle, and bug risk in non-custodial stablecoins. For stablecoins based on leverage markets (e.g., Dai), we've shown that stability incentives of participants in the underlying market can break down during turbulence, termed "deleveraging spirals". We predicted/demonstrated these in [13] and formally characterized them in [14]. These deleveraging spirals were later validated in Maker during the 'Black Thursday' crisis in March 2020. We also showed in [6] how wider cryptocurrency leverage markets can break down in the presence of persistent market illiquidity, contributing to decentralized financial crises.

A design gap in current stablecoins, as we suggest in [12], is the incorporation of well-designed buffers to help survive transitory events. In [14], we show that non-custodial stablecoins can be stable in particular regions in which expected collateral returns are positive (formally a "submartingale") and can break down outside of this. We suggest that critical stablecoin design work is needed to extend stability to survive realistic deviations from such ideal submartingale settings. As there is little that derivative design can do to help systems survive permanent downturn events (e.g., when the ecosystem can no longer survive long-term), we focus our efforts on the survival of significant but transitory downside events. Toward this goal, we suggest that real world systems must have adequate buffers so as to survive transitory events and expand the stable regions of stablecoins.

We suggest that buffered stablecoin designs can go further to expand design possibilities beyond the leverage-based stablecoins which preside today. In particular, instead of leverage mechanisms, we consider the application of automated market maker (AMM) mechanisms, which may have more stable incentive dynamics under market turbulence than leverage markets as they are based on demand for asset exchange, which may increase with turbulence, as opposed to demand for speculative leverage, which may collapse. AMMs provide an exchange service amongst assets in a liquidity pool using an algorithmic exchange price, which is usually either intended to converge to the true market price (e.g., Uniswap, Balancer pools) or to influence the true market price of a created asset (e.g., NXM in Nexus Mutual). In the first case, AMM mechanisms can have an imperfect stabilizing effect on the value of liquidity provider (LP) positions. For instance, LPs in constant product markets achieve a constant mix portfolio that in effect averages returns among assets, profits from volatility harvesting, and profits from providing a valuable exchange service.[1] This can be beneficial regarding stable value insofar as the constant-mix portfolio stratifies risk. In the second case, AMM mechanisms can constrain price movements of a created asset.

We propose a novel design class: *gyroscopic stablecoins*. This class uses AMM mechanisms in combination with a gyroscopic reserve to maintain stability. The reserve accretes 'angular momentum' in the gyroscope, which serves as a rainy day fund that is used by a specially designed AMM to stabilize a primary market for the stablecoin. The reserve deploys assets in ways that stratify risk across

[1] Note that constant product markets aren't the most efficient implementation of a constant mix portfolio. They suffer from 'divergence loss' (also commonly called 'impermanent loss') from effectively rebalancing assets as non-optimal prices as underlying assets diverge in price. They are profitable insofar as fees from exchange volume make up for this.

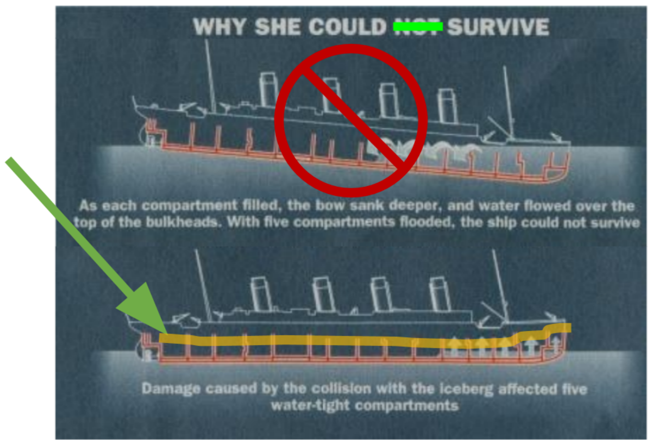

Figure 1: (Titanic analogy) how to prevent cascading failure in asset baskets.

tail risk groups while accreting value to the system. Gyroscopic stablecoins are designed to be probabilistically stable while containing the cascade potential of complex decentralized finance (DeFi) risks. We suggest that gyroscopic stablecoin mechanisms can align incentives of participants toward stability over a wider range of scenarios, leading to more flexible and robust systems.

