

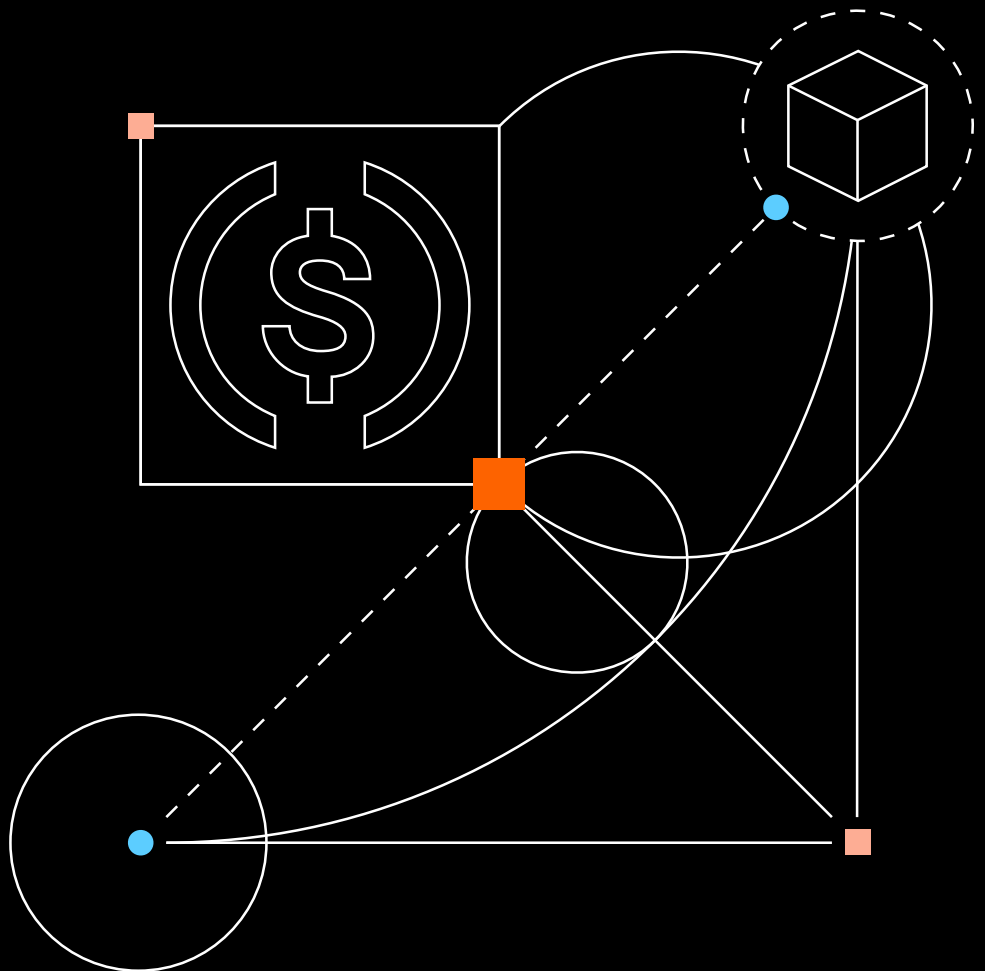


Galaxy Research

Digital Dollars

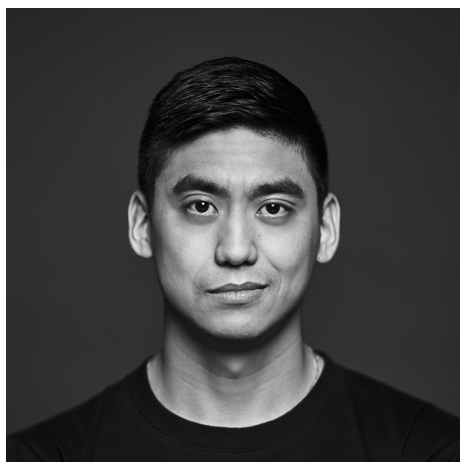
An Overview of Stablecoins Today and Tomorrow

AUGUST 15, 2022





Author & Acknowledgements



Charles Yu, CFA

Research Associate

email: charles.yu@galaxy.com

twitter: [@fullnodechuck](https://twitter.com/fullnodechuck)

We would like to thank the following people for their support in researching and publishing this report: Alex Thorn, Tyler Williams, Francesca Don Angelo, Lucas Tcheyan, Leulaye Maskal, Sal Qadir, Sebastian Benkert, and Sammy Scheman.

This report is a product of Galaxy Digital Research, a research organization within Galaxy Digital, the leading provider of financial services in the digital assets, cryptocurrency, and blockchain technology sector. Galaxy Digital Research provides top-tier market commentary, thematic views, tactical insights, and deep protocol research.

View our publicly available research at galaxy.com/research. Contact us at research@galaxy.com.



Contents

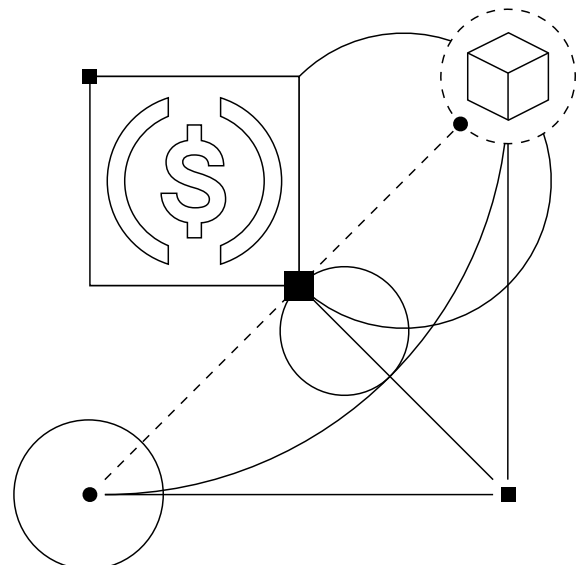
Key Takeaways	4
Introduction	5
Importance of Stablecoins	5
The Different Types of Stablecoins	7
Fiat-backed Stablecoins	8
Tether	8
Fiat-backed Stablecoin Landscape	18
Competitive Dynamics	19
Fiat-backed Stablecoin Issuers – Interest income	19
Financial Analysis of Fiat-backed Stablecoins	20
Primary Risks of Fiat-backed Stablecoins	24
Overcollateralized Stablecoins	25
Stability Mechanism of Overcollateralized Stablecoins	25
MakerDAO (DAI)	26
Other Overcollateralized Stablecoins	30
Competitive Dynamics of Overcollateralized Stablecoins	32
Financial Analysis of Overcollateralized Stablecoins	34
Main Concerns with Overcollateralized Stablecoins	36
Algorithmic Stablecoins	37
Stability Mechanism of Algorithmic Stablecoins	37
TerraUSD (UST)	38
Algo Stables Competitive Landscape	41
Competitive Dynamics of Algo Stables	43
Primary Risks with Algorithmic Stables	43
Peg Breaks and Failures of Stablecoins	44
Analysis of the Different Categories of Stablecoins	46
Trade-offs	46
Financial Analysis of All Stablecoins	48
Risk Assessment Framework for Stablecoins	50
Best Practices for Stablecoin Issuers	51
Regulation	52
Regulation In the US	52
Regulation Outside the US	55
Outlook	56
Predictions	57



Key Takeaways

This report explores dollar-pegged stablecoins, providing a comprehensive overview of their evolution over time. It covers the major stablecoins in existence today and explains the designs and stability mechanisms used, details the competitive dynamics of each type, and analyzes their stability and usage. We provide a risk assessment framework for evaluating the many stablecoins available in today's market and share our outlook for how stablecoins will progress.

- At a \$150bn+ market cap, stablecoins have become an increasingly important part of the crypto economy
- Stablecoin designs largely fall into 3 main categories (fiat-backed, overcollateralized, and algorithmic) – each of which comes with different advantages/shortfalls, stability mechanisms, and competitive dynamics
- Tether, the long-standing leading stablecoin by market value and volume, has endured a long history of criticisms but its market dominance has eroded rapidly in recent months, mostly to the benefit of Circle's USDC
- MakerDAO's DAI has emerged as the leader among “decentralized” stablecoins, but its current form has deviated significantly from its original vision as it has become significantly reliant on USDC for stability, leaving much to be desired
- The collapse of Terra USD (and all the failures of other algorithmic stablecoins before it) has led most protocols or platforms behind algorithmic stablecoins to fundamentally alter their designs to more collateralized models
- On-chain transaction data and price histories provide meaningful insights to assess the resilience and usage of each type
- New stablecoins products continue to emerge with innovative features, but potential users should be prepared with a risk assessment framework while conducting due diligence for each offering
- Comprehensive regulatory regimes overseeing stablecoins could soon be established across major global economies, which will have significant consequences for the issuance, redemption, usage, and adoption of stablecoins
- Despite recent stablecoin failures and macro headwinds, the evolution of stablecoins is not slowing, and the stablecoins that endure the toughest challenges are likely to gain share and thrive





Introduction

Stablecoins are digital representations of other assets for use on blockchains and in the crypto economy. While stablecoins may also be designed to track the price of other underlying assets such as gold and other exchange-traded commodities, this report will focus on stablecoins linked to the US dollar, the most common use of stablecoins today.

Importance of Stablecoins

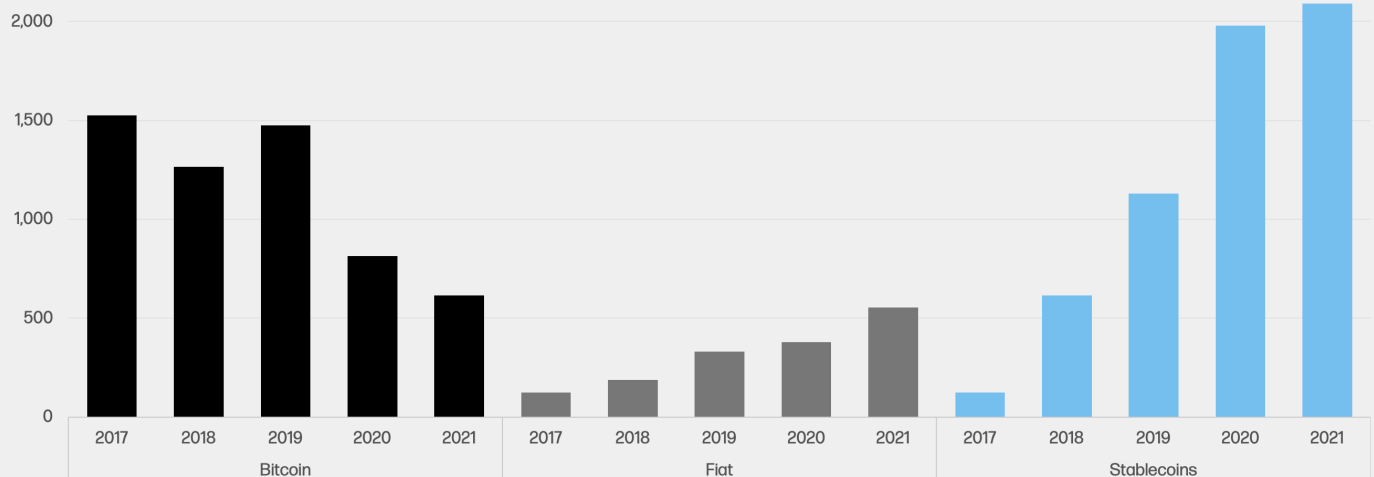
To some, stablecoins are a boring innovation, especially when they may be looking to escape the perils of the US dollar for a more sound, transparent monetary system as promised by Bitcoin. Stablecoins have the thankless job of maintaining parity to paired assets, where, if successful, there is only downside risk with no potential for price appreciation. Achieving and maintaining parity with another asset has been an exercise in innovation for hundreds of years—more recently, the age of tokenization has yielded many approaches, both successful and unsuccessful. While there is a continuously growing graveyard of failed experiments, there are also bright spots. The reality is that stablecoins are important

bridges connecting the digital and physical worlds that serve important functions in the crypto economy and help facilitate the adoption of blockchains. Stablecoins combine the benefits of the open crypto economy with the price stability of widely accepted fiat currencies and have the potential to transform the way that people and businesses use money.

