What Drives the (In)stability of a Stablecoin?

***Abstract*—In May 2022, an apparent speculative attack, followed by market panic, led to the precipitous downfall of UST, one of the most popular stablecoins at that time. However, UST is not the only stablecoin to have been depegged in the past. Designing resilient and long-term stable coins, therefore, appears to present a hard challenge. To further scrutinize existing stablecoin designs and ultimately lead to more robust systems, we need to understand where volatility emerges. Our work provides a game-theoretical model aiming to help identify why stablecoins suffer from a depeg. This game-theoretical model reveals that stablecoins have different price equilibria depending on the coin's architecture and mechanism to minimize volatility. Moreover, our theory is supported by extensive empirical data, spanning 1 year. To that end, we collect daily prices for 22 stablecoins and on-chain data from five blockchains including the Ethereum and the Terra blockchain.**

***Index Terms*—Stablecoin, Price Instability, Financial Risks**

I. Introduction

Stablecoins aim to provide stable value by minimizing price fluctuations, often by pegging to fiat currencies like the US Dollar. To this end, they can adopt a pegging mechanism similar to a traditional pegged currency where the central bank adjusts the market supply and demand to attain the target exchange rate by holding foreign reserves that can be exchanged for national currency [1]. However, the blockchain use of a stablecoin diversifies a stablecoin design, allowing for a more progressive, albeit often complicated, pegging mechanism. They can rely on cryptocurrencies to maintain the peg, and some stablecoins even attempt to stabilize a price without relying on reserves consisting of exogenous assets.[1]

The primary pegging mechanism for stablecoins involves users buying or selling them at a price close to the target (e.g., 1 USD) to maintain stability. If the market price varies from the target, users can engage in arbitrage between the stablecoin system and secondary markets. Therefore, the stablecoin systems need to hold reserves. *Collateralized stablecoins* use reserves of exogenous assets for backing and come in two types depending on the asset type: fiat-collateralized and crypto-collateralized. On the other hand, *Algorithmic* stablecoins use endogenous cryptocurrencies.

Stablecoins can also be integrated with lending systems, known as *over-collateralized* stablecoins. Here, users deposit more collateral than the value of stablecoins they receive, essentially incurring debt. They can retrieve their collateral upon repaying the stablecoins. If the collateral's value drops, risking bad debt, other users can liquidate the position by repaying the stablecoins and claiming the collateral. This system encourages buying stablecoins at a lower price if the market price falls below the target, helping realign the market price with the peg.

In fact, a crypto-collateralized stablecoin is a term often associated with a broad categorization of any stablecoin backed by cryptocurrencies. However, in this study, we further partition this broad categorization based on how redemption takes place. In other words, we differentiate between crypto-collateralized and over-collateralized stablecoins while both use cryptocurrencies as collateral; crypto-collateralized stablecoins purchase and sell stablecoins to users at a target price to maintain the peg. On the other hand, over-collateralized systems apply a lending system.

Although stablecoins are designed for relative price stability, their designs contain weaknesses that may threaten price stability, and price history shows that it is quite common for pegs to break. The Terra stablecoin (UST), one of the most representative algorithmic stablecoins, collapsed in the second week of May 2022 [2, 3]. As an algorithmic stablecoin, Terra uses an endogenous cryptocurrency, Luna, to maintain the peg of UST at 1 USD; the system mints 1 USD worth of Luna to the users for each UST they redeem to the system. Therefore, if the market price of UST falls below 1 USD, users should sell their coins to the system instead of the market for a higher profit. However, this redemption process has a risk; it inflates the market with the minted Luna, driving the price of Luna down and making each subsequent UST redemption mint even more Luna. As a result, a significant deviation from the target price could lead to a larger deviation. Another example of a USD-pegged stablecoin is Tether, where there have been doubts regarding the reserve coverage, raising concerns about bank run risks [4, 5].

1) Implications of our work: The statistically observed difference in price volatility of stablecoins [6] and several collapse events including Terra UST beg the question of how mechanism design choices get translated into stablecoin price stability. Currently, it is unclear how and to what extent these design-dependent risks are reflected in the actual stablecoin price stability. Bearing the risks does not necessarily directly lead to actual price instability. For example, although many people point out a bank run risk[2] of Tether, we also often observe that it did not significantly affect its price in the real world. Even when Tether was fined multiple times due to some evidence that may suggest holding partial reserves, its price was still around $1. Indeed, in general, fiat-collateralized stablecoins that store reserves in fiat money are regarded as more stable assets than other stablecoin types [6]. In contrast, many crypto-collateralized stablecoins that hold collateral in cryptocurrencies often depreciate below $1 and return more slowly to the pegging state. In particular, considering when UST depegged, unlike the Tether case at that time, UST could not quickly return to the peg even though the market cap of Luna, which is the asset backing it, exceeded its market cap in the early stage of the catastrophic event [2, 3, 7, 8]. These suggest that the relationship between design risks and

[1]It refers to assets that are run independently of the stablecoin system. For example, Bitcoin and Ethereum.

[2]It can be triggered by a lack of reserves stored by a stablecoin system.

price instability is not straightforward, which makes it hard to understand their inherent relationship clearly.

The goal of this work is to assist in developing a solid, common theory that can model the relationship between stablecoin designs and price volatility and further compare the effects of their design differences. Our work helps to understand why stablecoins show different price volatility by modeling them in a common framework, taking into account the difference in asset types that various stablecoin systems use to purchase coins from users. The type of asset paid to users by a system can matter; a volatile asset can lower the user's recognized payment value due to a price fluctuation during the payment transaction process. We show that this factor would significantly affect a level of stablecoin price stability.

2) Related work: While many works [4, 5, 9, 10, 11] have analyzed the systematic risks of different stablecoin designs, models explaining the price (in)stability of stablecoins are relatively sparse. Note that having risk in a stablecoin design does not always lead to price drops (e.g., the Tether case), and thus, studying systemic risks alone may not be sufficient to understand stablecoins. [12, 13] model some stablecoins like DAI. [1] models how stablecoins backed by 100% reserves, such as USDC, maintain price stability through arbitrage with minting and redemption. [14] explains a shape of redemption curves of several stablecoins.

