Short Paper: Stablecoin Risks and Design

Ariah Klages-Mundt

Sep. 2019

Abstract

Non-custodial stablecoins backed by cryptocurrencies have become popular methods for bootstrapping price stability on public blockchains. We introduce a model of these systems and explore liquidity, deleveraging, and interest rates. We demonstrate that deleveraging feedback effects can exacerbate collateral drawdown. These insights are consistent with historical stablecoin movements. From these insights, we suggest design improvements that aim to improve long-term stability. We also introduce new attacks that exploit arbitrage-like opportunities around stablecoin liquidations. Using our model, we demonstrate that these can be profitable. These attacks may induce volatility in the 'stable' asset and cause perverse incentives for miners, posing risks to blockchain consensus.

1 Introduction

A stablecoin, often referred to as the "holy grail of crypto", is a cryptocurrency with added economic structure that aims to stabilize price/purchasing power. Stablecoins are meant to bootstrap price stability into cryptocurrencies as a stop-gap measure for adoption. Current projects are either *custodial* and rely on custodians to hold reserve assets off-chain (e.g., $1 per coin) or *non-custodial* and set up a risk transfer market through on-chain contracts. Non-custodial stablecoins aim to retain the property of reduced counterparty/censorship risk.

Non-custodial stablecoins transfer risk from stablecoin holders to speculators, who hold leveraged collateralized positions in cryptocurrencies.[1] A dynamic deleveraging process balances positions if collateral value deviates too much, as determined by a price oracle. This is similar to a tranche structure, in which stablecoins act like senior debt, with the addition of dynamic deleveraging. Two major risks in these stablecoins emerge around market structure collapse and oracle/governance manipulation. The effects of these risks are witnessed in bitUSD, Steem Dollars, and NuBits, which have suffered serious depegging events in 2018, and Terra and Synthetix, which suffered oracle attacks in 2019. Other designs, such as Dai [**?**], share similar design characteristics. Stablecoins currently serve as a central role in an increasingly complex decentralized finance environment, involving composability with crypto lending protocols.

[1] 'Leverage' means that speculators holds $> 1\times$ initial assets but face new liabilities.

In this paper, we introduce a simple model of a non-custodial stablecoin and explore design considerations based on this model. We develop design insights on deleveraging risks in stablecoin markets, which can exacerbate collateral drawdown in stablecoins, demonstrate profitable bets that can be made on stablecoin liquidation events, and describe profitable attacks that can induce stablecoin volatility and incentivize blockchain consensus reorganizations.

1.1 Relation to Prior Work

With the exception of [?], there is little rigorous mathematical work on non-custodial stablecoins. They apply option pricing theory to value tranches in a proposed stablecoin using PDE methods. In doing so, they need the simplifying assumption that payouts (e.g., from liquidations) are exogenously stable, whereas they are actually made in ETH and can cause price feedback effects in the stable asset. In particular, stablecoin holders either hold market risk or are required to re-buy into a reduced stablecoin market following liquidations. This motivates our model to understand stablecoin feedback effects.

Stablecoins share similarities with currency peg models, e.g., [?] and [?]. In these models, the government plays a mechanical market making role to seek stability and is not a player in the game. In contrast, in non-custodial stablecoins, decentralized speculators take the market making role. They issue/withdraw stablecoins to optimize profits and are not committed to maintaining a peg. In a stablecoin, the best we can hope is that the protocol is well-designed and that the peg is maintained with high probability through incentives. A fully strategic model would be a complicated (and likely intractable) dynamic game.

Our model resembles classical market microstructure models (e.g., [?]); it is a multi-period system with agents subject to leverage constraints that take recurring actions according to their objectives. In contrast, the stablecoin setting has no exogenously stable asset that is efficiently and instantly available. Instead, agents make decisions that endogenously affect the price of the 'stable' asset and affect futures incentives.

2 Model and Dynamics

We introduce a simple stablecoin model, inspired by [?], and describe its dynamics. A more expansive mathematical model and derivation of analytical results will be submitted elsewhere and is considered separate from this paper.

2.1 Model

The model contains a stablecoin market and two assets with prices measured in USD. ETH is a risky asset with exogenous prices p_t^E and STBL is an ETH-collateralized stablecoin with endogenous price p_t^D. The stablecoin market connects stablecoin holders, who seek stability, and speculators, who make leveraged bets backing STBL. The STBL protocol requires the STBL supply be over-collateralized in ETH by a factor of β.

