Gyroscopic Stablecoins: Lite Paper

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 accretion buffers to maintain stability. The accretion buffer serves as a growing store of '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 gyroscopic buffer 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. 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 crypto ecosystem.

1 Introduction

All stablecoins come with significant failure risks, as we characterize in [10]. 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 [11] and formally characterized them in [12]. These deleveraging spirals were later validated in Maker during the 'Black Thursday' crisis in March 2020.

As we suggest in [10], a design gap in current stablecoins is the incorporation of well-designed buffers to help survive transitory events. In [12], 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 leveraged-based stablecoins which preside today. In particular, in place of leveraged 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 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 toward 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 automated market maker (AMM) mechanisms in combination with gyroscopic buffers to maintain stability. The buffer 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 gyroscopic buffer deploys assets in ways that stratify risk across 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.

We briefly compare with some related stablecoin mechanisms before describing the class of gyroscopic mechanisms in detail in the next section. The design of gyroscopic stablecoins builds on our preliminary work in the first place project at the 2020 IC3 Bootcamp [9] and an early version in a 2018 proposal [8].

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 such constructions atop AMMs

[1]Note that constant product markets aren't the most efficient implmeentation 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.

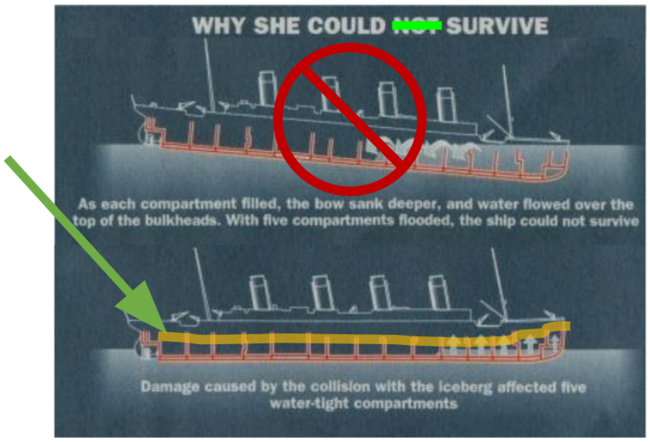


Figure 1

is that the failure of one (or a few) assets can cascade into failure of the entire basket via the exchange mechanism. 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 buffer 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 buffer's resources[2].

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'

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

holders. Instead, Maker's intended buffer is an auction of MKR, 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 three economic components. We illustrate this class of designs with concrete examples in the following section.

The *Gyroscopic Buffer* contains the assets backing the system. Creation of stablecoins adds to the buffer and redemption of stablecoins subtracts from the buffer. The buffer 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 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 buffer 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 buffer. 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 vs. buffer 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 buffer health and with the size of recent outflows to protect the buffer from exhaustion. In this way, the system can still function even if buffer value per stablecoin is less than \$1. The stablecoin minting AMM incorporates a 'value of systemic insurance' from the health of the buffer and the effects of minting on buffer dilution per stablecoin in addition to the target \$1 value.

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

2.1 Risk Segregation in the Buffer

Portfolio risk segregation incorporates recent work on stablecoin risks [10, 11, 12], Protocols for Loanable Funds (PLFs) [4, 5, 7], and Constant Function Market Makers (CFMMs) [1, 2, 3]. 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 buffer 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. For underlying asset risks, we draw on our work in [10]. 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.

- *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. 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, 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.

- *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 a dynamic mint/redeem fee. This can be thought of akin to ETF arbitrage: if the secondary market deviates too much from net asset value, then it will be profitable to route orders through the primary market (by creating/redeeming stablecoins). Normally, this 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 fee captures the ETF arbitrage value.

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 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 buffer system is most important. The minting fee is designed to account for this value of insurance and to price in the dilutionary effect of minting on buffer value per stablecoin.

2.3 Governance

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

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

The question of governance design builds on research questions discussed in [10]. 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.

