

Wonderland Research Challenge — Stablecoins

Author: Francesco Petrora

Date: 29th October 2025

Introduction

Stablecoins have emerged as one of the most significant innovations within the crypto-financial ecosystem, aiming to reconcile the volatility inherent in digital assets with the stability of fiat currencies. By design, stablecoins function as digital representations of money that maintain a relatively constant value through different forms of collateralization or algorithmic control mechanisms. Their economic relevance extends beyond simple payment facilitation they underpin decentralized finance (DeFi), serve as a bridge between traditional and on-chain financial systems, and enable global capital mobility independent of national borders.

From a monetary economics perspective, stablecoins represent an experimental evolution of private money creation in the digital age, synthetic currencies that attempt to replicate the functions of fiat money through distinct institutional architectures. Within this framework, USDT (Tether), USDC (USD Coin) and DAI stand out as dominant dollar-pegged stablecoins whose underlying mechanisms illustrate the contrast between market-driven trust, regulatory-driven transparency and algorithmic control.

In the next figure we can observe the total market cap of stablecoins across all the different blockchains and the USDT dominance that, as for today, it is almost 60% of the market accounting for the biggest operated volume of the world. In the graph we can see this dominance as the dark green area accounts for USDT dominance and the dark blue shows the dominance of the USDC.

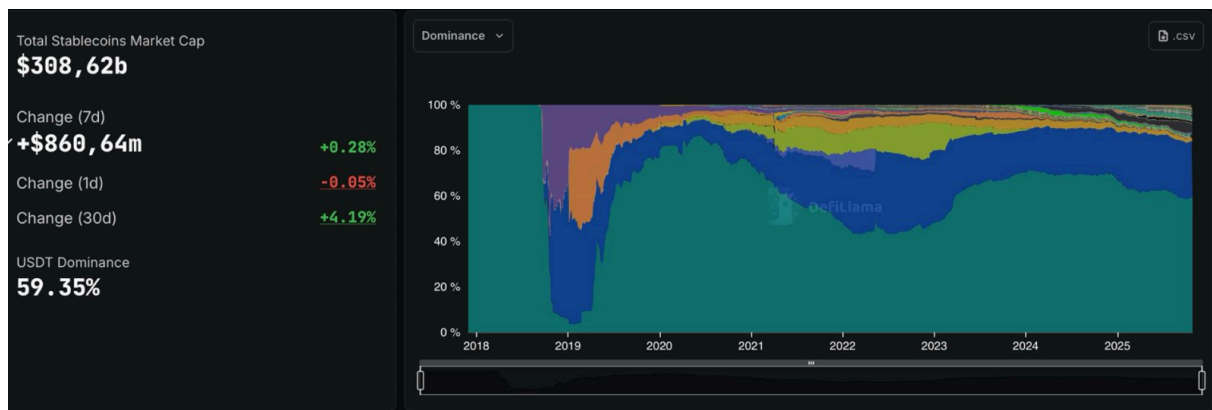


Figure 0: Total market cap of stablecoins across different blockchains

a) Analysis

USDT

USDT, issued by Tether Limited, is designed as a fiat-collateralized token maintaining a one to one parity with the U.S. dollar. Each USDT in circulation is nominally backed by an equivalent amount of real-world assets, including cash deposits, short-term government securities, and money-market instruments held in custody by Tether Limited. Its whitepaper describes USDT as a digital token backed by fiat currency, whose principal innovation lies in using the Bitcoin blockchain, through the Omni Layer protocol, to embed a verifiable record of issuance and transfers. Tether's Proof of Reserves framework mathematically equates total tokens in circulation to fiat deposits under custody, formalized in the so-called "Solvency Equation" ($TUSD = DUSD$).

By publishing both on-chain data and audited bank balances, the company aimed to maintain confidence in its peg. However, the structure remains inherently centralized, Tether Limited retains sole authority to issue and redeem tokens, and users must ultimately rely on the solvency and operational integrity of a single corporate entity and its banking partners. The whitepaper itself acknowledges this institutional dependency as a necessary trade-off to ensure liquidity and simplicity, while deferring full decentralization to future system iterations.