In order to focus on the effects of speculator decisions in this paper, we simplify the stablecoin holder demand as exogenous. At time t, $\mathcal{D}_t$ is the quantity demanded of STBL at \$1 price. The quantity demanded changes with price subject to a constant price elasticity $-\gamma$. For simplicity, we take the exogenous demand to be constant $\mathcal{D}$ over time and $\gamma = 1$. In this case, demand is constant in dollar terms. Stablecoin holders can only redeem for ETH in global settlement.

A speculator, Alice, has ETH locked in the system and decides the STBL supply, which represents a liability against her collateral. At the start of step t, there are $\mathcal{L}_{t-t}$ STBL coins in supply; Alice holds n_{t-1} ETH and chooses to change the STBL supply by Δ_t ($\mathcal{L}_t = \mathcal{L}_{t-1} + \Delta_t$). If $\Delta_t > 0$, Alice sells new STBL on the market for ETH at the market clearing price p_t^D, which is added to n_t. If $\Delta_t < 0$, Alice uses ETH to buy STBL on the market, reducing n_t. To decide Δ_t, Alice optimizes next period expected equity based on her expectations and subject to the collateral constraint of STBL. For simplicity, we treat Alice's expected ETH return as constant r. Then, Alice optimizes

$$\max_{\Delta_t} \quad r n_t p_t^E - (\mathcal{L}_{t-1} + \Delta_t) \tag{1}$$

$$\text{s.t.} \quad n_t p_t^E \geq \beta(\mathcal{L}_{t-1} + \Delta_t). \tag{2}$$

Notice that n_t depends on Δ_t through the clearing price p_t^D.

We suggest that this optimization is a candidate for 'honest' behavior of a STBL speculator as it is consistent with Alice acting on perceived arbitrage in mispricings of STBL from the peg. In essence, Alice expects to increase (reduce) leverage 'at a discount' when p_t^D is above (below) target. This is the typically cited mechanism by which these systems maintain their peg and thus how the designers *intend* for speculators to behave. However, this assumes that p_t^D is sufficiently stable/mean-reverting to \$1 and so this behavior may not in fact be a best response. We consider a wider range of behaviors in a companion paper.

Given supply and demand, the STBL market clears by setting demand equal to supply in dollar terms. This yields the clearing price $p_t^D = \frac{\mathcal{D}_t}{\mathcal{L}_t}$. This clearing equation is related to the quantity theory of money and is similar to the clearing on the Uniswap decentralized exchange (DEX) [**?**] but processed in batch.

In our examples, we use the following parameter setup: $\beta = 1.5$ (value used in Dai), $r = 1.00583$ (historical daily ETH return 2017-18), $\mathcal{L}_0 = 100 \cdot r$, $n_0 = 1.8$, $\mathcal{D} = 100$. The setup is a steady state in the stable region, described in Result **??**.

2.2 Model Dynamics

In a companion paper, we derive analytical results about dynamics in this model. We summarize these here to the extent that we use them.

Result 1. *The speculator (Alice) faces limits to how quickly she can reduce leverage, conceptually because the clearing price* $p_t^D = \frac{\mathcal{D}_t}{\mathcal{L}_{t-1}+\Delta_t}$ *increases with* Δ_t.

Result 2. *If the speculator's (Alice) collateral constraint remains unbinding, the system converges to steady state with stable price, zero variance, and $\mathcal{L}_t \to \mathcal{D}r$.*

2.3 Expanded Model: Adding an Attacker

Expanding the model from our companion paper, we additionally consider an agent Bob, who can speculatively enter/exit the STBL market. Bob can buy δ dollar-value of STBL at some time t with the goal of selling it at a later time s for $\delta + \varepsilon$. These occurrences change the demand structure: $\mathcal{D}_t = \mathcal{D} + \delta$, $\mathcal{D}_s = \mathcal{D} - (\delta + \varepsilon)$.

3 Stablecoin Design Considerations

3.1 Deleveraging Affects Collateral Drawdown

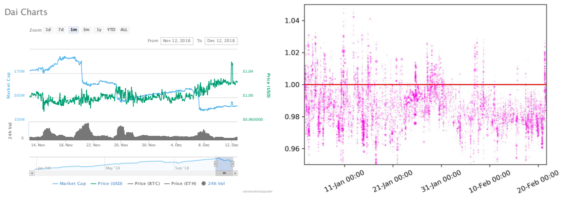
Result **??** causes a STBL market price effect from leverage reduction. This can lead to a *deleveraging spiral*, in which Alice repurchases STBL to reduce leverage at increasing prices as liquidity dries up. More collateral needs to be sold to achieve deleveraging, leaving less in the system. Subsequent deleveraging becomes more difficult as the price effects compound.

