Algorithmic Stablecoins as Perpetual Convertible Bonds —A new solution to the stablecoin trilemma

arthur@chiprotocol.io July 5 2023

Article Overview

Stablecoins optimise stability at the expense of centralisation (e.g., USDC) or over-collateralisation (e.g., DAI), proving the tradeoff that they are often faced with (stablecoin trilemma). In this article, we introduce an alternative stability mechanism which achieves stability in prices with solvency, capital efficiency and preservation of resistance to censorship. It will be shown that this is analogous to a firm issuing perpetual convertible bonds, which can be converted into common stock or the equivalent of another asset.

Outline

The article is organised as follows. Section 1 unfolds the stablecoin trilemma and the motivations for a new stability regime. Section 2 briefly describes convertible bonds. Section 3 presents the stochastic model used for the rest of the article. Section 4 outlines the supply dynamics of stablecoins in response to price changes. Section 5 introduces a new stability mechanism with convertible bonds-like features. Finally, Section 6 outlines the research's findings and explores its potential applications. Readers familiar with stablecoins and convertible bonds can begin from Section 5.

1 Introduction

The Stablecoin Trilemma

The combined market capitalisation of stablecoins is around $130 billion [1], however a majority of these stablecoins are centralised (such as USDT, USDC, BUSD, etc.), which goes against the fundamental principles of decentralised and censorship-resistant blockchains. Alternatively, stablecoins not backed by off-chain collateral are over-collateralised by other crypto assets (e.g. ETH). While over-collateralisation leaves incentives for liquidations, it does not create capital efficiencies in the system. Moreover, it gives exposure to the volatility of the underlying collateral (e.g., forced behaviours with exogenous liquidations).
To mitigate large fluctuations in the stablecoin's market capitalisation, on-chain and collateral-backed stablecoins use fiat-backed stablecoins as the backing asset. The above mechanism results in a trust-constrained model for stablecoins originally introduced as

[1] https://coinmarketcap.com/view/stablecoin/

"decentralised" (e.g., de-peg of centralised stablecoin implies de-peg of the on-chain stablecoin - see Figure 1[2]).

Figure 1: March 2023, USDC-FRAX de-peg

As of today, the use case of Decentralised Finance (DeFi) has been bounded by the issuance of stablecoins from permissioned third parties (e.g., Circle and Tether). While this brought access to fiat-like currencies to DeFi users, it exposed the entire system to the severity of inherent weaknesses of the trust-based models.

This research attempts to recreate a perpetual convertible bond combined with a stability mechanism aimed at offering economic incentives while maintaining the system solvent. The introduction and expansion of a stable and algorithmic token will prevent further contagion by centralised monopolies in DeFi markets.

2 Convertible Bonds

Convertible bonds (CBs) are hybrid securities the holder can convert into a specified number of common shares in the issuing company or the equivalent value in cash[3].

Let us assume that the firm's value $V(t)$ is given by the sum of its equity $X(t)$ and convertible bonds $C(t)$ so that for $t \geq 0$, the equity value is defined as follows:

$$X(t) = V(t) - C(t) \tag{1}$$

The firm's objective is to maximise its equity value by minimising the convertible bonds' value (1). Conversely, the bondholder aims to exercise his conversion option to maximise the convertible bond's value, minimising the firm's equity (1). This creates a zero-sum

[2]https://coinmarketcap.com/currencies/usd-coin/
[3]https://en.wikipedia.org/wiki/Convertible$_{b}ond$

game between the two parties ("symmetric market rationality") [1] in which equilibrium is found when neither party can improve his position by adopting any other strategy [2].

3 Model

We assume the protocol's asset value (e.g., ETH) to follow a random and stochastic process [3].

$$dV = \mu V dt + \sigma V dW \tag{2}$$

Where μ (drift) indicates the expected long-term return on the underlying assets, σ is the volatility, and W is the one-dimensional Geometric Brownian Motion[4].