Figure 1 depicts market cap data and circulating tokens for USDT with a percentage of tokens in each of the main blockchains. Figure 2 shows the price movement around the peg to the dollar.

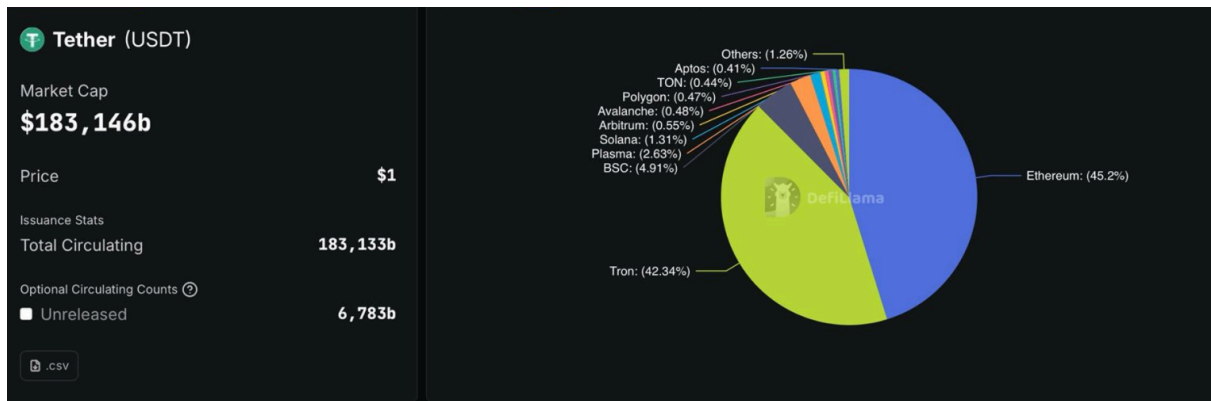


Figure 1: Market cap data and circulating tokens for USDT



Figure 2: Price movement around the peg to the dollar for USDT

In practice, USDT's sustainability derives not from algorithmic mechanisms but from market confidence, the collective belief that redemption claims will be honored. As a result, its stability operates analogously to a fixed-exchange-rate regime under imperfect convertibility: credibility substitutes for convertibility during stress periods. This model has proven effective at scale, as Tether now accounts for the majority of global stablecoin transaction volume, yet it exposes users to traditional financial risks, including counterparty risk, reserve opacity, and jurisdictional concentration. The economic implication is that USDT functions as a de facto shadow dollar, privately issued and globally liquid, but lacking the institutional discipline typical of regulated financial intermediaries.

As of today, however, many observers and market participants speculate that Tether may not be maintaining full parity with the U.S. dollar through genuine reserves. Critics argue that the company could be issuing unbacked USDT, that is, tokens not fully collateralized by dollar-denominated assets or U.S. Treasury bills. If such allegations were ever proven true, it could trigger a systemic default risk for Tether and propagate a contagion effect throughout the crypto ecosystem. Much like a classic bank run, once collective confidence collapses, users would rush to redeem their holdings, only to discover that the circulating supply exceeds actual reserves. This erosion of trust could precipitate a liquidity crisis across exchanges and DeFi protocols, as USDT remains the principal settlement asset in global crypto markets.

USDC

USDC, created by Circle Internet Financial under the Centre Consortium, represents a more regulated and institutionalized approach. It operates under a full-reserve custodial architecture, where each token corresponds to a U.S. dollar or a short-term Treasury instrument held in segregated accounts with regulated financial institutions. Circle's legal framework, articulated in its USDC Terms of Use, subjects the issuer to U.S. money-transmitter and anti-money-laundering laws, ensuring compliance and periodic attestation by third-party auditors. From an economic standpoint, USDC functions as a digitally native representation of high-quality liquid assets, effectively transforming the infrastructure of dollar settlement without altering its credit structure. Its sustainability rests on the credibility of regulated custody and legal accountability, aligning it more closely with a money-market-fund-like instrument than with a crypto-native token. Yet this same compliance orientation introduces centralization and policy dependence. Circle can freeze addresses, halt redemptions, or modify terms subject to U.S. jurisdiction. Thus, while USDC offers superior transparency and regulatory legitimacy relative to USDT, it does so at the cost of permissionlessness and global neutrality illustrating how institutional trust can substitute for decentralization.

