Stablecoin Economics and Speculative Attacks: A Game-Theoretic Approach

Ayush Gupta[1], Girik Gupta[2]

[1]CEO, LayerEdge

[2]Intern LayerEdge

Abstract: ***Stablecoins serve as the backbone of many decentralized finance (DeFi) ecosystems, offering price stability in an otherwise volatile cryptocurrency market. This paper analyzes the economic design of stablecoins- both algorithmic (un- or under-collateralized) and asset-backed (collateralized)- and employs game-theoretic models to examine their susceptibility to speculative attacks. We present mathematical frameworks illustrating peg- maintenance mechanisms, discuss equilibrium conditions for stable pegging, and use real-world examples of USDC, DAI, and Terra-Luna to highlight the key success and failure factors. Policy and protocol design recommendations are provided to help mitigate risks of de-pegging and bank-run dynamics.***

Keywords: Stablecoins, Algorithmic Stablecoins, Collater- alization, Speculative Attack, Game Theory, DeFi

1. Introduction

Stablecoins are cryptocurrencies pegged to a reference asset- often the U.S. Dollar- to provide price stability in an inherently volatile crypto market.

Their stable price makes them vital for decentralized finance (DeFi) use-cases such as lending, borrowing, trading, and payments.

Despite their importance, stablecoins remain exposed to market shocks and potential crises of confidence that may lead to rapid de-pegging or collapse.

In traditional finance, currency pegs and fixed exchange rates frequently face speculative attacks [1].

Stablecoins, while leveraging blockchain technology, often face analogous attack vectors and crises. Drawing upon monetary economics, game theory, and empirical crypto data, this paper seeks to:

- Classify stablecoins into *asset-backed* (centralized or decentralized collateralization) and *algorithmic* (un- or under-collateralized) categories.
- Develop *game-theoretic* models explaining how stablecoin protocols respond to external shocks.
- Investigate *speculative attack* dynamics under various stablecoin mechanisms.
- Illustrate real-world successes and failures (USDC, DAI, Terra-Luna) in the context of our models.

2. Literature Review

Monetary Economics and Currency Pegs: Classical models such as Krugman-Flood-Garber (KFG) describe how pegged currencies can collapse under capital flight [1].

Obstfeld extends these frameworks to account for self-fulfilling crises, highlighting the role of coordination among speculators [2].

Stablecoin Mechanism Design: Ametrano introduced the concept of "Hayek Money," offering a rules-based supply adjustment approach for achieving price stability [3].

MakerDAO [4] pioneered an on-chain collateralization scheme for decentralized stablecoins, emphasizing governance-driven adjustments of parameters such as stability fees.

Game Theory and Speculative Attacks: Early treatments focus on currency crises, demonstrating how rational speculators may coordinate to attack a currency if they believe others will do the same [5].

In a global game framework, even slight shifts in expectations can tip the system into crisis.

Empirical Studies of DeFi: Recent research underscores how trust, liquidity, and reliable oracles are key to determining whether blockchain-based protocols replicate or deviate from classical financial crises [6].

3. Theoretical Underpinnings

1) *Types of Stablecoins*

Asset-Backed (Collateralized)

- *Centralized*: Fully backed 1:1 by fiat reserves in a bank (e.g., USDC).
- *Decentralized*: Over-collateralized on-chain (e.g., DAI locks ETH or other crypto assets as collateral).

Algorithmic (Un- or Under-Collateralized)

- *Rebase / Elastic Supply*: The supply is algorithmically expanded or contracted (e.g., Ampleforth), relying on rebase mechanisms that adjust holders' token balances.
- *Seigniorage-Style*: A secondary token absorbs volatility (e.g., Terra-Luna) through mint-and-burn or coupon-based approaches.

2) *Speculative Attack Models in Economics*

Speculative attacks typically unfold when market participants suspect a peg might fail, prompting them to sell or short the pegged asset.