As money, stablecoins address many of the long-standing pain points associated with crypto. The effective ones are stable, global, easy to transfer, and storable in non-custodial wallets, making it simple for anyone to use them without a bank account. While unbanked payments uses are still nascent, stablecoins are heavily used for crypto trading today. In the early days of the crypto economy, most trading pairs were denominated in BTC, but this wasn't ideal given bitcoin's high price volatility. The creation of Tether, the first stablecoin, enabled quick and easy trade settlement in dollars and provided a lifeline to crypto exchanges that mostly lacked access to the traditional banking system but wanted to offer pairs based on USD. The shift from BTC to stablecoins for quote pairs has been dramatic over the years, as data from Kaiko illustrates.

Spot Instruments by Quote Asset - Number of Instruments Listed Per Year

Source: Galaxy Digital Research



Data: Kaiko instrument explorer



Critics often dismiss cryptocurrencies and blockchain because they struggle to see why bitcoin or ether would be used for payments, failing to recognize the merits of the underlying technology. Stablecoins offer a clear and viable use case today, combining the properties of fiat currencies with the enhancements of public blockchains to function as a widely accepted **unit of account** for pricing assets and as a stable **medium of exchange** to facilitate payments.

An open financial system provides improvements over the traditional closed financial system through more efficient money movement and data. Compared to traditional payment flows and bank transfers, crypto markets and networks operate 24/7 and can offer a lower-cost alternative that enables instantaneous and borderless settlements leaving more money in the hands of consumers and businesses. Stablecoins can also support financial inclusion in a world where nearly 2bn people, or ~25% of global citizens, are unbanked (and many others underbanked as they lack access to basic financial services). Anyone with a mobile device and an internet connection can leverage US-dollar-backed stablecoins to store and send money. That means the open financial system can be accessed by those who need it the most—including those living in high-inflationary economic regions and those under authoritarian regimes—offering a digital currency that is a better **store-of-value** than their depreciating restricted local currencies.

Stablecoins adoption has accelerated as the underlying infrastructure of Bitcoin and Ethereum has continued to develop and integrate into the global economy. The explosion of DeFi in recent years has led to even more demand for stablecoins as a tool for leverage, risk management, savings, and other financial activities.

Stablecoins are one of the fastest growing asset categories and represent a \$150bn+ asset class (~15-20% of the global crypto market cap). Indeed, 3 of the top 6 crypto assets by market capitalization are stablecoins today. The growth of stablecoins as an asset class has outpaced Bitcoin and Ethereum during both the bull market of 2021 and the market correction experienced in 2022.

Crypto Growth by Asset Class

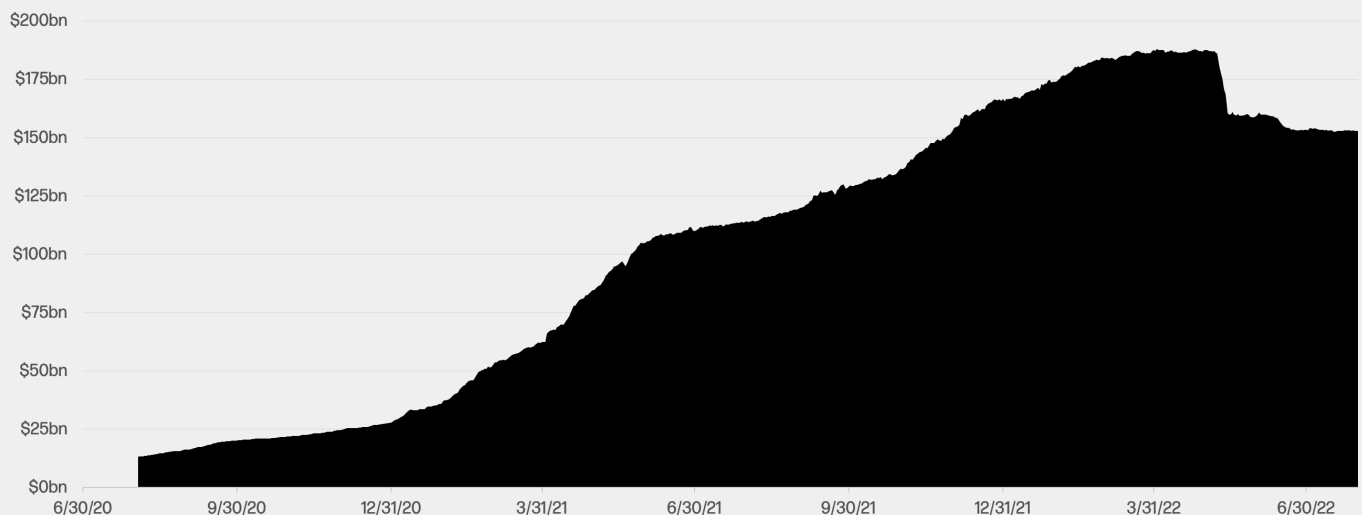


Market Cap (\$bn)	12/31/20	12/31/21	6/30/22
Global Crypto Market	\$787	\$2,337	\$921
% growth		197%	-61%
Stablecoins	\$28	\$167	\$153
% of global crypto	4%	7%	17%
% growth		499%	-9%
Bitcoin	\$539	\$876	\$366
% of global crypto	69%	37%	40%
% growth		62%	-58%
Ethereum	\$84	\$440	\$126
% of global crypto	11%	19%	14%
% growth		424%	-71%

Source: CoinGecko

Stablecoin Total Market Capitalization

Source: Galaxy Digital Research



Data: DeFi Llama



The Different Types of Stablecoins

Not all stablecoins are the same. Several different types of stablecoins have emerged with different price stability mechanisms. The composition of reserve assets varies considerably across popular stablecoins, with some stablecoins backed entirely by off-chain assets including cash or short-term, highly liquid assets, and others backed by assets significantly less liquid than cash or cash equivalents. Stablecoin design considerations: (i) peg, (ii) collateral, (iii) collateral amount, (iv) mechanisms, (v) price information.

Stablecoin designs can largely be categorized into three main categories:

- **Fiat-backed (centralized or custodial) stablecoins.** As the most popular type of stablecoin, centralized stablecoins follow an IOU model where a central entity backs the value of stablecoin with assets, and the issuer provides a mechanism to create new tokens or redeem existing tokens for underlying collateral on a one-to-one basis.
- **Overcollateralized, crypto-backed stablecoins.** Rather than going through a trusted, centralized issuer, overcollateralized stablecoins are issued through programmable smart contracts typically on non-custodial borrowing/lending protocols where various crypto assets are accepted as collateral and the reserves each stablecoin are always verifiable on-chain.

- **Algorithmic (undercollateralized) stablecoins.** Algo-stables are a newer class of stablecoins that maintain price stability with the help of a separate asset to absorb volatility. Rather than being explicitly backed or fully collateralized, algorithmic stablecoins are designed to maintain price parity with a certain asset through market forces via smart contracts to increase/decrease supply.

These are just the general distinct classifications that we've seen to date, but there also exist several stablecoins that exist outside of these categories such as commodity-backed stablecoins that are fully collateralized by physical assets, or, as seen more frequently this past year, stablecoins that fit within multiple categories by combining aspects from both algorithmic and overcollateralized models.

In this report, we explore the different types of stablecoins, profile some of the most prominent stablecoins and their issuers within each category, examine the competitive dynamics that are unique to each approach, summarize the trade-offs between individual stablecoins as well as the different stablecoin categories, highlight some of the key risks facing stablecoins, and analyzing them along key factors.

Primary Stablecoin Approaches



Stablecoin Approaches	Examples	How they work (Backing)
Fiat-backed or "custodial"	USDT, USDC, BUSD, TUSD, USDP	Requires centralized, trusted off-chain partners (direct line to US banks + audit firms), and implicit sponsor firm (i.e. Circle).
Crypto-backed or "Overcollateralized"	DAI, MIM, LUSD	Minting new units requires greater amount of collateral deposits; units taken out of circulation with debt repayment or liquidation.
Algorithmic or "Undercollateralized"	UST, USDN, USDD, FRAX, FEI	Algo stables are un-/under-collateralized, targeting price stability by using formulas / market incentives to adjust token supply.



Fiat-backed Stablecoins

Fiat-backed stablecoins are collateralized by off-chain financial assets and rely upon centralized and regulated entities for the issuance/redemption of units and the custody of reserve assets. Since the composition of reserves are not verifiable on the blockchain, issuers of fiat-backed stablecoins rely on reserve attestations conducted by independent auditors to confirm the existence of reserve assets. Historically, though, these attestations have lacked key details about the components of reserve assets and have been reported infrequently on an end-of-period basis and with a lag. While the frequency and detail of reserve attestations has generally increased over the years, the specificity of these attestations varies across issuers and uncertainty remains in the market due to their opacity.

Issuance of fiat-backed stablecoins is the process of creating new tokens, which requires the issuer to be sufficiently capitalized with liquid assets; issuers mint new digital dollars for their customers for every dollar that they take in. **Redemption** is the process by which a customer returns tokens to the issuer, thereby removing them from circulation, and receives fiat currency from the issuer in return. Tokens returned to the issuer are either destroyed or placed in the issuer's treasury for future issuance. Issuance and redemption of fiat-backed stablecoins is available to direct customers of the issuer, usually restricted to institutional clients, which must onboard through robust verification process that includes complete KYC compliance checks.

Stablecoin issuers provide varying levels of guarantees that redemptions of tokens may always be at the rate of \$1.00. The issuance and redemption process may also be subject to certain minimum amounts, incur additional fees, and could take several days to process. Stablecoin users who want faster access to liquidity may swap their stablecoin on an exchange or secondary marketplaces (outside of the issuer's redemption process), which subjects the stablecoin to price risk through supply/demand forces. However, large variances from par typically do not persist if the issuer's redemption mechanism is believed to be working properly - price deviations present arbitrage opportunities that often see traders step in by buying the stablecoin in the open market at a discount to par so that it can then be redeemed directly with the issuer. Fiat-backed stablecoin issuers typically market themselves based on the quality and composition of their reserves (many committed to 100% cash & cash equivalent backings), the verification of reserve funds, the regulatory licenses they obtain, and the ease at which units can be created and redeemed.