Existing attempts to elucidate stablecoin price (in)stability are limited, and generalizing these models is challenging due to the diverse designs of stablecoins. Moreover, various distinctions within stablecoin models, such as the differences in reserve assets, are not as well-developed. A common framework for analyzing stablecoin price stability would not only aid in understanding the link between design and stability but also allow for comparisons across various stablecoin types. Additionally, there's potential to refine this model to more accurately reflect the subtle differences among stablecoin categories. Our approach involves developing a flexible model capable of analyzing redemption mechanisms across different stablecoin types.

II. Base Model

In this section, we model a stablecoin system using a game-theoretical framework. Based on the stablecoin model, we will analyze four types of stablecoins and quantify their price (in)stability degrees later. We first present Table I that summarizes the parameters used throughout the paper.

A. Game-theoretical framework

If a stablecoin is to be pegged at 1, the pegging state is defined as $p^s = 1$, where p^s indicates the current market price of the stablecoin. A pegging mechanism of the stablecoin system intervenes in the exchange market to maintain the peg. Considering that many stablecoins are currently suffering from downward price instability rather than upward price instability, in this paper, we focus on the mechanism that recovers a price when a stablecoin depreciates below 1. If the price falls below 1, the mechanism tries to decrease market supply and increase market demand by incentivizing users not to sell and to buy stablecoins in the market. Thus, designing a proper payoff function of users would be a key to achieving price stability. Note that we will not consider that the stablecoin system can halt the exchange market like a circuit breaker.

Notation	Definition
θ	A state of fundamentals
$e(\theta)$	A reached stablecoin price for given economic state θ without any system intervention
M (or M')	The total quantity of coins that users choose to sell to the market at the moment (or in the future)
$p(M)$ (or $P(M')$)	A stablecoin price for given M (or M')
v (or v')	A value that the system pays users who redeem their stablecoins at the moment (or in the future)
$i(\cdot)$	An incentive function for users to keep holding their stablecoins
Q	The total quantity of coins whose users want to redeem at one point
V^f	The total value of fiat reserves in a fiat-collateralized stablecoin
c	A cryptocurrency used to back stablecoins in crypto-collateralized, algorithmic, and over-collateralized systems
p_u^c	c's price to which users refer
p_s^c	c's price to which the system assumes
$V^c(\theta)$	A total value of crypto reserves in crypto-collateralized stablecoins
$r^c(Q, \theta)$	A ratio between p_u^c and p_s^c
$D^L(\theta)$	The total quantity of stablecoins that users should redeem in the liquidation process of over-collateralized systems at one point
$D_{u_i}(\theta)$	The stablecoin debt of user u_i that did not enter the liquidation process in over-collateralized systems
$o(\theta)$	The system's estimated value of cryptocurrencies that an over-collateralized system pays to users who redeem their stablecoins

TABLE I: List of parameters

If a pegging mechanism functions effectively, p^s will eventually reach its target value of 1. However, in the absence of any system intervention in the market to adjust the coin price (i.e., if a pegging mechanism gives up a price recovery), its equilibrium price is determined by the economic characteristics, referred to as the fundamental state θ [15]. A higher value of θ signifies "stronger fundamentals". In other words, a high θ indicates a favorable economic condition where assets can appreciate. We express the coin price without system intervention as an increasing function $e(\theta)$ of θ, where the value of $e(\theta)$ is assumed to be always below 1.

We model a one-shot game. Users can transact their coins with each other in the exchange market and issue coins from or redeem them to the system according to the pegging mechanism. Because we focus on the mechanism that recovers a price below 1, it is enough to consider only redemption as an interaction between users and the system.

On the supply side, stablecoin holders can select their actions among 1) selling their coins in the market, 2) redeeming coins to the system, and 3) holding coins continuously. If they decide to sell coins to the market, their payoff would be the current stablecoin price p^s. If they choose to redeem coins to the system, they are paid a value v by the system, where v is characterized according to each stablecoin design. Lastly, when they keep holding their coins, their payoff depends on

2

the future value of the stablecoin and an incentive provided by the system for users to keep holding their stablecoins (e.g., savings interest for a stablecoin). Here, let $i(\cdot)$ denote an incentive function for users to keep holding stablecoins, and it has a stablecoin value as input of a function.[3] The future stablecoin value can be expressed as $\max\{p^{s\prime}, v'\}$, where $p^{s\prime}$ indicates the price at which users will trade coins in the market in the future and v' indicates the redemption value that users can get from the system when redeeming coins in the future.[4] As a result, the payoff of users who decided to keep holding their stablecoins can be expressed as $\max\{i(p^{s\prime}), i(v')\}$ (or it is also possible to be expressed as $i\left(\max\{p^{s\prime}, v'\}\right)$).[5] Note that $i(x)$ is equal to x when the system provides no incentive for users to keep their coins (e.g., zero savings interest). Meanwhile, the greater the incentives, the greater the value of the function i.

In terms of the demand side, potential buyers can select their actions among 1) not buying coins in the market (i.e., not joining the stablecoin market), 2) buying coins in the market and immediately redeeming the coins to the system, and 3) buying coins in the market and keeping the coins in their pocket. Note that their actions are done in the one-shot game. In fact, their payoff equals the above described payoff (of stablecoin holders) minus p^s. Specifically, if they decide not to buy coins, their payoff would be 0. On the other hand, if they decide to go for the second action, their payoff would be $v - p^s$. Lastly, if they choose the third action, their payoff would be $\max\{i(p^{s\prime}), i(v')\} - p^s$. Given this, the game analysis would be the same with considering only the payoff of stablecoin holders on the supply side. Therefore, for simplicity, we will consider only the payoff of stablecoin holders.

According to the basic economic theory, the stablecoin price is determined by the market supply and demand. In our model, the stablecoin price is expressed as a function of only the market supply from the above paragraph. The market supply is related to the set of all users who decide to sell their coins to the market. When M denotes the total quantity of coins that the users decide to sell to the market at the moment, p^s can be expressed as $p(M)$, where p indicates a decreasing function that converts from M to a price. Therefore, $p(M)$ would decrease and increase if more users choose to sell their coins in the market (i.e., an increase in M) and choose other actions (i.e., a decrease in M), respectively. Similarly, we will express the future stablecoin price $p^{s\prime}$ as $p(M')$, denoting the future market supply by M'. Lastly, we assume that $p(\cdot)$ is always equal to or less than 1 to focus on when a stablecoin depreciates below 1.