If enough participants act simultaneously, they can force a peg to break even if fundamentals are not strictly compromised. Key concepts include:

- **Peg Break Condition**: Occurs when the cost of defending the peg (e.g., high interest rates, reserve liquidation) exceeds perceived benefits for the defending authority or protocol.
- **Self-Fulfilling Prophecies**: If participants believe a collapse is imminent, their collective actions (exits, redemptions) can create the very collapse they fear [2].

4. Game-Theoretic Framework

We now formalize stablecoin peg dynamics through game-theoretic constructs, focusing on both collateralized and algorithmic mechanisms.

1) Asset-Backed Stablecoins

Consider a stablecoin S pegged to $1, with:
R: The amount of reserve assets (fiat or crypto).
D: The total circulating supply (demand) of S.
α: The collateral ratio, so $R \geq \alpha \times D$. For a fully collateralized stablecoin, $\alpha \geq 1$.

a) Peg Maintenance via Collateral:

A holder can redeem S for $1 of the reserve (minus fees) in a centralized model, or by burning S in a decentralized system that returns a proportional amount of on-chain collateral.

Arbitrage typically drives $P(S) \approx 1$, since if S trades above $1, holders can sell for a premium, and if it trades below $1, they can buy and redeem it for full $1 value.

$$P(S) \approx 1 \quad \text{iff} \quad 0 \leq (1 - \kappa) \leq \alpha, \tag{1}$$

where κ is the redemption fee or friction cost.

b) Bank-Run and Speculative Attack Model:

A bank-run or speculative attack scenario unfolds if a fraction θ of stablecoin holders simultaneously seek redemption.
If

$$\theta D > \frac{R}{p},$$

the system cannot honor all redemptions (for peg $p = 1$, this simplifies to $\theta D > R$), causing the peg to break.

In a global game framework [7], each agent i observes a noisy signal σ_i about reserves R and decides whether to redeem or hold.

When many agents coordinate on a "run" strategy based on low σ_i signals, the peg can collapse in a self-fulfilling manner.

2) Algorithmic Stablecoins

Algorithmic stablecoins maintain $P(S) = 1$ via supply adjustments that expand or contract S based on market conditions.
They often incorporate a secondary governance or utility token G.

a) Seigniorage-Style vs. Rebase Mechanisms:

- *Seigniorage-Style*: If $P(S) > 1$, the protocol mints new S and sells or distributes it, often rewarding G holders. If $P(S) < 1$, the protocol burns S (or issues coupons convertible later) to reduce supply.
- *Rebase (Elastic Supply)*: If $P(S) > 1$, all user balances are increased proportionally; if $P(S) < 1$, balances are decreased. This keeps the "unit price" near $1 but can be counterintuitive for users.

b) Dynamic Equilibria and Attack Thresholds:

In a simplified discrete-time model, the stablecoin price evolves as

$$P(S_{t+1}) = P(S_t) \cdot \frac{\text{Net Demand}}{\text{Net Supply}}. \tag{2}$$

Speculative attacks occur if a fraction γ of participants dump or redeem S simultaneously.

If $\gamma > \gamma^*$, where γ^* is a critical threshold determined by protocol design (e.g., mint/burn capacity, liquidity, perceived governance token value), a reflexive feedback loop can drive $P(S)$ below $1, often irreparably.

$$\Pi(S, G) = \begin{cases} 1, & \gamma \leq \gamma^*, \\ 0, & \gamma > \gamma^*. \end{cases}$$

When γ exceeds γ^*, the system's endogenous backstop (like governance token G) may collapse in value, failing to defend the peg.