While regulatory standards to oversee stablecoin issuers and their practices have not yet been established by core regulatory bodies or any international standard setters, stablecoin issuers have taken a proactive approach towards expected regulatory compliance as

it relates to disclosures, risk management standards, and reserve practices. So, while no stablecoin arrangement is fully regulated, some activities may be (e.g., KYC/AML & counter financing of terrorism (CFT) requirements may call for certain entities to register with FINRA or obtain money transmitter licenses). The lack of proscriptive regulations also means that there can be some leeway that stablecoin issuers to operate as not every issuer required to provide the same redemption guarantees to its holders, particularly relevant when evaluating on-shore vs. off-shore fiat-backed stablecoin issuers.

To illustrate, we compare the two largest issuers of stablecoins: Tether (USDT) and Circle (USDC).

Tether

Formed in 2014, Tether (with a capital T) is the issuer of the largest stablecoin, tether (or USDT). Tether is closely connected with the crypto exchange Bitfinex, sharing the same parent company, iFinex, and is registered in the British Virgin Islands. USDT was originally issued on the Omni Layer Protocol, built on top of Bitcoin, in October 2014, before expanding to other blockchains including Ethereum. In addition to USDT, Tether also issues stablecoins that track EUR, CNH, MXP, and physical gold.

USDT initially found product-market fit as a way for users and exchanges to circumvent the banking system at a time when banks were not willing to support crypto companies and traders. During the 2017 bull market, very few exchanges, even those in the United States, were able to get and maintain bank accounts, and Tether filled that void, providing a token that could be used for USD-denominated trading. USDT is popular offshore, especially in China, where it has been a key part of the workflow for converting fiat to crypto. Due to national regulations prohibiting financial institutions from servicing crypto exchanges, users typically convert their fiat into USDT at an OTC desk before depositing the USDT on an exchange. While this process is somewhat cumbersome, it allows Chinese users to access crypto in a tightly regulated environment and serves as a major source of demand for USDT. Note: While USDT is still available for US persons and business to use, Tether stopped directly serving US individuals and corporate customers since the start of 2018, restricting them from issuance/redeeming services.

Today, USDT is mainly use as an on- and off-ramp as well as in trading pairs for crypto trading across several exchanges. It currently ranks #3 among all cryptocurrencies behind BTC and ETH with a market cap of over \$70bn, and is available on 12 blockchains including Tron, Solana, Avalanche, and others.



USDT Market Cap by Network



Network	(in \$bn)	% total
Tron	\$32.01	48%
Ethereum	\$30.99	47%
Solana	\$1.80	3%
Omni	\$0.75	1%
Avalanche	\$0.55	1%
Algorand	\$0.16	0%
Others	\$0.22	0%
Total	\$66.48	100%

Source: [Tether Transparency](#) (data as of 8/5/22)

USDT's presence on Tron is particularly notable. Tron has relatively weak settlement assurances and is generally not viewed as a very secure platform. But as a centralized asset, USDT is only minimally affected by Tron's poor settlement assurances, and as such is well-suited to take advantage of the lack of congestion on the platform. Specifically, because USDT tokens represent an IOU for assets held in reserve by the centralized Tether Limited entity, and because Tether can freeze and reissue these IOUs at will, there's no need for the more durable finality offered by Bitcoin or Ethereum. Many of the asset's core applications are time-sensitive, making them an ideal fit for Tron, which has quick block times and mostly low fees due to less network congestion than Bitcoin or Ethereum. USDT is used as an on-ramp into crypto, a quote currency for spot and derivatives trading, a vector for cross-exchange arbitrage, and an instrument for international dollar-denominated transfers.

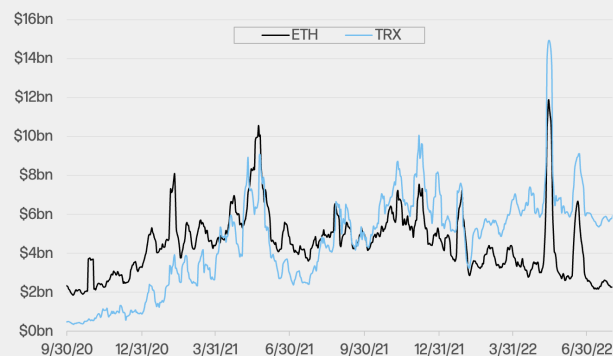
Tether's Controversy and Legal Issues

In the past, critics have often questioned Tether's operations and the authenticity of its reported reserves. Some of the initial criticisms claimed Tether was printing USDT "out of thin air" as a means to buoy liquid digital asset prices (like BTC) – this theory appears to have been based on dubious data and didn't hold scrutiny given the growth of Tether issuance coupled with the decline in BTC's USD-denominated exchange rate. More recent and durable criticism has arisen over the specific assets that are held in its reserves, particularly the non-cash holdings, and whether they are liquid enough to be converted to cash to meet all redemption requests in full and in a timely manner were a bank run scenario to materialize.

In April 2019, New York State Attorney General (NYAG) Letitia James [said](#) they were investigating crypto exchange Bitfinex—operated by the same parent company as Tether—alleging that both Bitfinex and Tether defrauded investors "in a cover-up to hide the apparent loss of \$850 million of co-mingled client and corporate funds." In February 2021, NYAG's Letitia James [fined](#) parent company iFinex \$18.5m and ordered both parties to cease trading activity with New Yorkers after state investigations found that Tether made false statements about having sufficient reserves to back every USDT in circulation. To increase transparency, the court also asked Tether to provide

USDT – Daily Xfer Val Adj on Ethereum vs. Tron (7d-MA)

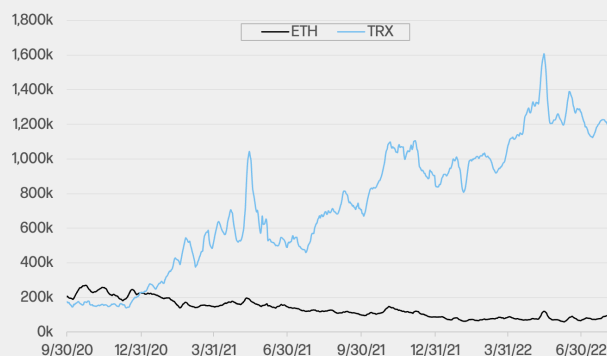
Source: Galaxy Digital Research



Data: Coin Metrics

USDT – Daily Tx Count on Ethereum vs. Tron (7d-MA)

Source: Galaxy Digital Research



Data: Coin Metrics

quarterly reserve reports for the next two years, which have been ongoing. Shortly after the NYAG settlement, in October 2021, the CFTC [ordered](#) Tether and Bitfinex to pay civil monetary fines totaling \$42.5m over false claims that Tether was fully backed by US dollars.

After both the NYAG and the CFTC settlements, Tether was hit with a class-action lawsuit in December 2021, that similarly [alleged](#) the company had misrepresented its reserves, calling its practices "immoral, unethical, oppressive, and unscrupulous." Tether quickly [responded](#) to the claim, calling it "another nonsense, copycat lawsuit" and a "shameless money grab." Several of those claims have already been dismissed but litigation is still ongoing.

Today, Tether is still facing criticisms over the opaqueness of its reporting, including that its executives have yet to deliver a full audit after [claiming](#) in July 2021 that an audit was "months" away, though in early July 2022, CTO Paolo Ardoino [stated](#) in an interview that Tether had selected a "Big 12" auditing firm. The reported assets



included in Tether's attestation reports has been a prominent concern, particularly that as each asset class carries varying levels of liquidity and credit risk (e.g., individual line-items such as CP, secured loans, and "other investments") that results in asset-liability mismatches and could impact redeemability. In addition, market participants have little visibility into Tether's reserve assets in real-time, with end-of-period reporting for its quarterly attestations creating opportunities for Tether to hold riskier assets that can then be replaced with safer assets closer to the end of each quarter. Regardless of the validity of some of these criticisms, which we may never uncover, Tether [claims](#) it has been de-risking its reserve profile and that Tether has so far met every one of its redemption requests in a timely manner.

Tether Issuance and Redemptions

Minting of Tether tokens is available to Tether customers. Tether requires a minimum of at least \$100,000 for new deposits and withdrawals in order to mint/redeem USDT, charging a fee of 0.1% on both transactions. Tether maintains a portion of USDT supply in treasury, split among several treasury wallets on each blockchain (e.g., its [Ethereum wallet](#), [Tron wallet](#)). The USDT supply held in these wallets are considered "authorized but not issued," meaning they are not counted in the market cap of USDT. USDT is only issued or released for circulation after Tether customers make their fiat deposits at Tether's partner banks and the USDT is sent out from the treasury.

Tether typically mints USDT in \$1bn increments and uses its Treasury balance to gradually draw down from to meet customer issuance requests in a timely manner (rather than minting new USDT to then transfer to customers on-demand). Tether CTO Paolo Arduino has claimed its practice of managing "authorized but not issued" tokens in this manner is for security purposes—i.e., to reduce the number of times that Tether must access and utilize the sensitive cryptographic keys required to mint USDT. Tether manages its Treasury similarly for redemptions: as users send

in redemption requests by sending USDT to the Treasury wallet, the USDT is taken out of circulation – though it technically isn't "burned" until Tether sends the USDT to an inaccessible address, which Tether also does in large, periodic transactions (illustrated by decreases in "Circulating Supply" line shown in chart below).

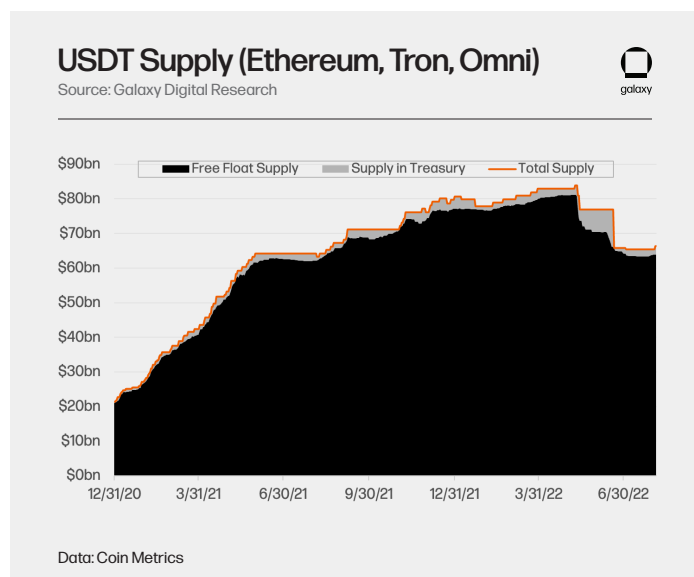
Given Tether's issuance and redemption fee of 0.1%, arbitrage opportunities are presented when Tether price deviates outside the range of \$0.999 – \$1.001. When the price falls below \$0.999, traders can purchase tethers in the secondary market to be redeemed through Tether at nominal value for a profit. Conversely, if Tether is trading above \$1.001, traders could go to Tether to mint new coins to then be sold in the market at a gain. However, Tether may trade outside of this range if there are no willing arbitrageurs or if traders have concerns that their redemptions cannot be met either in full or in a timely manner.