In summary, in our model, the payoff function of users is as follows.

$$\text{payoff} = \begin{cases} p(M)(= p^s) & \text{if they sell coins to the market,} \\ v & \text{if they redeem coins to the system,} \\ \max\{i(p(M')), i(v')\} & \text{if they keep holding coins} \end{cases} \quad (1)$$

B. A unique pegging equilibrium

To maintain a stablecoin's peg (i.e., $p(M) = 1$), it's crucial to set the values of v and v' appropriately, as these influence rational user decisions. To guarantee the peg, there should be a reachable, unique equilibrium in which $p(M) = 1$. Here, that the state $p(M) = x$ is an *equilibrium* indicates that a user's rational decision on whether to keep or change its action to increase their expected payoff cannot change the stablecoin price $p(M)$ (i.e., the stablecoin price is fixed at x). Moreover, we say the state is *reachable* if rational actions of users make the stablecoin price $p(M)$ return to x in the case where $p(M) \neq x$; for example, if $p(M)$ is less than x, rational users sell fewer coins to the market, which would recover $p(M)$ to x by decreasing a value of M.

A sound stablecoin system should choose a proper value of v and v' that equilibrates only the state $p(M) = 1$. The following theorem presents two sufficient conditions and one necessary condition to make the pegging state (i.e., $p(M) = 1$) the reachable and unique equilibrium.

Theorem 1: To have a reachable and unique equilibrium as $p(M) = 1$, *the following two conditions are sufficient:*

$$\max\{v, i(v'), i(p(M'))\} > p(M) \text{ if } p(M) < 1,$$

and

$$\max\{v, i(v'), i(p(M'))\} \geq 1 \text{ if } p(M) = 1.$$

Moreover, the first condition is necessary.

The theorem says that to ensure a unique pegging equilibrium, we must design a stablecoin as follows: having a sufficiently high v or v', or designing a (large) incentive function $i(\cdot)$ for users to keep holding their coins.

Consider when there is little incentive (i.e., $i(x) \approx x$). Then Theorem 1 implies that, to guarantee the peg, either v, v', or $p(M')$ must be greater than $p(M)$ for any $p(M) < 1$. In the case where the market price of the stablecoin is less than the target price, if v or v' is high enough to satisfy this, users would redeem their coins to the system or keep holding coins, instead of selling them now in the market, which decreases M and increases the market price. On the one hand, if users expect the stablecoin price to increase (i.e., $p(M') > p(M)$) due to the promising economic situation, they would keep holding coins rather than selling them immediately in the market, which also naturally increases the market price. However, recall that we assumed that the stablecoin price without any system intervention in the market is $e(\theta)$ (< 1) in Section II-A. Therefore, in this paper, we do not consider the situation where the price will naturally increase to 1 without any pegging mechanism by an economic uptrend.

However, this is not the only way to ensure a reachable and unique equilibrium as the state that $p(M) = 1$. If a system can

[3] For simplicity, we will omit a discount factor or time discounting because it does not significantly affect the results.

[4] Note that we omitted a time variable for simplicity.

[5] In fact, users cannot be sure about the future value of the stablecoin. Therefore, in a more advanced model setting, the expected payoff would be expressed as $\int_x i(x) f\left(\max\{p^{s\prime}, v'\} = x\right) dx$ (i.e., an expected value based on the user's expectation on the future stablecoin value), where $f(\max\{p^{s\prime}, v'\})$ is a probability density function based on user expectation on $\max\{p^{s\prime}, v'\}$. However, in this work, we simplify it, assuming users believe a specific value of the future stablecoin price for sure, because the simplification does not change the results and implications.

3

give users sufficient incentives to hold coins, it is also possible to, even with low v, v', and $p(M')$, make the pegging state the unique equilibrium. Note that with a high value of the function i, $i(v')$ and $i(p(M'))$ can be greater than $p(M)$. As great incentives, we can come up with large savings interest for a stablecoin. Intuitively, such incentives are conducive to a decrease in market supply necessary for a price increase. Due to the page limit, we omit the proof of Theorem 1. For details, please see our full paper [16].

III. Model for each stablecoin type

We describe how v is characterized in various types of stablecoins. Here, v and v' would be the same because all stablecoins analyzed in this paper have a pegging mechanism independent of time. First, to ease the reader's understanding, we start with an intuition justifying how we will represent each type of stablecoins with our base model.

A stablecoin system can pay users the target value (i.e., \$1) or more upon redemption to keep its price from dropping below this target. However, the actual value received by users can be less, depending on the type of assets used for payment. For example, consider a stablecoin system holding cryptocurrencies as reserves to maintain the peg. However, the high price volatility of cryptocurrencies can lead to unexpected events that threaten the stability of these stablecoin systems. Even if the systems were to reward a user with \$1 in cryptocurrency, the user might not end up receiving assets worth \$1. That is because there exist several challenges, such as delayed price oracles, as well as the sheer time difference between transaction creation and execution. The challenges cause payment value discrepancies between users and the system. Indeed, we have experienced stablecoins depegging permanently because their oracle update interval was set to 10 minutes (cf. Iron [17]). As a result, the stablecoin's price stability can be threatened if the collateral is a volatile asset.

If a system backs its stablecoin with higher-risk assets like endogenous cryptocurrencies, stability risks increase. The backing assets would receive greater downward market pressure from the stablecoin redemption process, which involves releasing these assets into the market. This can trigger liquidation spirals and market panics in reserve assets, rapidly devaluing the stablecoin. A notable instance was Luna's drastic price fall in the UST system during significant redemptions in May 2022. At that time, even though the Luna system paid users \$1 based on its Luna price oracle, users couldn't expect to earn \$1 due to a rapid decline in Luna's price.

With these intuitions in mind, we characterize v of various types of stablecoins. Table II summarizes v of stablecoins that will be described below.