First, we briefly compare with some related stablecoin mechanisms before describing the class of gyroscopic mechanisms in Section 2 and detailed examples in Section 3. The design of gyroscopic stablecoins builds on our preliminary work in the first place project at the 2020 IC3 Bootcamp [11] and an early version in a 2018 proposal [10].

Comparison with current basket stablecoins that use AMMs. At present, several basket stablecoins use a naive construction, wherein a basket of assets backs the stablecoin. A central issue with such constructions atop AMMs is that the failure of one (or a few) assets can cascade into failure of the entire basket via the exchange mechanism.[2] For stablecoin purposes, we liken this problem to the design of water-tight doors on the Titanic, in which the flooding of a few compartments had a spillover effect onto the remaining compartments.

Gyroscopic stablecoins control for this issue in two main ways:

1. by segregating reserve assets into pools in such a way that the possibility of contagion between the pools is minimized;

2. by designing the AMM to prevent the exhaustion of the reserve's resources.

[2] For instance, currently every Curve Finance stablecoin pool except one would fail if USDT failed, every Curve stablecoin pool would fail if USDC failed, every Curve BTC pool would fail if wBTC failed, and every Curve BTC pool except one would fail if renBTC failed.

To continue the Titanic analogy, this is like constructing the water-tight doors all the way to the ceiling.

Comparison with current stablecoin insurance mechanisms. Some stablecoins add a layer to the protocol intended to globally buffer against shortfalls. In particular, many current stablecoins generate cash flows from fees that are securitized into governance tokens (e.g., MKR in Maker). To cover a shortfall situation, the value of future cash flows can be auctioned off by selling new governance tokens. However, the value of future cash flows can evaporate in death spiral situations. Alternatively, a portion of past cash flows can be diverted to serve as a buffer to cover shortfalls. There is in fact a spectrum between these options, in which securitized cash flows can be sold at arbitrary times to maintain an adequate buffer. This is a largely unexplored spectrum in stablecoins. For instance, Maker has a 'system surplus' account that served as a buffer during Black Thursday. This was not in fact intended as a stability buffer and is typically used to accrue fees until they reach a size for returning to 'equity' holders. Instead, Maker's intended buffer is an auction of MKR equity, arguably to be conducted at the worst possible time, to cover shortfalls.

2 A New Design Class: Gyroscopic Stablecoins

Our proposed class of gyroscopic designs combines four economic components. We illustrate this class of designs with concrete examples in Section 3.

The *Gyroscopic Reserve* contains the assets backing the system. Creation of stablecoins adds to the reserve and redemption of stablecoins subtracts from the reserve. The reserve also tends to grow over time by deploying assets in a risk-segregated portfolio of vaults. The portfolio aims to diversify tail risks but does not necessarily need to be stable in value itself. It is rebalanced/changed at discrete times to mitigate contagion from the failure of individual vaults. However, a vault itself may contain many assets and may be rebalanced continually (e.g., an AMM pool). Via this portfolio, the reserve deploys system assets to earn a yield while controlling for complex DeFi contagion risks.

The *Primary Market AMM* creates a primary market for minting and redeeming stablecoins balanced against the reserve. It is intended to price the last-resort liquidity for the stablecoin and effectively bound the stablecoin's prices on the secondary markets, where normal activity is intended to occur. The AMM is custom-designed to balance stablecoin pricing bounds with reserve health. The redemption AMM aims to provide variable support for the stablecoin price peg during volatile times while incentivizing redeemers to prefer redeeming during healthy times and to thwart economic attacks against the peg. For instance, the redemption rate may change with reserve health and with the size of recent outflows to protect the reserve from exhaustion. In this way, the system can still function even if reserve value per stablecoin is less than \$1. The stablecoin minting AMM incorporates a 'value of systemic insurance' from the health of the reserve and the effects of minting on reserve dilution per stablecoin in addition to the target \$1 value.

The primary market AMM structure can in turn be used to optimize the shape of *Secondary Market AMMs*, and thus increase their efficiency for ordinary stablecoin usage.