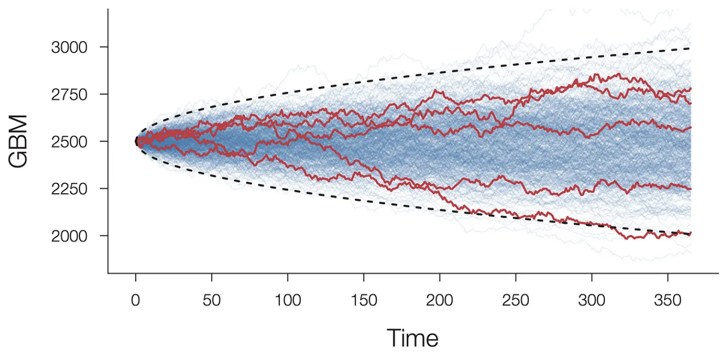

Figure 2: Geometric Brownian Motion

We aim to express the value dynamics of the convertible stablecoins $C(t)$ in response to movements in the protocol's value $V(t)$. Following the application of Ito's Lemma and by imposing no-arbitrage conditions, we find the fundamental value PDE of the perpetual convertible stablecoins:

$$\frac{1}{2}\sigma^2 V^2 C_{vv} + rVC_v - rC = 0 \tag{3}$$

4 Stablecoins and Supply Dynamics

Before deep diving into a convertible bond-like stablecoin, let's first provide some formulae which describe how stablecoins' supply changes in response to price variations. Let $P(t)$ denote the price of the stablecoin, and K its target price. Suppose this is a USD pegged, so $K = \$1$

[4]https://lambert-guillaume.medium.com/a-guide-for-choosing-optimal-uniswap-v3-lp-positions-part-1-842b470d2261

Lemma 1: If the stablecoin's price deviates from its target, then units can be added or removed so that the value of its circulating supply remains invariant.

Stated differently, the change of X % in stablecoin price over an interval must be followed by a change in stablecoin supply by X % [4]. Define $Q(t+1)$ and $Q(t)$ as the desired and current stablecoin's circulating supply respectively. According to Lemma 1, we define the following equations:

$$Q(t+1) = Q(t) \times \frac{P(t)}{K} \tag{4}$$

$$\Delta = Q(t+1) - Q(t) \tag{5}$$

where Δ denotes the required change in the stablecoin's supply to achieve the desired circulating supply.

Specification 1: If the stablecoin's price is trading at its target price, then its supply must remain constant:

$$P(t) = K \implies \Delta = 0 \tag{6}$$

Specification 2: If the stablecoin's price is trading above its target price, then its supply must be expanded:

$$P(t) > K \implies \Delta > 0 \tag{7}$$

Specification 3: If the stablecoin's price is trading below its target price, then its supply must be contracted:

$$P(t) < K \implies \Delta < 0 \tag{8}$$

5 Stabilising the price of a perpetual convertible stablecoin with callable features

Define the *price* rule set in advance by the protocol to let the stablecoin holders exercise their options to convert into shares.

Rule 1: To exercise the option and convert the stablecoin into shares, its price must be below \$1: $P(t) < K \implies \Delta < 0$, where $|\Delta|$ denotes the units of stablecoins which can be converted into shares.

Define the *solvency* rule set a priori by the protocol to allow conversion in shares tokens.

Rule 2: The protocol approves conversion into shares when there are insufficient assets to back the value of the total stablecoin's circulating supply following a callback for a fixed value, K.

$$V(t) - |\Delta|K < C(t) \tag{9}$$

Define $q(t)$ as the number of shares received at the time of conversion:

$$q(t) = \frac{|\Delta| \cdot K}{S(t)} \tag{10}$$

where $S(t)$ is the price of the shares token ante conversion. Define $S(t+1)$ the shares token price post conversion:

$$S(t+1) = \frac{V(t)}{m(t) + q(t)} \tag{11}$$

with $m(t)$ being the total quantity of outstanding shares token before conversion. Thus, define the conversion value:

$$q(t)S(t+1) \tag{12}$$

Specify *conversion* strategy for the stablecoin holder:

Strategy 1: If the stablecoin has not been called, we assume the holder adopts a strategy of the form: "convert as soon as the value of the firm equals or exceeds V_o , and the price of the convertible stablecoin is less than K". For $V_o > 0$, define:

$$V_o \triangleq \sup\{V(t) : V(t) - |\Delta|K < C(t)\} \cdot \mathbf{1}[P(t) < K] \tag{13}$$

where V_o denotes the highest value of the protocol's assets (in a deficit state) for which the stablecoin is converted for $q(t)$ of shares token.