Type	v
Fiat	1 if $Q \leq V^f$, otherwise V^f/Q
Crypto	$r^c(Q,\theta)$ if $Q \leq V^c(\theta)$, otherwise $r^c(Q,\theta) \cdot V^c(\theta)/Q$
Algo	$r^c(Q,\theta)$
Over	$r^c(Q,\theta) \cdot o(\theta)$ if $0 < D^L(\theta)$ or $0 < D_{u_i}(\theta)$, otherwise 0

TABLE II: v by stablecoin type

A. Fiat-collateralized stablecoins

We first look at fiat-collateralized stablecoins such as USDT and USDC. In these stablecoins, the system issues coins and purchases them from the market at 1 in fiat currency to achieve the peg. However, taking coins out of the market is possible only when the system's fiat reserves are not exhausted. We let Q and V^f denote the total quantity of coins whose holders want to redeem at one point and the total value of the fiat reserves at the moment, respectively. If $Q \leq V^f$, users can always be paid 1, and v is 1. On the other hand, if $Q > V^f$, users have two cases where they receive 1 or not. Then, under the assumption that users are uniform, the expected value would be V^f/Q because the probabilities of users to get 1 and 0 is V^f/Q and $1-V^f/Q$, respectively. Therefore, in that case, the expected value of v would be V^f/Q.

B. Crypto-collateralized stablecoins

These stablecoins[6] (e.g., USDN) are similar to fiat-collateralized stablecoins except that the reserves are stored in cryptocurrencies. Specifically, the pegging mechanism pays 1 in cryptocurrencies to users in return for taking back a stablecoin from them. However, unlike fiat collateral, the cryptocurrency price fluctuates, which can cause the discrepancy between the cryptocurrency price values that users and the system refer to due to non-zero transaction time and a discrete cryptocurrency price oracle update within the system. Thus, the value users earn can differ from 1.

Here, the cryptocurrency used as collateral is denoted by c. Let p_u^c and p_s^c denote c's price to which users and the system refer, respectively. In addition, the total value of cryptocurrency reserves is determined by the characteristics of the economy, which is a fundamental state θ. Therefore, the total value of cryptocurrency reserves is denoted by a strictly increasing function $V^c(\theta)$ of θ; naturally, the condition of greater asset value and higher asset growth is stronger fundamentals. Then v is p_u^c/p_s^c in the case of $Q \leq V^c(\theta)$; users receive $1/p_s^c$ cryptocurrencies by redeeming a stablecoin only when the crypto reserves are not depleted.

In fact, a ratio p_u^c/p_s^c is for the fluctuation of c's price; a greater drop in c's price implies a smaller value of the ratio below 1. The price change of crypto collateral is affected by an economic situation that can be represented by the state of fundamentals, and also the stablecoin redemption action of users. Note that in the redemption process, the system should pay the users, which implies that a part of the crypto collateral should be unlocked and flow into the market. This can lower the cryptocurrency price by increasing its circulating supply and/or bringing other secondary market impacts. Given this, we will denote p_u^c/p_s^c by a function $r^c(Q,\theta)$, where r^c is strictly decreasing for the first input Q and strictly increasing for the second input θ. That is, p_u^c/p_s^c decreases as users redeem more stablecoins in a short period, while p_u^c/p_s^c increases as the economic condition is better. As a result, v is expressed as $r^c(Q,\theta)$ when $Q \leq V^c(\theta)$.

[6]Note that they are different from over-collateralized stablecoins in this paper.

4

On the other hand, if $Q > V^c(\theta)$, users can consider two cases where they receive $r^c(Q,\theta)$ or not. Then because the probability of users to get the reward is $V^c(\theta)/Q$ under the assumption that users are symmetric, the expected value would be $r^c(Q,\theta) \cdot \frac{V^c(\theta)}{Q} = r^c(Q,\theta) \times \frac{V^c(\theta)}{Q} + 0 \times \left(1 - \frac{V^c(\theta)}{Q}\right)$. Therefore, in this case, the value of v that users expect is $r^c(Q,\theta) \cdot V^c(\theta)/Q$.

Additionally, note that r^c and V^c depend on the cryptocurrency c used as collateral; therefore, even for the same inputs, the values of r^c and V^c can differ by which cryptocurrency the system uses. For example, consider a system that employs a robust exogenous cryptocurrency such as Bitcoin or Ethereum. How many of these cryptocurrencies the system will unlock to the market in the redemption process does not significantly influence their price because their value comes from other external sources. Therefore, in that case, Q's impact on r^c can be negligible. On the contrary, it can become significant (i.e., $\Delta r^c(Q,\theta)/\Delta Q$ would be larger) when c's value comes from the system's usage (e.g., endogenous cryptocurrencies designed to back stablecoins).

C. Algorithmic stablecoins

This category of stablecoins uses an endogenous cryptocurrency that the system can directly mint and burn to stabilize the stablecoin price. As the most representative example, UST falls into this category. An algorithmic stablecoin system sells and buys stablecoins to the market at the price 1, where the payment is processed with its endogenous cryptocurrency (e.g., Luna in the Terra system). However, as mentioned when describing crypto-collateralized stablecoins, the value that users receive may be different from 1. Then, similar to crypto-collateral stablecoins, v is $r^c(Q,\theta)$. A different point with crypto-collateralized stablecoins is that crypto-collateralized stablecoins have v as $r^c(Q,\theta)$ only when the reserves are not exhausted, while v always has this value in algorithmic stablecoins because they can always pay users by minting their endogenous cryptocurrencies.

D. Over-collateralized stablecoins

This type of stablecoin, including USDX and DAI[7], is also popular. Users must deposit cryptocurrency exceeding 1 in value to mint a stablecoin, essentially creating a debt. Here, we can consider the minted stablecoins as the user's debt. The system returns this collateral when the user redeems the stablecoins, meaning only debtors can redeem and receive value. If collateral values drop, triggering liquidation, other users can redeem stablecoins on the debtor's behalf to acquire the collateral. Given this, v should depend on whether users are stablecoin debtors or non-debtors.

First, let $D^L(\theta)$ denote the total quantity of stablecoins that users *should redeem* to the system in the liquidation process at one point. $D^L(\theta) = 0$ indicates that a liquidation process was not triggered for any collateral at the moment. Meanwhile, if $D^L(\theta)$ is equal to the stablecoin's circulating supply, it suggests that a liquidation process was initiated for all collateral, encouraging users to redeem all stablecoins in the market. We also denote user u_i's stablecoin debt that didn't enter liquidation as $D_{u_i}(\theta)$, which increases with worsening economic conditions because more collateral is at risk (i.e., $D_{u_i}(\theta)$ is an increasing function of θ). If $D_{u_i}(\theta) = 0$, user u_i cannot redeem its stablecoins unless a liquidation process exists for some collateral. Note that $D_{u_i}(\theta) = 0$ implies that user u_i is a non-debtor or its deposited collateral is in the liquidation progress. According to the definition of notations $D^L(\theta)$ and $D_{u_i}(\theta)$, their relationship is as follows: $D^L(\theta) + \sum_{u_i} D_{u_i}(\theta)$ should be the same as the stablecoin's circulating supply. Therefore, when $D^L(\theta)$ is the stablecoin's circulating supply, $D_{u_i}(\theta)$ would be zero for any user u_i.