A *reserve securitization* component allows future yield on reserve assets at times to be securitized and sold to boost current reserve size.[3]

2.1 Risk Segregation in the Reserve

Segregation of DeFi portfolio risks stems from our work in [12] characterizing the multitude of different risks arising from different stablecoin design choices. The goal is to design vaults in ways such that risks are segregated into discrete vaults, which may fail but will not contaminate the remaining vaults. In so doing, the gyroscopic reserve will be robust to the risks posed by individual vaults.

Vault strategies introduce risks stemming from the underlying assets (e.g., stablecoin risks) and the form of deployment. Among custodial stablecoins, we segregate assets based on common counterparty, bank run, and jurisdictional risks. Among non-custodial stablecoins, we segregate assets based on the primary values ($\sim$ collateral type) backing the stablecoins, different oracle and governance systems, and composability and smart contract bug risks.

We then consider the following types of asset deployments and risks therein: Constant Function Market Makers (CFMMs)[4], Protocols for Loanable Funds (PLFs), and rebate/reward pools.

- *CFMM pools*. CFMM pools can be thought of as continually rebalanced portfolios that provide an exchange service between constituent assets. These pools face a drag from volatility as the rebalance mechanism creates arbitrage opportunities when prices change. These pools are well-designed if the trading service is more valuable (through fees) than the drag, or if assets are mean-reverting and can profit from volatility harvesting (see, e.g., [3]). A rebalancing portfolio can be structured to have a damping effect on transient price declines if the assets have low correlation (e.g., if one of the assets is a stablecoin). This creates a reduced volatility region distinct in mechanism from leverage-based stablecoin designs. More customized CFMM designs can also replicate various options strategies[5], which can be deployed to further separate risks from one pool to another.

- *PLF pools*. These can be interpreted as AMMs for interest rates and introduce distinct liquidity and collateral risks to other pools (see, e.g., [6, 7, 9]).

[3] In this version of the lite paper, we focus on the design of gyroscopic reserves and primary market AMMs and leave design of optimal reserve securitization components to further development.

[4] For fundamental analyses of CFMMs see [2, 1, 5].

[5] Akin to synthetic portfolio insurance, see Ch. 13 in [8].

- *Rebate/reward pools.* Many DeFi protocols incentivize liquidity provision in the form of protocol ownership (aka yield farming). Rebate pools will automate the collection and compounding of these rewards. This may blend with the previous types of pools. An important consideration is to segregate risks into discrete vaults so that the system is robust (vs. simply targeting the highest current yield).

2.2 Primary vs. Secondary Stablecoin Markets

The stablecoin's primary market mint/redeem AMM is intended to perform the role of market maker of last resort and comes with dynamic mint and redeem prices. This can be thought of akin to ETF arbitrage: if the secondary market deviates too much from fundamental values at which stablecoins can be created or redeemed, then it will be profitable to route orders through the primary market (by creating or redeeming stablecoins). In traditional finance, this is limited to ETF 'authorized participants' who perform creation/redemption arbitrage. In our system, anyone can interact with the primary market entirely on-chain, and orders can automatically be routed through it; in this case, the mint/redeem spread captures the ETF arbitrage value to grow the reserve.

In normal settings, after initial system growth, we expect that secondary markets for the stablecoin will provide more efficient trades and will avoid mint/redeem spreads and fees. During extraordinary times, like cryptocurrency market crises, secondary markets may be overwhelmed. This could occur, for instance, if there is a large flight to safety, and so excess demand for robust stablecoins. These are the particular settings in which the value of insurance from the reserve system is most important. The minting price is designed to account for this value of insurance and to price in the dilutionary effect of minting on reserve value per stablecoin.

2.3 Governance

The system will need some form of governance over time to handle the following tasks.

- Rebalance/change the reserve portfolio over time;
- Make securitization decisions (may be automated to some degree);
- Select price feeds for the system to use;
- Potentially modify primary market AMM parameters over time.

The question of governance design builds on research questions discussed in [12]. Note that the design can contain relatively limited governance surfaces and is a simpler problem in this setup as opposed to other stablecoin designs as there is only one type of interested party: stablecoin holders. This contrasts with other non-custodial stablecoin designs that require balancing competing incentives of stablecoin holders, leveraged borrowers, and governance token holders. Note also that the price feed surface area can be limited at the expense of other functionality. For instance, the surface area in example Design A in the following section has very limited price feed surface area.