In addition, Tether makes no guarantees that redemption requests will be met promptly or in-full. This is explicitly expressed in Tether's [legal disclaimer](#): "Tether reserves the right to delay the redemption or withdrawal of Tether Tokens if such delay is necessitated by the illiquidity or unavailability or loss of any Reserves held by Tether to back the Tether Tokens, and Tether reserves the right to redeem Tether Tokens by in-kind redemptions of securities and other assets held in the Reserves."

Tether Reserves

Since the NYAG's 2019 ruling, Tether has provided more detailed line items for each of the components of its reserves on an end-of-period quarterly basis through its attestation reports, which have been certified by independent auditor MHA Cayman. MHA Cayman provides an "assurance," not an audit, that Tether Limited's policies and procedures as they related to the company's preparation of the data reviewed by MHA Cayman were "appropriate," rather than whether they were followed. MHA Cayman does not actually review underlying data to confirm or deny whether claims made by Tether regarding its reserves are materially accurate. Instead, MHA Cayman solely offers an assurance that Tether's reporting is "correctly stated" from an accounting standpoint "based on the balances set out" by Tether. Essentially, MHA Cayman confirms that Tether's production conforms to its own procedures for making such a production and that it is properly formatted for accounting standards. Lastly, in addition to these quarterly reports, Tether also provides less-detailed daily aggregate balances that shows current issued and authorized amounts.

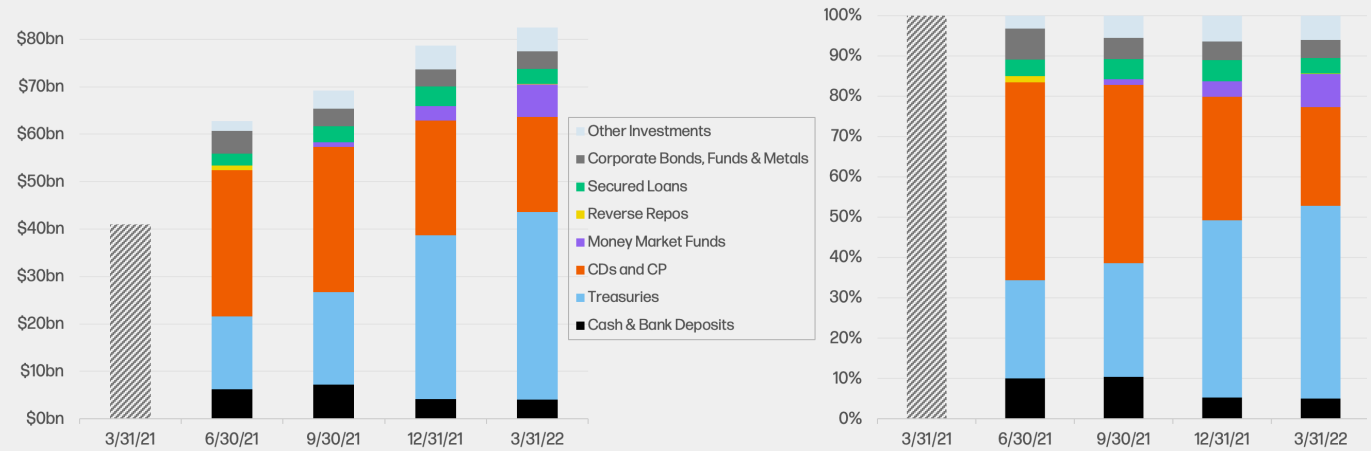
Tether Limited is listed as the custodian for USDT. In the past, Tether has declined to reveal where the exact locations of where reserves are held, [noting](#) that it is a private company with no obligations to do share that information (though some of Tether's reserves have been [revealed](#) to be held at several small Bahamas banks).





Tether Reserves - Asset Breakdown and Mix

Source: Galaxy Digital Research



Data: Tether Transparency Reports

Tether Quarterly Reserve Composition



Reserve Assets (\$bn)	3/31/21	6/30/21	9/30/21	12/31/21	3/31/22	3/31/21	6/30/21	9/30/21	12/31/21	3/31/22
<u>Cash & Cash Equivalents, Other ST Deposits, CP</u>										
Cash & Bank Deposits		\$6.28	\$7.24	\$4.19	\$4.10	0.0%	10.0%	10.5%	5.3%	5.0%
US Treasuries		N/A	N/A	N/A	\$39.20	0.0%				47.6%
Non-US T-bills		N/A	N/A	N/A	\$0.29	0.0%				0.3%
Treasuries		\$15.28	\$19.43	\$34.53	\$39.49	0.0%	24.3%	28.1%	43.9%	47.9%
CDs and CP		\$30.81	\$30.60	\$24.17	\$20.10	0.0%	49.1%	44.2%	30.7%	24.4%
Money Market Funds		\$0.00	\$1.00	\$3.00	\$6.80	0.0%	0.0%	1.4%	3.8%	8.2%
Reverse Repos		\$1.00	\$0.00	\$0.00	\$0.11	0.0%	1.6%	0.0%	0.0%	0.1%
Total Cash & CE, Other ST Deposits, CP		\$53.37	\$58.27	\$65.88	\$70.59	0.0%	85.0%	84.3%	83.7%	85.6%
Secured Loans		\$2.52	\$3.45	\$4.14	\$3.15	0.0%	4.0%	5.0%	5.3%	3.8%
Corporate Bonds, Funds & Metals		\$4.83	\$3.61	\$3.63	\$3.73	0.0%	7.7%	5.2%	4.6%	4.5%
Other Investments	\$41.02	\$2.05	\$3.83	\$5.02	\$4.96	100.0%	3.3%	5.5%	6.4%	6.0%
Total Assets	\$41.02	\$62.77	\$69.16	\$78.68	\$82.42	100.0%	100.0%	100.0%	100.0%	100.0%
Digital Token Liabilities	\$40.86	\$62.61	\$68.99	\$78.48	\$82.19					
Non-Digital Token Liabilities	\$0.01	\$0.02	\$0.02	\$0.06	\$0.07					
Total Liabilities	\$40.87	\$62.63	\$69.01	\$78.54	\$82.26					
Total Equity (\$m)	\$149m	\$144m	\$146m	\$137m	\$162m					

Source: Tether Transparency Reports



Over time, cash & cash equivalents and short-term deposits have formed a larger portion of Tether's reserve composition. Cash & cash equivalents, other short-term deposits, and corporate paper stood at roughly ~85% of total reserve assets as of 3/31/22. For the 3/31/22 [reserves report](#), Tether broke out the "Treasuries" line item to show the split between US and non-US Treasuries. Tether reduced its holding mix of CDs and CP—which some have alleged to be issued by risky Chinese entities—by more than half since 6/30/21 from 49% to 24% at 3/31/22.

In the 3 months since its latest reserves attestation report (3/31/22), Tether has stated that it has further [reduced](#) its CP holdings by nearly 50% to \$8.4bn (including \$5bn of which will expire on July 31) in its commitment to eventually taking its CP exposure down to zero. More recently, Tether confirmed that total CP exposure had been [reduced](#) to \$3.7bn at July-end and that it expects the CP balance will go to zero by early November 2022. However, at the time of writing (August 8, 2022), Tether has yet to produce a Q2 2022 attestation report.

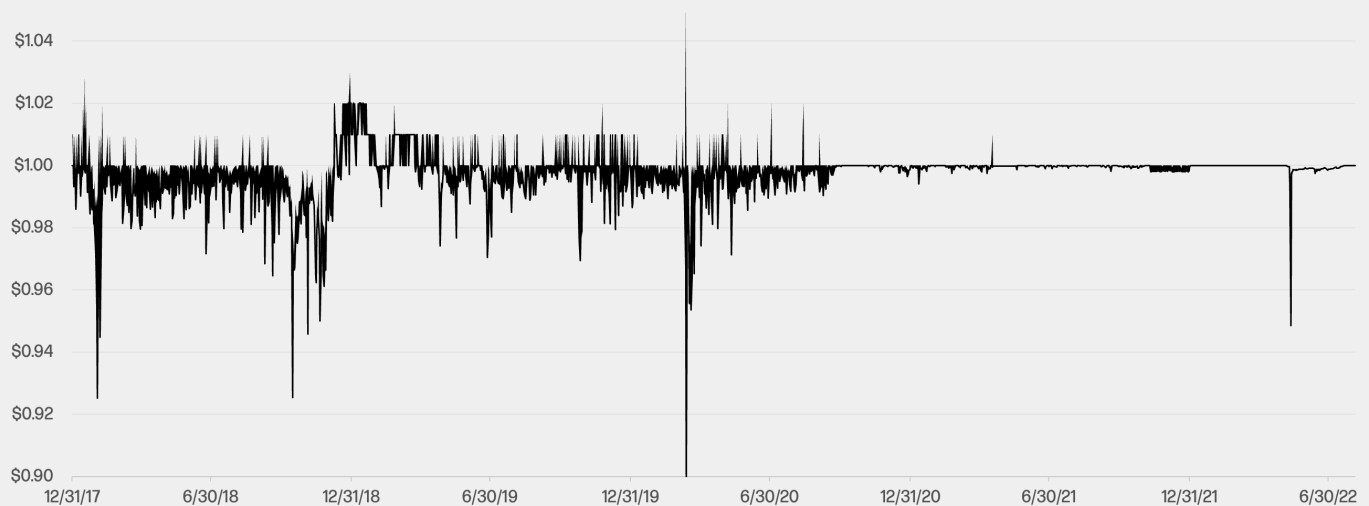
Tether De-Pegs

Since inception through late 2020, Tether has traded in a relatively wide range, frequently trading above or (more often) below its nominal value during intra-day trading. 2018 saw USDT trade below \$0.98 on 39 days of the year. Price volatility of Tether has dramatically decreased since then, as 2019 and 2020 saw just 10 and 11 days, respectively, that Tether traded below \$0.98 during intra-day, including on 3/13/20 when its price briefly fell below \$0.90. This was followed by 0 days during 2021—in fact, Tether price didn't fall below \$0.995 on any of the days during the year.

Tether's price stability continued its improvement from 2021 through this year until the collapse of Terra USD (UST) reignited fears that Tether's reserves were insufficient to cover its liabilities in a timely manner. Following the collapse of UST, USDT traded below \$0.95 on 5/12/22. During Tether's de-pegging to \$0.95, the price of USDC saw the opposite reaction, rising to \$1.05 across several exchanges, suggesting USDT holders exited their positions for the supposedly "safer" stablecoin. As it turns out, even though Tether has attempted to improve its risk profile in with greater reserve allocations to cash and short-term assets, its peg concerns have persisted, sparking back up after the market turns. In the short term, those fears appear to have eased, as USDT has traded back above \$0.999 since 5/13/22, though this slight \$0.001 discount persisted on continued selling pressure for over two months before USDT finally fully recovered back to \$1 by mid-July.