Lastly, we consider the notation $o(\theta)$: Crypto collateral to be paid per stablecoin from the system to users has a value of $o(\theta)$ from the system's perspective.[8] For example, if the collateral value deposited by user u_i is 1.5 times the stablecoin debt based on the system's price oracle, then $o(\theta)$ would be 1.5. The value of $o(\theta)$ would be greater than 1 unless the state of fundamentals θ is too small, because the system requires collateral worth more than 1 when issuing a stablecoin debt to a user. As a result, v of user u_i would be expressed as follows: $r^c(Q,\theta) \cdot o(\theta)$ if $0 < D^L(\theta)$ or $0 < D_{u_i}(\theta)$, otherwise zero. That is, it means that users can be paid by redeeming stablecoins to the system, only when there are liquidation processes or they are stablecoin debtors whose deposited collateral did not enter a liquidation process.

IV. Equilibrium for Each Stablecoin Type

In this section, we will analyze the equilibria and price instability for each type of stablecoin. To focus on the equilibria changing with v and v' (i.e., equilibria varied by a stablecoin design), we consider that users have little incentive to keep holding coins (i.e., $i(x) \approx x$). We also assume that values of the future status variables including the future fundamental state θ' can approximate values of the current status variables such as the current fundamental state θ to simplify the equilibrium analysis by reducing the dimension of parameters. If we consider the future fundamental state as a variable θ' independent of θ, our results would be extended to two dimensions of fundamental states $[\theta, \theta']$.

We first present Figure 1 that illustrates the result visually, which makes it possible to compare stablecoin designs intuitively. In the figure, $\theta_{\max}$ and $\theta_{\min}$ indicate the maximum and minimum values of θ, respectively. The blue bar represents a range of θ in which a unique pegging equilibrium exists so the peg is guaranteed. The yellow range of θ has multiple equilibria, including the pegging state of $p(M) = 1$, which implies that the peg state is not guaranteed even though it can be reached. More specifically, in this range, the pegging state is a self-fulfilling equilibrium; users' belief totally determines the destiny of stablecoins. Finally, in the red range of θ, there

[7] More specifically, the current version of DAI has a mixed mechanism of crypto collateralization using other stablecoins and over-collateralization.

[8] Strictly speaking, $o(\theta)$ would be different by each pair of collateral and debt, but we simplify it by standardizing the value over a pair because it does not affect our main theoretical analysis and result.

5

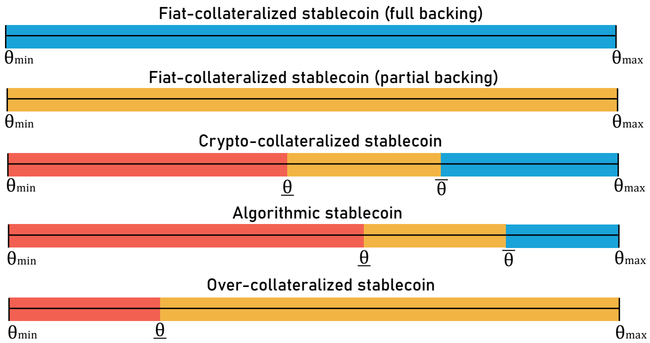


Fig. 1: **An equilibrium state for given θ by stablecoin type.** Each color bar represents a zone of θ with a different equilibrium state. In the blue zone, a unique pegging equilibrium exists. In the yellow zone, there are multiple equilibria, including the pegging state of $p(M) = 1$. In particular, the pegging state is a self-fulfilling equilibrium there. In the red zone, there is only a depegging equilibrium.

is only a depegging equilibrium, which implies that the peg cannot be achieved. Therefore, the wider the blue range, the better the stablecoin design.

A value of $\overline{\theta}$ indicates a lower bound for having a unique pegging equilibrium, and $\underline{\theta}$ is an upper bound for having only a depegging equilibrium. Therefore, according to Figure 1, stablecoins fully backed by fiat assets have $\overline{\theta}$ as $\theta_{\min}$. Stablecoins partially backed by fiat assets do not have a value of $\overline{\theta}$ and $\underline{\theta}$. Furthermore, an over-collateralized stablecoin does not have $\overline{\theta}$. In crypto-collateralized, algorithmic, and over-collateralized stablecoins, the values of $\overline{\theta}$ and $\underline{\theta}$ would depend on c. Specifically, if the system employs a more robust crypto asset in its pegging mechanism, the blue zone can widen by decreasing $\overline{\theta}$. On a side note, a significant incentive function i can also help expand the blue zone and narrow the yellow and red zones.

We now describe below the equilibrium state of stablecoin systems in detail. Due to the page limit, we omit the proofs of theorems. For details, please see our full paper [16].

A. Fiat-collateralized stablecoins

As described in Section II, fiat-collateralized stablecoins have v as 1 if $Q \leq V^f$, otherwise V^f/Q. The following theorem presents equilibria of fiat-collateralized stablecoins.

Theorem 2: Fully backed fiat-collateralized stablecoins have a unique pegging equilibrium for any θ. On the other hand, for any θ, partially backed fiat-collateralized stablecoins have multiple equilibria including the pegging state due to users' self-fulfilling beliefs.

According to Theorem 2, fully backed fiat-collateralized stablecoins can guarantee the peg. Meanwhile, a system partially backing its stablecoin has multiple equilibria, so it is difficult to predict the consequence. The system can reach the pegging state, but it is not guaranteed. In particular, it suffers from a self-fulfilling belief of users; if users believe only a few stablecoin holders will redeem their coins, the users with that expectation would not need to redeem their coins to the system right now, which fulfills the expectation by themselves and, in turn, results in price stabilization. On the other hand, let us assume that users believe that too many holders will redeem coins so that the reserves of the system cannot cover it. Then users should immediately redeem their coins to the system, which realizes the expectation by themselves and puts the stablecoin in danger by bringing about the depreciation of the stablecoin.