At this point, we focus on the economic design of gyroscopic stablecoins and leave governance design to further development.

3 Examples of Gyroscopic Designs

To illustrate, we consider three concrete examples of gyroscopic stablecoins, which represent different parameter choices within this class of designs. To aid in illustration, let's define the primary market AMM via the pair of functions

$$f(y, z) = \text{AMM marginal redemption offer}$$
$$g(y, z) = \text{AMM marginal mint offer}$$

where $y =$ the reserve dollar value per stablecoin issued (which we will also refer to as the net asset value, or NAV[6]), $z =$ other system state variables (e.g., z may include a moving sum of inflows and outflows), and the outputs of f and g are in dollar value of reserve assets. For simplicity, we ignore exchange fees in this section, but they could be added.

3.1 Minting stablecoins in the primary market

The primary market minting AMM provides an upper bound on the stablecoin price. When $y \leq 1$, the minting price is the target \$1. However, when $y > 1$, the minting price ought to take into account the insurance value of the reserve. To motivate the pricing of this insurance, consider a utility function U that describes the utility of existing stablecoin holders as a function of y. Notice that if a new stablecoin is minted for the price of \$1, then y (and so also $U(y)$) decreases because the reserve value is diluted. One way to price the insurance value of the reserve is to charge a new minter a fee that accounts for the change in utility to existing stablecoin holders, i.e. the externality, as a result of minting.

Considering z as a moving average of inflow, let y_{-z} be the value y would have taken without the recent inflow z. Then g could look like

$$g(y, z) = 1 + \max\Big(0, U(y_{-z}) - U(y)\Big)$$

which prices the insurance value of the reserve as the cost in utility from reserve dilution to existing stablecoin holders. Figure 2 illustrates a minting AMM using g with log utility.

Note that this formulation of g and the measurement of utility as a function solely of y is likely too simplistic to capture everything. Regardless, we suggest it provides a reasonable candidate for pricing reserve insurance for the purpose of upper bounding the price.

[6]Note that, contrary to typical usage of "NAV", the stablecoin shouldn't necessarily trade at the NAV, which just represents the fundamental value that can support the peg.

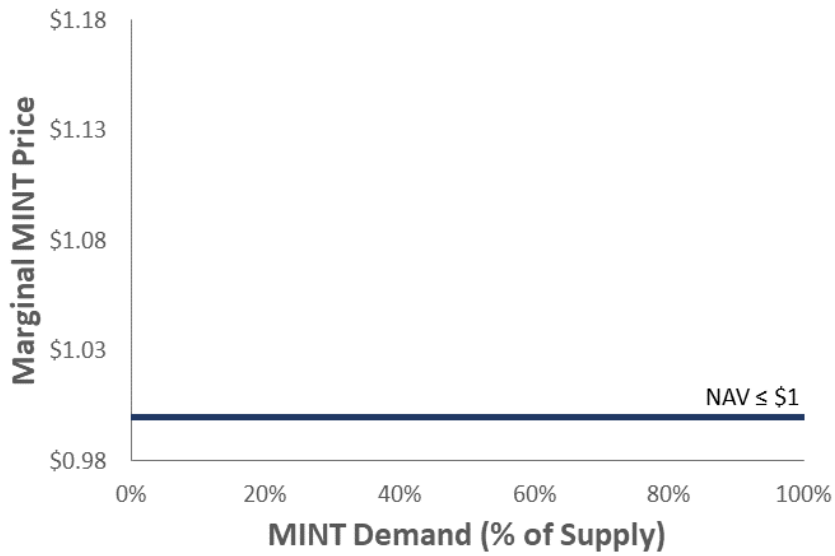

Figure 2: Dynamic minting price as function of NAV and inflows.

3.2 Design A $\sim$ ETF of stablecoins with a rainy day fund

Design A can be interpreted like an ETF of stablecoins with an additional rainy day fund that grows over time. The rainy day fund provides insurance against the failure of individual stablecoins in the basket. In this case, the reserve can be divided into the ETF basket backing the stablecoins and the rainy day fund, both of which may be deployed in risk-segregated ways. One stablecoin is redeemable through the primary market AMM for a share of the underlying basket and vice versa after accounting for the insurance value of the rainy day fund. This is the design originally described in [10, 11]. Figure 3 describes this structure.