5. Case Studies

a) USDC: A Centralized Success

- *Mechanism*: Circle holds fiat reserves in audited U.S. bank accounts, claiming 1:1 backing for all USDC in circulation.
- *Why It Worked*: Regulatory compliance and transparent audits reduce uncertainty; redemption can be done for
- $1 on a near-instant basis, and high public confidence pushes γ^* very high.
- *Game-Theoretic Insight*: With a clear redemption facility and perceived low counterparty risk, there is little incentive to coordinate on a run.

b) DAI: A Decentralized, Collateralized Success

- *Mechanism*: MakerDAO smart contracts lock collateral (like ETH) at over 150% ratio. Users mint DAI by locking sufficient collateral, and the system liquidates under-collateralized positions automatically.
- *Why It Worked*: Over-collateralization provides a significant buffer. The on-chain liquidation process helps maintain confidence in DAI's ability to remain near $1.
- *Game-Theoretic Insight*: With $\alpha > 1$, a moderate fraction θ of users redeeming or exiting at once still leaves the system solvent, thus raising γ^*.

c) Terra-Luna: An Algorithmic Failure

- *Mechanism*: Terra's UST was algorithmically pegged to
- $1 by swapping UST and LUNA. If *UST* < $1, it could be exchanged for $1 worth of LUNA, and vice versa when *UST* > $1.
- *Why It Failed*: A large wave of redemptions occurred, triggering hyperinflation of LUNA in an attempt to uphold the peg. As LUNA's price collapsed, it became unable to absorb UST's selling pressure.
- *Game-Theoretic Insight*: The critical fraction γ^* was relatively low due to the lack of real collateral. Once a moderate group of actors believed in an imminent
- collapse, the protocol's defense mechanism (minting LUNA) backfired, accelerating the downfall.

6. Discussion: Policy and Design Implications

- **Reserve Transparency**: Frequent and verifiable audits, or on-chain proofs of reserve, help minimize information asymmetry and raise γ^*.
- **Over-Collateralization and Circuit Breakers**: Decentralized stablecoins benefit from robust liquidation rules and circuits that halt extreme cascades.
- **Robust Governance Token Dynamics**: Algorithmic stablecoins that rely on a governance or secondary token
- must ensure that this token has intrinsic or consistently recognized value, so that γ^* remains high.
- **Regulatory Frameworks**: Clear minimum reserve ratios, legally enforceable redemption rights, and periodic disclosure requirements can mitigate systemic risk in both centralized and decentralized contexts.

7. Conclusion

The stability of a stablecoin hinges on the interplay of *economic fundamentals, game theory, and investor confidence*. Asset-backed coins such as USDC maintain pegs effectively through rigorous redemption mechanisms and trusted custodians, significantly raising γ^*.

Decentralized collateralized designs like DAI illustrate how over-collateralization and on-chain governance can contain crises even under large market swings.

Algorithmic models, especially those reliant on purely endogenous secondary tokens, face greater risk from self-fulfilling runs, as seen in the Terra-Luna collapse.

Speculative attacks on stablecoins mirror classical currency crises, emphasizing the need for real collateral, robust equilibrium conditions, and prudent mechanism design.

Future research should examine cross-chain stablecoin architectures, advanced liquidity management, and the role of international regulatory cooperation to prevent contagion effects.

References

[1] P. Krugman, "A Model of Balance-of-Payments Crises," *Journal of Money, Credit and Banking*, vol. 11, no. 3, pp. 311–325, 1979.

[2] M. Obstfeld, "Models of Currency Crises with Self-Fulfilling Features,"

[3] *European Economic Review*, vol. 40, no. 3–5, pp. 1037–1047, 1996.

[4] F. M. Ametrano, "Hayek Money: The Cryptocurrency Price Stability Solution," *SSRN Electronic Journal*, 2016.

[5] MakerDAO, "Maker White Paper," 2017. [Online]. Available: https://makerdao.com/en/whitepaper

[6] M. Obstfeld, "Rational and Self-Fulfilling Balance-of-Payments Crises,"

[7] *American Economic Review*, vol. 76, no. 1, pp. 72–81, 1986.

[8] C. R. Harvey, A. Ramachandran, and J. Santoro, "DeFi and the Future of Finance," *SSRN Electronic Journal*, 2021.

[9] S. Morris and H. S. Shin, "Unique Equilibrium in a Model of Self- Fulfilling Currency Attacks," *American Economic Review*, vol. 88, no. 3, pp. 587–597, 1998.