B. Crypto-collateralized & algorithmic stablecoins

Next, we look at crypto-collateralized and algorithmic stablecoins. Crypto-collateralized stablecoins have a value of v as $r^c(Q, \theta)$ if $Q \leq V^c(\theta)$, otherwise $r^c(Q, \theta) \cdot V^c(\theta)/Q$. In algorithmic stablecoins, v is $r^c(Q, \theta)$. We present their equilibria in Theorem 3.

Theorem 3: We denote the total market supply of stablecoins by T^s. Then, in crypto-collateralized and algorithmic stablecoins, $\overline{\theta}$ is a value such that $r^c\left(T^s, \overline{\theta}\right) = 1$, and $\underline{\theta}$ is a value such that $r^c(0, \underline{\theta}) = 1$. Here, for crypto-collateralized stablecoins, we assume that $V^c(\underline{\theta}) \geq T^s$. Then both crypto-collateralized and algorithmic stablecoins have a unique pegging equilibrium for any $\theta \geq \overline{\theta}$, multiple equilibria including the pegging state for any θ in the range $[\underline{\theta}, \overline{\theta})$, and depegging equilibria for any $\theta < \underline{\theta}$.

Crypto-collateralized and algorithmic stablecoins can guarantee the peg under good economic conditions. However, under poor economic conditions, even if the reserves are sufficient to back the stablecoins fully, they would not be able to reach the pegging state because users who redeem their coins cannot, in effect, receive 1 due to a downward price fluctuation of the cryptocurrency, the payment medium. In the mediocre economic status, there are multiple equilibria including the pegging state; the successful peg is up to users' belief in others' redemption actions because the stablecoin redemption affects whether a cryptocurrency price can be less than 1 in that economic condition.

The values of $\overline{\theta}$ and $\underline{\theta}$ depend on r^c according to Theorem 3; $\overline{\theta}$ and $\underline{\theta}$ are the values such that $r^c\left(T^s, \overline{\theta}\right) = 1$ and $r^c(0, \underline{\theta}) = 1$, respectively. Note that $\overline{\theta}$ is greater than $\underline{\theta}$ because r^c decreases and increases as the first and second inputs increase, respectively. The more robust cryptocurrency the systems use to back stablecoins, the gentler the slope of r^c. That is, for a more robust cryptocurrency c, r^c can be greater, so $\overline{\theta}$ and $\underline{\theta}$ become lower. For example, crypto-collateralized stablecoins can use Bitcoin, Ethereum, or even other stablecoins as their collateral to widen the blue zone. Meanwhile, algorithmic stablecoins should use endogenous cryptocurrencies according to their protocol, which would have a narrower blue zone and a wider red zone.

C. Over-collateralized stablecoins

Finally, we consider over-collateralized stablecoins. The stablecoin has v for user u_i as follows: $r^c(Q, \theta) \cdot o(\theta)$ if $0 < D^L(\theta)$ or $0 < D_{u_i}(\theta)$, otherwise zero. Here, $o(\theta)$ is greater than 1 as long as θ is not too low. Theorem 4 presents equilibria of over-collateralized stablecoins.

6

Theorem 4: We assume that $r^c(0,\theta) \cdot o(\theta) < 1$ when $D^L(\theta) = T^s$. Then over-collateralized stablecoins have multiple equilibria including the pegging state for any $\theta \geq \underline{\theta}$, and depegging equilibria for any $\theta < \underline{\theta}$, where $\underline{\theta}$ satisfies $r^c(0,\underline{\theta}) \cdot o(\underline{\theta}) = 1$. Moreover, $\underline{\theta}$ of over-collateralized stablecoins is smaller than that for crypto-collateralized and algorithmic stablecoins.

In over-collateralized stablecoins, stablecoin debtors can redeem their coins anytime, while non-debtors cannot unless a liquidation process starts for some collateral. Therefore, users' belief regarding redemption by debtors plays an important role in maintaining the peg; if users believe that many stablecoin debtors will redeem their coins, debtors with this expectation will redeem their coins now to settle their debt cheaper because they expect an increase in the stablecoin price due to other debtors' redemption. This leads to a rise in a stablecoin price by fulfilling their expectation by themselves. On the contrary, if users believe that only a few debtors will redeem their coins, debtors with the expectation do not need to redeem their coins immediately because they do not think the coin price will increase. Therefore, the stablecoin price will not increase by vindicating their decision.

On the other hand, if the collateral value is less than 1 due to severely bad economic conditions, the system would not be able to attain the pegging state.

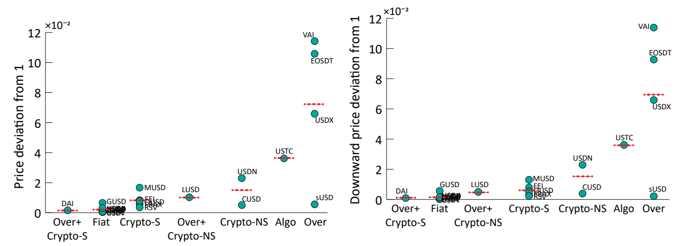
Moreover, where a system pays users more than 1 based on its price oracle, v can be not less than 1 even with a price drop of cryptocurrencies. This makes $\underline{\theta}$ of over-collateralized stablecoins smaller than that for crypto-collateralized and algorithmic stablecoins.

V. Empirical Analysis

We found that existing stablecoin designs have different price equilibria by their unique value of v. Here, we conduct an extensive empirical analysis using observational data to see whether actual stablecoin prices have fluctuated in agreement with our theory.