We also consider two further twists for the rainy day fund.

- Rainy day fund cash flows can be securitized and may be sold at times to recapitalize the reserve. This is like harnessing future cash flows to fill the reserve as opposed to accruing past cash flows.
- Rainy day fund 'insurance' can be separable from the stablecoin and accessible via subscription (e.g., compare to Danish green bonds).

Compared to the generalized design, Design A restricts the type of underlying assets to mainly other stablecoins and takes the primary market AMM redemption function to be

$$f(y) = \min(1, y).$$

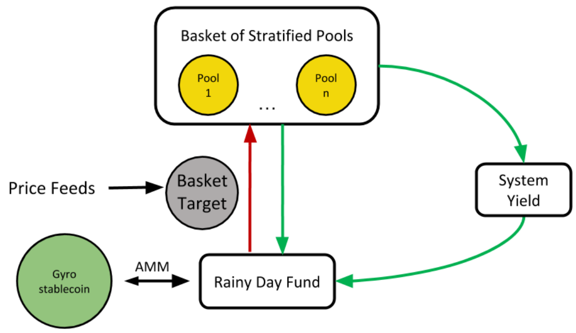

Figure 3: Rainy Day Fund structure for Designs A, B.

3.3 Design B ∼ money market fund with pegged redemption

In Design B, the reserve is composed of a combination of stable and volatile assets and mimics a money market fund that aims for a pegged redemption rate of \$1. For instance, some portfolio vaults may deploy assets in mixed stable-volatile pair AMM pools. Each stablecoin is redeemable for \$1 worth of reserve assets, subject to a possible devaluation/peg break, and vice versa accounting for the insurance value of a healthy reserve. The reserve grows as yield is earned in the portfolio. The excess value of the reserve can be interpreted akin the rainy day fund in Design A, which serves to continously smooth the redeemable value per stablecoin to keep the peg at \$1. If the excess falls below 0, then the stablecoin is devalued (like a money market mutual fund 'breaking the buck').[7] As in Design A, similar twists are available on the rainy day fund formulation.

Compared to the generalized design, this example again takes the primary market AMM function to be $f(y) = \min(1, y)$.

3.4 Design C ∼ currency peg model

Design C resembles the previous designs in effect but with a more flexible structure. The reserve contains all assets, deployed in various ways, and is interpreted as a reserve fund. A stablecoin can be created by depositing \$1 plus an insurance fee payable in the reserve assets as determined by g. A stablecoin can be

[7]For research modeling money market mutual funds, see, e.g., [17]. The application of a reserve securitization component that helps to recapitalize in the event of shortfalls can be modeled similarly to sponsor support in the context of that model.

redeemed through the primary market AMM that scales the redemption rate based on net outflows and reserve value per stablecoin determined by f. Under normal conditions (e.g., low net outflow), redemption value is \$1 (minus possible fee). In times of crisis, redemption value may be flexible below \$1. For instance, it could scale as a function of net outflows down to the reserve value per stablecoin, if less than \$1. This has the effect of preserving reserve health and incentivizing redeemers to wait to redeem at better prices later.

Under this design, the reserve value per stablecoin may be $<$ \$1 (which could be interpreted as under-collateralized) at times without breaking the peg in a similar way to how currency peg models work (see e.g., [15]). In effect, this works by setting up game theoretic incentives among stablecoin holders to coordinate on \$1 value for the stablecoin supposing the reserve is of a sufficient size and the stablecoin itself is economically usable. Note that the design may still aim to be fully (or over-) collateralized long-term.

A particular concern for the primary market AMM design is that when redemptions are allowed at values greater than the reserve value per stablecoin, then the AMM needs to be robust to speculative attacks against the peg that try to deplete the reserve. With flash loans/minting, this would be particularly dangerous, and so redemptions would probably be best subject to a reasonable delay. An AMM design that adjusts the short-term exchange rate dynamically based on changes in outflows (and other system state) can also help to disrupt economic attacks while continuing to target a long-term stable exchange rate.