USDT Price (intra-day low - closing price)

Source: Galaxy Digital Research

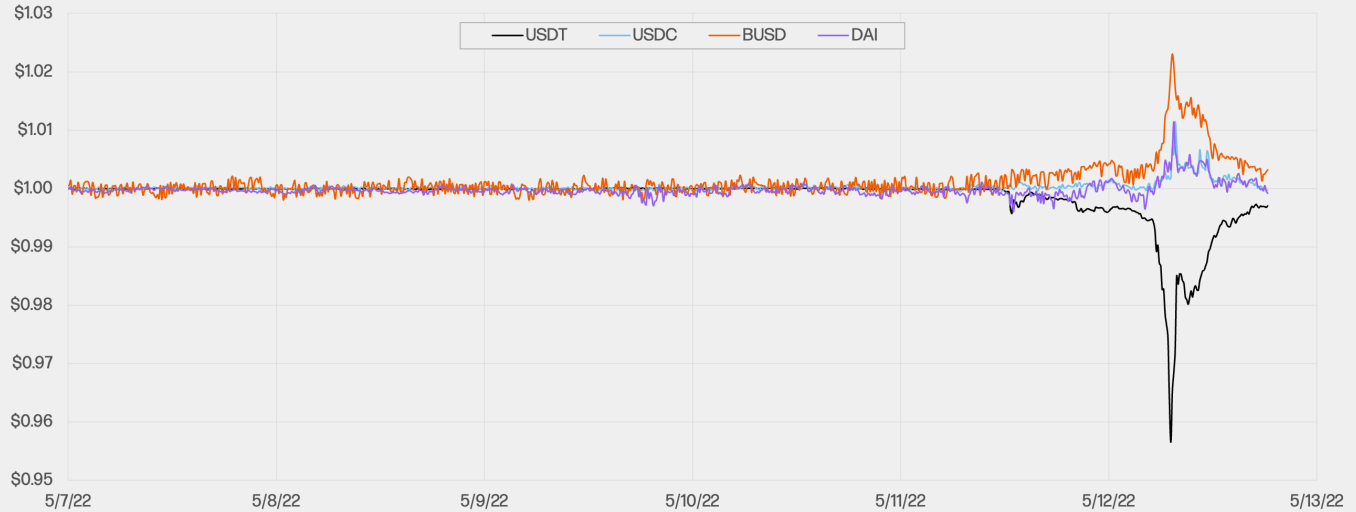


Data: CoinMarketCap



Price of USDT vs. Other Select Stablecoins (May 7-13, 2022)

Source: Galaxy Digital Research

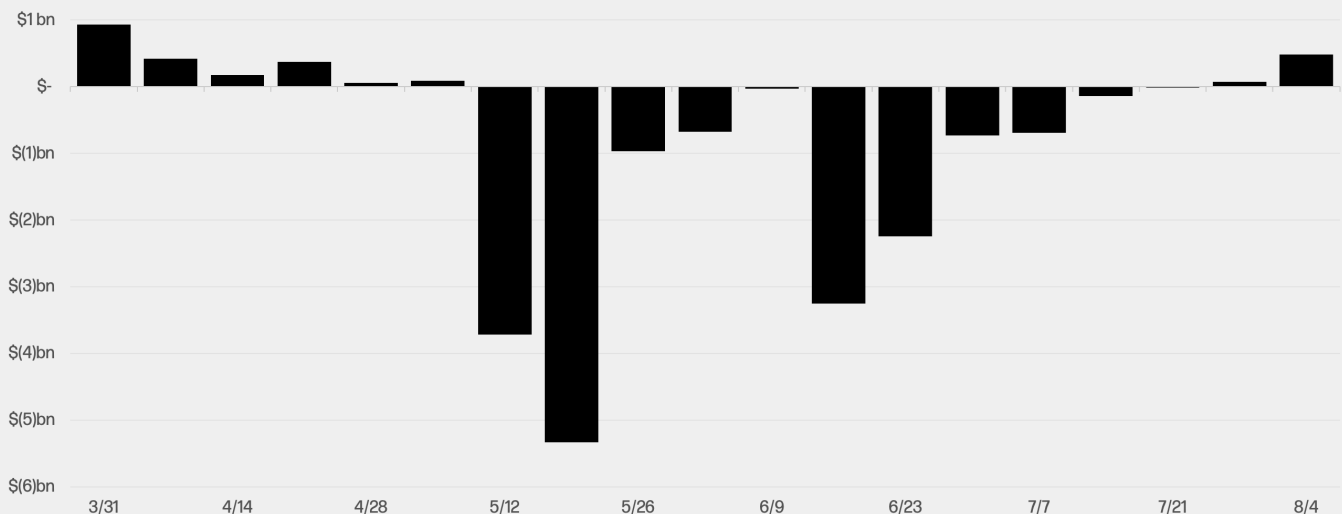


Data: Amberdata.io

Tether also experienced a significant increase in redemption requests, partly driven by USDT holders looking to access the limited liquidity they believed to be held in Tether's reserves, while other investors looked to take advantage of the arbitrage presented by the de-pegging – rarely seen since 2020. According to the flows in/out of its treasury addresses on Ethereum and Tron (and adjusting for mints/burns out of known addresses), Tether processed \$12.5bn in redemptions requests during the month of May, including over \$10bn over the 10-day period between 5/11/22 – 5/20/22 as the circulating supply of USDT dropped from \$81bn to \$71bn. This is estimated to have brought in at least \$22m in revenue for Tether in May based on its 0.1% fee structure on issuance/redemptions.

USDT Free Float Supply – Weekly Net Changes (2022)

Source: Galaxy Digital Research



Data: Coin Metrics



USDT - ETH

	Tx Count				Volume (USDT in bn)				Revenue (fees)
	<u>Tx_Cnt_MINT</u>	<u>Tx_Cnt_BURN</u>	<u>Tx_Cnt_REDEEM</u>	<u>Tx_Cnt_ISSUANCE</u>	<u>Vol_MINT</u>	<u>Vol_BURN</u>	<u>Vol_REDEEM</u>	<u>Vol_ISSUANCE</u>	@0.1% Volume
7/31/21	0	0	24	16	0.00	0.00	0.81	0.02	\$837,174
8/31/21	3	0	8	29	3.00	0.00	0.41	4.24	\$4,646,725
9/30/21	0	0	28	32	0.00	0.00	0.96	1.00	\$1,956,824
10/31/21	0	0	12	32	0.00	0.00	1.35	1.57	\$2,924,643
11/30/21	4	0	17	29	4.00	0.00	2.05	3.96	\$6,008,762
12/31/21	2	0	37	38	2.00	0.00	3.09	5.24	\$8,326,733
1/31/22	0	0	27	23	0.00	0.00	1.67	3.20	\$4,868,133
2/28/22	0	0	14	13	0.00	0.00	0.62	0.43	\$1,048,447
3/31/22	0	0	19	10	0.00	0.00	1.29	0.36	\$1,650,791
4/30/22	0	0	8	12	0.00	0.00	0.19	0.36	\$543,019
5/31/22	0	1	37	14	0.00	3.00	5.05	1.29	\$6,341,679
6/30/22	0	1	57	6	0.00	4.50	2.95	0.22	\$3,169,007
7/31/22	0	0	21	4	0.00	0.00	0.59	0.09	\$683,063
Total	9	2	309	258	9.00	7.50	21.03	21.98	\$43,004,998

Source: Etherscan

USDT - TRON

	Tx Count				Volume (USDT in bn)				Revenue (fees)
	<u>Tx_Cnt_MINT</u>	<u>Tx_Cnt_BURN</u>	<u>Tx_Cnt_REDEEM</u>	<u>Tx_Cnt_ISSUANCE</u>	<u>Vol_MINT</u>	<u>Vol_BURN</u>	<u>Vol_REDEEM</u>	<u>Vol_ISSUANCE</u>	@0.1% Volume
7/31/21	0	0	6	16	0.00	0.00	0.02	0.15	\$164,084
8/31/21	3	2	18	41	3.00	3.00	3.29	3.32	\$6,617,862
9/30/21	4	0	13	51	4.00	0.00	0.80	3.72	\$4,525,886
10/31/21	0	0	5	18	0.00	0.00	0.17	1.77	\$1,934,271
11/30/21	5	2	10	55	5.00	3.00	3.19	4.38	\$7,568,992
12/31/21	5	3	22	88	5.00	4.50	4.86	6.16	\$11,017,238
1/31/22	1	2	20	28	1.00	2.75	2.99	1.21	\$4,196,189
2/28/22	2	0	10	80	2.00	0.00	0.43	1.87	\$2,296,088
3/31/22	3	0	6	85	3.00	0.00	0.23	3.08	\$3,312,701
4/30/22	0	0	8	76	0.00	0.00	0.21	1.10	\$1,314,114
5/31/22	1	2	39	23	1.00	4.00	7.39	0.48	\$7,869,646
6/30/22	0	1	47	10	0.00	6.60	3.97	0.69	\$4,660,113
7/31/22	0	0	16	22	0.00	0.00	0.64	0.95	\$1,587,434
Total	24	12	204	571	24.00	23.85	27.56	27.92	\$55,477,184

Source: TronScan

USDT - Ethereum Addresses

USDT - Tron Addresses

Treasury	0x5754284f345afc66a98fbb0a0afe71e0f007b949	TKHuVq1oKVruCGLvqVexFs6dawKv6fQgFs
Token	0xdAC17F958D2ee523a2206206994597C13D831ec7	TR7NHqjeKQxGTCi8q8ZY4pL8otSzzgJLj6t
Burn/Mint	0xc6cde7c39eb2f0f0095f41570af89efc2c1ea828	TBPxhVAsuzoFnKyXtc1o2UySEydPHgATto



USD Coin (USDC)

USDC is the second most popular stablecoin today and was launched on Ethereum as a US-based alternative to Tether and other USD-pegged stablecoins in September 2018, just months after Tether stopped serving US customers. USDC is issued by Circle, but it was originally founded and developed by both Coinbase and Circle, which form the **Centre** consortium that governs USDC. The purpose of governing through this consortium was to strive for an industry standard using USDC as an example. USDC is issued through **Circle** but it also has local issuers that are regulated in the jurisdictions that they operate. Circle is a financial technology company that's headquartered in Boston, Massachusetts and offers payments technology and treasury infrastructure to help bridge crypto with the traditional world. According to its website, "USDC is fully backed by cash and short-dated U.S. government obligations, so that it is always redeemable 1:1 for U.S. dollars."

USDC's adoption grew quickly as it has found footing as an on-ramp between fiat and crypto through relatively stable banking access for the US-based exchanges. Since its inception, USDC's rapid growth has been eating into Tether's leading share in the stablecoin market. As of 7/31/22, the circulating supply of USDC was ~55bn—approximately 83% of USDT supply. USDC has been integrated on 9 blockchains including Solana, Avalanche, Algorand, Stellar, and Flow.

