An Overview of Stablecoin Architecture

Summary

Crypto stablecoins are a type of cryptocurrency that aims to maintain a stable value relative to a target asset, such as a fiat currency or a commodity. This is achieved through a variety of mechanisms, including fiat collateralization, algorithmic stabilization, and hybrid models.

Stablecoins offer a number of advantages over traditional cryptocurrencies, including:

- Price stability: Stablecoins are designed to maintain a stable value, making them more suitable for use as a medium of exchange and store of value.
- Lower volatility: Stablecoins are less volatile than traditional cryptocurrencies, which makes them more attractive to risk-averse investors.
- Global reach: Stablecoins can be used to send and receive payments anywhere in the world with low fees and fast transaction times.
- Programmability: Stablecoins can be programmed to execute smart contracts, which enables new and innovative financial applications.

There are generally four main types of crypto stablecoins:

- Fiat-collateralized stablecoins: These stablecoins are backed by fiat currencies, such as the US dollar or the euro. The issuer of the stablecoin holds a reserve of fiat currency equal to the value of all outstanding stablecoins. This type of stablecoin is considered to be the most stable, but it is also the most centralized.
- Crypto-collateralized stablecoins: These stablecoins utilized native cryptocurrencies as their collateral and are minted once a user locks up native crypto worth 150%+ worth of the newly minted stablecoin into a Collateralized Debt Position (CDP).
- Algorithmic stablecoins: These stablecoins use algorithms to maintain their peg to a target asset. The algorithm typically adjusts the supply of the stablecoin based on its price. This type of stablecoin is more decentralized than fiat-collateralized stablecoins, but it is also more complex and riskier.
- Hybrid stablecoins: These stablecoins combine elements of both fiat-collateralized and algorithmic stablecoins. For example, a hybrid stablecoin might be backed by a basket of assets, including fiat currencies and cryptocurrencies. This type of stablecoin offers a balance of stability and decentralization.

Despite their promise, crypto stablecoins face a number of challenges, including:

- Technology risk: Because stablecoins can be designed in numerous ways to optimize for different things, technological risk associated with these nascent financial products is ever-present. It is important to carefully evaluate each stablecoin separately based on its design and intentions.
- Centralization risk: Some stablecoins are highly centralized, meaning that the issuer has a great deal of control over the stablecoin. This could (and has) lead to censorship or abuse.
- Regulation: The regulatory landscape for stablecoins is still evolving. Governments around the world are developing regulations to address the potential risks posed by stablecoins, such as money laundering and terrorist financing.

Crypto stablecoins have the potential to revolutionize not only the crypto industry but also the traditional finance (TradFi) sector as well. They offer a number of advantages over traditional financial systems, including lower fees, faster transaction times, and global reach.

Overview

Navigating the cryptocurrency landscape demands both risk tolerance and a strategy to weather the often-turbulent market conditions. Enter stablecoins, digital assets designed to provide investors with a semblance of stability amid the inherent volatility associated with crypto assets. Thanks to their combination of stability, liquidity, and speed, stablecoins have become an unignorable aspect of nearly all crypto sectors.

The essence of a stablecoin's value stability stems from its underlying collateral. Unlike conventional cryptocurrencies, which can see drastic price swings within short time frames, stablecoins operate with a pegged value. This peg, often linked to established fiat currencies like the USD, provides a predictable and stable asset value. The actual value of the stablecoin remains in equilibrium with the fiat currency to which it is anchored, eliminating the wild price fluctuations common in the crypto domain.

Stablecoins seamlessly merge the frictionless attributes of blockchain transactions with the robustness of well-established currencies like the USD. This fusion brings forth an unparalleled blend of efficiency and reliability, all while never having to leave the on-chain blockchain environment. For crypto traders, this capability ensures that they remain shielded from potential market downturns without having to constantly transfer assets between crypto and traditional banking systems.

Because of these attributes, stablecoins have emerged as an indispensable cornerstone of the crypto economy. Their influence spans a myriad of functions, from trading to lending, and even asset management. Despite the bear market in crypto prices in 2023, interest in stablecoins has remained considerably more stable.

Although stablecoins, as a whole, are gaining prominence in the cryptocurrency world due to their promise of stability, it is crucial to understand that their structures differ, and these distinctions can significantly impact their reliability and use cases. The most straightforward (and popular) mechanism to ensure stability in a stablecoin is to back it on a 1:1 ratio with fiat currency, usually held in a bank. This methodology, chosen by market frontrunners like USDT and USDC, guarantees that for every coin in circulation, there's a corresponding dollar in reserves.

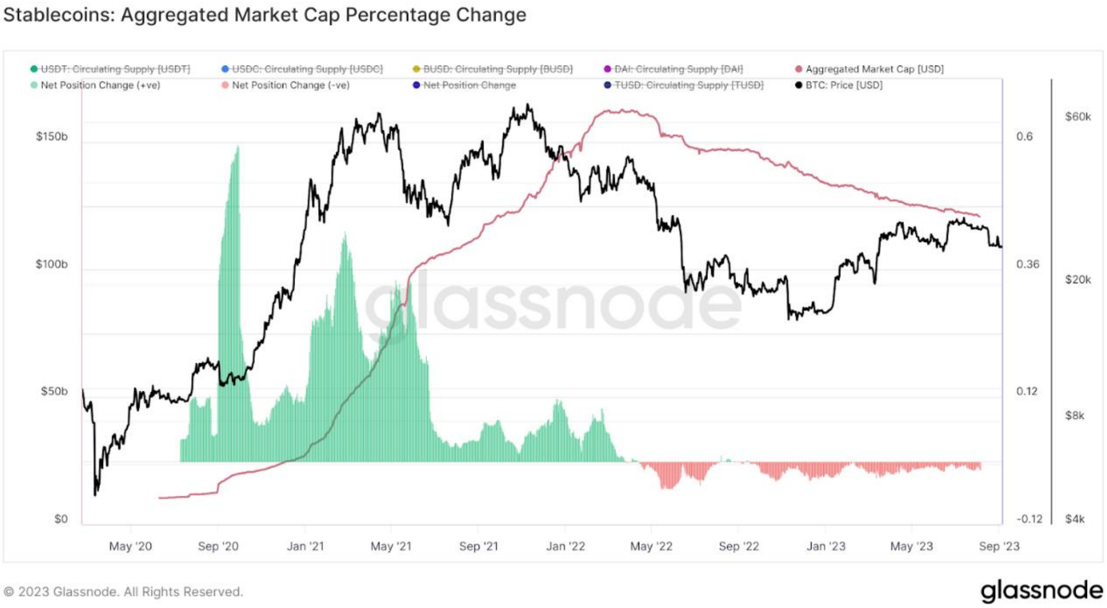
However, while such a system is relatively simple to implement, it does not solve the issues around counterparty risk and censorship resistance that other crypto assets look to solve. The use of fiat as collateral means that the stablecoin inherits the vulnerabilities associated with traditional currencies. Additionally, relying on a centralized entity to hold reserves necessitates trust in that institution's credibility, deviating from the decentralized ethos that cryptocurrency enthusiasts often advocate for.

Not all stablecoins tie their value to fiat currencies. Some stablecoins, like PAXG, choose a different route and are collateralized by commodities, such as gold. This offers an alternative store of value that's theoretically more tangible and resistant to inflation compared to fiat.

For cryptocurrency investors and users, understanding stablecoins' nuances is paramount. With an impressive market capitalization and wide-ranging applications, stablecoins have solidified their place in the crypto ecosystem. But as centralized, fiat-backed stablecoins continue to dominate the market, new entrants and models challenge the status quo. As the stablecoin market diversifies and evolves, continuous research and vigilance are essential for those aiming to utilize these instruments effectively.

Stablecoins as a Whole

Crypto stablecoins are becoming increasingly popular, both among retail and institutional investors. The total market capitalization of stablecoins has grown from around $5 billion in early 2020 to over $120 billion in September 2023.

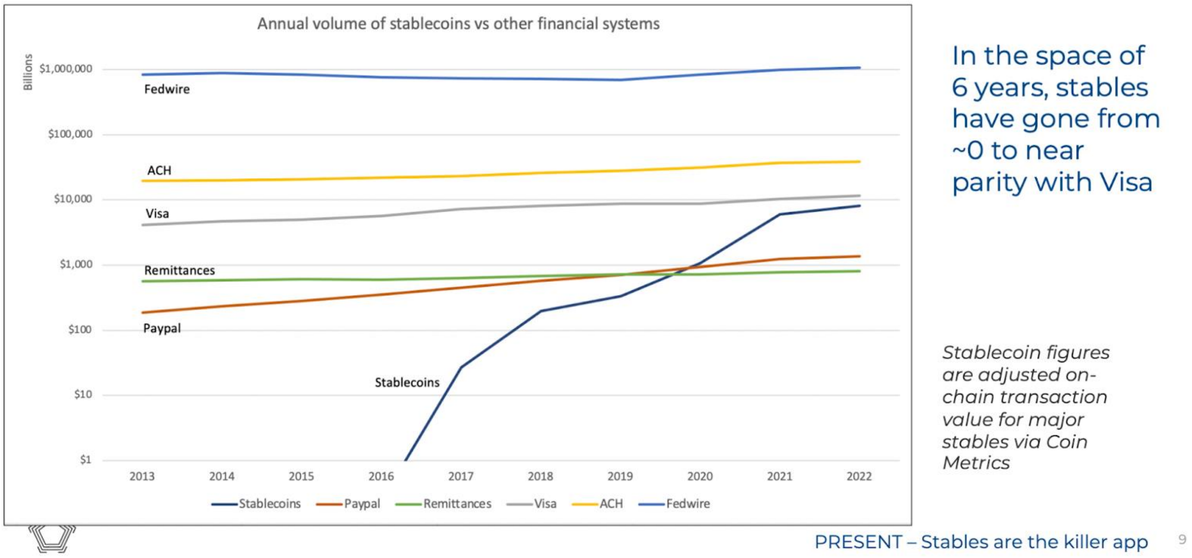


Source: Glassnode

Stablecoins are being used for a variety of purposes, including:

- Payments: Stablecoins can be used to make payments to merchants and individuals around the world.
- Investing: Stablecoins can be used to invest in other cryptocurrencies or to earn interest through yield farming.
- Remittances: Stablecoins can be used to send and receive remittances quickly and cheaply.
- Financial services: Stablecoins are being used to develop new financial services, such as decentralized lending and borrowing platforms.

In a notable achievement of adoption, the transferred values of stablecoins in 2022 outpaced those of established payment giants such as PayPal and Mastercard (second image). Such a comparison offers a glimpse into their increasing popularity and utility. However, there's a caveat: the frequency of stablecoin transactions remains significantly lower (0.5-3%) than that of the numbers reported by traditional payment networks. This discrepancy suggests that, while stablecoins might be catching up in value transfer, they are typically reserved for larger, less frequent transactions.



In the space of 6 years, stables have gone from ~0 to near parity with Visa

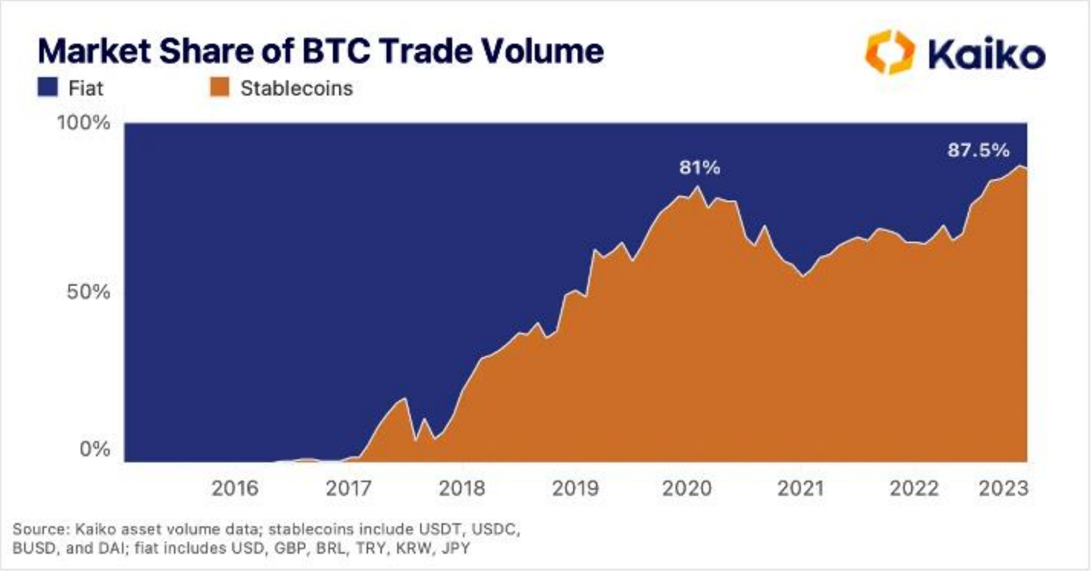
Stablecoin figures are adjusted on-chain transaction value for major stables via Coin Metrics

PRESENT – Stables are the killer app

Source: CoinMetrics, Nic Carter, Token2049 Presentation

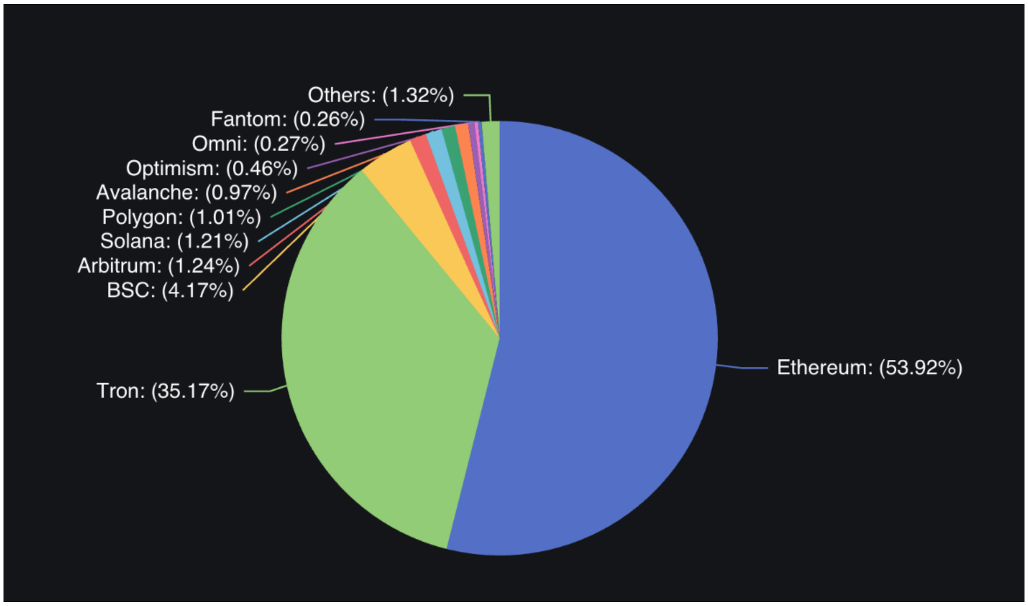
Several factors suggest that stablecoins will continue on their upward trajectory, like Paypal's recent PYUSD release and Visa's announcement to utilize USDC and the Solana blockchain for transaction settlement. As these traditional entities embrace blockchain-backed fiat representations, it paves the way for a more comprehensive adoption by conventional users.

Although TradFi announcements and experimentation are exciting, as it stands today, stablecoins' primary use case remains crypto trading. As of late 2022, an overwhelming majority (approximately 90%) of Bitcoin's trading volume is denominated in stablecoins, predominantly Tether's USDT. This shift underscores the market's preference for a stable medium of exchange and store of value in a notoriously volatile trading environment.