The following example illustrates a deleveraging spiral. The system starts in a steady state. Then ETH price declines trigger three waves of liquidations, forcing Alice to liquidate her collateral to deleverage at rising costs.

t	p_t^E	Δ_t	$\mathcal{L}_t$	p_t^D	n_t
0	85		100.583	0.994	1.8
1	83	-3.115	97.468	1.026	1.761
2	82	-4.105	93.363	1.071	1.708
3	81	-4.57	88.793	1.126	1.644

One might think the spiral effect is good for stablecoin holders. As we explore in the next section, this can be the case for a short-term trade. However, it siphons off collateral value, which can be detrimental longterm. Building on Result **??**, the deleveraging spiral can cause volatility to be bounded above 0 with high probability outside of the stable region. The deleveraging spiral can cause a 'kink' in the probability distribution at the boundary of the stable region: once outside, the system can be more likely to remain outside.

Moving beyond our simplified model, note that a deleveraging spiral will occur unless outside demand reduces accordingly. For instance, if demand (in USD terms) decreases by $d(p_1^D)$ at price p_1^D (e.g., if demand is elastic with $\gamma > 1$), then a deleveraging spiral occurs when $\frac{d(p_1^D)}{\Delta_1(d)} > \frac{\mathcal{D}}{\mathcal{L}_0}$. Higher elasticity is expected if there are good substitutes for STBL–e.g., other stablecoins that avoid these problems. The deleveraging spiral can also be interpreted (and potentially modeled) in terms of value of price insurance. During downturns, this insurance may come at a premium if demand is not very elastic.



(a) (b)

Figure 1: Data from Dai market. (a) Deleveraging feedback Nov-Dec 2018 (coinmarketcap). (b) Dai DEX market prices (image from Kenny Rowe, Tweet).

This suggests the question: do alternative non-custodial designs suffer similar deleveraging problems? We compare to an alternative design described in [?]. In this design, the stablecoin is restricted to pre-defined leverage bounds, at which algorithmic 'resets' partially liquidate both stablecoin holder and speculator positions at $1 price. While this quells the price effect on collateral, it *shifts* the deleveraging risk from speculator to stablecoin holder. The stablecoin holder is liquidated at $1 price but, if they want to maintain a stablecoin position, they have to re-buy in to a smaller market at inflated price. Of the many designs, it is unclear which deleveraging method would lead to a system that survives longer.

A preliminary analysis of Dai market data suggests that our results apply. Figure **??** shows the Dai price appreciate in Nov-Dec 2018 during multiple large supply decreases. Figure **??** shows trading data from multiple DEXs over Jan-Feb 2019; price spikes occur in the data from speculator liquidations.

3.2 Interest Rates

Result **??** suggests that STBL will trade below $1 in the stable region when $r > 1$. This is empirically seen in Figure **??**. An interest rate charged to speculators can balance the market (the 'stability fee' in Dai). This can temper expectations by reducing r. In the stable steady state, setting the interest rate to offset the average expected ETH return will achieve the price target. However, this is practically difficult as r changes over time and is difficult to measure accurately. It also depends on holding periods of speculators. It is an open question how to target these fees in a way that maintains long-term stability.

3.3 Potential Design Mitigations

In the case of Dai, our results suggest some design improvements. These focus on widening the stable domain and lessening the severity of the unstable domain.

A good mechanism of fees may quell deleveraging spirals. Dai imposes fees on speculators when they liquidate positions (e.g., liquidation penalty, stability fee, penalty ratio). These can *amplify* deleveraging spirals by increasing deleveraging costs and disincentivizing new capital from entering the system during crises. Counter-cyclic fees could widen Dai's stable domain by reducing feedback effects. Dynamic fees tuned to inflow/outflow could additionally disincentivize herd behavior to deleverage at the same time.

Different 'collateral of last resort' use. In Dai, MKR serves a 'last resort' role in addition to governance. If collateral is insufficient to cover Dai liabilities in global settlement, MKR makes up the difference supposing the MKR market is liquid enough to do so. This may place an incentive on MKR to trigger global settlement early, at the expense of stablecoin holders, if they expect a successful relaunch of Dai after the crisis. Incentives may be better aligned if the 'last resort' role of MKR is alternatively to quell deleveraging spirals. This could be achieved by automatically positioning the MKR supply as collateral to expand Dai supply in crises.