Figures 3 and 4 show the percentage of USDC in each of the principal blockchains as well as the peg to the US dollar.

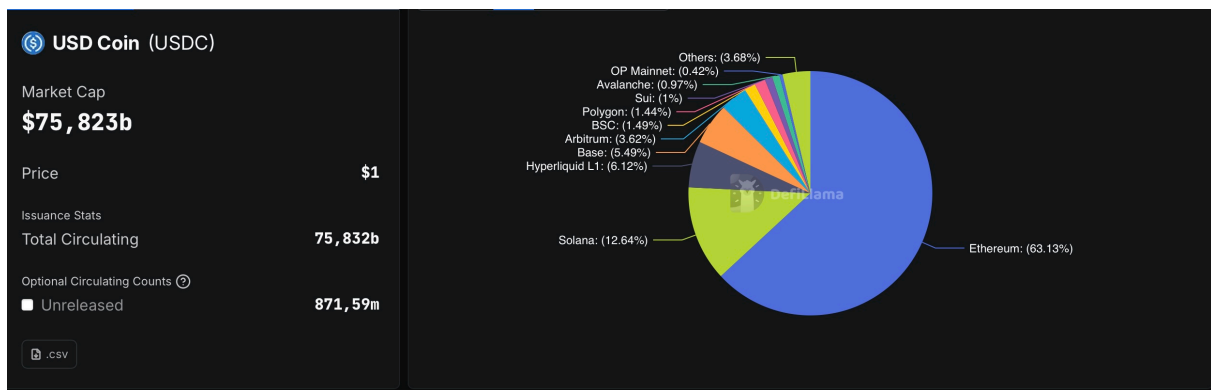


Figure 3: Market cap data and circulating tokens for USDC



Figure 4: Price movement around the peg to the dollar for USDC

DAI

In contrast, DAI, developed by MakerDAO, exemplifies the decentralized and crypto-collateralized model of monetary stability. According to its whitepaper, DAI is a stablecoin whose value is softly pegged to the U.S. dollar through a system of collateralized debt positions, autonomous feedback mechanisms, and external incentives. Rather than being backed by fiat, DAI is issued when users lock volatile crypto assets such as ETH, wrapped BTC, or even tokenized stablecoins like USDC, into smart-contract vaults that over-collateralize the position. The system dynamically maintains solvency through liquidation auctions and the stability fee, which functions analogously to an interest rate in traditional monetary policy. Governance decisions including collateral types, risk parameters, and interest rates are determined by holders of the MKR token,

creating an endogenous monetary policy governed by decentralized voting. This mechanism effectively replaces institutional trust with algorithmic trust market incentives, transparency, and code enforcement collectively uphold the peg. Nonetheless, DAI's sustainability is not absolute. Its exposure to crypto-asset volatility and reliance on certain centralized assets as collateral (USDC) introduce systemic feedback risks, while over-collateralization imposes a capital efficiency cost.

As well as with the other stablecoins, figure 5 and 6 shows the same parameters of market cap and token allocation in each blockchain as well as its historic price.