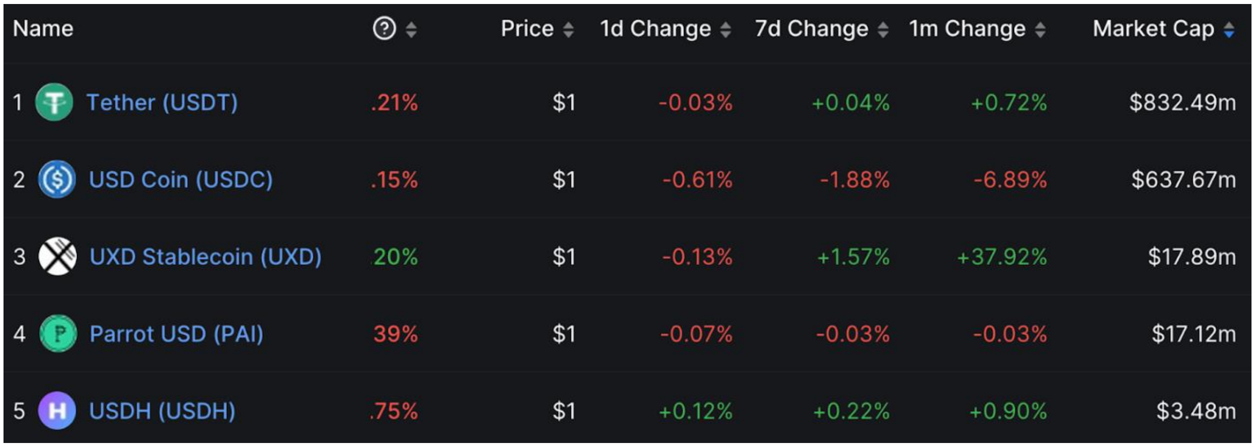
Source: Kaiko, as of January 2023

The stablecoin ecosystem is largely dominated by the two industry leaders, Ethereum and Tron. The two blockchains are currently home to ~90% of all stablecoin TVL in the crypto ecosystem. Despite the top-heavy distribution, stablecoins are critical for any protocol's adoption and well-known names like Binance, Arbitrum, Solana, Polygon, and more are looking to grow their stablecoin economies despite the bear market. Stablecoins on Solana are still a small portion of the overall stablecoin supply at ~1.2%, albeit still good for ~5th place among major blockchains.



Source: DeFiLlama

Tether (USDT) and USDC constitute nearly all the stablecoin TVL on Solana (~99%), while a slew of long-tail stablecoins round out the other ~1%.



Name	?	Price	1d Change	7d Change	1m Change	Market Cap
1 Tether (USDT)	.21%	$1	-0.03%	+0.04%	+0.72%	$832.49m
2 USD Coin (USDC)	.15%	$1	-0.61%	-1.88%	-6.89%	$637.67m
3 UXD Stablecoin (UXD)	20%	$1	-0.13%	+1.57%	+37.92%	$17.89m
4 Parrot USD (PAI)	39%	$1	-0.07%	-0.03%	-0.03%	$17.12m
5 USDH (USDH)	.75%	$1	+0.12%	+0.22%	+0.90%	$3.48m

Source: DeFiLlama

The Many Different Stablecoin Designs

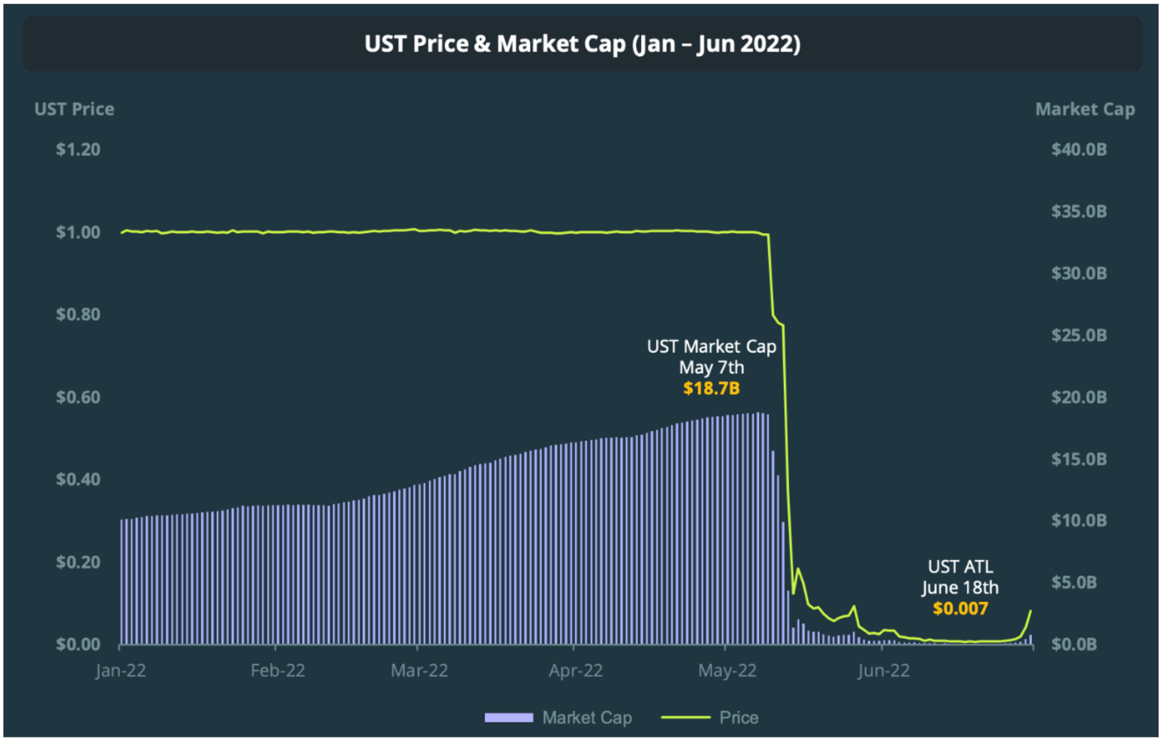
Despite (nearly) all stablecoins sharing the same objective, to maintain a stable peg, there exist dozens of different implementations across the crypto landscape. Each approach comes with its own set of pros and cons, tradeoffs and compromises, and risks/rewards. It is crucial for the end user to understand the stablecoin design because as we have seen time and time again, just because it is called a “stablecoin” does not guarantee the asset will remain stable forever.

What Is the Peg and Why Is It So Important?

A "peg" defines a set exchange rate between two assets, differentiating itself from "floating" currencies that lack a fixed price and operate on a more flexible monetary framework. Within the cryptocurrency realm, a peg dictates the precise value a token seeks to maintain. This concept is predominantly observed in stablecoins, digital currencies designed to sustain consistent value over prolonged periods.

While the inception of the crypto ecosystem aimed at introducing an alternative to conventional fiat currencies, there are undeniable benefits to a reliable stablecoin that maintains a $1 USD peg. One benefit of anchoring a cryptocurrency to a fiat standard is the semblance of stability it introduces amidst the notorious volatility of the crypto market. Look no further than crypto’s largest and most mature asset: Bitcoin. Its meteoric rise to ~$69,000 in 2021, only to plummet to a sobering ~$17,000 within a year illustrates just how volatile the industry can be. Stablecoins, however, act as a stabilizing mechanism for a digital currency, shielding investors from precipitous value swings.

However, this stability isn't always guaranteed. “Depegging" events are not uncommon and emerge when the value of a stablecoin diverges from its designed peg. To illustrate, when a fiat-anchored stablecoin valued at $1 USD dips below this benchmark, it's perceived as having depegged. This deviation often triggers alarms about the currency's efficacy and is especially treacherous for stablecoins that lack collateral or rely on algorithms. In instances where a market downturn outstrips the algorithm's capability to adjust, the stablecoin can lose its peg, engendering further challenges. Terra UST stands as a testament to the vulnerabilities of algorithm-driven stablecoin depegging.



Source: CoinGecko

In the following sections, we attempt to bucket several stablecoin projects into broad categories based on shared designs and implementations. Within each section, we will explore the nuances and differences that make each stablecoin unique, despite sharing the same category or designation.

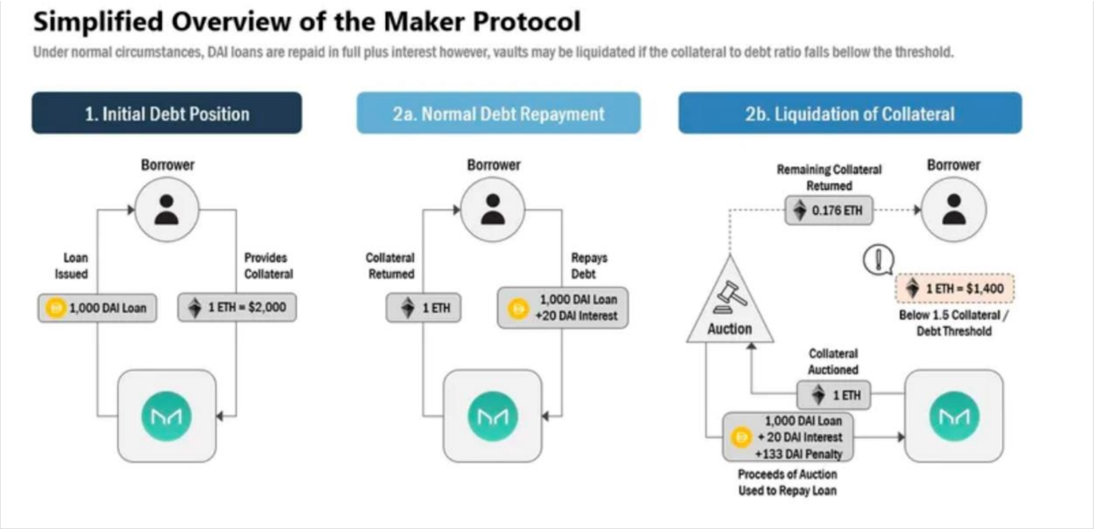
Crypto-collateralized Debt Positions (CDPs)

Stablecoins underpinned by other digital currencies, such as Bitcoin or Ether, are termed crypto-collateralized stablecoins. Given the inherent volatility of these reserve cryptocurrencies, the collateral necessary to create a stablecoin frequently surpasses 150% of the coin's value. It's imperative for the collateral reserves to consistently surpass the value of the stablecoin issued as a safeguard against insolvency. The largest (by market cap) and most famous crypto-backed stablecoin is Dai.

A core advantage of Dai is its transparent and over-collateralized nature. Unlike traditional systems where third-party trust is paramount, every Dai token is backed by ETH secured in transparent smart contracts on Ethereum. The transparency of this arrangement allows users to inspect the system's solvency in real-time and close out the loan position at any time.

MakerDAO's DAI

MakerDAO is a Distributed Autonomous Organization (DAO) on Ethereum's blockchain purpose-built to produce Dai, an over-collateralized stablecoin whose price stability is pegged to the US dollar. Using Ethereum as its foundation, MakerDAO empowers users to lock their Ether (ETH) and other approved crypto assets in smart contracts as a form of collateral and borrow against the collateral in the form of Dai. The stability of Dai, as opposed to the volatile nature of most cryptocurrencies, stems from a meticulous balance of collateralized debt positions (CDPs), self-regulating feedback mechanisms, and strategically placed incentives for third-party participants.


Simplified Overview of the Maker Protocol
Under normal circumstances, DAI loans are repaid in full plus interest however, vaults may be liquidated if the collateral to debt ratio falls bellow the threshold.
1. Initial Debt Position
2a. Normal Debt Repayment
2b. Liquidation of Collateral
Borrower
Loan Issued
Provides Collateral
1,000 DAI Loan
1 ETH = $2,000
Borrower
Collateral Returned
Repays Debt
1 ETH
1,000 DAI Loan +20 DAI Interest
Remaining Collateral Returned
0.176 ETH
Borrower
1 ETH = $1,400
Below 1.5 Collateral / Debt Threshold
Auction
Collateral Auctioned
1 ETH
1,000 DAI Loan + 20 DAI Interest +133 DAI Penalty
Proceeds of Auction Used to Repay Loan

MKR-DAI Diagram. Source: Messari

Consider a scenario: A DeFi user decides to use 10 ETH, valued at $30,000, as collateral within a Maker vault. Based on the vault's parameters, this would permit them to borrow up to ~20,000 Dai, given a 150% maximum collateralization ratio. If a user instead opts for a safer route, borrowing just 10,000 Dai, the collateralization ratio amplifies to 300%. Notably, fluctuations in Dai's market price do not impact the core dynamics of the vault. For instance, if Dai's price drops to $0.99, the vault's metrics remain constant, though it does present users with a strategic opportunity to purchase Dai at a reduced price and settle their loan.

Central to Dai’s stability are two significant components:

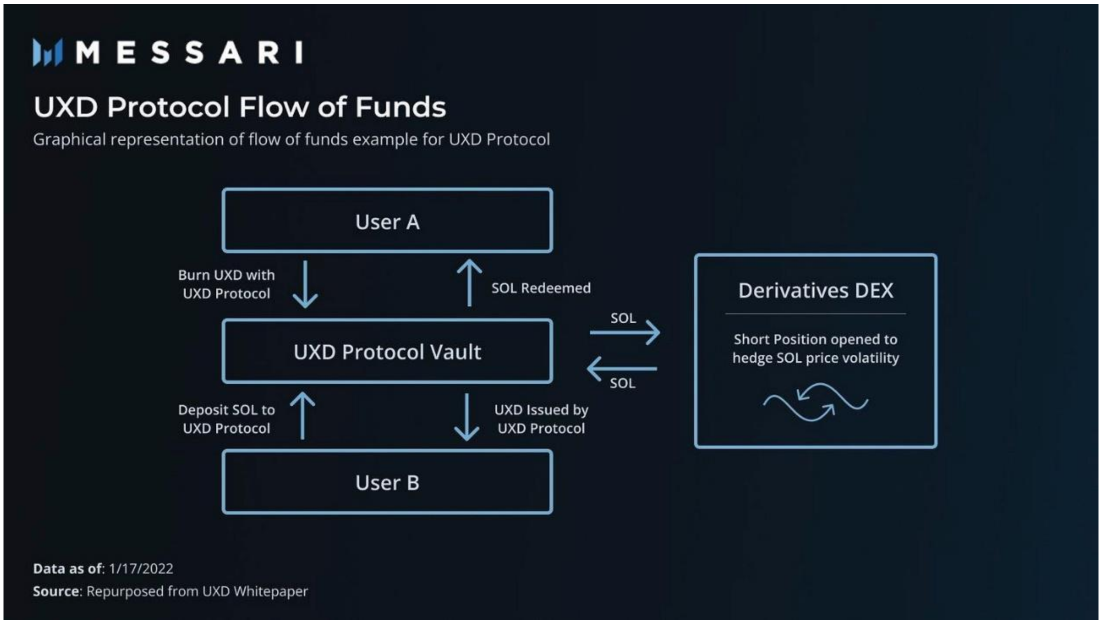
- The Stability Fee: Serving as the interest rate for borrowing Dai, the Stability Fee acts as a regulatory lever for Dai's supply. When the demand for Dai is less than optimal, the Stability Fee can be increased, making it less attractive for users to take out Dai loans. This reduction in borrowing can help keep Dai's price pegged to the US dollar.
- The Savings Rate: This is the interest given to those who deposit Dai, which assists in shaping Dai demand. An increase in the Savings Rate can stimulate demand for Dai, ensuring that supply and demand are harmoniously balanced.

UXD

UXD, a Solana-based stablecoin, is also backed by crypto collateral similar to Dai but takes it’s design a step further to try and ensure price stability around its $1 USD peg. UXD introduces a delta-neutral strategy in addition to the deposited collateral. Let's illustrate: when an individual deposits an equivalent of $1 in SOL to the UXD protocol, they're credited with 1 UXD. The system subsequently enters a short position on a decentralized futures exchange, utilizing the deposited $1 SOL as collateral. Through a strategic balance between long spot and short future, the protocol effectively ensures that the equivalence of $1 SOL to 1 UXD remains consistent, regardless of SOL's market fluctuations.

How UXD Works

Investors can deposit collateral, such as SOL, into the system. In return, they obtain an equivalent value in UXD - a one-to-one relationship between the deposited collateral and the issued stablecoin. Additionally, holding onto UXD provides investors with an attractive annual percentage yield (APY) of 5–40%, derived from the funding rate.