Due to the perpetual characteristics of the convertible stablecoin, the free boundary problems associated with the optimal call and optimal conversion become "free point" problems [5]. Set the protocol's value $V_o^\star \in V(t)$ for which conversion becomes optimal.

Define the optimal conversion value of the convertible stablecoins:

$$C(V_o^\star) = \theta V_o^\star = q(t)^\star S(t+1) \tag{14}$$

with θ denoting a conversion factor.

Define boundary condition:

Definition 1: For $V(t) \to 0$ the protocol has defaulted, and it's convertible stablecoins have zero recovery.

$$C(V(t) \to 0) = 0 \tag{15}$$

Definition 2: For V_o defined as in Strategy 1, the value of the convertible stablecoins becomes the conversion value θV_o

Proof: PDE given by (3) is parabolic. Let $C = V^\gamma$ be the guess solution for the value of convertible stablecoins. Compute the following derivatives:

$$C_v = \gamma V^{\gamma-1} \tag{16}$$

$$C_{vv} = \gamma(\gamma-1)V^{\gamma-2} \tag{17}$$

Substitute to get the following ODE:

$$\frac{1}{2}\sigma^2 V^2 \gamma(\gamma-1)V^{\gamma-2} + rV\gamma V^{\gamma-1} - rV^\gamma = 0 \tag{18}$$

Determine the positive and negative roots:

$$\gamma_1 = 1 \tag{19}$$

$$\gamma_2 = -\frac{2r}{\sigma^2} \tag{20}$$

Rewrite the general value solution of the form:

$$C(V) = A_1 V^{\gamma_1} + A_2 V^{\gamma_2} \tag{21}$$

Recall boundary condition to find A_2:

$$\lim_{V\to 0} C(V) = 0 \implies A_2 = 0 \tag{22}$$

since γ_2 is the negative root. Solve for A_1 by setting:

$$\theta V_o^\star = A_1 V_o^\star \implies A_1 = \frac{\theta V_o^\star}{V_o^\star} \tag{23}$$

Hence, the value equation of the perpetual convertible stablecoins becomes:

$$C(V) = \frac{\theta V_o^\star}{V_o^\star} V = \theta V = q(t)S(t+1) \tag{24}$$

Introduce the *price* rule which is set in advance by the protocol to allow a call back:

Rule 3: To call back stablecoins, price must be below \$1: $P(t) < K \implies \Delta < 0$, where $|\Delta|$ denotes the amount of stablecoins which the protocol can call back for a fixed value, K.

Define a *solvency* rule set a priori by the protocol to make the call:

Rule 4: The protocol calls back stablecoins when there are sufficient assets to back the value of the total stablecoins' circulating supply following the surrender by the holder:

$$V(t) - |\Delta|K \geq C(t) \tag{25}$$

Consider the *call* strategy of the form:

Strategy 2: "Call the first time the value of the protocol's assets equals or exceeds V_e , and the price of the convertible stablecoin is less than K." For $0 < V_o < V_e$ define:

$$V_e \triangleq \inf(V(t) : V(t) - |\Delta|K \geq C(t)) \cdot \mathbf{1}[P(t) < K] \tag{26}$$

where V_e denotes the lowest value of the protocol's reserves (in a surplus state) for which the holder surrenders in exchange for K worth of another asset.

For $0 < V_o < V_e$, define the value function $f(x, V_e, V_o)$ for the convertible stablecoins satisfying the boundary conditions $f(0) = 0$, $f(V_o) = \theta V_o$. If $x \geq V_o$, and $P(t) < K$, $f(x, V_e, V_o)$ takes the following forms:

$$f(x, V_e, V_o) = \begin{cases} \theta x & \text{if } \mathrm{V}_o \leq x < V_e \\ |\Delta|K & \text{if } x \geq V_e \end{cases} \tag{27}$$

Define the *price* rule which is set in advance by the protocol to let the shares token holders burn and issue convertible stablecoins:

Rule 5: To purchase convertible stablecoins with shares burn, price must be at or above \$1: $P(t) \geq K \implies \Delta > 0$, where Δ denotes the amount of stablecoins which can be issued by the protocol.