Despite marketing its stablecoin as being relatively safer than Tether, Circle has also found itself in the crosshairs of US litigation. Circle received an [investigative subpoena](#) from the SEC in July 2021 that requested "documents and information regarding certain

of our holdings, customer programs and operations." The subpoena came just one month after Circle announced its fixed rate yield product for USDC, called Circle Yield, which was going to be offered by Coinbase to its customers. Before Coinbase customers could access the 4% USDC APY program, Coinbase [pulled](#) the launch of Coinbase Lend as it awaits more regulatory clarity. Circle Yield is currently offered through Circle Bermuda to accredited investors and is issued in the United States as a registration-exempt security pursuant to Reg D under the Securities Act of 1933 (not available in AK, MN, NY, HI).

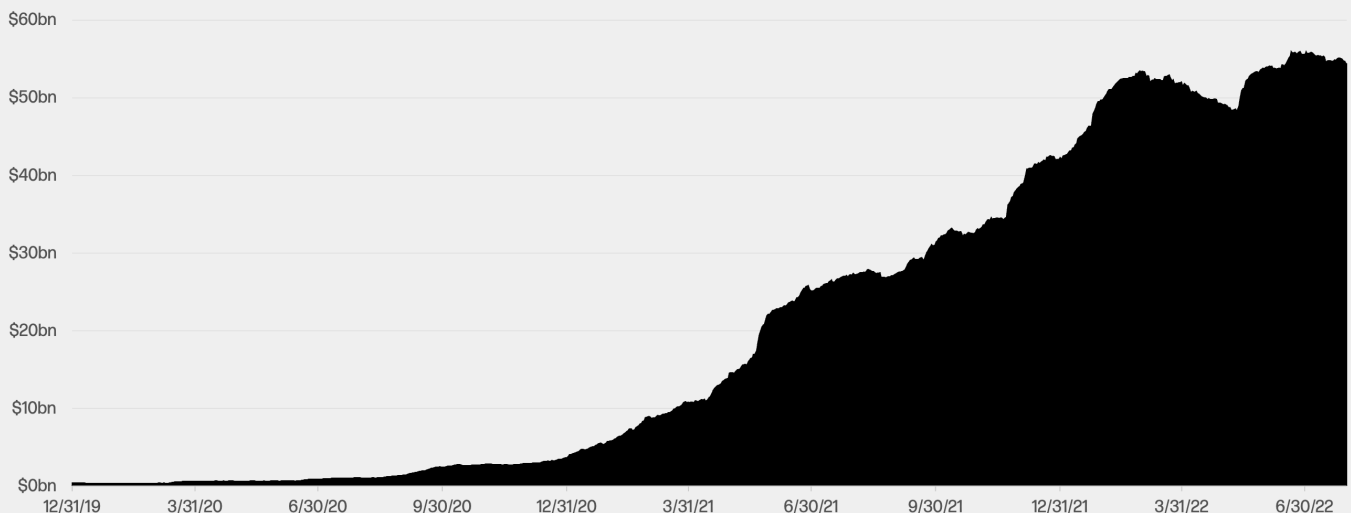
In August 2021, CEO Jeremy Allaire [shared](#) that Circle intends to become a full-reserve national commercial bank that will be regulated and supervised by the Fed, Treasury, OCC, and the FDIC. However, at the time of writing, Circle has yet to achieve registration with any of those banking regulators (the Treasury isn't a banking regulator per-se, but Circle does comport to FinCEN AML/KYC requirements). Circle currently operates through state-based virtual currency and money transmitter licenses—though it notably lacks either a trust license or the elusive BitLicense from the New York Department of Financial Services (NYDFS). Competitor stablecoin issuers Paxos (behind Pax Dollar (USDP) and Binance USD (BUSD)) and Gemini (behind Gemini USD (GUSD)) both possess licenses from NYDFS.

USDC Issuance / Redemption

Minting and redemption of USDC requires one to open a Circle Account. Circle and its banking partners do not charge fees when minting USDC or redeeming USDC for dollars. Minting USDC requires users to send USD to the bank of a licensed CENTRE issuer, and the issuer then verifies the funds have been deposited and submits

USDC Market Cap

Source: Galaxy Digital Research



Data: CoinGecko



a request to USDC's relevant token contract to mint an equivalent amount of USDC which is then deposited to the users wallet.

Redemption of USDC follows a similar process in reverse – the user submits a request for redemption from a USDC issuer, which sends the USDC to the smart contract to be burned or taken out of circulation, and then the equivalent amount fiat funds from the USDC reserves are transferred to the customer's bank account upon successful verification and validation.

Unlike the minimum requirements to create and redeem USDT, there is no minimum tokenization amount when minting USDC, but redemption of USDC for dollars has a minimum requirement of \$100. Minting occurs within minutes after deposits have settled in Circle's account (though this is still subject to slow bank transfers which may take 2 business days to process). The mint and redeem functions for USDC are available to users 24/7 (also subject to bank hours and delays). Circle has banking partners that may enable faster settlements including Silvergate, which is working on enabling real-time settlements available 24/7 for its banking customers.

USDC Reserves

USDC reserves are held in segregated accounts that cannot be used by Circle and are protected in the event of a Circle bankruptcy. USDC has reserve attestation reports published monthly by Grant Thornton LLP which date back to October 2018. Most of these

attestation reports confirm that the total fair value of assets held on behalf of USDC holders is at least equal to the total USDC in circulation on approved blockchains (less tokens allowed but not issued and blacklisted tokens).

Starting May 2021, the attestation reports provided more detail behind the breakdown of USDC reserves. On May 31, 2021, USDC had 61% in cash & cash equivalents, with the remainder split among Yankee CDs, US Treasuries, Commercial Paper, Corporate Bonds, and Municipal Bonds & US Agencies. But following an update in August 2021, reserves held in Yankee CDs and Treasuries contradicted Coinbase's assertion on its website that "each USDC is backed by one US dollar held in a bank account," which resulted in Coinbase modifying its description of USDC to say USDC is "backed by fully reserved assets." Over time, the reserves for USDC have slowly transitioned to be 100% backed by just cash & cash equivalents, achieving this by 9/30/21.

On July 5, 2022, Circle released a [statement](#) saying 80% of USDC reserves were in US T-bills with durations of 3 months or less – all purchased by BlackRock and custodied at BNY Mellon. The remaining 20% was in cash held at banking partners including Silvergate, Signature Bank, and New York Community Banks—these balances are meant to meet redemptions of USDC upon request, to be available outside of normal banking business hours, 24/7/365.

USDC Monthly Reserve Breakdown



Reserve Assets (in \$bn)	5/31/21	6/30/21	7/31/21	8/31/21	9/30/21	10/31/21	5/31/21	6/30/21	7/31/21	8/31/21	9/30/21	10/31/21
Cash & Cash Equivalents	\$13.4	\$11.7	\$13.0	\$25.3	\$31.7	\$33.0	61%	46%	47%	92%	100%	100%
Yankee CDs	\$2.9	\$3.7	\$4.1	\$0.4			13%	15%	15%	1%	0%	0%
US Treasuries	\$2.7	\$3.3	\$3.4	\$1.3			12%	13%	12%	5%	0%	0%
Commercial Paper	\$2.0	\$2.4	\$2.2	\$0.5			9%	10%	8%	2%	0%	0%
Corporate Bonds	\$1.1	\$4.0	\$4.5				5%	16%	16%	0%	0%	0%
Municipal Bonds & US Agencies	\$0.1	\$0.1	\$0.2				0%	0%	1%	0%	0%	0%
Total Assets	\$22.2	\$25.2	\$27.4	\$27.5	\$31.7	\$33.0	100%	100%	100%	100%	100%	100%

Source: [center.io](#)



Circle vs. Tether

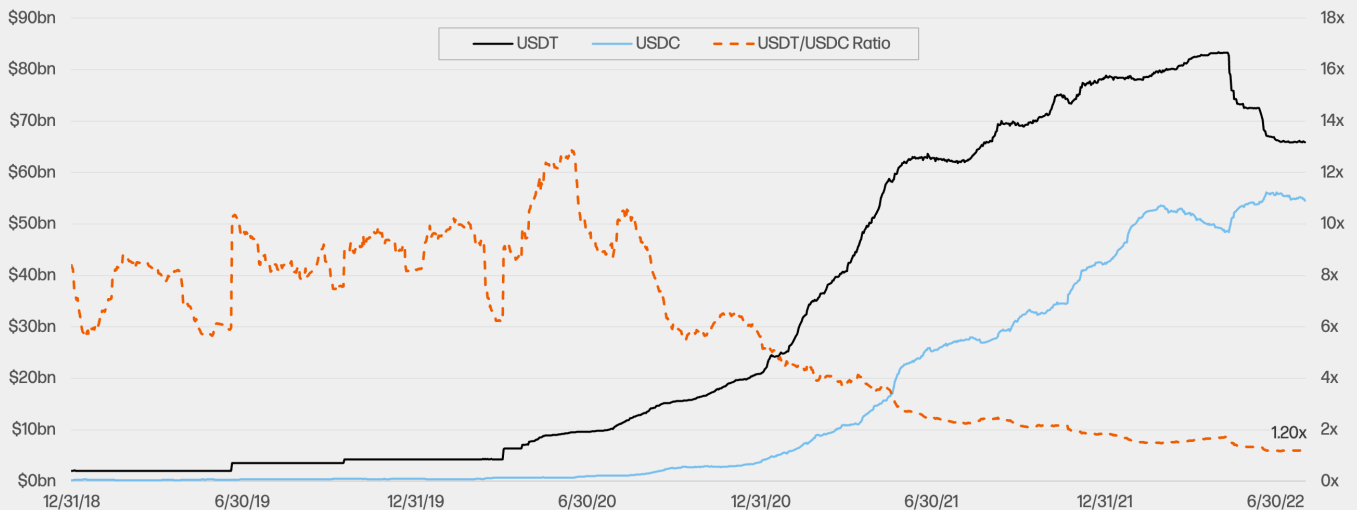
USDT's lead against USDC in terms of market cap (across all networks) reached a recent peak of more than 12x in May 2020, but has since fallen at a rapid pace. As of July 31, 2022, the market cap of USDT stood at \$65.95bn compared to \$54.5bn for USDC, representing a USDT/USDC ratio of just 1.20x—the lowest ratio in the stablecoins' history.

At the start of 2022, USDC's free float supply on Ethereum surpassed that of USDT and it has since continued to widen the gap; as of 7/31, USDC supply totaled \$45bn – 44% more than the \$31bn in USDT on Ethereum.

USDC has typically a greater % of its supply on Ethereum locked in smart contracts compared to Tether – YTD, USDC has averaged more than 2.1x the level of USDT on this metric. This would align with the presumption that Tether is mostly used as an on- and off-ramp for trading at exchanges (due to banking restrictions in China) whereas in the US, most users can on-ramp using dollars from their bank accounts rather than having to rely upon stablecoins, enabling more if its supply to be used outside of exchanges.