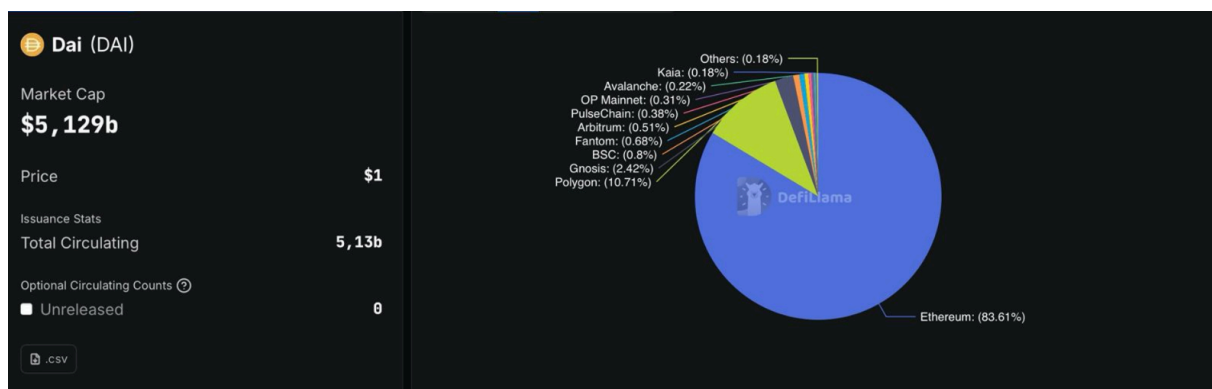


Figure 5: Market cap data and circulating tokens for Dai

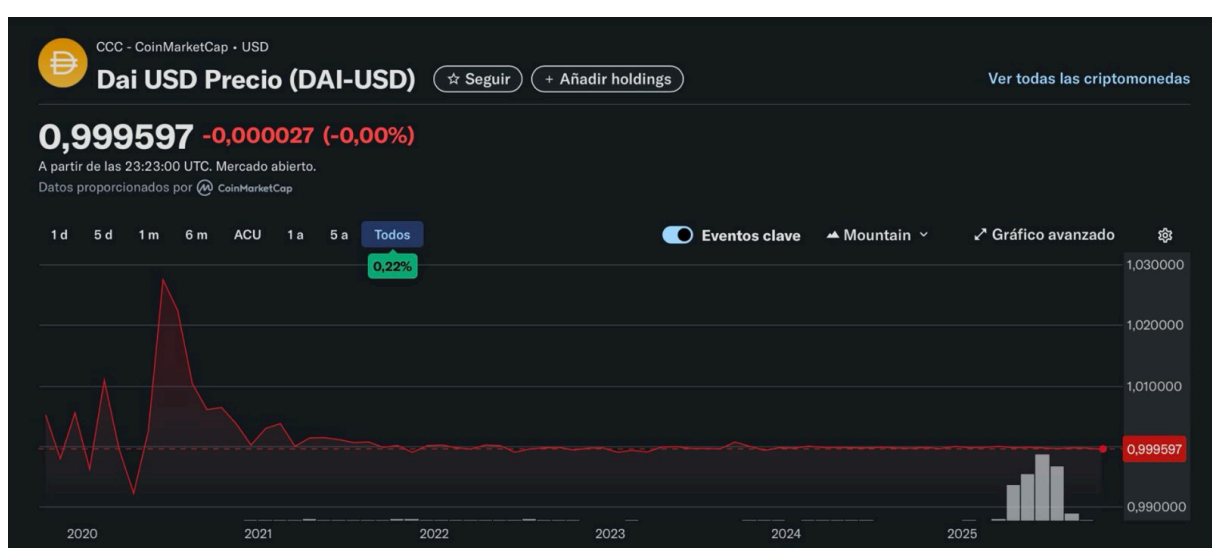


Figure 6: Price movement around the peg to the dollar for Dai

Discussion

Viewed through a comparative macro-financial lens, USDT, USDC, and DAI delineate a continuum of monetary architectures within the stablecoin ecosystem. USDT embodies liquidity dominance grounded in reputation and scale, USDC institutionalizes transparency through regulation and DAI operationalizes decentralization through incentive design and smart-contract governance. Each achieves nominal stability through distinct mechanisms, corporate solvency, regulatory oversight, or algorithmic collateralization and thereby reflecting alternative approaches to the classical trilemma of monetary design: stability, decentralization, and credibility. Together, they provide a natural experiment in the privatization of money, where technology redefines not the function of currency, but the very source of trust on which monetary systems depend.