To illustrate, a simplistic[8] formulation of the AMM redemption function could look like

$$f(y, z) = \max\Big(\texttt{decayCurve}(z), \min(1, y)\Big),$$

where the `decayCurve` function decays from 1 and depends on system state z such as historical outflows. Figures 4-5 illustrates a dynamic redemption AMM like this.

Since this design can still function under-collateralized, it also allows a more flexible launch. For instance, short-term growth can be fueled while accruing an under-collateralized reserve, and structure can gradually shift to the long-term dynamics envisioned. It's worth noting that minting new stablecoins when the reserve is under-collateralized and redeeming stablecoins when the reserve is over-collateralized are both good for the system as they increase reserve value per stablecoin. Further flexibility could also be explored with different monetary policies (defined in f, g) than simply a currency peg.

Parallels with the monetary economics literature. Design C can be considered as a variant on a crawling or managed float system, as defined by functions f and g, for a currency peg. The monetary economics literature on these topics provides a starting point to understand this design.

[8] Provided solely to illustrate the ideas but which is missing some important properties that we won't go into here.

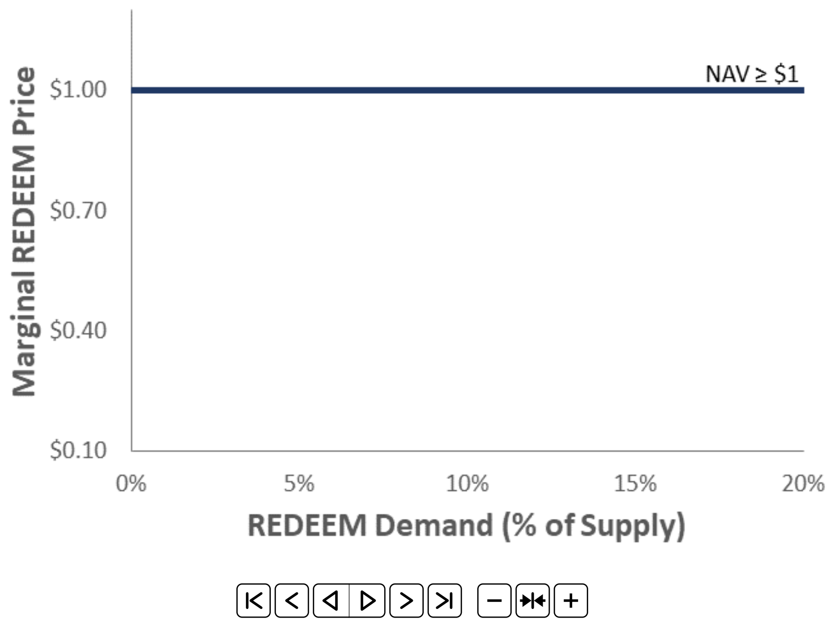

Figure 4: Dynamic redemption price as function of NAV and outflows.

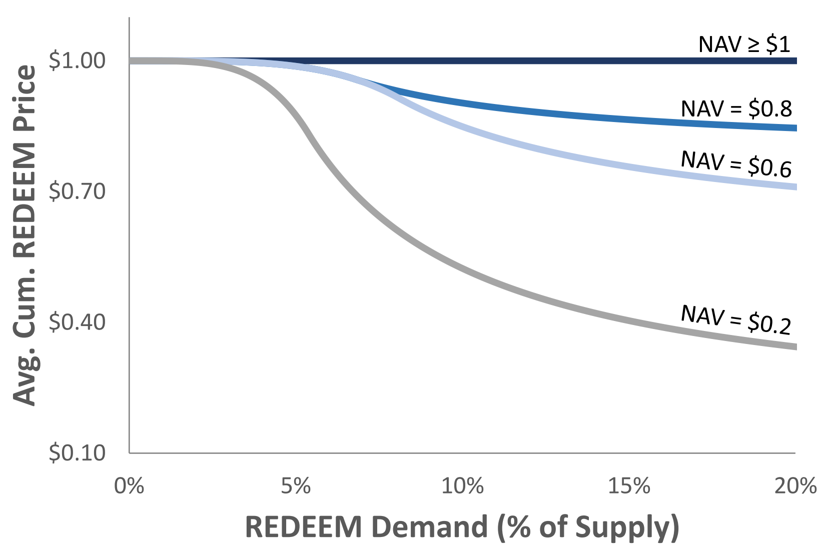

Figure 5: Average cumulative redemption price (starting from $z = 0$).