MESSARI

UXD Protocol Flow of Funds

Graphical representation of flow of funds example for UXD Protocol

User A
Burn UXD with UXD Protocol
SOL Redeemed
UXD Protocol Vault
SOL
SOL
Derivatives DEX
Short Position opened to hedge SOL price volatility
Deposit SOL to UXD Protocol
UXD Issued by UXD Protocol
User B

Data as of: 1/17/2022

Source: Repurposed from UXD Whitepaper

Source: Messari

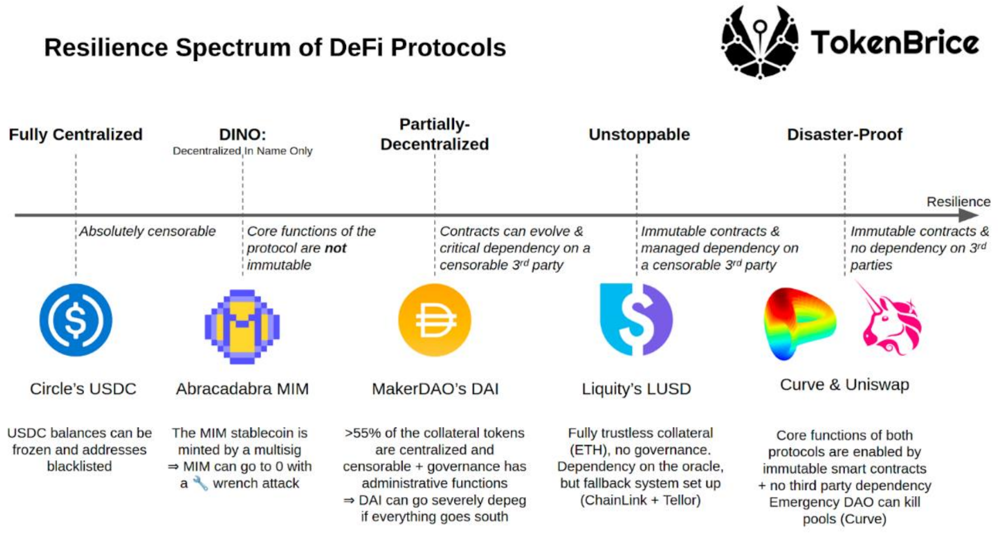
To ensure a level of protection against the notoriously unpredictable crypto market, the protocol engages in shorting the exact amount of this collateral. This process creates what financial experts refer to as a "perfectly hedged" position. This essentially means that the value of the collateral remains unswayed by market changes. For instance, consider a scenario wherein the collateral's price drops by 10%. While this would result in a 10% decrease in USD value for the deposited asset, the short position would concurrently gain 10% in USD value. The outcome? The collateral's USD value remains unchanged.

The UXD protocol's stability and success largely hinge on the efficacy of arbitrageurs. When there's a deviation in the UXD price from the $1.00 benchmark, traders possess the capability to deposit or retrieve UXD in exchange for collateral. They can then harness this opportunity to gain a risk-free profit, effectively maneuvering the token back to its peg. This intricate algorithmic architecture empowers the protocol to adeptly utilize volatile assets as backing for each UXD token at a 1:1 ratio, all while emulating stable assets as collateral.

Users can burn their UXD tokens with the protocol and in return, they're given the equivalent USD value in their preferred collateral token. The protocol then takes the necessary steps to close the short position for the exact dollar equivalent of the UXD that has been burned. The liberated collateral is seamlessly channeled back to the UXD protocol, and from there, it finds its way back to the user.

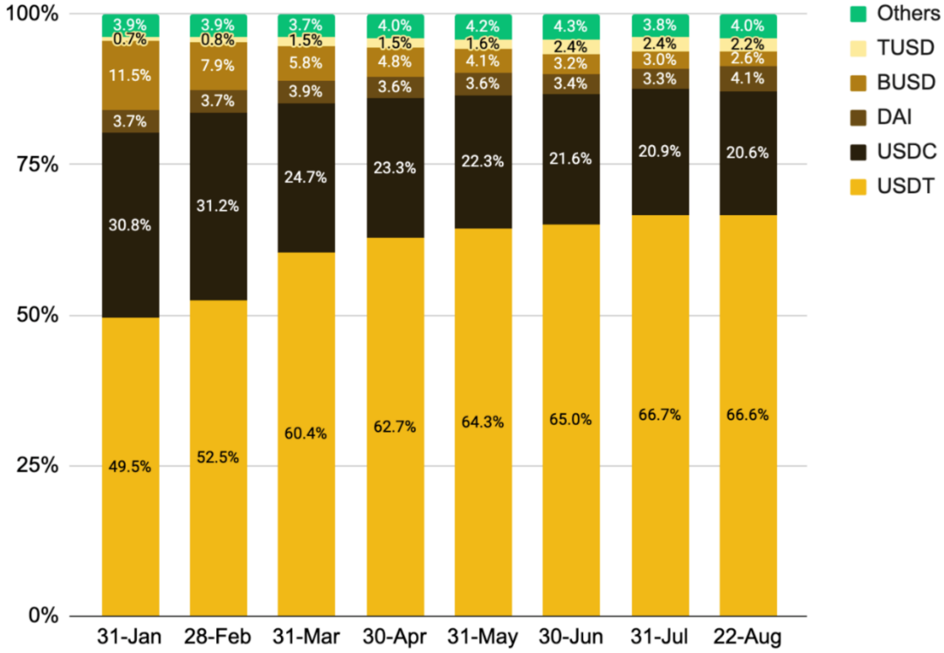
Fiat-collateralized (Exogenous) Stablecoins

Fiat-collateralized stablecoins are USD-pegged crypto stablecoins backed by U.S. dollars (and bonds) and maintained by a centralized entity. The digital currency is anchored to the price of an underlying asset (e.g.: US dollars, euros, yuan, gold) and redeemable 1-for-1 with the underlying currency. Importantly, they do not, in any way, provide the same censorship or seizure-resistant guarantees of a native crypto asset like BTC or ETH. They are centralized dollar IOUs, maintained by for-profit companies, on blockchain rails.


Resilience Spectrum of DeFi Protocols
TokenBrice
Fully Centralized
DINO:
Decentralized In Name Only
Partially-Decentralized
Unstoppable
Disaster-Proof
Resilience
Absolutely censorable
Core functions of the protocol are not immutable
Contracts can evolve & critical dependency on a censorable 3rd party
Immutable contracts & managed dependency on a censorable 3rd party
Immutable contracts & no dependency on 3rd parties
Circle's USDC
Abracadabra MIM
MakerDAO's DAI
Liquity's LUSD
Curve & Uniswap
USDC balances can be frozen and addresses blacklisted
The MIM stablecoin is minted by a multisig ⇒ MIM can go to 0 with a 🔧 wrench attack
>55% of the collateral tokens are centralized and censorable + governance has administrative functions ⇒ DAI can go severely depeg if everything goes south
Fully trustless collateral (ETH), no governance. Dependency on the oracle, but fallback system set up (ChainLink + Tellor)
Core functions of both protocols are enabled by immutable smart contracts + no third party dependency Emergency DAO can kill pools (Curve)

Source: TokenBrice

Four primary centralized stablecoins, namely USDT, USDC, BUSD, and TUSD, together account for an astounding 85%+ of the entire stablecoin market. Of these, Tether's USDT has been making waves, consistently cementing its dominance. It currently boasts an impressive 66% of the market share, making it the undisputed leader in the space. The rise and consolidation of USDT have had implications for its counterparts. As it surged ahead, other stablecoins felt the ripple effects, witnessing a dip in their market shares.



Source: DeFi Llama, as of August 22, 2023

Source: DeFiLlama

Despite fiat-collateralized stablecoins all claiming to be backed 1-to-1 with U.S. dollar equivalents, the nature of their reserves varies significantly. USDC's backing mainly comprises US Treasury Bills and cash equivalents, fostering a sense of confidence among its users. In contrast, Tether's USDT maintains a diversified reservoir of assets that encompasses commercial paper, corporate bonds, and money market funds, among other investment avenues.

But the industry learned in March 2023 that the allure of asset-backed stablecoins doesn't necessarily render them immune to centralization risks. A pertinent case study is the unfortunate episode involving Silicon Valley Bank (SVB). Known for its extensive services to tech-oriented businesses, the bank found itself ensnared in a bank run on March 10, 2023. The dire circumstances led to its inevitable collapse and subsequent acquisition by the Federal Deposit Insurance Corporation (FDIC).

This was more than just a hiccup for the cryptocurrency community. Of the $42 billion collateralizing USDC, a staggering $3.3 billion in cash was anchored with SVB. The fallout was immediate. USDC's peg wavered, dropping from its standard $1 to approximately $0.88 on March 11, 2023. Relief came a day later when regulators assured that depositors would be compensated. Consequently, USDC bounced back, regaining its $1 peg by March 12. Yet, the incident underscored the looming centralization risks confronting asset-backed stablecoins.

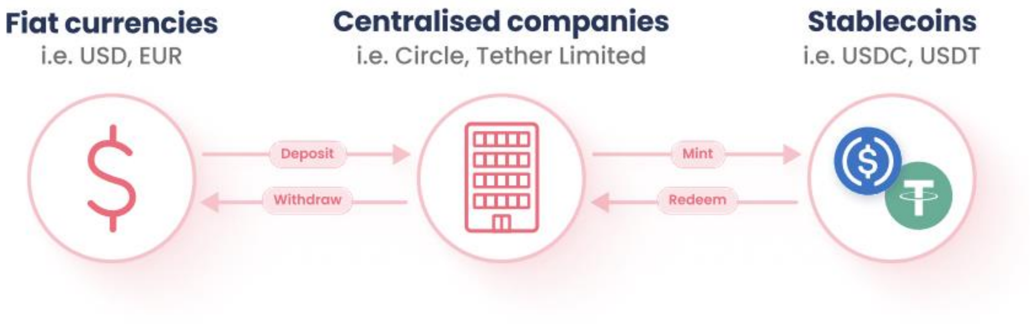
While the peg recovered, USDC has grappled with challenges, failing to bounce back to its former (market cap) highs. Likewise, BUSD has been on a downward trajectory, especially after Binance announced it will end support for BUSD this year. This has further contributed to its dwindling market share.

Tether (USDT)

Established in 2014 as "RealCoin," US Dollar Tether (USDT) has emerged as the industry leader in the world of stablecoins. Harnessing the benefits of the underlying blockchain technology, USDT provides an avenue for individuals and institutions to store, transmit, and acquire digital U.S. dollars with less friction than in the traditional financial system. While it predominantly mirrors the US dollar, Tether also offers other stablecoins pegged to other assets like euros (EURT), the Chinese yuan (CNHT), and even gold (XAUT).

What sets USDT apart is its combination of liquidity and its ability to facilitate rapid, peer-to-peer transactions, and price-stable transactions across a multitude of blockchains worldwide. Additionally, its transaction fees are a fraction of those associated with many conventional payment networks as well as being public and transparent. This streamlined approach is advantageous for holders, as USDT acts as a dollar-denominated bearer asset. Just like with traditional crypto assets, possession is guaranteed by a private key, allowing for full self-custody and P2P transactions without a third party's involvement.

Given USDT’s success, one may assume it became the industry leader thanks to some novel technological design. However, USDT's allure is not solely rooted in its technological prowess but in the issuer’s ability to reliably mint and redeem tethers. Its core principle revolves around Tether LLC holding an off-chain equivalent of $1 USD for every USDT released into circulation. Simultaneously, for every redemption, a corresponding USDT is removed from the blockchain. As such, the cornerstone of USDT's prominence hinges not on its technological framework but on the integrity and trustworthiness of Tether - an irony that is not lost on many in the crypto space.

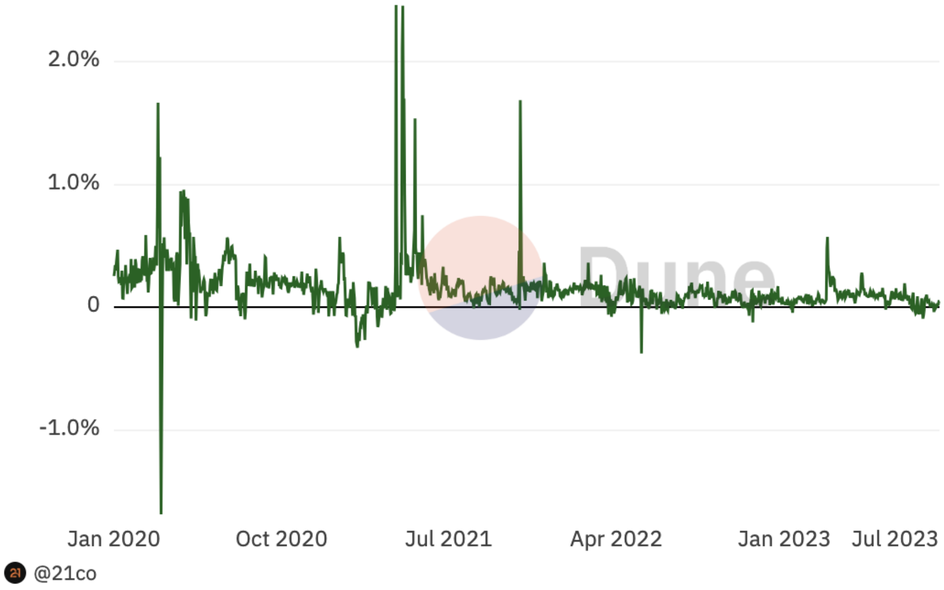


A simplified flow of funds in Fiat-backed stablecoins.

Source: Redstone.finance

Tether Ltd., stationed in Hong Kong, retains exclusive rights to modify the supply of USDT. According to the company, when fiat currency enters their bank account, they issue an equivalent amount of USDT. In the reverse scenario, Tether Limited retracts the corresponding supply when users exchange USDT to withdraw fiat currency.

Tether's redemption process diverges from its crypto counterparts in that holders wishing to exchange their USDT for USD must meet the minimum fiat withdrawal threshold of $100,000 and undergo a Know Your Customer (KYC) procedure. This high $100,000 redemption minimum, as well as a fee for redemptions, has caused friction for arbitrageurs in the current low liquidity environment and its effects can be seen in the price/peg. Given these constraints, it's often more economically viable for holders to offload USDT on open markets rather than pursuing a direct USD redemption with Tether.



Source: Dune

As liquidity levels taper off, the market's ability to absorb substantial USDT sales diminishes. Although the “depeg” from the $1.00 price isn’t substantial, a sustained discount on USDT (or any stablecoin) hurts the confidence in the stablecoin. The continuation of this trend might seriously undermine trust in the stablecoin.

USDC

USDC, a US dollar asset-backed stablecoin run by Circle, is the second-largest stablecoin and the leading stablecoin in the DeFi ecosystem. USDC differs from USDT in its approach to regulation and compliance by, rather than skirting them, leaning into and even touting its unwavering commitment to full compliance and transparency within the TradFi and regulatory systems. USDC and Cirlce see this as an advantage over their competitors and regularly subject their reserves to audits executed by neutral, third-party accounting firms.

Integral to the very fabric of USDC's operations is a cadre of licensed, regulatory-compliant banking associates, including esteemed entities such as Silvergate Bank, J.P. Morgan, and Signature Bank. These institutions play pivotal roles, extending crucial services such as fund transfer and custodial responsibilities.

In stark contrast to Tether, with its non-audited reserves and reliance on off-shore banks, USDC utilizes entrenched TradFi names like BlackRock and the Bank of New York Mellon to manage its predominately cash positions and custody. Meanwhile, US Treasuries are entrusted to credible third-party custodians, further solidifying the foundation of trust.

Several distinctive characteristics accentuate the USDC model:

- Transparency and Preparedness: USDC showcases a commitment to transparency, underscored by its proactive stance on instituting measures to brace for potential regulatory examinations down the line.
- Fiat-backed Assurance: While some stablecoins tether their worth to the speculative value of their utility or the volatile tides of other digital currencies, USDC's backbone is resolutely fiat collateral.
- Regulatory Oversight: The issuance and operations of USDC fall within the gaze of U.S. state money transmission regulators, ensuring that Circle's activities endure constant scrutiny.

The minting of new USDC tokens is initiated when entities deposit US government-backed currency into their Circle accounts. This act transmutes the physical asset into its digital counterpart on an exact one-to-one correspondence. As dollars flow into these accounts, Circle reciprocates by introducing an equivalent volume of USDC into circulation, enriching the digital ecosystem.

Conversely, when entities intend to exchange their USDC for tangible US dollars, they transfer their USDC into their Circle account which is then burned (removed from circulation), initiating a seamless, fee-free redemption process. This act subsequently contracts the circulating volume of USDC on the appropriate blockchain.

“Other” Collateral Types

LST-backed Stablecoin

Interestingly, the most common form of collateral in crypto might not be what one would expect – it's United States Treasury Bills. Stablecoins like USDT and USDC primarily use short-dated Treasury Bills as collateral. Despite the reliance on these traditional financial assets, the crypto space has recently begun to show an increasing appetite for decentralized, crypto-native, and yield-bearing collateral in the form of liquid staking tokens (LSTs).