The evolution of DAI also reveals the complex trade-offs between decentralization and stability. With the introduction of the Peg Stability Module (PSM) in 2020, MakerDAO allowed users to swap USDC and DAI at a 1:1 face value, fundamentally altering its monetary mechanics. Prior to the PSM, DAI could only be created through over-collateralization, for example, locking 150% of the intended issuance value in ETH. However, when DAI's market price exceeded its peg due to excess demand, the system lacked a corrective mechanism. The PSM resolved this by enabling arbitrage between DAI and USDC, if DAI traded above \$1, users could mint DAI by depositing USDC and sell it for profit, pushing the price back down. While this innovation stabilized the peg, it also reduced DAI's effective decentralization, as a significant portion of its collateral now consists of USDC, a centralized and regulated asset. This shift illustrates the inherent paradox of decentralized monetary systems, where efforts to enhance stability often reintroduce centralized dependencies, blurring the boundary between algorithmic and institutional trust.

In addition to this analysis of existing stablecoins and their underlying mechanisms, I believe it would be important to design a stablecoin that follows a monetary policy rule, such as the Taylor Rule.

$$i_t = 2 + \pi_t + a(\pi_t - \pi^*) + b(y_t - y_t^*)$$

where:

- i_t is the prescribed value of the policy interest rate in period t

- $\pi_t - \pi^*$ is the deviation of the actual inflation rate from its target in period t
- $y_t - y^*$ is the output gap (deviation of actual real output from potential output) in period t
- a and b are positive numbers

I was unable to identify an existing stablecoin that explicitly applies this principle, but I consider it a promising development for a currency tailored to staking or lending platforms. By implementing such a rule, it would be possible to determine an equilibrium interest rate for the platform, based on a target inflation rate of the previously issued tokens and the observed inflation rate, while also incorporating the growth of on-chain activity (e.g., transaction volume) to evaluate whether the platform is operating above or below its reference level of economic activity. The value of the currency could then adjust dynamically as the interest rate changes, making it more or less attractive depending on its yield.

However, during my research for protocols of this kind, I came across Basis, which sought to implement a comparable monetary framework which can be understood as implementing an algorithmic central bank.

The Basis protocol accomplishes this by algorithmically adjusting the supply of Basis tokens in response to changes in, for example, the Basis-USD exchange rate. This implements a monetary policy similar to that executed by central banks around the world, except it operates as a decentralized, protocol-enforced algorithm, without the need for direct human judgment.

What I think is important about this is that it's not backed by anything other than the fact that it is stable. Because it is not backed by dollars, the way Basis plans to maintain its stability is by executing open market operations. In other words, that means the buying and selling of securities in the open market, in order to produce an expansion or contraction of the amount of money in the system. In Basis's case, it means an algorithm buys and sells what it calls "Basis bonds" on the blockchain of course in response to changes in demand. When the price is below a dollar, the protocol automatically sells the "bond token" on the blockchain for Basis. So the bond tokens go into circulation and Basis goes out of circulation, and that's how the supply of Basis contracts. It's almost exactly like an open-market operation from a central bank.

It allows people to essentially buy a bond for less than par value, which is what traditional monetary systems do. When Basis is selling these bond tokens, their par value is 1 because they (the bondholders) are eventually going to get paid

back one full Basis. But the market participants can buy them for less than one full Basis. That effectively contracts the supply and provides an incentive for people to buy Basis on the market.

I found it relevant and important to briefly include the functionality of this protocol, since Basis represents one of the most innovative attempts to apply traditional monetary and financial principles to a stablecoin framework that operates without any collateral backing. Unlike the three stablecoins analyzed above, Basis sought to maintain price stability not through reserves or over-collateralization, but through algorithmic monetary policy, adjusting supply and demand via the issuance and redemption of bonds and shares. This design made it conceptually closer to a central bank operating under a rule-based regime, where stability is achieved through endogenous market incentives rather than external guarantees.

b) Design

While working on the previous part of the challenge, I realized that by exploring the example of the Basis protocol, I had already been addressing the second question from Section B. For that reason, I will begin this section by expanding on that example, as it naturally connects to the idea of designing a stablecoin in an environment where collateral assets are highly risky or unreliable.