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 in Design C 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., [15]). 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 [15], 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 f 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.[9] Compared to a typical currency peg, the curvature of f 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 f 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 f, which serves to further raise the costs of attack.

Lastly, we contrast with the bank run model in [4]. 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 the Design C 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 [18]

[9]While certain uncollateralized (or "implicit collateral", see [12]) stablecoins also propose similar narratives as here, they do so without a fundamental force, such as from the gyroscopic reserve, pushing coordination toward the $1 equilibrium. Accordingly, one may question whether the stable equilibrium may really be $0 price in such cases.

for further discussion of the following points). First, the curvature of f 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.[10]

3.5 Secondary Market AMM Design

As already discussed, ordinary usage of gyroscopic stablecoins are intended to be directly through secondary markets, where gyroscopic stablecoins can be traded for other assets and stablecoins, as opposed to minting and redeeming gyroscopic stablecoins for reserve assets through the primary market AMM. We now discuss how secondary market AMM curves can be optimized by using pricing bounds arising from the primary market AMM.

An off-the-shelf CFMM such as current formulations of Balancer, Uniswap, or Curve would price liquidity for all (hypothetical) levels of the assets in the pool. An alternative is to shape a CFMM curve to price liquidity within bands encompassing the primary market AMM price bounds.[11] Trades that would result in prices outside of the band would be routed directly to the primary market AMM, mitigating the requirement for the secondary market AMM to price liquidity at such points. In this design, capital is targeted at feasible price points within the secondary market AMM, reducing the amount of capital that serves to support portions of the AMM curve that would not rationally be reached. In turn, this serves to improve capital efficiency. Figure 6 illustrates this idea.

Designed in this way, the improved efficiency of the secondary market AMM would provide lower slippage on trades, which should attract more exchange volume for less deposited capital, meaning higher fees per LP share from efficient targeting of capital. Such a design would present risks similar to those in Curve pools. For instance, in the event that the LP finds themselves at either the mint or redeem bounds, the exposure of the LP would be concentrated to one of the underlying pool assets. Additionally, dependence of the shape on the mint redeem bounds implies dependence on the oracles that contribute to the mint and redeem calculations. Relatively small oracle errors may be sufficient to affect the CFMM shape and hence the secondary market performance.

Once the secondary markets become sufficiently liquid, the pools comprising the markets could themselves be incorporated in a strictly risk-segregated manner into the reserve assets in the form of LP shares. This would serve to boost gyroscopic stablecoin secondary market liquidity and usage and possibly

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

[11] This could be implemented via a mechanism such as 'virtual reserves', which don't require liquidity providers to contribute to them (see, e.g., formulations in [16]), and could serve to improve the capital efficiency of the pool.

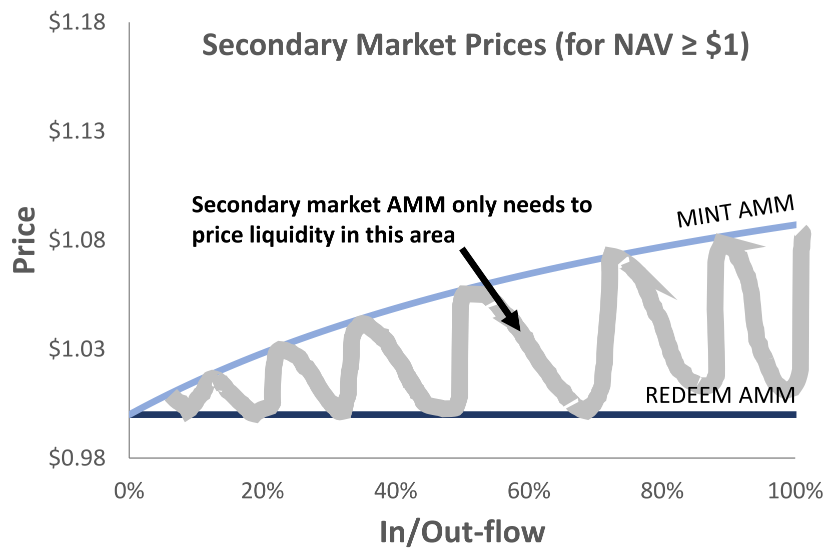

Figure 6: Secondary market AMM needs to price assets within the area between the primary market prices. Shown for NAV ≥ 1, but similar for NAV < 1.

further enhance stability.