USDC vs. USDT Market Cap

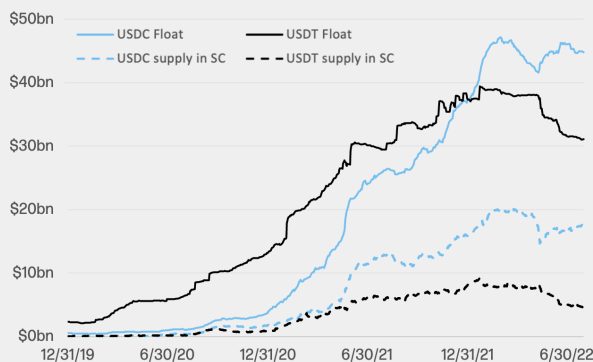
Source: Galaxy Digital Research



Data: CoinGecko

USDC vs. USDT –Supply on Ethereum: Float vs. Locked in Contracts

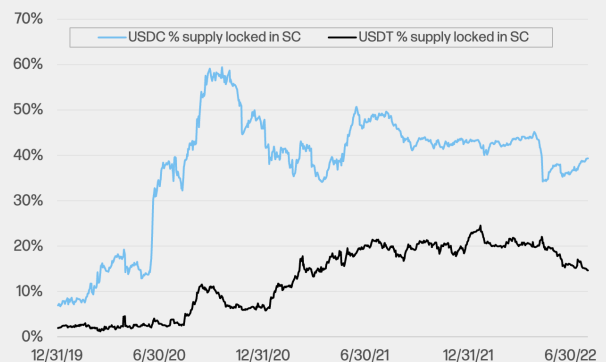
Source: Galaxy Digital Research



Data: Coin Metrics

USDC vs. USDT –Supply on Ethereum: % Locked in Contracts

Source: Galaxy Digital Research



Data: Coin Metrics



Fiat-backed Stablecoin Landscape

- Binance USD (BUSD)** is the 3rd largest fiat-backed stablecoin at \$18bn, only one-third of the circulating supply of USDC and one-fourth of the circulating supply of USDT. BUSD was created in partnership between Binance and **Paxos**, which is a trust company and custodian regulated by the NYDFS (Paxos also issues **Pax Dollar (USDP)** and **PAX Gold (PAXG)**). During the initial discussions with the NYDFS, Paxos had agreed that USDP and BUSD would only be issued on the Ethereum blockchain (BUSD token on BNB Chain is issued by Binance as Binance-Peg BUSD).
 - Paxos first provided a breakdown of its reserves for BUSD and USDP for the period ended 6/30/21, which came shortly after Tether first disclosed a breakdown of its reserves following the settlement with the NYAG. Relative to Tether and Circle, Paxos showed a safer and more liquid reserve composition with 96% held in cash & cash equivalents and the remainder held in US T-bills. More recently, for the period ended 6/30/22, Paxos committed to providing an greater level of transparency beyond what its regulators require by providing the CUSIP of all securities backing USDP and BUSD – a practice that it intends to follow on a monthly basis moving forward. Circle has since followed suit starting with the period ended 6/30/22.
- True USD (TUSD)** is issued by Techteryx and is based in Shenzhen, China. TUSD relies on Chainlink and Armanino's TrustExplorer solution to provide real-time assurances for both on-chain and off-chain balances, including those that are held in TrueUSD's escrow bank accounts. With Armanino sending real-time audited data to Chainlink, TUSD introduces Proof of Reserve & Supply reference contracts that provide increased transparency compared to other fiat-backed stablecoins that rely upon monthly attestation reports. The issuer is partnered with banks including Signature Bank, Silvergate, Prime Trust, First Digital Trust, and BitGo.
- Others fiat-backed stablecoins include stablecoins issued by centralized exchange entities (Huobi-branded **HUSD** issued by Stable Universal / **Gemini Dollar (GUSD)** issued by Gemini). HUSD asserts it is backed 100% by cash held in money market accounts and does not contain "cash equivalents" such as US T-bills, bank CDs, or other money market funds. GUSD reserves are held in accounts at FDIC-insured banks or money market funds holding short-term US T-bonds. Gemini is the only stablecoin issuer other than Paxos to be regulated by the NYDFS.

Fiat-Backed Stablecoins



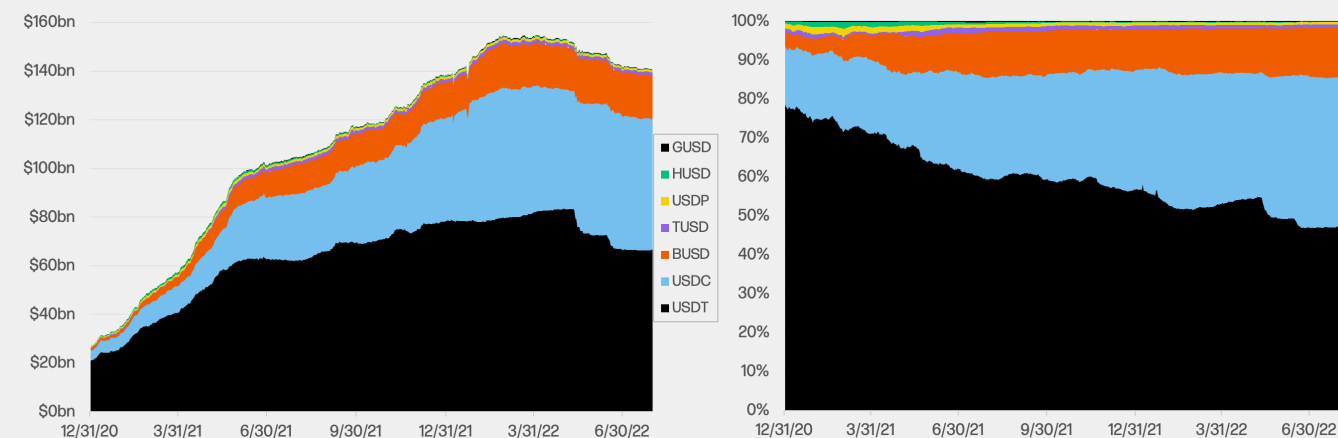
	 USDT	 USDC	 BUSD	 TUSD	 USDP	 GUSD
Name	Tether	USD Coin	Binance USD Coin	True USD	Pax Dollar (fka Paxos Standard)	Gemini Dollar
Mcap Tokens (\$bn)	\$65.9bn	\$54.5bn	\$17.9bn	\$1.2bn	\$871m	\$176m
Date Launch	2014	2018	2019	2018	2018	2018
Legal Entity	Tether Holdings Ltd	Centre Consortium LLC (governance) / Circle Internet Financial LLC (issuer)	Paxos Trust Company (issuer) / Binance (marketing)	Techteryx Ltd.	Paxos Trust Company	Gemini Trust Company, LLC
Legal Entity Location	British Virgin Islands	New York, NY	New York, NY	Shenzhen, China	New York, NY	New York, NY
Reserve Attestation	Yes	Yes	Yes	Yes	Yes	Yes
Auditor	MHA Cayman	Grant Thornton LLP	Withum	Armanino	Withum	BPM LLP
Reporting Frequency	Quarterly	Monthly	Monthly	"Live"	Monthly	Monthly
Native Integrations (# blockchains)	11	9	2	4	1	1
Native Integrations	Tron, Eth, Solana, Omni, Avalanche, Algo, EOS, Liquid, SLP, StateMine, Polygon	ETH, Solana, Avalanche, Tron, Algo, Stellar, Hedera, Flow, Cronos	ETH, BNB	ETH, BNB Chain, Avalanche, and Tron	ETH	ETH
Registrations	Money Services Business with FinCEN	USA: sale of checks and money transmitter licenses, UK: E-Money Issuer License	Trust charter from NY; token approved by NYDFS	Money Services Business with FinCEN	Trust charter from NY; token approved by NYDFS	Trust charter from NY
Custodian	Tether Ltd	BNY Mellon, NY Community Bank, Signature, Silvergate, US Bancorp, others	Paxos Trust Company	Signature Bank, Silvergate Bank, Prime Trust, First Digital Trust, and BitGo	Paxos Trust Company	State Street Bank
Min. Redeem Amt	\$100k	\$100	\$60k for individuals; \$500k institutions	\$10k	n/a	n/a

Source: company websites, CoinGecko (Mcap data as of 7/31/22)



Fiat-backed Stablecoins – Market Cap and % Share

Source: Galaxy Digital Research



Data: DeFi Llama

Competitive Dynamics

All stablecoins mentioned thus far in this report are currently issued by for-profit private businesses. Each seeks to drive adoption of their stablecoin, though they may prioritize different uses of the stablecoin which impact their competitive dynamics. Fiat-backed stablecoin issuers also look to drive adoption of their stablecoin through different use cases including banking integrations for on- and off- ramps, payments, usage on trading venues, availability in DeFi platforms, etc.

Fiat-backed stablecoins compete on trust and regulation (most stablecoin users never interact with the issuance/redemption processes). That means that they typically market themselves based on the quality of their reserves (many committed to 100% cash & cash equivalent backings) along with frequent reserve attestations. Having third-party confirmations from trusted partners also goes a long way in establishing trust for stablecoin issuers. The direct customers of stablecoin issuers are often segmented by geography, with on-shore issuers (e.g. Circle, Paxos, Gemini) servicing US customers and off-shore issuers (e.g. Tether) finding more adoption with global customers, including most based in Asia.

The primary competitive factors that fiat-backed stablecoin issuers compete on:

- **Reserve composition and transparency.** Token holders of stablecoins are taking on counterparty risk through the issuers so to properly assess that risk, they require auditability or sufficient details on the types and amount of assets held in reserves. Safer reserve profiles, strong collateral management practices, more frequent updates, and greater detail of reporting will likely win over customers that prioritize safety over ancillary product offerings such as yield.

- **Distribution architecture.** Stablecoin issuers work closely with bank partners, custodians, and exchanges for distribution. The licenses obtained by the issuers impacts the jurisdictions that they operate and who they can do business with. These licenses often have restrictions on the composition of reserves and the types of assets permitted to be held in backed reserves.
- **Other product offerings.** They may offer customers ancillary products and offerings that may influence the adoption and utility of their stablecoin including banking integrations, payment services, yield, blockchain integrations, etc.

Fiat-backed Stablecoin Issuers – Interest Income

Fiat-backed stablecoin issuers have a similar business model to traditional commercial banks, where the primary source of revenue comes from net interest—the difference between interest income earned on deposits less interest expenses—making deposit growth the core objective. In their current form, however, no fiat-backed stablecoin issuers pays any interest to depositors, enabling them to generate significantly higher margins than traditional banks. Rising interest rates also benefit the issuers substantially. For a stablecoin with \$1bn in deposits, each 25 bps increase results in \$2.5m in incremental interest income.