Thus far, Ethereum (ETH) has been the undisputed king of DeFi collateral across multiple chains and, thanks to its recent move to Proof of Stake and the proliferation of liquid staking tokens like stETH and rETH, also leads in the LST-backed stablecoin market. The TVL (Total Value Locked) in Liquid Staking services such as Lido, Frax, and RocketPool is currently at nearly $18 billion, showing a significant demand for using these assets as collateral.

The benefits of LSTs as collateral are multifold. Not only do users gain staking rewards, but they can also use their staked assets as collateral to borrow further capital, allowing for significant capital flexibility. Projects like Lybra, Gravita, Raft, and Curve’s crvUSD are accepting LSTs as collateral for their stablecoins.

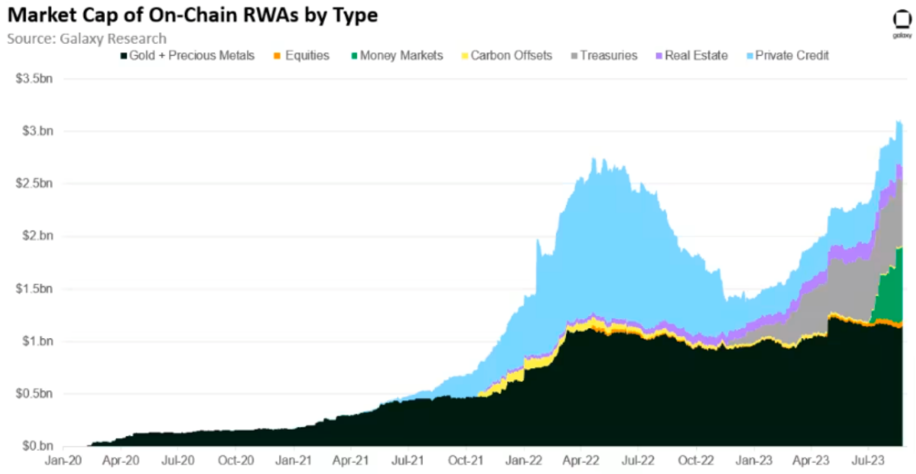
However, LSTs also carry risks associated with smart contracts, and the risk increases with more complex derivatives. Nonetheless, assets like stETH and wstETH from Lido have shown their security through rigorous audits and battle-testing. Additionally, many DeFi lending protocols have introduced siloed pools to contain bad debt should there be issues with a specific collateral type, thereby minimizing the risks associated with volatility.

In conclusion, the lending market within DeFi is maturing rapidly. As it continues to develop, crypto assets are gaining enough liquidity and price stability to form a robust base for collateral in a stable lending industry. The demand for and production of crypto-native collateral and products is poised to grow, offering new ways for crypto investors to gain yield and leverage.

Real-world Assets (RWA)-backed Stablecoins

"Real World Assets" or RWAs are any asset that is not native to the underlying blockchain. By this definition, fiat-backed stablecoins like USDT and USDC are backed by RWAs. However, USD-backed stablecoins are often bucketed into their own category given their straightforwardness and because they constitute ~90% of the market.

Typically, when discussing RWAs, one is referencing other off-chain assets from the TradFi world like treasuries, bonds, private debt, real estate, and other assets. Due to the sheer size of these markets (trillions), many crypto projects have begun experimenting with utilizing RWAs, including using them as collateral for their stablecoins.



RWAs on-chain have now surpassed $3 billion. Source: Galaxy Digital

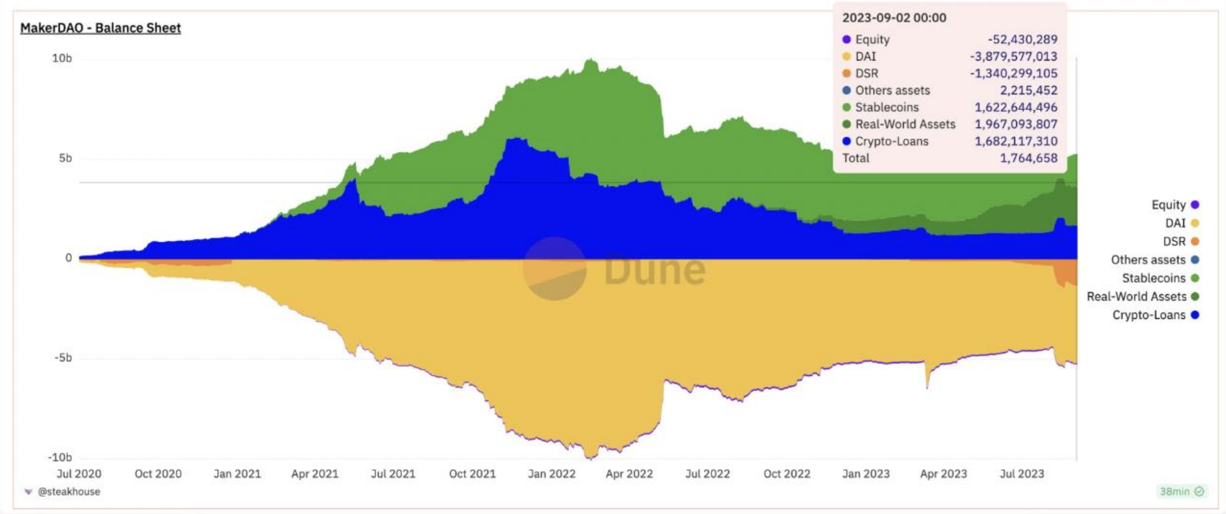
One of the market leaders in this area is Dai. As discussed in the prior section, Dai is the product of a crypto over-collateralized loan. However, over the years, MakerDAO has experimented with all sorts of collateral types, ranging from solely ETH in the early days, to predominately other stables like USDC in 2021, and now, as of 2023, has begun branching into the RWA space.

At its core, Maker's RWA initiative aims to further diversify the protocol's collateral in order to minimize risk and hedge against DAI's reliance on one collateral type. Maker has demonstrated a notable expansion of DAI backed by RWA within MakerDAO from August 2022 to the end of Q2

2023. Notable collaborations include those with Monetalis Clydesdale, Huntingdon Valley Bank, and BlockTower.

Monetalis Clydesdale's collaboration, specifically, presents MakerDAO with several benefits including an avenue to direct its latent PSM USDC towards more fluid bonds, enhancing the utilization of assets that would otherwise remain dormant.

Huntington Valley Bank offers another dimension to MakerDAO's RWA strategy. By facilitating a DAI credit line for the bank that's secured against the bank's own assets, MakerDAO positions itself to earn revenue from real-world loans. This ensures a more sustainable revenue stream for the DeFi project and treasury.



Source: Dune

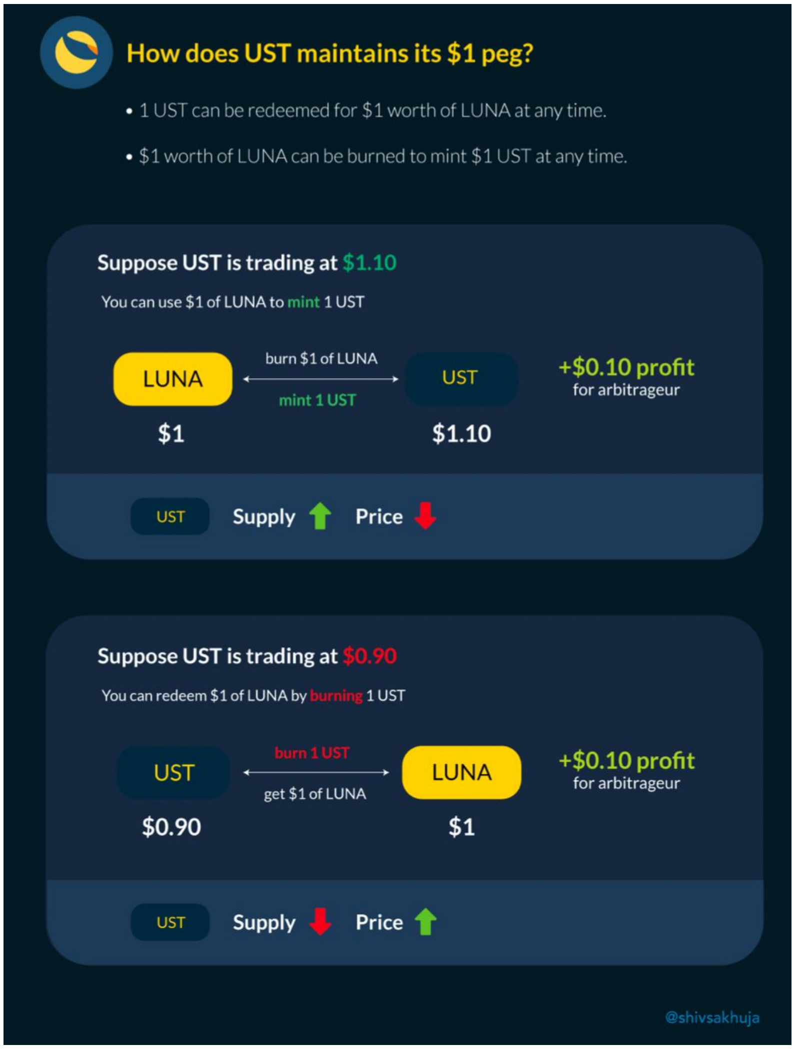
Algorithmic Stablecoins

Algorithmic stablecoins—which have been around for years but have fallen out of favor since the infamous Terra LUNA collapse—have no exogenous collateral backing them but rather use endogenous collateral and algorithms to control the stablecoin peg and the underlying tokenomics. They usually exhibit some or all of the following properties:

- No exogenous collateral backing the token
- Partially/fully collateralized by a native token (endogenous)
- Floating peg (e.g. RAI)
- Peg is (theoretically) maintained by code, seigniorage, and/or arbitrage opportunities

Unlike their counterparts that tether their value to tangible assets or other cryptocurrencies, algorithmic stablecoins embrace the principle of seigniorage, which in itself is rooted in time-honored currency issuance practices. Historically, seigniorage has been almost entirely contained to governmental authorities and denotes the profit the government realized from the issuance of its own currency. However, in the digital world, this age-old principle is repurposed to regulate the stability of stablecoin value by manipulating its supply relative to its demand.

To understand the seigniorage mechanism in the context of cryptocurrency, one must appreciate its inherent ability to recalibrate the supply of a stablecoin based on its prevailing market value. Imagine a scenario where the market value of a stablecoin outpaces its predetermined value. In such cases, the seigniorage mechanism springs into action, augmenting the stablecoin's supply by generating new tokens. These fresh tokens are then ushered into the market, inducing an anticipated dip in the price owing to the increased supply. Such a strategy aims to recalibrate the stablecoin's value, nudging it closer to its foundational value.



How does UST maintains its $1 peg?

- 1 UST can be redeemed for $1 worth of LUNA at any time.
- $1 worth of LUNA can be burned to mint $1 UST at any time.

Suppose UST is trading at $1.10

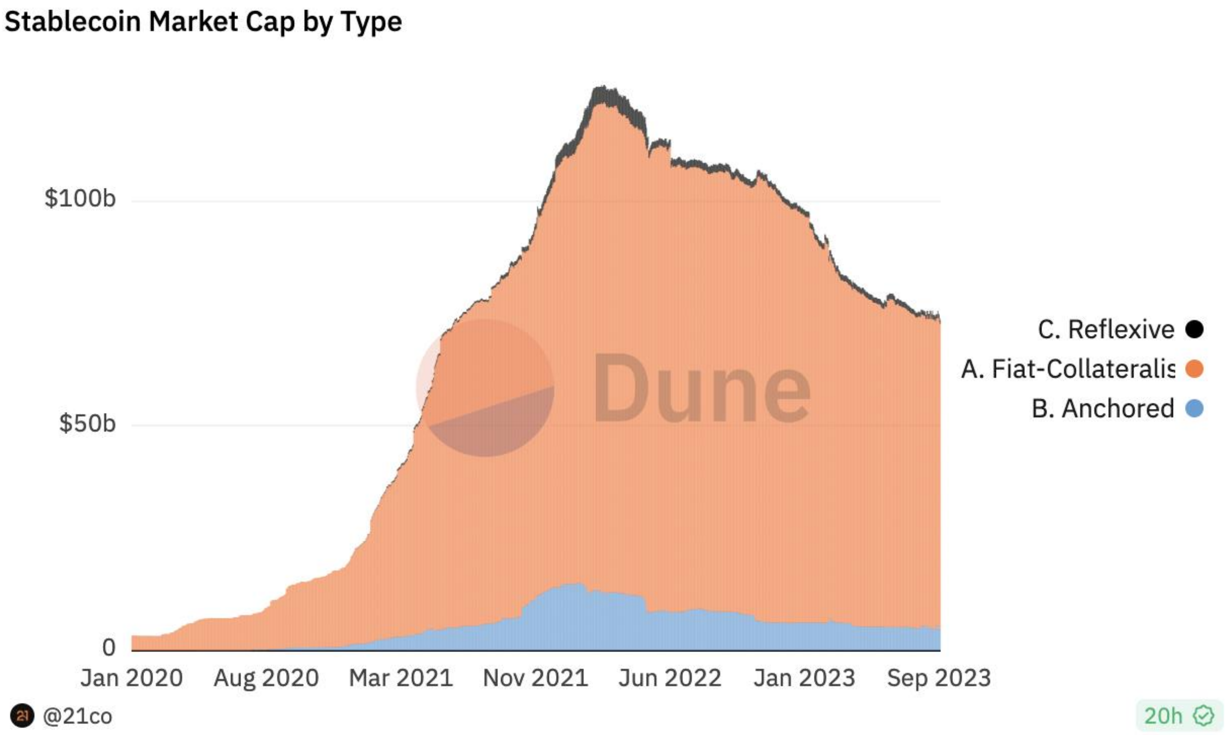
You can use $1 of LUNA to mint 1 UST

Suppose UST is trading at $0.90

You can redeem $1 of LUNA by burning 1 UST

Conversely, when the market undervalues the stablecoin, slipping beneath its target, the mechanism works in the opposite direction. It dives into the market to acquire and effectively remove tokens, contracting the circulating supply. This action, in theory, should spur an uptick in the token's price, aligning it once again with its foundational value.

What sets algorithmic stablecoins apart, then, is not a backing of assets or collateral but the allure of a 100% decentralized stablecoin totally separated from the fiat world. Algorithmic stablecoins, while intriguing and innovative, have not yet proven to be resilient or stable. Numerous attempts at an algorithmic stablecoin have completely failed in catastrophic fashion, incinerating billions of dollars in the process. And if that wasn't enough, issues around token centralization, regulation, and actual adoption loom large.



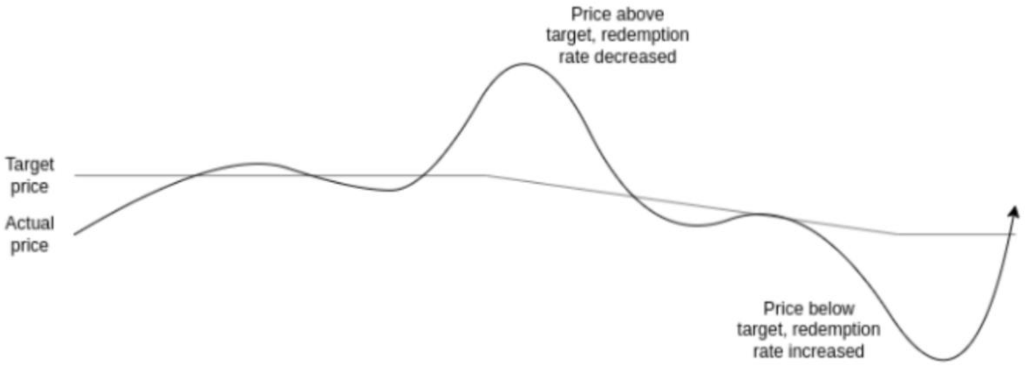
Algorithmic (reflexive) stablecoins represent a small minority of the stablecoin market cap. Source: Dune

Because of all these, it is more fitting to view these stablecoins as synthetic assets, mirroring the $1 benchmark, rather than an organic currency. Their primary utility, as it stands, gravitates towards niche areas like arbitrage trading and interest (yield) farming.