3.6 Examples of Risk-Segregated Portfolio Structure

The following is a simple candidate portfolio structure for segregating tail risks, though not necessarily the best. It is constructed by stratifying the qualitative characterization of risks from [12]. The yield on rebate pools can be captured separately and rebalanced periodically with the larger portfolio.

References

[1] Angeris, G., and Chitra, T. Improved price oracles: Constant function market makers. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (2020), p. 80–91.

[2] Angeris, G., Kao, H.-T., Chiang, R., Noyes, C., and Chitra, T. An analysis of uniswap markets. *Crypto Economic Systems 2020* (2020).

[3] Bouchey, P., Nemtchinov, V., Paulsen, A., and Stein, D. M. Volatility harvesting: Why does diversifying and rebalancing create portfolio growth? *The Journal of Wealth Management 15*, 2 (2012), 26–35.

Category	Vault	Assets
Custodial	Tether	Balancer pool: USDT / XAUt
	Trust Token	Balancer pool: TUSD / TGBP
	Paxos (US)	Balancer pool: PAX / PAXG
	Ex-US (kind of)	Balancer pool: USDC / EURS
Non-custodial	Maker-Compound	cDai recycling vault
	Maker	Balancer pool: Dai / ETH
	Synthetix	Balancer pool: sUSD / ETH
	Synthetix-Aave	aSUSD
	UMA	Balancer pool: fixed term uUSD rollover
	Empty Set Dollar	Balancer pool: ESD / ETH

Table 1: For illustration purposes only, each protocol may have significant risks, this just illustrates how these risks might be segregated.

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

[5] Evans, A. Liquidity provider returns in geometric mean markets. *arXiv preprint arXiv:2006.08806* (2020).

[6] Gudgeon, L., Perez, D., Harz, D., Livshits, B., and Gervais, A. The decentralized financial crisis. In *2020 Crypto Valley Conference on Blockchain Technology (CVCBT)* (2020), IEEE, pp. 1–15.

[7] Gudgeon, L., Werner, S., Perez, D., and Knottenbelt, W. J. Defi protocols for loanable funds: Interest rates, liquidity and market efficiency. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (2020), pp. 92–112.

[8] Hull, J., et al. *Options, futures and other derivatives/John C. Hull.* Upper Saddle River, NJ: Prentice Hall,, 2009.

[9] Kao, H.-T., Chitra, T., Chiang, R., and Morrow, J. An analysis of the market risk to participants in the compound protocol.

[10] Klages-Mundt, A. Proposal: a framework for designing better stablecoins. `https://github.com/aklamun/Stablecoin_grant_proposal_122018`, 2018.

[11] Klages-Mundt, A., Gudgeon, L., and Perez, D. Rainy day fund stablecoin. `https://www.initc3.org/events/2020-07-26-IC3-Blockchain-Camp.html`, 2020.

[12] Klages-Mundt, A., Harz, D., Gudgeon, L., Liu, J.-Y., and Minca, A. Stablecoins 2.0: Economic foundations and risk-based models. In *Proceedings of the 2nd ACM Conference on Advances in Financial Technologies* (2020), pp. 59–79.

[13] Klages-Mundt, A., and Minca, A. (in) stability for the blockchain: Deleveraging spirals and stablecoin attacks. *arXiv preprint arXiv:1906.02152* (2019).

[14] Klages-Mundt, A., and Minca, A. While stability lasts: A stochastic model of stablecoins. *arXiv preprint arXiv:2004.01304* (2020).

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

[16] Niemerg, A., Robinson, D., and Livnev, L. Yieldspace. `https://yield.is/YieldSpace.pdf`, 2020.

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

[18] Selgin, G. 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.