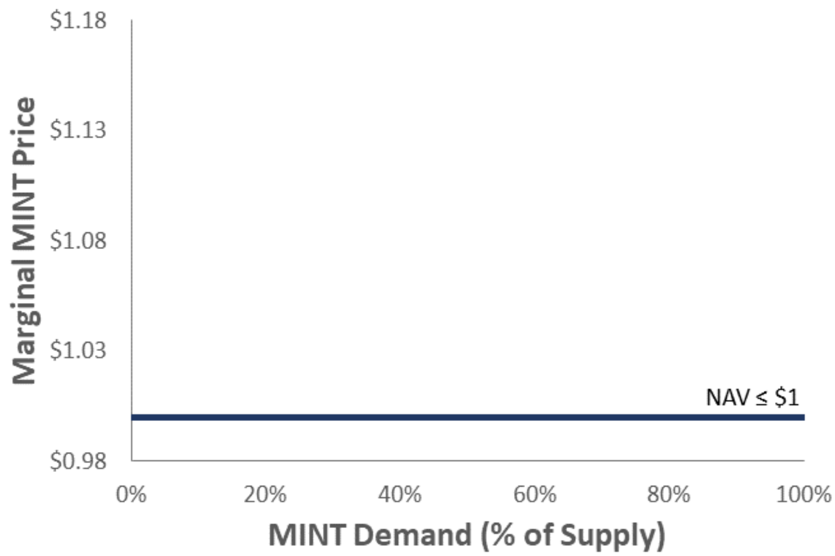
3 Examples of Gyroscopic Designs

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 functions

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

where $x =$ the number of stablecoins to redeem, $y =$ the buffer dollar value per stablecoin issued, $z =$ other system state variables, and the outputs of f, g are in dollar value of buffer assets.

[insert a bit about the general idea of g, e.g., using log utility to formulate a price of insurance]



3.1 Design A ∼ 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 buffer 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 [8, 9].

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 buffer. This is like harnessing future cash flows to fill the buffer as opposed to accruing past cash flows.
- Rainy day fund 'insurance' can be separable from the stablecoin 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

$$f(x, y) = x \min(1, y) \quad \text{(minus a possible fee).}$$

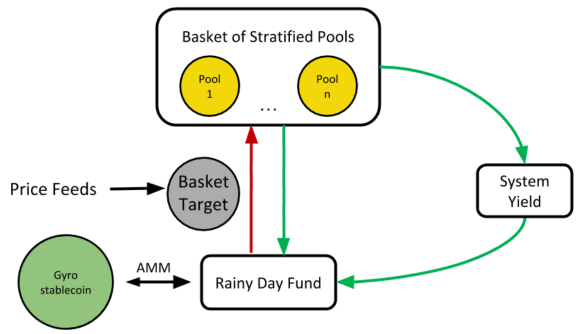


Figure 2

3.2 Design B $\sim$ money market fund with pegged redemption

In Design B, the buffer 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 buffer assets, subject to a possible devaluation/peg break, and vice versa accounting for the insurance value of healthy buffer. The buffer grows as yield is earned in the portfolio. The excess value of the buffer can be interpreted akin the rainy day fund in Design A, which serves as a continously smooth the buffer 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', see e.g., [13]). As in Design A, similar twists are available on the rainy day fund formulation.

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

3.3 Design C $\sim$ currency peg model

Design C resembles the previous designs in effect but with a more flexible structure. The buffer 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 in the buffer assets. A stablecoin can be redeemed through the primary market AMM that scales the redemption rate based on net outflows and buffer value per stablecoin. Under normal conditions (e.g., low net outflow), redemption value is \$1 (minus possible fee). Under crisis events, redemption value may be flexible below \$1. For instance, it could scale as a function of net outflows down to the buffer value per stablecoin, if less than \$1. This has the effect of preserving buffer health and incentivizing redeemers to wait to redeem at better prices later.

Under this design, the buffer 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., [6]). In effect, this works by setting up game theoretic incentives among stablecoin holders to coordinate on \$1 value for the stablecoin supposing the buffer is of a sufficient size and the stablecoin itself is economically usable. Note that the design still aims to be fully (or over-) collateralized long-term.