Designing a stablecoin in an environment where all potential collateral assets are highly volatile and prone to liquidation fundamentally challenges the conventional architecture of fiat-backed or crypto-collateralized models. When collateral cannot serve as a reliable source of value, stability must instead emerge from endogenous monetary policy rule based algorithms.

A viable design in this high-risk environment would therefore resemble an algorithmic stablecoin governed by an explicit monetary policy reaction function, inspired by traditional macroeconomic frameworks such as the Taylor Rule. In conventional monetary economics, the Taylor Rule prescribes how a central bank adjusts its policy rate in response to deviations of inflation and output from their target levels. Translating this into a crypto-economic setting, the protocol could dynamically adjust interest rates on staking or lending, token emission rates, or redemption incentives based on deviations between the target token inflation rate and the observed inflation of the circulating supply, and the growth rate of on-chain activity relative to a reference baseline.

If inflation of the token supply rises above the target, the system could increase the staking or borrowing rate, incentivizing users to lock tokens and thereby

reducing circulating supply. Conversely, if inflation falls below the target or economic activity weakens, the protocol could lower the rate, stimulating issuance and spending.

The goal is to emulate a form of monetary equilibrium, where the interest rate, token supply, and network activity jointly stabilize the token's value not through external collateral, but through algorithmic monetary discipline.

Such a system could also incorporate bond and share mechanisms similar to those pioneered by Basis (Basecoin), one of the earliest attempts at a collateral-free stablecoin. As previously seen, Basis introduced a three-token model, stablecoins, bonds, and shares, designed to manage supply through market-driven issuance and redemption. When the stablecoin traded above its peg, new tokens were issued and sold, diluting shareholders; when it traded below, the system issued bonds to absorb liquidity, redeemable when prices recovered.

The principal innovation of this design lies in shifting the foundation of stability from asset-backing to expectation management. In the absence of safe collateral, the protocol's credibility must arise from consistent rule enforcement, transparency, and the rational anticipation of future policy actions. This model transforms the stablecoin from a passive claim on reserves into an active monetary instrument, one whose value is stabilized through systematic, data-driven policy reactions rather than static collateral guarantees.

In contrast to the mechanisms explained before, in a hypothetical environment where all collateral assets are perfectly stable and cannot lose value under any circumstance, the design of a stablecoin would become a lot easier. Without the need to hedge against price fluctuations or liquidation risks, any asset could serve as collateral, and a fixed exchange rate could be maintained indefinitely. The system would not require incentive mechanisms such as over-collateralization ratios, stability fees, or liquidation thresholds, since the collateral's value would remain constant over time.

In such a world, it would be possible to design a fully decentralized stablecoin architecture, as no external governance or risk management would be necessary. For instance, if assets like Bitcoin or Ethereum were entirely non-volatile, they could be used directly as collateral at a fixed rate (1 ETH = 1 Coin) without the need for any dynamic adjustment or capital buffer. The protocol would only need to monitor supply equivalence to ensure that the issued tokens match the underlying collateral, maintaining perfect solvency through accounting parity alone.

From a macroeconomic perspective, this system would resemble an ideal currency board, where money supply is entirely backed by a non-depreciating asset and price stability is inherent to the underlying value of that asset. Monetary policy would become redundant, as no mechanism for demand management or market intervention would be required. While purely theoretical, this thought experiment highlights how the very need for stablecoin design arises from market imperfection and asset risk. If risk disappeared, so too would the necessity for monetary innovation.

c) Model

This subsection models the economics of a run against an algorithmic stablecoin using the Terra–UST collapse as a benchmark case. I decided to use this example to help me explain the mechanisms of a “death spiral” or “bank run” in a de-peg of an algorithmic stablecoin in order to create a simple model based on the events that produced the crisis in 2022.