RAI

RAI is an ETH-backed decentralized stablecoin. However, unlike its peers, RAI distinguishes itself through its unique reliance on a reflex index instead of a traditional pegging mechanism, meaning it is not designed to maintain a $1 USD peg but rather a floating peg. This different approach offers RAI the elasticity to respond seamlessly to real-time supply and demand dynamics. Central to its design is the dynamic target price, termed the "Redemption Price", which stands as the linchpin for its stability mechanisms. RAI will adjust in response to market conditions vs. the Redemption Price:

- If RAI's price is above the target, the redemption rate decreases, reducing RAI holding incentives and increasing negative RAI holding incentives by being a lender, subsequently lowering the price.
- If RAI's price is below the target, the redemption rate increases, enhancing RAI holding incentives and decreasing negative RAI holding incentives by being a lender, pushing the price upward.


Price above target, redemption rate decreased
Target price
Actual price
Price below target, redemption rate increased

Source: Rai

Distinct from fiat-backed stablecoins like USDC and USDT, RAI's foundation is rooted deeply in decentralization. Eschewing any fiat backing, RAI exclusively uses ETH as collateral and targets a floating peg. The goal is to create a more stable version of ETH.

This controlled volatility makes RAI an attractive proposition for its integration as collateral in lending platforms or as a reserve asset within DAO treasuries. RAI's value isn't static. Instead, it adjusts in response to market fluctuations, arising from engagements between SAFE depositors and RAI possessors, with the Redemption Price guiding these value adjustments.

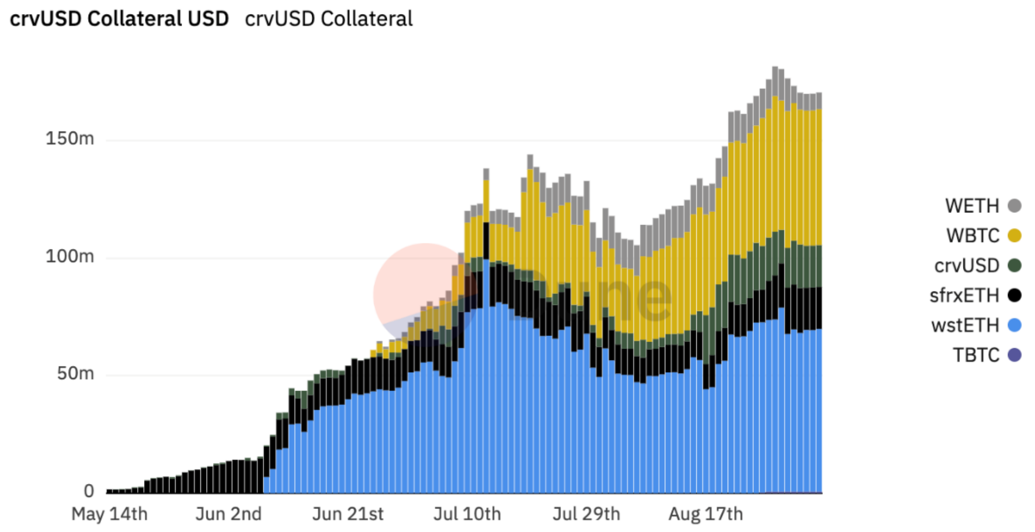
Application-specific/DeFi Stablecoins

With stablecoins proving their product-market fit over the last couple of years, top DeFi protocols like Aave, Frax, and Curve have taken notice. Aave and Curve, specifically, are long-standing “blue chip” DeFi protocols that have large enough TVLs and user counts that may also benefit from a native stablecoin within the protocol. The release of Aave's GHO coin and Curve's crvUSD also serve to benefit the protocols as strategic revenue generators and provide more autonomy to the dApp rather than relying on another stablecoin like Dai. This strategic shift diminishes the reliance on third-party interventions or influences and creates new revenue streams.

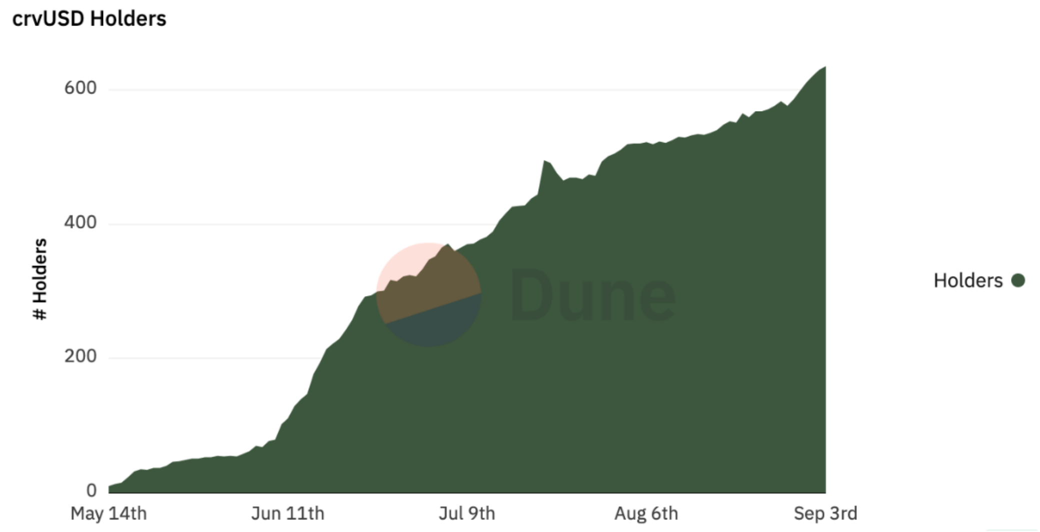
At a high-level glance, the basic foundations of both GHO and crvUSD resemble Maker’s Dai. Like Dai, these coins are overcollateralized in a CDP-like position and bear semblance in issuance approaches. However, both stablecoins contain specific design nuances that leverage the core mechanisms of their respective parent protocols. For Aave, that’s leveraging the TVL in its borrowing/lending dApp, and for Curve, it’s utilizing its DEX design to optimize liquidations. GHO and crvUSD represent an evolutionary stride in decentralized stablecoins that look to compete with the centralized market leaders of USDT and USDC.

crvUSD

Curve Finance introduced its own Curve-native stablecoin, crvUSD, in 2023. As of Q3 2023, crvUSD has been live for several months and has amassed ~$160M in TVL. So far, crvUSD accepts collateral including : sfrxETH , wstETH, wBTC, wETH.



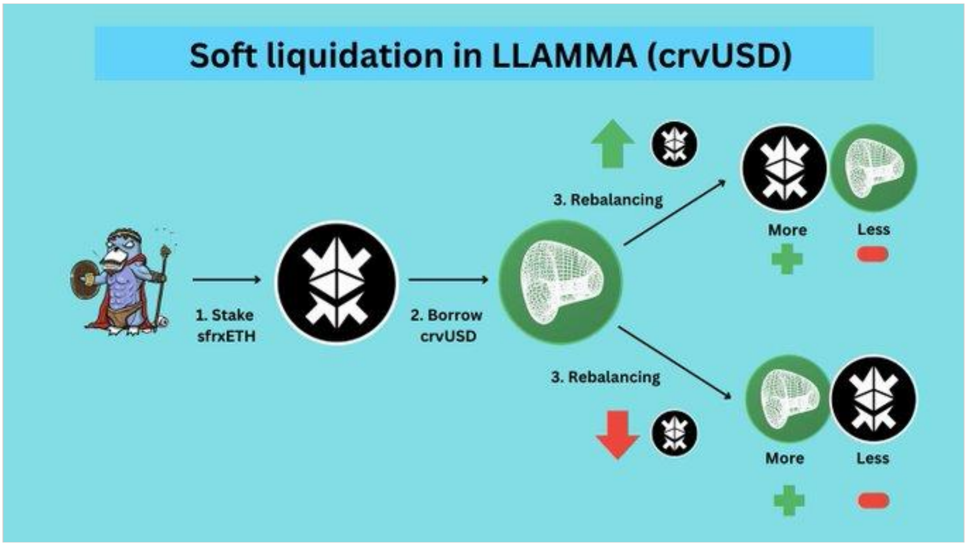
Source: Dune



Less than ~650 crvUSD holders signify small market penetration thus far. Source: Dune

While crvUSD is certainly an application-specific stablecoin due to its development and reliance on Curve.finance, it also straddles other stablecoin sectors as it utilizes LSTs for collateral and has elements of an algorithmic stablecoin thanks to its novel liquidation mechanism. Enter crvUSD's LLAMMA - the Lending-Liquidating Automated Market Maker Algorithm. This unique liquidation system presents a paradigm shift from traditional liquidation models, prioritizing borrower welfare and systemic resilience.

Traditional liquidation methods in the DeFi ecosystem often come with sharp, immediate consequences for borrowers. However, LLAMMA introduces a procedure termed as 'soft liquidations.' Instead of abruptly liquidating the borrower's collateral, LLAMMA transforms it into a Liquidity Provider (LP) position. This transition facilitates an ongoing recalibration of collateral via a specialized Automated Market Maker (AMM). By adopting this model, the platform sidesteps the extreme volatility synonymous with conventional forceful liquidations seen on many borrowing platforms.



Source: twitter.com/poopmandefi

The LLAMMA protocol serves dual purposes. First, it offers stablecoin users an avenue to diffuse the risks of depegging or liquidation. This is achieved by diversifying collateral positions across multiple tiers or bands. This diversification strategy is paramount, especially considering the historical episodes where rapid market downturns had debilitated several DeFi platforms. By endorsing phased liquidation of assets, LLAMMA averts the pitfalls of instantaneous price collapses.

Furthermore, the LLAMMA system shields borrowers from the brunt of full-blown losses that instantaneous liquidations entail. Instead of rendering borrowers' assets void, LLAMMA’s mechanism incrementally reduces potential losses. Concurrently, it safeguards the protocol against accumulating bad debt, a peril every DeFi platform grapples with.

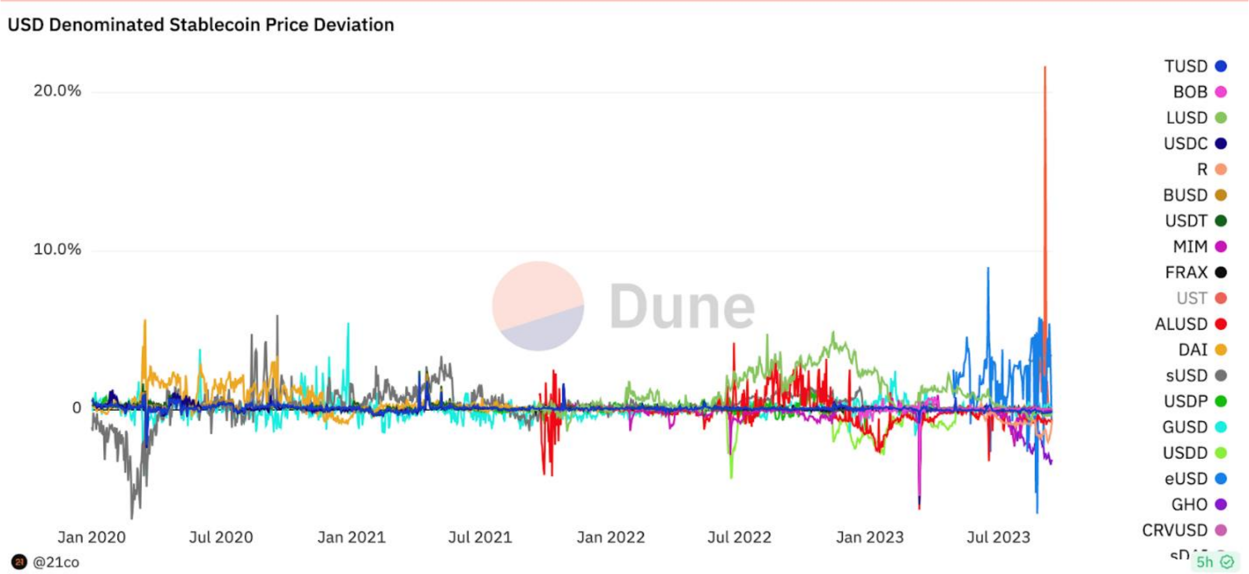
When the value of collateral starts to wane, crvUSD doesn't stand idle. It harnesses the liquidity reservoirs of Curve pools to recalibrate the collateral's composition automatically. For instance, if the market sees a dip in ETH, the platform will judiciously convert ETH to stablecoins like USDC. This strategy establishes a fortified buffer, ensuring the collateral remains at a comfortable distance from its liquidation threshold. One can envision this as a proactive approach, where the protocol uses debt to modulate the gap between the prevailing price and the liquidation marker.

Risk Factors to Consider in Stablecoin Design

General Risks for All Stablecoins

Price Stability/Depeg Risk

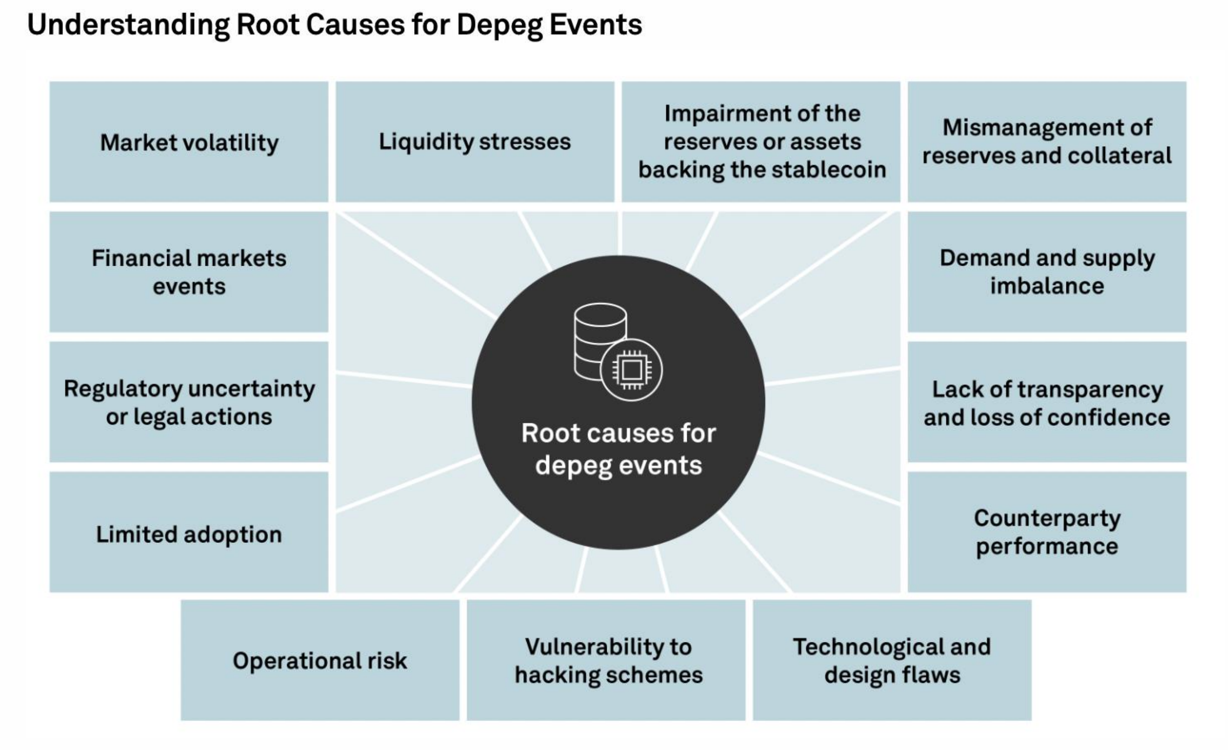
Despite the moniker of “stablecoins,” these crypto assets are not immune to market and external pressures. They can, and do, deviate from their targeted value, usually $ 1 USD (image below). Such events are often a culmination of microeconomic factors like sudden demand surges, liquidity challenges, or alterations in the foundational collateral.



A chart simply illustrating that stablecoins rarely trade at exactly $1. Source: Dune

Macro events, like inflationary trends or interest rate amendments, can equally sway stablecoin demand. Consider an inflationary environment where the underlying asset's purchasing power dwindles. This can compel the stablecoin to depeg.

Externalities, such as regulatory headlines or even technical snafus like network congestion or smart contract vulnerabilities, can also be catalysts. A government's decision to prohibit stablecoins, for instance, would severely dent demand, instigating a depegging event.