1) Top 22 stablecoins: In the analysis, we considered stablecoins that aim to be pegged at USD, and that existed for one year before the UST downfall (i.e., May 13, 2021, to May 12, 2022). We selected, based on market cap, the top 22 stablecoins among the ones satisfying the above criteria, and then collected their daily price data from CoinMarketCap [18]. The selected stablecoins have various types: Fiat-collateralized (*Fiat*), crypto-collateralized using other stablecoins as collateral (*Crypto-S*), crypto-collateralized using other non-stablecoins (*Crypto-NS*), algorithmic (*Algo*) and over-collateralized (*Over*). Some stablecoins combine different pegging mechanisms. For example, DAI allows users to swap the coin with other stablecoins, such as USDC, in a 1:1 ratio, while having a loan mechanism to maintain the peg [19]. LUSD also runs crypto-collateral and over-collateral mechanisms simultaneously [20]. As a result, our data includes 8 Fiat (USDT, USDC, BUSD, TUSD, USDP, GUSD, HUSD, USDK), 5 Crypto-S (FRAX, FEI, OUSD, MUSD, RSV), 2 Crypto-NS (USDN, CUSD), 1 Algo (USTC), 4 Over (USDX, sUSD, VAI, EOSDT), 1 Crypto-S+Over (DAI), and 1 Crypto-NS+Over (LUSD).

2) Stability levels of stablecoins: Given that a time point corresponds to one value of θ, we can compare the actual stability levels of stablecoins with the ones expected by our theory. We evaluate the stability level of stablecoins by analyzing how much their price has deviated from \$1. We use two metrics to measure a (downward) price deviation from 1. The metric to estimate a price deviation is defined as $\sqrt{\frac{\sum_{i=0}^{N-1}(p_i-1)^2}{N}}$, where p_i indicates one price data point in the data set. That is, it means a standard deviation of price from 1. The metric to estimate downward price deviation is defined as $\sqrt{\frac{\sum_{i=0}^{N-1}(\min(p_i-1,0))^2}{N}}$, which implies a price deviation considering only when a price falls below 1. Figures 2a and 2b show price deviation and downward price deviation from 1 by stablecoin type, respectively.



(a) Price deviation from 1

(b) Downward price deviation from 1

Fig. 2: (Downward) price deviation by stablecoin type. The x-axis is arranged in ascending order of the average values by stablecoin type. Red dot lines represent an average value by stablecoin type.

We can see that Fiat and Crypto-S using other stablecoins have been relatively stable. Over-collateralized stablecoins (Over) have been overall unstable, but there is also a large deviation across the samples. Note that the yellow zone that over-collateralized stablecoins possess largely in Figure 1 has multiple equilibria, which makes it not easy to predict a price state. On the other hand, because Crypto-NS and Algo categories have only one or two samples, it is difficult to compare them with other types meaningfully. However, we find that some algorithmic stablecoins have collapsed like UST or have changed their pegging mechanism; for example, Nubits have disappeared by not overcoming a severe peg break [21]. USDD also changed its original algorithmic pegging mechanism to the crypto-collateralized mechanism using combination of stablecoins and other cryptocurrencies [22, 23]. Therefore, one may suspect that the general poor stability of algorithmic stablecoins results in the small sample number.

Another point is that Crypto-S+Over and Crypto-NS+Over are observed to be more stable than Crypto-S and Crypto-NS, respectively.[9] In fact, this is also expected by our theoretical analysis. Theorem 4 states that $\underline{\theta}$ of over-collateralized stablecoins is smaller than that for crypto-collateralized, which

[9]Here, we would not claim the observation is statistically valid due to a small sample number.

7

implies that crypto-collateralized stablecoins can reduce the red zone by combining with an over-collateralized mechanism. In addition, the combination of crypto-collateralized and over-collateralized systems does not affect the blue zone because all users can redeem their stablecoins in any case through the crypto-collateralized mechanism. As a result, the price stability of Crypto-S+Over and Crypto-NS+Over is empirically observed in agreement with our theory.

3) Relationship between a price and v: According to our theory, a stablecoin price should be depegged when v is less than \$1, which should bring a correlation and causality between a price and v. We collected actual redemption transactions of one year (05/13/2021∼05/12/2022) to analyze the relationship between v and a stablecoin price. On-chain data collection was prioritized by high market cap, diversity of design, and ease of access to data. In the process, we were able to collect on-chain data for a total of 11 stablecoins from five different blockchains, Ethereum, Terra, BSC, Celo, and Waves: DAI, FRAX, FEI, OUSD, MUSD, LUSD, USDN, CUSD, USTC, sUSD, and VAI. The value of v was calculated considering the quantity of the asset earned when users redeemed their stablecoins and the asset's market price. Because we could obtain only daily price data (i.e., end of day asset price) in USD, we used the *last redemption transaction data* for each day to reduce errors when calculating v. Note that the last redemption transaction occurs almost at the end of day considering the frequency of transactions. Here, note that we did not consider and subtract transaction fees by assuming that the difference between redemption and market transaction fees is negligible and by offsetting all the fees. Therefore, for fiat-collateralized stablecoins, v would be 1.

We first analyze the correlation between the downward v deviation and the downward price deviation of stablecoins. Considering 19 stablecoins (11 stablecoins, of which v was actually collected, and 8 fiat-collateralized stablecoins), there is a significantly strong correlation (Pearson's $\rho \approx 0.7150$, p-value≈0.0006, Bayes factor≈0.0165[10]) between the downward v deviation and the downward price deviation.

Type	Name	Correlation		Granger causality	
		Rho	P-value	F-stats.	P-value
Crypto-S+Over	DAI	0.1499	0.0136	5.8753	0.0160
Crypto-S	FRAX	0.1833	0.2576	1.1987	0.2809
	FEI	0.1845	0.0028	5.2799	0.0224
	OUSD	0.0934	0.2097	0.9743	0.3250
	MUSD	-0.0986	0.0620	1.2057	0.2729
Crypto-NS+Over	LUSD	0.3248	<0.0001	30.1870	<0.0001
Crypto-NS	USDN	0.4914	<0.0001	76.9957	<0.0001
	CUSD	0.1341	0.0104	12.3066	0.0005
Algo	USTC	0.8366	<0.0001	88.7618	<0.0001
Over	sUSD	0.7677	<0.0001	44.1318	<0.0001
	VAI	-0.0200	0.7560	9.9877	0.0018

TABLE III: Correlation and Granger causality between a stablecoin price and v

[10]This value represents "very strong evidence" for the correlation [24].

In addition, for each stablecoin, we performed the correlation analysis between v and a stablecoin price. Specifically, we examined the relationship between the last value of v and the closing stablecoin price for each day, and used the minimum value between v and 1 and the minimum value between a price and 1 to consider a downward fluctuation. We also saw if v has affected the stablecoin price through the Granger causality analysis. Table III presents the results, where we colored coins if they have significant correlation and causality.