A particular concern for the primary market AMM design is: when redemptions are allwoed at values greater than the buffer value per stablecoin, then the AMM needs to be robust to economic attacks against the peg by depleting the buffer. 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[3] formulation of the AMM redemption function could look like

$$f(x, y, z) = x \max\Big(\text{decay function}(x, z), \min(1, y)\Big),$$

where the decay function decays from 1 and depends on system state z such as historical outflows. [some better but more complex redemption function examples will be provided in an accompanying Jupyter notebook]

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

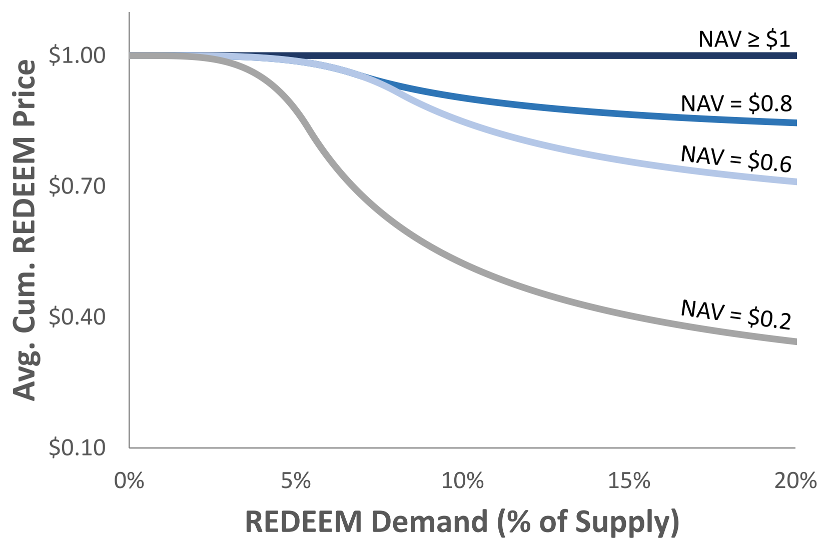


Figure 3: Average cumulative redeem price through primary market AMM starting at 0 local outflow

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

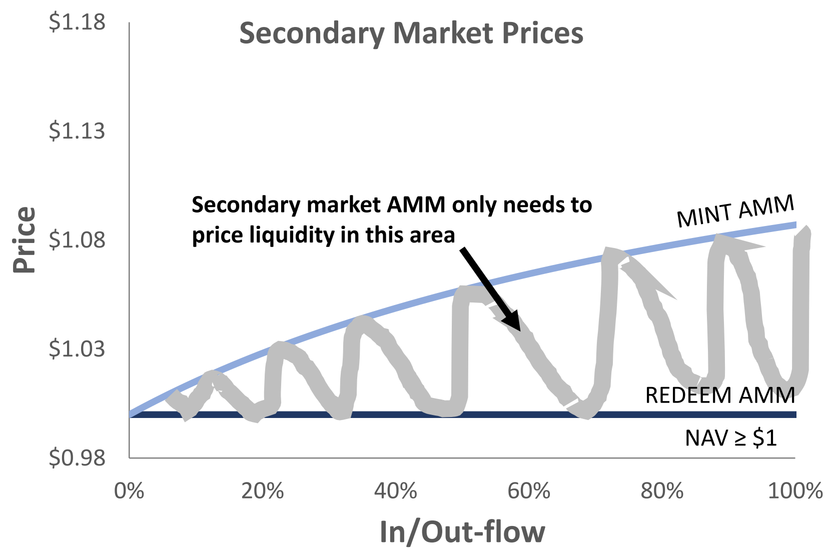


Figure 4: For NAV ≥ 1. Similar for NAV < 1.

under-collateralized buffer, and structure can gradually shift to the long-term dynamics envisioned.

3.4 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 [10]. The yield on rebate pools can be captured separately and rebalanced periodically with the larger portfolio.

4 Implementation Specs

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

Category	Vault	Assets
Custodial	Tether	Balancer pool: USDT / XAUt
	US-based	Balancer pool: TUSD / TGBP
	US-based Paxos	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] 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.

[5] 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.

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

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

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

[9] 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.

[10] 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.

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

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

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