Understanding Root Causes for Depeg Events
Market volatility
Liquidity stresses
Impairment of the reserves or assets backing the stablecoin
Mismanagement of reserves and collateral
Financial markets events
Demand and supply imbalance
Regulatory uncertainty or legal actions
Root causes for depeg events
Lack of transparency and loss of confidence
Limited adoption
Counterparty performance
Operational risk
Vulnerability to hacking schemes
Technological and design flaws

Source: SPGlobal

Depegging doesn't occur in isolation. The sequence typically involves:

- Initial Value Deviation: Triggered by any of the aforementioned reasons, the stablecoin's value begins to diverge from its peg.
- Market Reaction: Traders and investors, gauging the potential return to peg or further deviation, might buy or sell the stablecoin.
- Arbitrage Windows: These emerge when the stablecoin's value significantly strays from its peg, offering traders opportunities to capitalize on the difference.
- Issuer Intervention: If the deviation persists, the issuing authority might intervene, tweaking the supply or adjusting collateralization ratios to restore trust.
- Stabilization: Depending on market response and issuer actions, the stablecoin may stabilize, potentially returning to its original peg.

A depegging event unleashes multiple market risks. Here's what stakeholders need to be wary of:

- Market Unpredictability: Depreciation can inject volatility into the market. As positions shift rapidly in response, the uncertainty quotient rises, leading to potential losses.
- Reputation Concerns: A depegging event might tarnish the reputation of the stablecoin issuer and the trust in the asset's value, potentially leading to more selling pressure and further devaluation.
- Liquidity Hurdles: If a depeg causes a massive sell-off, this can lead to liquidity challenges on trading venues and even congestion on the underlying blockchain protocol, which may disrupt arbitragers' ability to make their trades and potentially restore the peg.

- Default Risks: The depeg might increase the chances of default by the stablecoin issuer or associated parties.

Base Layer/Protocol Risk

Early in 2023, the Tron blockchain network grappled with a significant security lapse that put digital assets worth $500 million in jeopardy. The discovery of this flaw was credited to the cybersecurity research team, 0d, at dWallet Labs. This critical zero-day vulnerability was identified within Tron's multisig accounts. Instead of requiring multiple signatures for transactions as designed, the flaw would have enabled any single signer to access and control the assets held in these accounts unrestrictedly. After the responsible disclosure, Tron's response was swift, rectifying the issue "within days" and averting a potentially massive security breach.

Prior to that in 2021, Polygon faced an even larger potential loss when a grave vulnerability was identified that could have jeopardized a staggering $24 billion in user assets. This exploit was centered on Polygon's smart contract mechanism. If left unpatched, malevolent actors could have easily minted over 9.2 billion MATIC tokens, nearly exhausting its total supply cap of 10 billion.

The alarming potential of this exploit did lead to one malicious actor successfully siphoning off $1.8 million in MATIC tokens. Fortunately, this attack was isolated, and swift action from Polygon's team mitigated further damage. White hat hackers highlighted the flaw on the ImmuneFi bug bounty platform on December 3 and Polygon's developers initiated an upgrade in under 48 hours.

Additionally, beyond simple bugs and code errors, today's stablecoins must be able to safely operate across dozens of separate blockchains. Stablecoins have often operated within the confines of their respective blockchain ecosystems, limiting their utility across different platforms. However, the industry is making strides in adopting common standards to facilitate interoperability. Communication protocols like Chainlink's CCIP, LayerZero, and Circle's CCTP are being developed to enable more seamless interactions between different stablecoins, regardless of their underlying blockchain platform. Such protocols can unlock increased liquidity and broader utility for stablecoins, making them more valuable to end-users and investors alike.

Smart Contract Risk with the Stablecoin Protocol

Fully autonomous, smart contracts removing middlemen and operating without bias sounds great but only if the code is safe. Using stablecoins on a blockchain means users not only need to be sure the actual blockchain is safe but also the project responsible for the stablecoin. Unfortunately, that is not always the case as Level Finance experienced in 2023. Level Finance, a DeFi protocol that issues an interest-bearing stablecoin, lost $1 million due to a glitch in its smart contract.

The core of the issue lay in a flaw that permitted the nefarious attacker to produce an excessive quantity of LUSD stablecoins without the mandated collateral backup. Essentially, the attacker could mint these stablecoins at will, subsequently trading them for other digital assets, thereby illicitly extracting value from the Level Finance ecosystem.

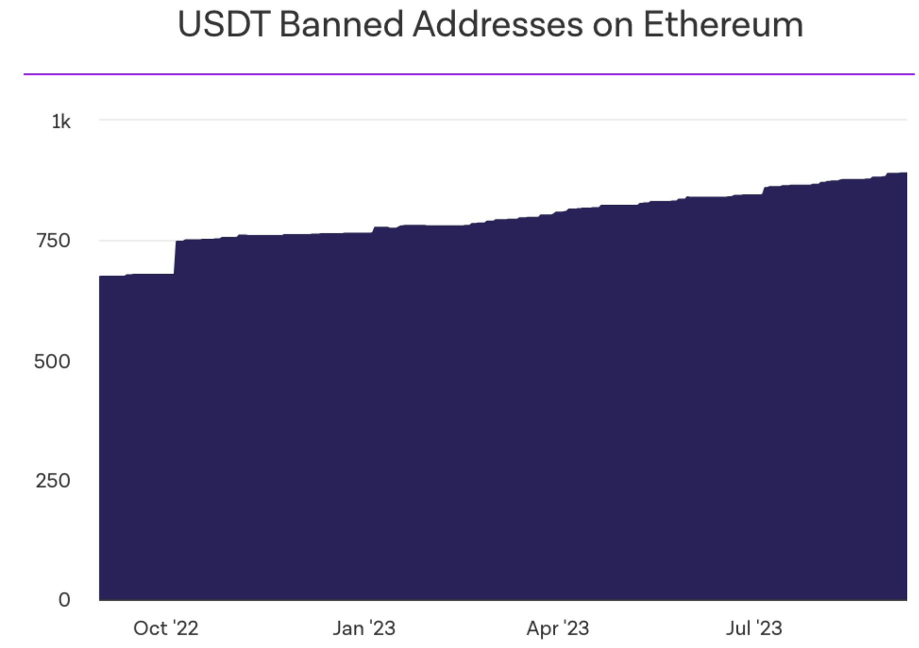
Other Risks and Considerations

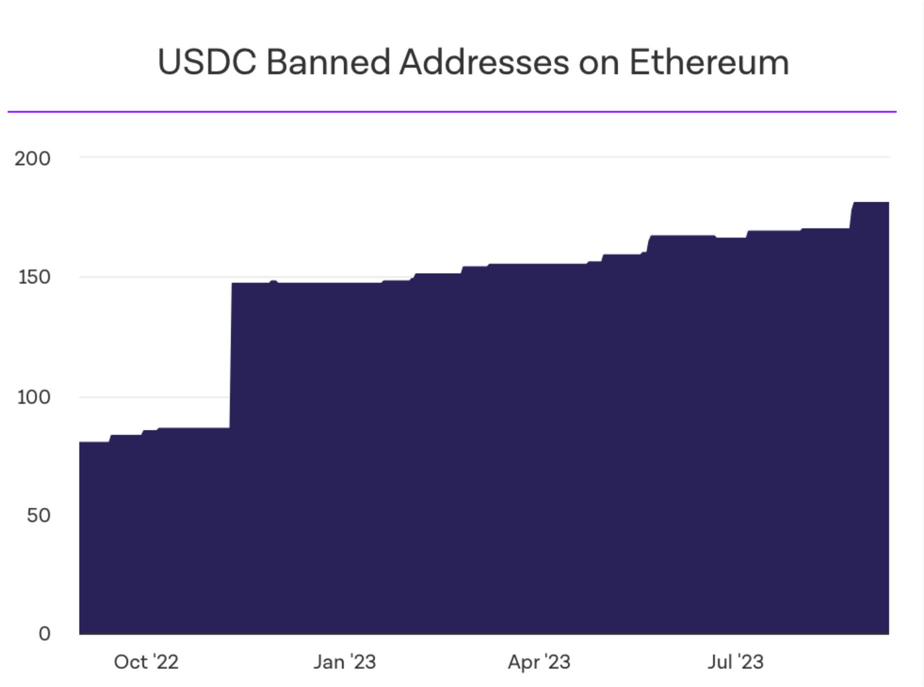
- Token Centralization/Governance Risk
- Liquidity Centralization (e.g. primarily all-in-one liquidity pool)
- Supply Constraints: is the growth of the stablecoin dependent on the growth of another sector (RWAs, decentralized futures, LSTs, etc.)
- Redemption/Arbitrage Risk: inefficient redemption mechanisms may impede the stablecoin design from functioning as designed
- Integrations into Other Protocols/Contagion Risk: the MIM-UST “Degenbox” Scare

Risks of Centralized, Fiat-collateralized Stablecoins

Centralization and Censorship

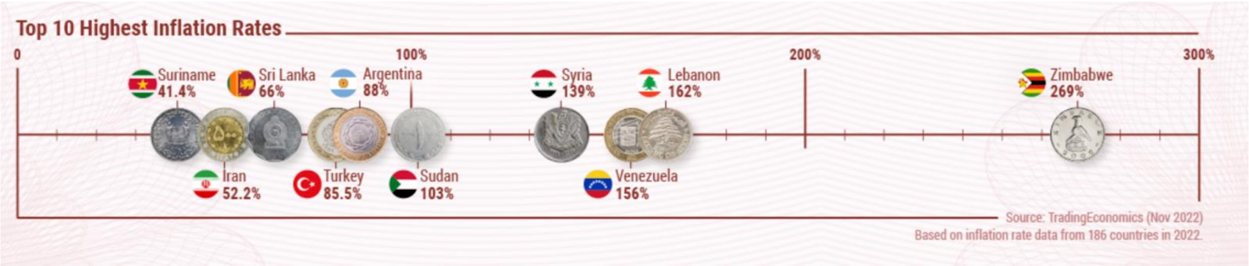
In an almost paradoxical fashion, the two leading stablecoins in the crypto space, USDT and USDC, embody a significant degree of centralization and counterparty risk. Every stablecoin displays some mixture of centralized and decentralized features. However, USDT and USDC stand out as they operate under the control of regulated, profit-driven companies that possess the authoritative power to mint new coins and, quite notably, freeze existing assets. Both projects have, on dozens of occasions, "blacklisted" addresses and frozen the funds held within them, something inconceivable to the average person’s understanding of “crypto.”





Source: TheBlock

Unfortunately, many of the people who could stand to benefit from access to USDT or USDC due to their own fiat money being subjected to high inflation, instability, or capital controls are the targets of these asset freezings simply because of their home government's relationship with the US. Citizens of countries like Iran, Syria, and Venezuela suffer from some of the highest inflation in the world (image below) but also find themselves cut off from USDT and USDC due to US sanctions against those countries. Because of this, these centralized, fiat-backed stablecoins do not pose a solution for people like them, illustrating the value in something like a truly decentralized, crypto-native stablecoin or crypto asset.

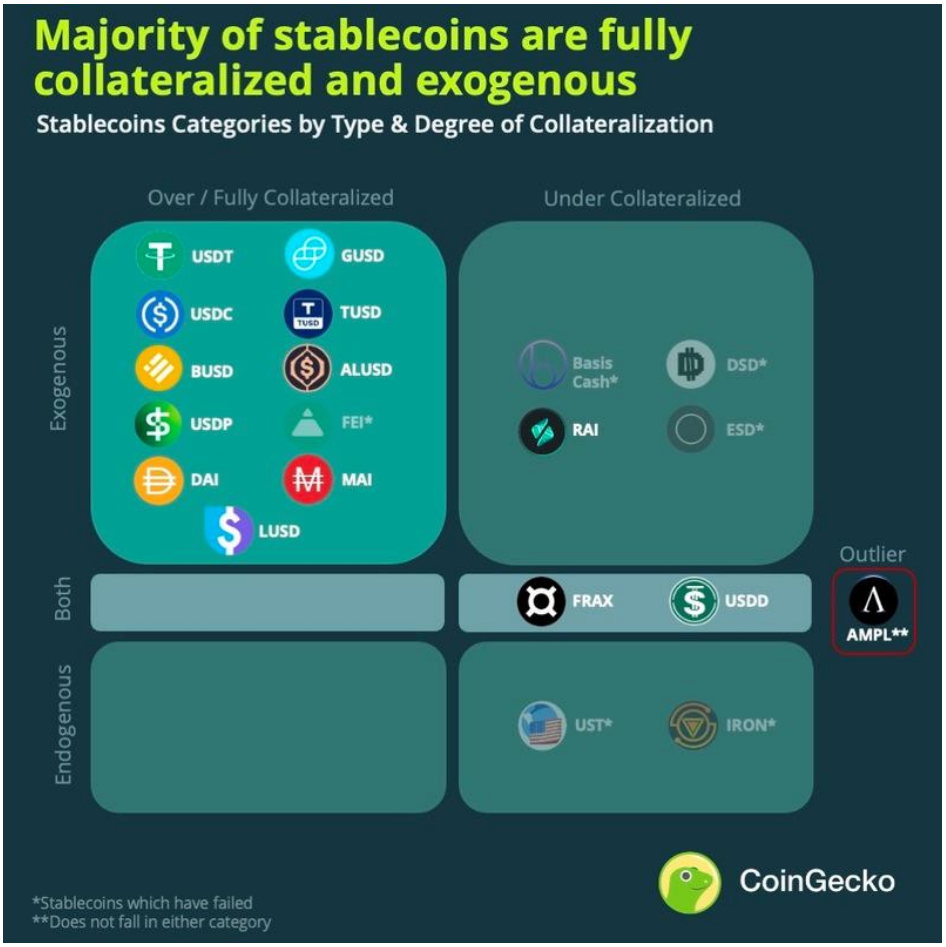


Source: elements.visualcapitalist.com

Additionally, due to their design, users of USDT and USDC must put 100% faith into Tether and Circle, respectively, to properly manage the hundreds of billions of dollars across the globe in real time. Should either company mismanage its global operation, the ramifications would be felt across the entire crypto economy.

Exogenous Collateral, Reserve Composition, and Transparent Audits

The collateral backing a protocol's stablecoin can be categorized as either endogenous or exogenous in nature. Endogenous assets, in this context, are crypto tokens intrinsically linked to the protocol, serving roles like equity or governance (akin to LUNA in the Terra and UST ecosystem). Conversely, ETH represents an exogenous crypto asset, which is often viewed as a more desirable form of collateral because its value remains independent of the protocol's progress and longevity. The US dollar would be ever more exogenous as it is not a crypto asset and has even less correlation to the underlying stablecoin.


Majority of stablecoins are fully collateralized and exogenous
Stablecoins Categories by Type & Degree of Collateralization
Over / Fully Collateralized
Under Collateralized
Exogenous
Both
Endogenous
USDT
GUSD
USDC
TUSD
BUSD
ALUSD
USDP
FEI*
DAI
MAI
LUSD
Basis Cash*
DSD*
RAI
ESD*
FRAX
USDD
Outlier
AMPL**
UST*
IRON*
CoinGecko
*Stablecoins which have failed
**Does not fall in either category

For these fiat-backed stablecoins, the crux of investor confidence often hinges on the clarity of their financial health and operations.

While many might assume that a "USD-collateralized" label signifies a one-to-one backing by the US dollar, the reality is more nuanced as the collateral backing these stablecoins is typically diversified into an array of assets. These might include cash equivalents such as US treasuries and commercial paper, but also encompass secured loans, and corporate bonds, among others.

Acknowledging the importance of transparency in this domain, there has been a concerted push towards enhancing clarity and reporting mechanisms for USD-collateralized stablecoins. Moody's, a renowned TradFi credit rating agency, is even devising a scoring methodology tailored for fiat-backed stablecoins. This system aims to assess these digital assets based on the robustness of their reserve attestations.

Circle's USDC, one of the prominent stablecoins in the market, has bolstered its commitment to transparency, releasing monthly reports detailing its reserves with attestations from Grant Thornton, a globally recognized accounting firm.

Regrettably, when it comes to Tether, transparency into its reserve composition and internal operations poses challenges for investors and users alike. While many financial institutions and companies in today's era leverage technology to provide real-time updates on their balance sheets, Tether is seemingly incapable of doing so. The company's balance sheet data is updated quarterly, a cadence that might have been standard in traditional finance, but in the rapidly moving digital currency ecosystem, could be seen as outdated. This periodicity leaves a considerable gap where market movements can happen, and investors are left in the dark.