In the beginning, Terra combined an on-chain mint/burn convertibility between UST and LUNA with a heavily subsidized savings protocol (called Anchor). The design created a loop, where as deposits surged to capture yield, the outstanding UST supply grew, and the system became more fragile to a coordination event. When the peg faltered in 2022, redemptions and arbitrage minted large amounts of LUNA, depressing its price and accelerating the “death spiral” that ultimately destroyed both tokens. The run unfolded across chains and was amplified by transparent on-chain observability, with large wallets exiting first.

In other words, UST functioned as a dollar-pegged liability convertible, via a native swap, into one dollar worth of LUNA, while the reverse operation minted UST against LUNA (burning LUNA). This arbitrage channel relied on accurate oracle prices and sufficient risk appetite by investors were the system remained viable only if swap-induced dilution of LUNA did not trigger pre-emptive LUNA selling (Burning UST, minting LUNA and therefore decreasing LUNA market cap and its value because of excessive supply).

Anchor’s (The lending protocol which captured deposits) role was pivotal, it offered 20\% yields and, prior to the crash, held roughly three-quarters of the UST float, a composition that maximized run externalities because a single venue concentrated all the deposits. This type of subsidy for deposits produced its growing unsustainability as deposits skyrocketed, as well as the fact that 75\% of circulating UST sat in Anchor before the 2022 collapse.

Before the crash, liquidity conditions around the UST Curve pool deteriorated amid migration to a new pool where large wallets withdrew UST from Anchor and sold on Curve, widening the discount and triggering further exits. The Luna Foundation Guard mobilized reserves in an attempt to restore the peg. Later on, UST traded below \$0.20 and LUNA had essentially collapsed.

In figure 8 we observe the collapse of the hourly price of LUNA and the de-peg of the UST compared to the price of Bitcoin.

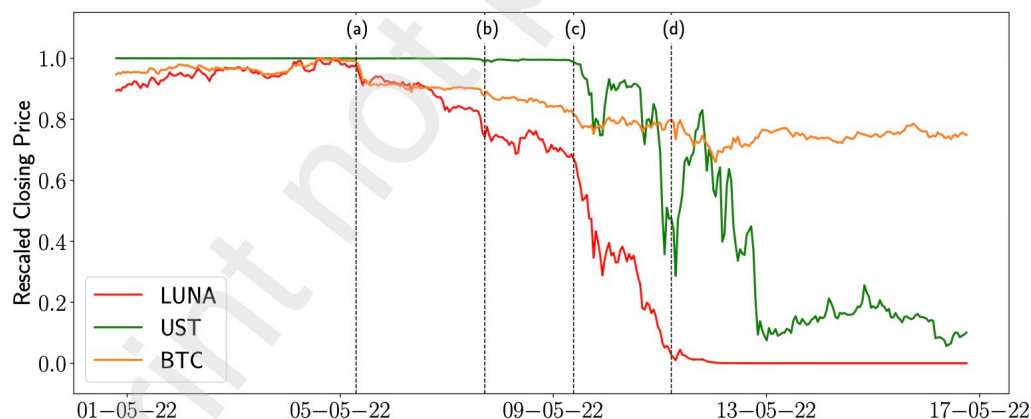


Figure 8: Collapse of the hourly price of LUNA

Figure 9 shows us the total collapse of the LUNA price against de dollar since its creation up to date.



Figure 9: Collapse of the LUNA price against de dollar since its creation up to date.

Now we consider an attacker who can trade across venues and use the native swap.

Let P_t^{UST} denote the secondary-market UST price, M_t the LUNA market cap, S_t^{UST} the UST supply, and ϕ_t a dilution factor mapping a UST-LUNA swap into incremental LUNA minted and expected price impact.

When $P_t^{UST} < 1$, swapping x units of UST via the native module yields x dollars' worth of new LUNA that can be sold at expected price $\mathbb{E}[p_t + 1^{LUNA}(x)]$.