Remark on oracle risks: Dai relies on a price oracle, which is chosen by MKR holders, who also determine who can trigger global settlement.[2] This opens an attack in which MKR holders can invest in one side of the system (Dai or leveraged positions), manipulate the oracle, and trigger global settlement at unfavorable rates to the other side and extract the collateral for themselves. Dai's oracle protections–price feed delay and maximum hourly price change–don't necessarily protect against this. However, one might expect market forces to make the MKR price match the cost of pulling off this attack (e.g., by buying or borrowing MKR) as otherwise the attack cashflow could be triggered. The MKR security may not rely on large fee revenue, thus the fee revenue may have a better use.

Uses of limited fee revenue. Dai produces limited fee revenue, most of which rewards MKR investors. A Dai savings rate has also been proposed to reward Dai holders as another tool to balance the Dai market. There is an inherent trade-off in using fee revenue. A Dai savings rate uses this revenue to improve stability in the stable domain. Alternatively, fee revenue can be channeled to an emergency fund that lessens the severity of the unstable domain.

4 Stablecoin Attacks

Attacking a stablecoin is different than traditional currency attacks. The focus is not on breaking the willingness of the central bank to maintain a peg. It instead involves manipulating the interaction of agents. We show that stablecoin design can enable profitable trades against stability that attack the system. These come from the existence of profitable trades around liquidations and the ability of miners to reorder transactions to extract value.

[2] Although, notably in the current Dai, these are controlled by a Maker Foundation multisig and most MKR is reputedly held by a few Maker individuals.

4.1 Profitable bets on liquidations

The following example demonstrates a profitable bet on a liquidation. Bob injects $\delta = 1$ in demand at $t = 1$, which acquires 1.0008 STBL coins at p_1^D. In $t = 3$, after the liquidation, Bob is then able to extract $\delta + \varepsilon = 1.083$ from selling the STBL coins. This yields a return of 8.3%. This is akin to a short squeeze on existing speculators. It takes advantage of the fact that liquidations occur at STBL market rate, which in turn affects the market rate.

t	p_t^E	$\delta + \varepsilon$	$\mathcal{D}_t$	Δ_t	$\mathcal{L}_t$	p_t^D	n_t
0	85		100		100.583	0.994	1.8
1	85	+1	101	0.502	101.085	0.999	1.806
2	82		101	−8.716	92.369	1.093	1.690
3	82	−1.083	99.917		92.369	1.082	1.689

Bob can do better by choosing δ, ε to maximize ε subject to $\frac{\delta+\epsilon}{p_2^D} \leq \frac{\delta}{p_o^D}$. Choosing $\delta = 4.5, \varepsilon = 0.59$ (not optimal) yields a return of 13%. He could also spread out δ over a longer period of time to achieve lower purchase prices.

From a practical perspective, the optimization is sensitive to misestimation of demand elasticity. While Dai has hit prices as high as \$1.37 historically (source: coinmarketcap), it hasn't typically reached prices above \$1.09. Thus smaller bets (relative to supply) may be safer. Regardless, these can be large opportunities in large systems. In addition, outside of this model, real implementations create arbitrage of $5 - 13\%$ to automate liquidations.

4.2 Attacks

Attack 1: Bob bets on an ETH decline and manipulates the market to trigger and profit from spiraling liquidations. This uses the short squeeze-like trades in the previous example. It can also be supplemented with a bribe to miners to freeze collateral top-ups. Bob could also enter as a new speculator at the high STBL prices after the attack and thus leverage up at a discount. Outside of the model, the attack may have a negative effect on the long-term STBL demand due to the induced volatility. This can be further beneficial to Bob, who can then also deleverage in the future at a discount.

Attack 2: Bob is a miner and reorgs the last part of the blockchain following an ETH decline to trigger and profit from spiraling liquidations. In the reorg, Bob creates a new timeline that inherits the ETH price trajectory (via oracle transactions). Bob can then censor speculator transactions (e.g., collateral top-ups) to trigger new liquidations and extract profit around all liquidations, which are guaranteed in the timeline. If the stablecoin system is large, the miner extractable value can be large (and is additive with other sources of extractable value). This creates the perverse incentive for miners to perform this attack if the attack rewards are greater than lost mining rewards. This is similar to the time-bandit attack in [**?**].