Furthermore, these quarterly reports, though informative, still leave many pertinent questions unanswered. For the astute reader, these reports lack clarity on several fronts:

- Financial Institution Partnerships: The identity of the financial institutions that hold Tether's cash deposits remains undisclosed. The geographical location of these institutions is equally unclear. Knowing the "who" and "where" can give investors insights into the financial stability, regulatory environment, and potential risks associated with these holdings.
- Foreign Treasury Details: While Tether's holdings in U.S. Treasury Bills might be known, details about non-U.S. Treasury Bills remain undisclosed.
- Interest Rate Exposure: The interest rate risk associated with many of Tether’s assets (and possibly some of USDC’s) is not completely known. As interest rates have exhibited extreme volatility over the last ~two years, this becomes more significant to the reserves held by each entity.
- Loan Terms and Collaterals: Details about the terms of secured loans taken by Tether, as well as the collateral backing these loans, are missing. Such details can provide a deeper understanding of the company's credit risk and the safety of its financial position.

Other potential hazards for USDT and USDC users include:

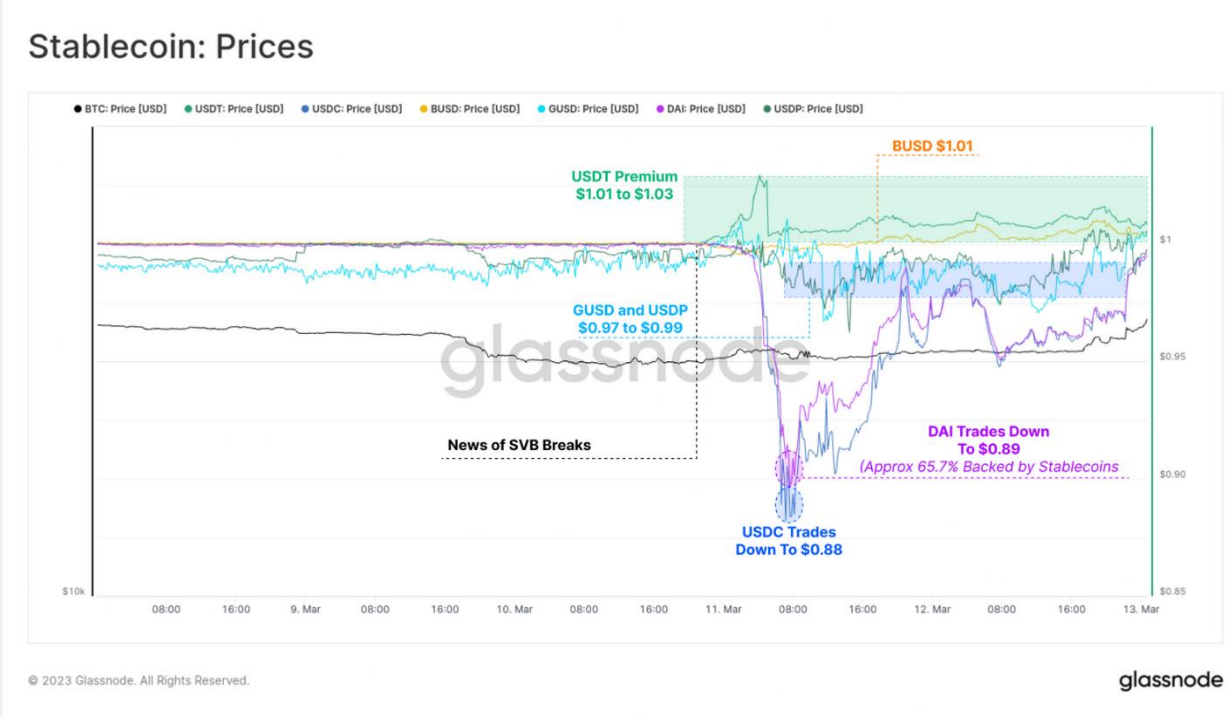
- Fluctuations in the U.S. dollar value.
- Uncertainties surrounding U.S. Treasuries.
- Possibility of bank runs.
- Improper risk mismanagement of funds or banking partners.
- Internal mismanagement or even malicious practices by the overseeing company.

Banking/Counterparty/Custody Risk

Because USDT and USDC are (essentially) digital representations or IOUs of the U.S. dollar, this brings forth another layer of centralization/risk: custodying the fiat collateral that backs the stablecoin. The onus of safeguarding these funds and ensuring their seamless transfer falls upon their banking partners and all the problems/frictions involved in traditional banking. Consequently, any turbulence - operational glitches, financial insolvency, or even unethical practices - encountered by these partners can create ripples, disturbing the very foundation of these stablecoins.

Despite the risks explained above, many still feel comfortable holding USDT and USDC, acknowledging that the risks sound no different than standard banking risks. And they would be correct to a certain extent. Plus, with such a large, reputable, and regulated company behind USDC like Circle, users assume extra protections that other stablecoins can offer, like insurance. However, while users might derive a sense of security from insurance mechanisms like the Federal Deposit Insurance Corporation (FDIC), digging into the details of Circle's recent practices illustrates how little protection users actually had in the event of a crisis. As Circle's 2021 data suggests, out of the staggering $10 billion parked in regulated financial institutions, a mere ~$1.75 million was under the protective umbrella of FDIC ("Circle Internet Financial Limited"). In the unfortunate event of a bank collapse, USDC holders could find themselves vying with other claimants for their due.

The reality was that a significant chunk of USDC's backing cash was vulnerable, lying beyond the FDIC's $250,000 insurance ceiling when it suffered banking issues in March 2023. Silicon Valley Bank ran into solvency issues and assets held at the bank were at risk. This caused USDC to depeg as ~8% of the US dollars backing the stablecoin were potentially unrecoverable.



Source: Glassnode

Regulatory Risk

Centralized stablecoins, in particular, have recently become a prominent focus for regulatory bodies, as evidenced by recent actions and proposals. One of the most noteworthy instances of this regulatory spotlight involves Paxos Trust (Paxos). The New York Department of Financial Services (NYDFS) initiated action against Paxos in 2023, instructing them to cease Binance USD (BUSD) issuance. The crux of NYDFS's contention was Paxos's purported negligence in its duty to carry out consistent risk assessments.

Further intensifying the scrutiny, the Securities and Exchange Commission (SEC) advanced its allegations against Paxos, suggesting that BUSD qualifies as a security through its Wells Notice. While the immediate repercussions of these actions only pertain to BUSD, it is evident that centralized stablecoins, by extension, are vulnerable to significant regulatory interventions.

Further evidence for the growing regulatory concerns around stablecoins was the introduction of the STABLE Act in December 2020. The essence of this act is anchored in the objective of thwarting potential malfeasance, lack of transparency, and the speculative emergence of a stablecoin-driven shadow banking system.

However, the requirements proposed are seen by many as particularly onerous, to the point of potentially killing off current stablecoin designs/issuers. If the act were to be ratified, stablecoin issuers would find themselves navigating the almost impossible requirements of:

- A necessity to procure a federal banking charter.
- An obligation to gain endorsements from both the Federal Reserve and the Federal Deposit Insurance Corporation (FDIC), and this, a full half-year prior to any stablecoin issuance.
- An additional stipulation to either secure FDIC insurance or establish dollar reserves directly within the Federal Reserve's precincts.

The intersection of stablecoin innovation and regulatory oversight is becoming increasingly pronounced. For stablecoin issuers, the current unclear regulatory environment leaves them unsure of how to grow while maintaining compliance. As the crypto industry and regulators continue their discussions, the hope is for a balanced approach that ensures both security and innovation.

Risks of CDP (crypto-collateralized) Stablecoins

Oracle Dependence/Centralization

At their core, oracles compile pricing data on assets from a multitude of sources, which CDP-backed stablecoins use in their protocols' stability mechanisms. These digital entities take on the pivotal task of ensuring the stability and reliability of the system, particularly during unpredictable market fluctuations and unforeseen black swan occurrences. The pivotal role oracles play becomes evident when considering the mechanics of crypto loans: for each loan extended, the value of the collateral must maintain a certain threshhold. Should an oracle indicate that a user's collateral-to-loan ratio dips beneath a pre-determined mark, the collateral deposited in the associated smart contract can be mobilized and liquidated to square off the corresponding stablecoins.

Such mechanisms are integral to both Collateralized Debt Positions (CDP) and Algorithmic stablecoins. Consequently, the selection of an oracle solution isn't a decision that should be taken lightly by the protocol. Factors that need meticulous consideration while opting for an oracle include:

- The oracle's capacity, reliability, and frequency in which it provides price feeds for the specific types of collateral in question, such as ETH, wstETH, or USDC.
- Its compatibility with both Layer 1 and Layer 2 Networks
- The inherent transparency, security, decentralization, and accuracy of the price feeds, along with the reliability of their sources.

An oracle exploit occurs when an oracle reports inaccurate data about an event or state of the external world. This can happen because the oracle purposefully acts maliciously or negligently, or the oracle’s data source is compromised.

There are two main types of oracle exploits:

- Misreporting: This is when an oracle reports a price that differs from the correct market-wide price of an asset. Regardless of whether misreporting occurs due to malicious or negligent behavior, any protocol relying on a faulty oracle for price data may be at risk of an exploit.
- Poor market coverage: This is when an oracle relies on only a subset of all trading environments to report the price of an asset. This can lead to the oracle misreporting the price of an asset if that subset is manipulated, even when the majority of trading environments and the market-wide price remain unaffected.

The risk of oracle exploits can be mitigated with a more secure oracle design. Features of secure oracles include:

- Sourcing price data from across all trading environments to provide proper market-wide coverage: This helps to ensure that the oracle is not vulnerable to price manipulation in a single trading environment.
- Protections from external tampering: This can be achieved by decentralizing the oracle or by using other security measures to prevent unauthorized access to the oracle's data.
- Economic incentives to report faithfully: This can be achieved by rewarding oracles for reporting accurate data and penalizing them for reporting inaccurate data.

Efficient Liquidations

We have established that when the value of a loan's collateral falls below the value of the borrower's outstanding debt, including interest, the under-collateralized position poses a threat to the health of the lending protocol. To prevent the accumulation of under-collateralized positions, many DeFi protocols enable third parties, who may not be users of the protocol, to repay the debt of under-collateralized or near-under-collateralized borrowers. By paying off these debts, these third parties, known as liquidators, can claim the collateral of the borrowers they cover at a discounted price. This process is referred to as liquidation.

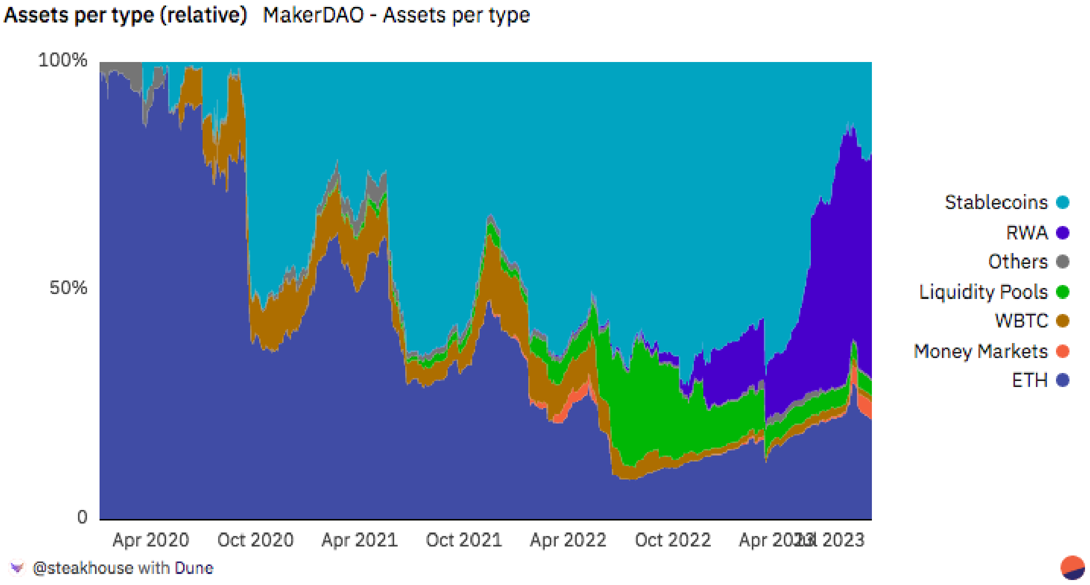
You might wonder why protocols rely on third parties for liquidating unhealthy positions rather than incorporating an automatic liquidation mechanism into their code. The reason lies in the high gas costs associated with sending liquidation transactions. If a protocol were to automate this process, the resulting gas expenses would significantly increase operating costs, potentially undermining profitability. In a now infamous event dubbed “Black Thursday” in the MakerDAO ecosystem, such an event unfolded. The ETH price crashed ~30% in one day, leading to mass on-chain activity and liquidations. However, the Ethereum chain was so heavily congested that “Keeper” bots were unable to submit bids at collateral auctions and many Dai borrowers were incorrectly fully liquidated, losing 100% of their money rather than the expected ~13%.

Moreover, designing an automated liquidation system is highly complex. A protocol would need to determine not only whether a position should be liquidated but also when to do so, taking into account market volatility. Curve’s crvUSD and its LLAMA mechanism are the latest attempts at on-chain, fully automated liquidations, albeit with its own “soft liquidation” approach. However, users must be discerning. Upon a crvUSD debt position's entry into soft liquidation, users are barred from making collateral adjustments – no withdrawals or additions. Their sole recourse lies in loan repayment with crvUSD or choosing self-liquidation.

In general, it is just more feasible to delegate this task to specialized third parties by providing incentives for them to liquidate these positions. If for whatever reason, liquidators cannot or are not incentivized to execute liquidations, the stablecoin peg will be at risk.

RWA/Exogenous Risk

As RWA adoption grows in the crypto ecosystem, so too do the risks associated with them, even for CDP-type stables. Maker and Frax are both leading “crypto native” stablecoins that have begun pivoting to incorporating more RWA into their accepted collateral in the name of peg stability and reserve diversification. Essentially every risk discussed above in the “Risks of Centralized, Fiat-collateralized Stablecoins” section now applies to these RWA portions of the collateral. Anytime a protocol introduces anything non-native to its blockchain, it then inherits all the risks associated with the “real world”: counterparty, custody, regulatory, etc. Blockchain code has no ability to recognize these things and, should any issues arise, they must be handled at the social layer, diminishing the “law is code” and immutability aspects of a blockchain. To make matters worse, there is very little case law for such matters in 2023, making any legal issue involving RWAs and blockchains a new, potentially messy, and almost certainly a controversial undertaking.



Source: Dune

Capital Efficiency

Capital efficiency refers to the amount of collateral required by a user to successfully mint a specified amount of stablecoins. While fiat-backed stablecoins boast a 1:1 ratio of USD to stablecoins, decentralized CDP stablecoins backed by cryptocurrencies mandate extensive collateral—often between 150% to 300%. This aspect, combined with the potential for liquidation, inarguably hampers their scalability.

Dai's operational model ensures that for every unit of Dai minted, there exists a surplus of collateral in the system. While this enhances the robustness of Dai, rendering it a reliable stablecoin, the strategy poses scalability concerns. Specifically, the requirement for higher collateral compared to the loan amount can be seen as both a strength and a potential limitation. For instance, the idea of depositing a collateral of $300 to acquire a $100 loan might seem counterintuitive, particularly when juxtaposed with fiat-backed or undercollateralized rivals in the market.

This model, arguably, has led to Maker ceding some market share to the more centralized stablecoins like USDT and USDC. Competitors that employ less collateral or even undercollateralized strategies offer a different value proposition, which might be more appealing to certain segments of the market.