The per-unit gross "arbitrage" value of the swap is approximately $1 - P_t^{UST}$, but the monetizable profit is reduced by:

1. Swap fees and caps.
2. Liquidation costs and slippage when selling LUNA into finite depth.
3. Endogenous price impact through ϕ_t , which increases with x and with the ratio S_t^{UST}/M_t .

The exciter's problem is to choose x to maximize:

$$\Pi(x) \approx x(1 - P_t^{UST}) - \underbrace{F_{\text{swap}}(x)}_{\text{fees/caps}} - \underbrace{\text{ImpactLUNA}(x; L)}_{\text{depth/slippage}} - \text{tx fees}$$

A "bank run" equilibrium emerges when many agents reach $\Pi(x) > 0$ simultaneously, and when expectations internalize that other agents' swaps will depress p^{LUNA} further via dilution, raising future .

More swapping produces more LUNA supply, which also decreases its value. Rational LUNA holders front-run by selling, causing the "death spiral."

If we define a fragility ratio:

$$\kappa_t \equiv \frac{S_t^{UST}}{M_t}$$

then, when κ_t is small, dilution from conversions is negligible and arbitrage restores the peg.

As κ_t approaches one, the system breaks and conversion flows produce large LUNA issuance, lowering M_t (the market cap) because of depreciation as the LUNA supply increases, which in turn raises κ_t further.

Withdrawals accelerate precisely when market participants observe that LUNA's market value converges to the outstanding UST, a small public signal producing a shift to the "run" equilibrium through rational expectations.

In reduced form, an attack is profitable when UST trades at a discount large enough that $x(1 - P_t^{UST})$ exceeds cumulative frictions, and when the agent expects subsequent dilution to degrade LUNA sufficiently fast that waiting is dominated by exiting now.

The run becomes self-fulfilling if many agents share this belief.

From this framework I find it interesting to observe that if we limit κ_t algorithmic stablecoins need explicit caps tying UST issuance to the market value of risk-absorbing equity (LUNA). Additionally, if most demand is subsidized savings (because of the subsidized deposits through Anchor), redemptions become one-sided when the subsidy is questioned. This was produced because demand for UST did not come from natural demand to transact and save money but from the incentive given by the subsidy for deposits in Anchor. Sustainable and natural demand reduces the massed-exit risk. Finally, we could create temporal limits for transactions or higher cost of conversion in order to reduce incentives to sell and reduce stress in users to bound ϕ_t and give market makers time to supply extra liquidity. Terra also raised native swap limits over time, which increased the surface for large and fast exits when confidence cracked.

Bibliography

1. Briola, A., Vidal-Tomás, D., Wang, Y., & Aste, T. (2022). Anatomy of a Stablecoin's Failure: The Terra–Luna Case.
University College London, Universitat Jaume I, Systemic Risk Centre (LSE). SSRN Working Paper No. 4184502.
[Available at SSRN](#)
2. Liu, J., Makarov, I., & Schoar, A. (2023). Anatomy of a Run: The Terra–Luna Crash.
MIT Sloan School of Management, London School of Economics, and NBER Working Paper.
[Available at MIT/LSE](#)

3. MakerDAO (2017). The Dai Stablecoin System Whitepaper.
[MakerDAO Whitepaper](#) oai_citation:0#DaiDec17WP.pdf
4. Tether Limited. (2014). Tether: Fiat Currencies on the Bitcoin Blockchain.
[Tether White Paper](#)
5. Circle Internet Financial LLC. (2025). USDC Terms and Conditions.
[Circle Legal Documentation](#)
6. Coinbase Global, Inc. (2025). Platform Overview and Legal Disclosures.
[Coinbase Official Site](#)
7. [DeFiLlama – Decentralized Finance Data Aggregator](#)
Comprehensive real-time dashboard of DeFi protocols, stablecoin metrics, and liquidity data. Used for historical and comparative analysis.
8. [Dune Analytics – On-chain Data Explorer](#)
Platform for blockchain analytics and visualization, providing on-chain datasets and SQL-based dashboards on stablecoins, swaps, and liquidity flows.