Define the *solvency* rule set a priori by the protocol to allow issuance of convertibles stablecoins with shares burn:

Rule 6: Protocol approves purchase of convertibles stablecoins with shares burn when there are sufficient assets to back the value of the total stablecoins' circulating supply post issuance:

$$V(t) + \Delta K > C(t) \tag{28}$$

Consider the shareholders' *burn* strategy of the form:

Strategy 3: "Burn the first time the firm's value equates or exceeds V_e, and the price of the convertible stablecoin is at or more than K". For $0 < V_o < V_e$ define:

$$V_e \triangleq \inf(V(t) : V(t) + \Delta K > C(t)) \cdot \mathbf{1}[P(t) \geq K] \tag{29}$$

where V_e denotes the lowest value of the protocol's assets (in a surplus state) for which stablecoins are issued with burn of $q(t)$ shares tokens.

Hence, by replicating the computations outlined in Proof, define the cost of the convertible stablecoins:

$$C(V) = \theta V = q(t)S(t) \tag{30}$$

Introduce the *price* rule which is set a priori by the protocol to issue convertible stablecoins for a fixed amount of another asset:

Rule 7: Protocol issues convertible stablecoins in exchange for K worth of another asset if its price is at or above \$1: $P(t) \geq K \implies \Delta > 0$, where Δ denotes the amount of stablecoins which can be issued.

Define a *solvency* rule set by the protocol to allow issuance of convertible stablecoins for another asset:

Rule 8: Protocol approves K worth of another asset in exchange for newly issued stablecoins if there are insufficient assets backing the value of the total stablecoins' circulating supply following issuance:

$$V(t) + \Delta K \leq C(t) \tag{31}$$

Consider the protocol's *issuance* strategy of the form:

Strategy 4: "Issue stablecoins the first time the protocol's value is equal or lower than V_o, and the price of the convertible stablecoin is at or more than K". For $0 < V_o$ define:

$$V_o \triangleq \sup(V(t) : V(t) + \Delta K \leq C(t)) \cdot \mathbf{1}[P(t) \geq K] \tag{32}$$

where V_o denotes the highest value of the protocol's assets (in a deficit state) for which stablecoins are issued for K worth of another asset.

For $0 < V_o < V_e$, define the cost function $g(x, V_e, V_o)$ for the convertible stablecoins satisfying the boundary conditions $g(0) = 0$, $g(V_o) = \theta V_o$. If $x \geq V_o$ and $P(t) \geq K$, $g(x, V_e, V_o)$ takes the following forms:

$$g(x, V_e, V_o) = \begin{cases} \Delta K & \text{if } \mathrm{V}_o \leq x < V_e \\ \theta x & \text{if } x \geq V_e \end{cases} \tag{33}$$

6 Conclusion and Applications

This article investigates an alternative stability mechanism for stablecoins. The proposed structure shares similarities with convertible bonds, albeit it presents variations by including price conditions.

Over-collateralised mechanisms of existing decentralised stablecoins have pre-set limitations which prevent them from competing with trust-based models. Introducing a convertible bond-like stablecoin in DeFi can battle-test its stability and solvency while injecting large amounts of decentralised liquidity in those markets. Eventually, this will counteract the monopolistic power of centralised stablecoin issuers.

References

[1] Miller, Merton H., and Franco Modigliani. "Dividend Policy, Growth, and the Valuation of Shares." The Journal of Business, vol. 34, no. 4, 1961, pp. 411–33. JSTOR, http://www.jstor.org/stable/2351143.

[2] Brennan, M. J., and E. S. Schwartz. "Convertible Bonds: Valuation and Optimal Strategies for Call and Conversion." The Journal of Finance 32, no. 5 (1977): 1699–1715. https://doi.org/10.2307/2326820.

[3] Black, Fischer and Myron S. Scholes. "The Pricing of Options and Corporate Liabilities." Journal of Political Economy 81 (1973): 637 - 654.

[4] Sams, R. H. A note on cryptocurrency stabilisation: Seigniorage shares. url:https://github.com/rmsams/stablecoins/blob/master/paper.pdf.

[5] Sîrbu, Mihai, Igor Pikovsky and Steven E. Shreve. "Perpetual Convertible Bonds." SIAM J. Control. Optim. 43 (2004): 58-85.