Risks of Algorithmic Stablecoins

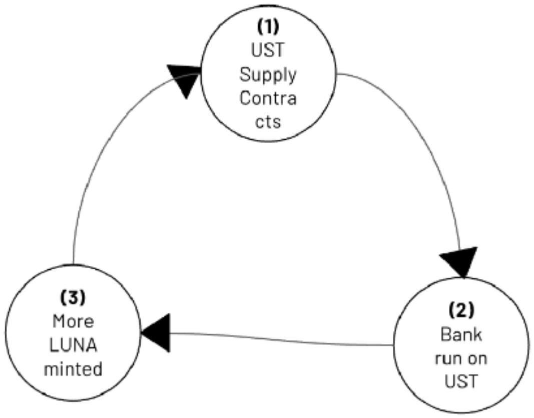
Nearly all of the aforementioned risks above also apply to algorithmic stablecoins. However, algorithmic stablecoins contain one, extremely important, risk that the others do not: endogenous collateral that is susceptible to increased reflexivity in volatile markets. Terra's UST stablecoin is the poster child for such risk.

UST’s “Death Spiral”/Reflexive Liquidation Risk

At its height, UST, Terra's stablecoin, held an impressive market capitalization of over $18.7 billion, ranking as the third-largest stablecoin globally. However, as macroeconomic challenges, including rising inflation, looming rate hikes, and a general downturn in the equity markets, emerged in early May 2022, the cryptocurrency market began to decline precipitously, including LUNA, the endogenous collateral backing UST.

LUNA's value began to crash (not uncommon in the crypto world), reducing the incentive to swap with UST, which subsequently led to the destabilization of UST's peg to the U.S. dollar. The downward momentum on UST initiated a feedback loop, often termed a "death spiral." Arbitrage traders exchanged UST for LUNA, subsequently selling it. This caused LUNA's price to plummet, requiring even more LUNA to be produced for every UST redeemed. This cycle led to a rapid increase in LUNA's supply, resulting in hyperinflation.

The Death Spiral - Scenario 2



(1) A contraction in UST supply leads to minting $LUNA

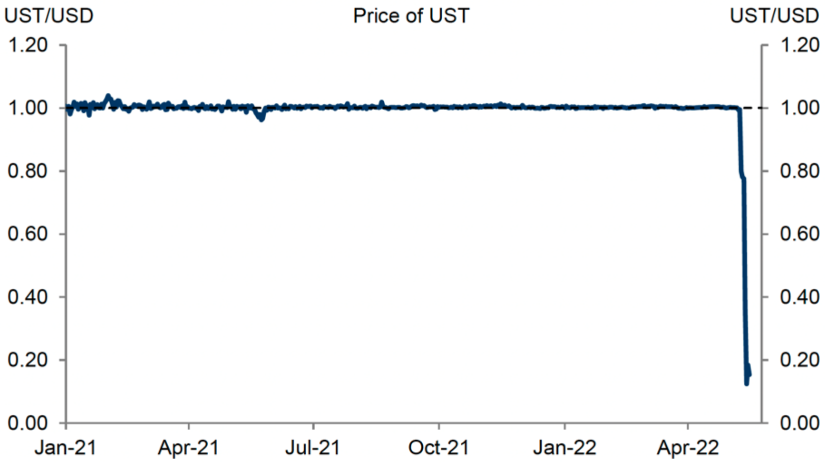
(2) $LUNA price declines. A sufficiently large decline may create a crisis of confidence in $UST as holders rush to redeem it for $LUNA

(3) More $LUNA is minted, leading to further price declines

Source: Forbes Crypto

As Terraform Labs intervened to restore balance by adjusting UST liquidity in key pools, their efforts proved ineffective against the prevailing selling pressure. The situation was exacerbated by a mass withdrawal from the Anchor Protocol, further devaluing UST.

In response, the Luna Foundation Guard (LFG) liquidated significant BTC reserves, lending these assets to stabilize the UST peg. Despite these efforts, UST's value plummeted to $0.63. Amidst the chaos, LUNA's price experienced a sharp drop, and Terra faced insolvency concerns. Attempts to mitigate the downward spiral intensified the market sell-off, with LUNA entering a hyperinflationary state. The once-thriving Terra ecosystem witnessed dwindling confidence as all three primary liquidity pools faced disruptions, pushing LUNA's circulating supply into hyperinflation and the UST peg into further decline toward $0.



Source: Forbes

The Future of Stablecoin Design

Despite stablecoins arguably displaying the most utility and product-market fit of any "cryptocurrency," we have demonstrated that the market leaders, fiat-backed stablecoins, compromised on nearly every crypto/cypherpunk ideal in the name of price stability and efficiency. USDT and USDC, while convenient, do not usher in the open and permissionless, censorship-resistant, alternative financial system that the crypto movement looks to build.

Because of that, many hypothesize that fiat-backed stablecoins could be just an interim solution until either something like BTC or ETH can be used as a medium of exchange or that a new decentralized stablecoin can emerge that provides the same security and utility as their centralized counterparts. This desire for a truly fiat- independent and crypto-native stablecoin has led dozens of new and experimental stablecoin implementations to launch in the last couple of years, too many to cover in just one report. Additionally, while 85+ stablecoins currently exist, many, so far, have failed to garner meaningful attention and adoption.

However, as crypto has proven time and again, it may be premature to write off any of these early projects at this stage. Therefore, let's quickly look at just some of the alternative stablecoin ideas that could become relevant over the course of the next crypto cycle.

Bitcoin-backed Stablecoin: NakaDollar

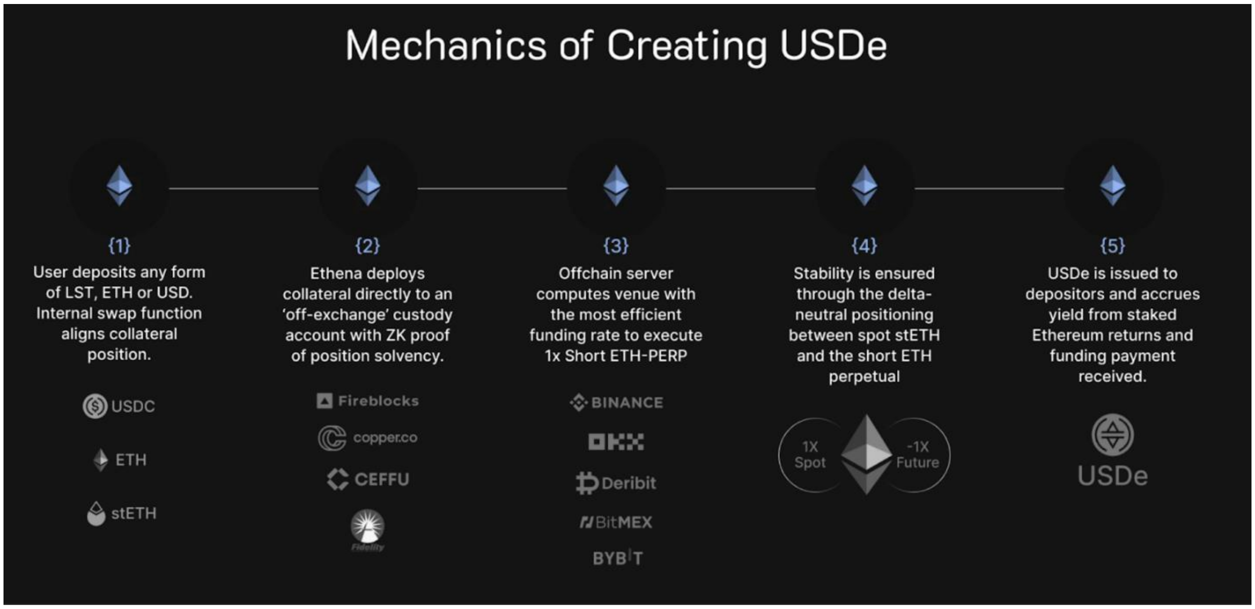
Arthur Hayes, a co-founder of the renowned cryptocurrency exchange BitMEX, recently proposed the idea of a bitcoin-backed stablecoin named NakaDollar (NUSD). What makes NakaDollar a unique stablecoin is that it is not just supported by fiat currency but by bitcoin and a bitcoin derivatives strategy. By holding a perpetual swap that shorts bitcoin—essentially betting against its price—alongside one dollar's worth of bitcoin, the stablecoin aims to self-stabilize. The financial mechanics here are such that any gains or losses incurred through these holdings would essentially negate each other, keeping NUSD's value anchored close to one U.S. dollar.

Notably, the design employs a unique synthetic pegging system that avoids interaction with fiat currencies in traditional banking systems altogether. By leveraging centralized derivative exchanges that list inverse perpetual swaps with the ticker XBTUSD, NakaUSD represents a USD equivalent. Specifically, when an investor deposits one bitcoin (BTC) on a derivatives exchange and takes a short position on an XBTUSD swap, they create a stablecoin collateralized by Bitcoin. This approach provides a natural hedge against Bitcoin's volatility and maintains a mathematical 1:1 peg with the U.S. dollar, making liquidation nearly improbable for the borrower.

One of the most appealing features of something like NUSD is that Bitcoin is currently the largest cryptocurrency by a wide margin and unlocking that currently inert collateral would provide instant liquidity for such a project. Unlike the current centralized stablecoins, the value of NUSD would be maintained by member crypto exchanges that list inverse bitcoin perpetual swaps, a type of derivative product settled with the underlying asset.

However, the NakaUSD model relies on centralized derivative exchanges to serve as the key custodians, again compromising on a truly decentralized vision for the benefits of liquidity and efficiency. This fusion of bitcoin collateral and off-chain derivative markets is intended to offer the best of both worlds.

A similar approach, also backed by Arthur Hayes but built on Ethereum, is Ethena. Ethena aims to develop a pseudo-decentralized stablecoin collateralized by a mix of ETH, LSTs, and other stablecoins pegged to $1 USD and maintained by hedging price exposure through bets against ETH, using perpetual swaps, similar to Hayes' NUSD.


Mechanics of Creating USDe

{1} User deposits any form of LST, ETH or USD. Internal swap function aligns collateral position.

{2} Ethena deploys collateral directly to an 'off-exchange' custody account with ZK proof of position solvency.

{3} Offchain server computes venue with the most efficient funding rate to execute 1x Short ETH-PERP

{4} Stability is ensured through the delta-neutral positioning between spot stETH and the short ETH perpetual

{5} USDe is issued to depositors and accrues yield from staked Ethereum returns and funding payment received.

Source: mirror.xyz

Yield-bearing, Treasury-backed Stablecoin

Prior to 2022, yield-bearing stablecoins were hardly a consideration considering the near-zero interest rate environment across much of the world. However, since rates across the globe have increased dramatically, this has led many to consider a stablecoin, backed by U.S. Treasuries, that also passes along some of the yield to its holders. These new iterations represent the next frontier in stablecoin innovation, yet they come with their own set of opportunities and challenges.

Amid rising U.S. interest rates, projects like Ondo Finance's $USDY and Mountain Protocol's $USDM have led this next wave in stablecoin innovation, offering stablecoins backed by U.S. Treasury Bills. Mountain Protocol, notably licensed by the Bermuda Monetary Authority, claims to be launching the first nationally regulated, yield-bearing stablecoin, named USDM. Designed primarily for non-U.S. users to gain access to U.S. Treasury yields, the ERC-20 token has set its current annual percentage yield (APY) at 5% (Mountain Protocol).

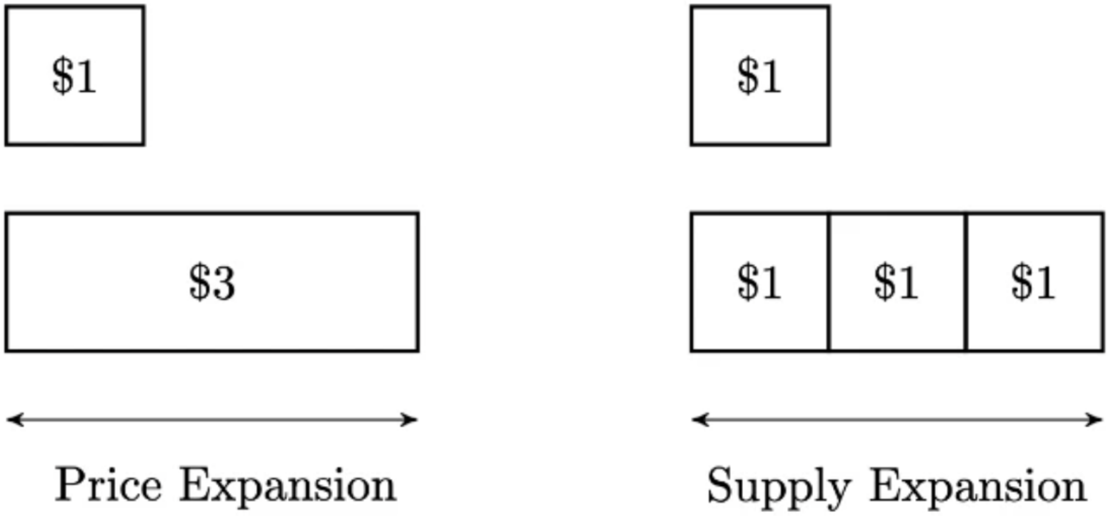
However, the optimism surrounding these stablecoin designs doesn't come without its skeptics. One criticism centers on the concern that if money's value increases over time due to the yield, consumers and businesses might delay spending, leading to a lack of monetary velocity and posing questions about the overall economic impact.

Additionally, there is the seemingly constant question around regulatory compliance and whether such a design would make the asset a security. These Treasury-backed stablecoins require permissioned access, requiring Know Your Customer (KYC) verification. Finally, there are also challenges to consider. While $USDY is a non-rebase token, $USDM is a rebasable token, which could make its integration into existing DeFi protocols problematic.

CPI-adjusted/rebasing Stablecoin

U.S. dollars are the world's reserve currency for a reason. It's stability, liquidity, and ubiquity are unmatched in the fiat or crypto worlds. However, even the USD is subjected to inflation, more now than ever. This has led some to experiment with an inflation-adjusted stablecoin that negates the negative purchasing power experienced by the actual USD.

The Ampleforth Protocol (AMPL) boasts an innovative rebasing mechanism and native stablecoin—SPOT—in an attempt to provide price stability, inflation resistance, and serve as robust units of account. The goal of Ampleforth is to keep pace with the Consumer Price Index (CPI) adjusted to the 2019 U.S. dollar. Its distinguishing feature lies in its ability to automatically adjust the number of tokens in circulation to maintain price stability. This is known as a rebasing token. Coded into the protocol is a feature that everyday at 2AM UTC, the supply of the total number of tokens is adjusted, provided that the price fluctuates by more than the current 5% deviation threshold.



Source: docs.spot.cash

If an investor owns a specific percentage (Y%) of the network before a rebase, they continue to own Y% afterward unless they make additional purchases or sales of AMPL tokens. This mechanism effectively controls inflation and ownership dilution, ensuring that an investor's proportional stake today retains its value tomorrow.

Conclusion

As covered in this report, stablecoins, despite their mundane name, contain every bit as much complexity and variety as their cryptocurrency counterparts. The devil is in the details and no two stablecoins present the same risks. At the highest level, stablecoins can be generally segmented into two distinct groups based on their collateral and degree of centralization: fiat-backed (exogenous collateral) stablecoins and CDP (crypto collateral) stablecoins. Despite the lack of censorship resistance and increased counterparty risk, the appetite for fiat-backed stablecoins like USDT and USDC is clear and shows little signs of slowing down. Stablecoins are becoming more intertwined with the TradFi markets with examples like PayPal's new pyUSD stablecoin available on Venmo, Shopify's integration with SolanaPay, and ongoing stablecoin regulation talks at the Congressional level.

However, decentralized stablecoins, while severely set back by Terra's UST collapse in 2022, have not given up the fight for a stablecoin that embodies the ethos of the cryptocurrency movement. Dozens of new, crypto-native stablecoin projects have been created to challenge USDT's and USDC's leading positions thanks to new advancements in liquid staking, oracles, derivative instruments, and general blockchain infrastructure. As the crypto space continues to evolve and push the boundaries of what was previously thought possible, decentralized stablecoins that have no dependencies on the legacy TradFi system remain a key aspect of a truly "crypto economy." But until that day comes, users can choose from the 85+ stablecoins currently trading that best suit their specific security, stability, and decentralization needs.

Disclaimer: This report was commissioned by the Solana Foundation. This research report is exactly that — a research report. It is not intended to serve as financial advice, nor should you blindly assume that any of the information is accurate without confirming through your own research. Bitcoin, cryptocurrencies, and other digital assets are incredibly risky and nothing in this report should be considered an endorsement to buy or sell any asset. Never invest more than you are willing to lose and understand the risk that you are taking. Do your own research. All information in this report is for educational purposes only and should not be the basis for any investment decisions that you make.