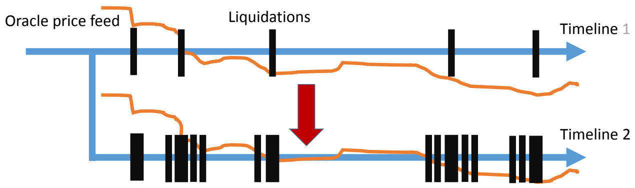


Figure 2: Attack 2, Bob reorgs the blockchain to extract value.

In Attack 1, Bob takes on market risk as the payoff relies on a future ETH decline and liquidation. It is a speculative attack that can induce volatility in the stablecoin. In Attack 2, Bob's payoffs are guaranteed if the reorg is successful. These payoffs incentivize blockchain consensus attack. A possible equilibrium is for miners to collude and share this value.

These attacks occur in a permissionless setting, in which agents can enter/exit at any time with a degree of anonymity. While in traditional finance, market manipulation rules can be enforced legally, in decentralized finance, enforcement is only possible to the extent that it can be codified within the protocol and incentive structure. We leave to future study a full exploration of these incentive structures in a game theoretic setting based on foundations set in, e.g., [**?**].

We discuss some preliminary ideas toward mitigating attack potential. Liquidations could be spread over a longer time period. This could potentially lessen deleveraging spirals by smoothing demand and increase the costs to reorg attacks. However, it presents a trade-off in that slow liquidations come with higher risks to the stablecoin becoming under-collateralized. We also suggest tying oracle prices and DEX transactions to recent block history so that a reorg attack can't easily inherit price and exchange history. Practically, however, this may be difficult to tune in a way that's not disruptive as small reorgs happen normally.

5 Discussion

In general, it is impossible to build a stablecoin without significant risks. As speculators participate by making leveraged bets, there is always an undiversifiable cryptocurrency risk. However, a stablecoin can aim to be an effective store of value assuming the cryptocurrency market as a whole is not undermined. In this case, it is *conceivable* to sustain a dollar peg if the stablecoin survives transitory extreme events. That is, to achieve long-term probabilistic stability, a stablecoin should maintain a high probability of exiting its unstable domain.

In this paper, we characterized deleveraging spirals that can exacerbate collateral drawdown in stablecoins, demonstrated profitable bets that can be made on stablecoin liquidation events, and described a speculative attack that can induce stablecoin volatility and a blockchain consensus attack that is incentivized by the stablecoin system. We also discussed design considerations around interest/fee mechanisms and last resort insurance for quelling deleveraging spirals and preliminary ideas for mitigating attacks.

The model we build in this paper is very simple, which allows us to understand dynamics and uncover attack vectors. A natural question is whether the 'honest behavior' intended by designers is really a best response for speculators. This motivates follow-up work to look at longer-term strategies of interacting speculators.

References

[1] MakerDAO. The Dai stablecoin system. Dai Whitepaper. `https://makerdao.com/whitepaper/Dai-Whitepaper-Dec17-en.pdf` (2017)

[2] Chao, Y., Dai, M., Kou, S., Li, L., Yang, C. Designing stable coins. Duo Whitepaper. `https://duo.network/papers/duo_academic_white_paper.pdf` (2018)

[3] Morris, S., Shin, H.S. Unique equilibrium in a model of self-fulfilling currency attacks. *American Economic Review*, 88(3):587–597 (1998)

[4] Guimaraes, B., Morris, S. Risk and Wealth in a Model of Self-Fulfilling Currency Attacks. *Journal of Monetary Economics*, 54(8):2205-2230 (2007)

[5] O'Hara, M. Market Microstructure Theory, Basil Blackwell, Cambridge, MA (1995)

[6] Aymanns, C., Farmer, D.J. The dynamics of the leverage cycle. *Journal of Economic Dynamics & Control*, 50:155–179 (2015)

[7] Zhang, Y., Chen, X., Park, D. Formal Specification of Constant Product ($x \times y = k$) Market Maker Model and Implementation. `https://github.com/runtimeverification/verified-smart-contracts/blob/uniswap/uniswap/x-y-k.pdf` (2018)

[8] Daian, P., Goldfeder, S., Kell, T., Li, Y., Zhao, X., Bentov, I., Breidenbach, L., Juels, A. Flash boys 2.0: frontrunning, transaction reordering, and consensus instability in decentralized exchanges. Preprint on arXiv. (2019)

[9] Biais, B., Bisiere, C., Bouvard, M., Casamatta, C. The blockchain folk theorem. Swiss Finance Institute Research Paper No. 17-75 (2018)