We can see that the significant correlation and causality between v and a price are manifested in most stablecoins. DAI, FEI, LUSD, USDN, CUSD, USTC, and sUSD showed a significant correlation and causality. Meanwhile, it was not observed for FRAX, OUSD, MUSD, and VAI. In particular, we find that stablecoins with relatively good stability of a price and v do not show a strong correlation and causality; overall, DAI and Crypto-S have a relatively high P-value in Granger causality. This could be resulted from the deviations caused by noise or other factors being more apparent in coins with good downward stability of v. Most representatively, we can think of *Fiat* where v is always 1. Definitely, their price deviations do not come from v.

In addition, the existence of correlation and causality between v and a price can be inconsistent across over-collateralized stablecoins; in our data, sUSD showed a significantly positive correlation and causality, but VAI showed an insignificant correlation. As described in Section V-2, it can be difficult to predict their consequences due to their wide yellow zone.

The last important point is that stablecoin systems with a popular and large incentive protocol have little correlation and causality between a price and v, which Theorem 1 points out. In fact, even though UST showed significant correlation and causality considering its collapse event, there was no significant correlation (Pearson's ρ =0.0421, P-value=0.5369) and causality (F=0.8426, P-value=0.3597) when only considering the period (Oct 01, 2021 to May 06, 2022) that an incentive protocol, Anchor, was greatly popular. Note that Anchor promises to give users nearly 20% annual percentage yield (APY), and it even held about 75% of the total UST market cap in some cases.

We recognize the limitation of empirical analysis to show the true causality because there are not only two variables, v and a price, in the real world. In fact, it is well known that deriving the true causality is really challenging. By analyzing the stablecoin price along with many variables other than v, we will be able to examine whether the true causality between v and the price exists. Nevertheless, we believe that the results of the empirical analyses confirm our theory to some extent.

VI. Concluding Remarks

We developed a common theory to characterize the stability properties of many stablecoins, considering reserve asset types and redemption mechanisms. Our model helps to improve understanding of design differences and establishes guidelines for future stablecoin design.

8

References

[1] R. K. Lyons and G. Viswanath-Natraj, "What keeps stablecoins stable?" *Journal of International Money and Finance*, vol. 131, p. 102777, 2023.

[2] M. L. Nihar Shah, "The Depegging of UST," https://jumpcrypto.com/the-depegging-of-ust/, 2022, [Online; accessed 18-Jun-2022].

[3] A. Barthere, L. Choe, B. Baraki, Y. L. Khoo, P. Grushyn, X. Y. Lim, and J. Ho, "On-Chain Forensics: Demystifying TerraUSD De-peg," https://www.nansen.ai/research/on-chain-forensics-demystifying-terrausd-de-peg, 2022, [Online; accessed 25-Jun-2022].

[4] 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*, 2020, pp. 59–79.

[5] D. W. Arner, R. Auer, and J. Frost, "Stablecoins: risks, potential and regulation," *Financial Stability Review*, vol. 39, pp. 95–123, 2020.

[6] K. Jarno and H. Kołodziejczyk, "Does the Design of Stablecoins Impact Their Volatility?" *Journal of Risk and Financial Management*, vol. 14, no. 2, p. 42, 2021.

[7] GSR, "Chart of the Week: Dissecting the Terra/UST Bank Run," https://www.gsr.io/insights/chart-of-the-week-dissecting-the-terra-ust-bank-run/, 2022, [Online; accessed 06-Aug-2022].

[8] A. Moskov, "Terra (UST and LUNA) Guide: Is Terra Legit and How Does It Work?" https://coincentral.com/terra-guide-ust-luna/, 2022, [Online; accessed 06-Aug-2022].

[9] Y. Kwon, J. Kim, Y. Kim, and D. Song, "The trilemma of stablecoin," *Available at SSRN 3917430*, 2021.

[10] A. Moin, K. Sekniqi, and E. G. Sirer, "Sok: A classification framework for stablecoin designs," in *International Conference on Financial Cryptography and Data Security*. Springer, 2020, pp. 174–197.

[11] J. P. Koning, "Algorithmic Stablecoins," https://www.aier.org/article/algorithmic-stablecoins/, 2021, [Online; accessed 21-Jul-2022].

[12] A. Klages-Mundt and A. Minca, "While stability lasts: A stochastic model of noncustodial stablecoins," *Mathematical Finance*, 2022.

[13] ——, "(in) stability for the blockchain: Deleveraging spirals and stablecoin attacks," *Cryptoeconomic Systems*, 2021.

[14] A. Klages-Mundt and S. Schuldenzucker, "Designing autonomous markets for stablecoin monetary policy," https://arxiv.org/abs/2212.12398, 2022.

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

[16] Anonymous Submission, "What Drives the (In)stability of a Stablecoin?" 2023.

[17] I. Kuznetsov, "Analysis of the TITAN fall - Going the distance," https://jeiwan.net/posts/analysis-titan-fall/, 2021.

[18] CoinMarketCap, "Top Stablecoin Tokens by Market Capitalization," https://coinmarketcap.com/view/stablecoin/, 2022, [Online; accessed 12-Sep-2022].

[19] MakerDAO, "Peg Stability Module," https://makerdao.world/en/learn/governance/module-psm/, 2022, [Online; accessed 13-Oct-2022].

[20] Liquity, "Redemptions and LUSD Price Stability," https://docs.liquity.org/faq/lusd-redemptions, 2022, [Online; accessed 13-Oct-2022].

[21] Brandon, "Stablecoin Cemetery," https://blog.hubbleprotocol.io/stablecoin-cemetery/, 2022, [Online; accessed 13-Oct-2022].

[22] TRON, "TRON DAO RESERVE," https://tdr.org/#/, 2022, [Online; accessed 13-Oct-2022].

[23] A. Beganski, "Tron's USDD Stablecoin Still Hasn't Recovered Its Dollar Peg," https://decrypt.co/103338/trons-usdd-stablecoin-still-hasnt-recovered-its-dollar-peg, 2022, [Online; accessed 13-Oct-2022].

[24] IBM, "Bayesian Inference about Pearson Correlation," https://www.ibm.com/docs/en/spss-statistics/saas?topic=statistics-bayesian-inference-about-pearson-correlation, 2022, [Online; accessed 14-Oct-2022].

9