The income generating potential on deposits varies significantly depending on the composition of reserves and the portfolio duration, which is largely dictated by competition with other stablecoin issuers and proactive compliance with expected upcoming regulatory guidance. Between the different stablecoin issuers, the balance between assets and cash requirement will be



	USDC Reserve Assets (June 2022)			Paxos - BUSD Reserve Assets (June 2022)		
	Market Value	% Total	Duration (est)	Market Value	% Total	Duration (est)
T-bills	\$42,122,235,732	76%	57.7 days	\$10,597,042,200	60%	42 days
Reverse Repo	\$-	0%	1 day	\$6,292,771,150	36%	1 day
Cash Deposits	\$13,581,264,959	24%	1 day	\$738,064,449	4%	1 day
Total Net Assets	\$55,703,500,691	100%		\$17,627,877,799	32%	
Token Duration	57.7 days (estimated)			27 days (reported)		
Portfolio Duration	43.9 days (reported)			25.6 days (estimated)		

Source: Circle + Paxos Reserve Breakdowns - June 2022

Ann Interest Income Estimates @\$55bn	
76% Tbills @ 2.36%	\$994,084,763
60% Tbills @ 2.17%	\$726,652,640
Difference	\$267,432,123

the primary determinant of the differences in revenue potential. Paxos + Gemini (BUSD, USDP, GUSD) generally have the most conservative reserve composition, as they are overseen by the relatively stringent NYDFS, while Circle (USDC) has slightly more operating flexibility. On June 30, 2022, T-bills represented 60% of BUSD's reserves and had an average duration of 42 days vs. 76% for USDC at an average duration of 58 days (our duration estimates). These differences in duration and portfolio mix can have a meaningful impact on interest income.

Using this framework, we can make some assumptions about issuer revenue. If we conservatively assume that returns on cash deposits are negligible and that Circle is earning roughly the current 8-week T-bill coupon equivalent rate of 2.36% based on its token duration, then Circle would generate ~\$1bn in annual interest income. However, if USDC had a reserve composition that had the duration and asset mix of Paxos, then Circle would only earn ~\$725m in annual interest income, ~\$275m (or 27.5%) less (holding portfolio size constant and assuming negligible returns on cash and reverse repos, as well as a ~20 bps difference in coupon equivalent rates based on token durations). If expected future regulation for stablecoin issuers requires each to follow similar reserve practices, then the gap in interest income potential would narrow significantly (more on regulatory discussion on p. xx).

Financial Analysis of Fiat-backed Stablecoins

Peg Stability

Based on the daily closing price (UTC), USDT has had the highest count of daily closing prices between \$0.9975-\$1.0025 of our sample of fiat-backed stablecoins with 398 days (7 more days than USDC) since January 1, 2021. USDT daily closing prices also had the lowest standard deviation compared to its competitors (\$0.0024 vs \$0.0027 for USDC).

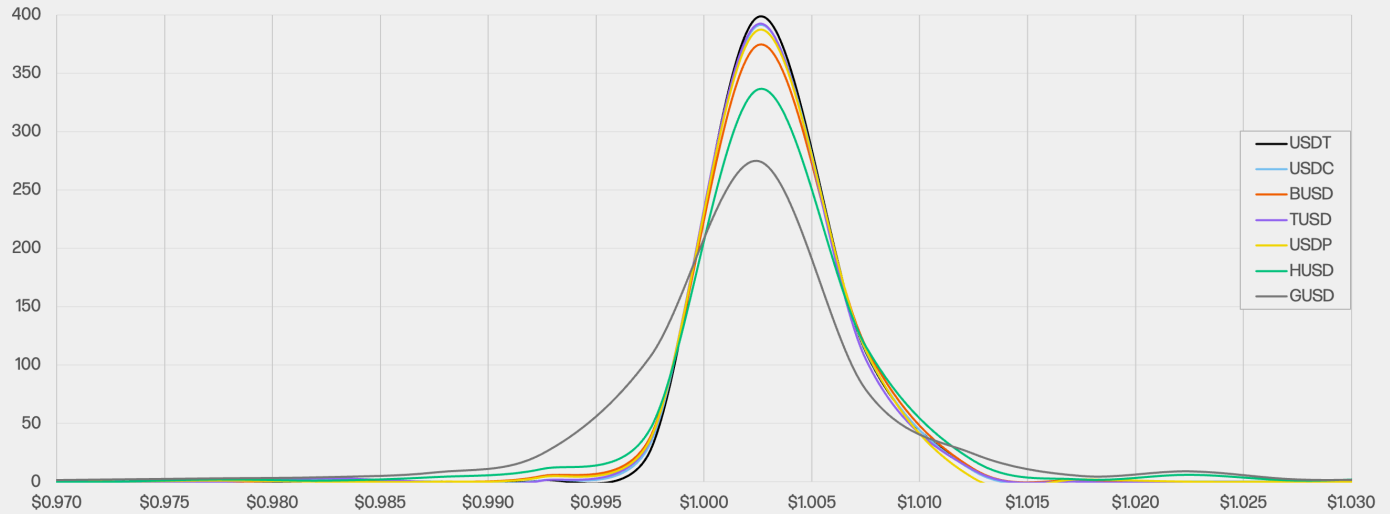
When looking at the daily low prices across the same sample and time range, USDT's daily low trading level averaged \$0.9994 - the closest to \$1 out of its group. However, USDT also saw 3 days where its price traded below \$0.995 including 1 day where its price fell below \$0.95 (May 12, 2022). Only Gemini Dollar had traded below that level in this sample. By frequency of days, BUSD had performed the best with 0 days that its price traded below \$0.995, followed by USDC with just 1 day below that level.

USDT had the most frequent number of days that its trading price stayed near \$1 (based on daily low prices), but **in terms of downside protection, BUSD has been the best performing fiat-backed stablecoin, followed closely by USDC.**



Fiat-backed Stablecoins: # Days Daily Close Price Ended Within Each Range (1/1/21-6/30/22)

Source: Galaxy Digital Research



Data: CoinGecko

Downside Price Performance of Fiat-backed Stablecoins



Days daily low price traded at or below (1/1/21-6/30/22)	USDT	USDC	BUSD	TUSD	USDP	HUSD	GUSD
\$0.925	0	0	0	0	0	0	2
\$0.930	0	0	0	0	0	0	1
\$0.935	0	0	0	0	0	0	0
\$0.940	0	0	0	0	0	0	0
\$0.945	0	0	0	0	0	0	1
\$0.950	1	0	0	0	0	0	1
\$0.955	0	0	0	0	0	0	2
\$0.960	0	0	0	0	0	0	4
\$0.965	0	0	0	0	0	0	8
\$0.970	0	1	0	0	0	0	9
\$0.975	0	0	0	0	0	2	11
\$0.980	0	0	0	1	1	2	19
\$0.985	0	0	0	0	0	2	40
\$0.990	0	1	0	0	2	21	77
\$0.995	2	0	0	3	49	90	235
>\$0.995	543	545	546	542	494	492	136
Total Days	546	546	546	546	546	546	546
Average Daily Low Price	\$0.9994	\$0.9993	\$0.9990	\$0.9988	\$0.9976	\$0.9963	\$0.9897
Standard Deviation	\$0.0023	\$0.00078	\$0.00075	\$0.012	\$0.0021	\$0.0034	\$0.0103

Source: CoinMarketCap

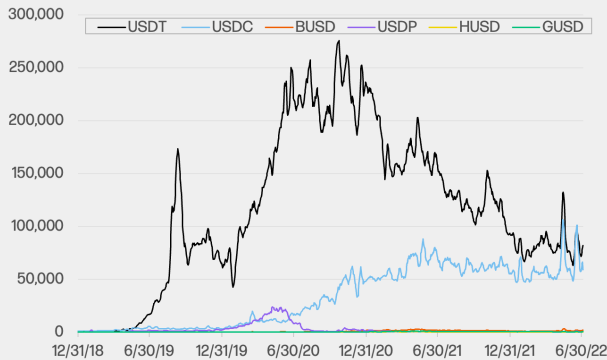


Usage

Note: the data shown in this section is for transfers on Ethereum only. It does not include USDT usage on Tron or BUSD usage on BNB Chain (both of which have higher activity levels than they do on Ethereum).

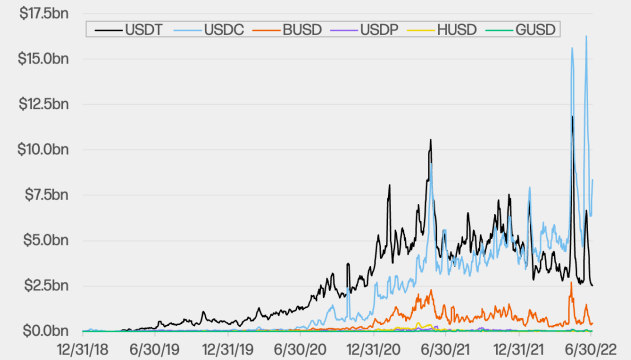
Fiat-backed Stablecoins - Daily Xfer Count (7d-MA) on Ethereum

Source: Galaxy Digital Research



Fiat-backed Stablecoins - Daily Xfer Value Adj (7d-MA) on Ethereum

Source: Galaxy Digital Research

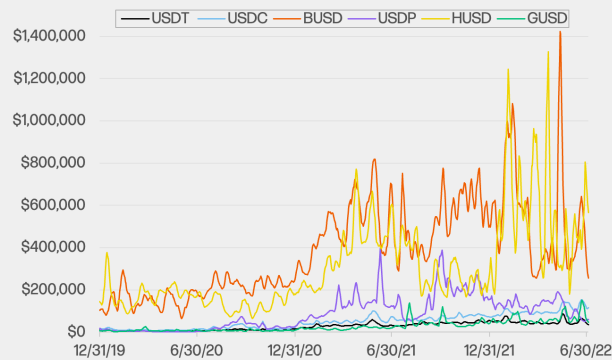


USDT and USDC have averaged over 60k transfers daily during 1H22, both considerably higher than their fiat-backed counterparts. Like their market cap dynamics, USDT's once-commanding lead over USDC has diminished considerably over time.

USDC's total transfer value on Ethereum has surpassed USDT's so far over 1H22, totaling \$1.14T compared to \$746bn for USDT. The next closest in total transfer volume on Ethereum is BUSD with \$123bn, ~12% of the volume of USDC despite it having roughly 2% of the transaction count.

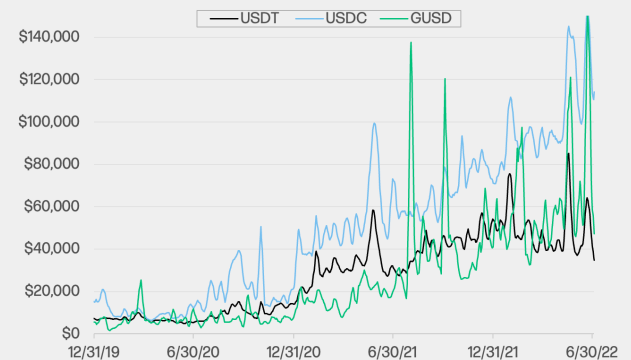
Fiat-backed Stablecoins - Daily Xfer Value / Tx (7d-MA)

Source: Galaxy Digital Research



Select Fiat-backed Stablecoins - Daily Xfer Value / Tx (7d-MA)

Source: Galaxy Digital Research





BUSD and HUSD transfers on Ethereum have the highest value of the group, averaging over \$500k per transaction during 1H22. This compares to \$106k for USDC and \$50k for USDT. In terms of median transfer value, HUSD leads at \$250k whereas the median transaction size of BUSD is closer to \$1k – in-line with the median of USDT and USDC. This reflects HUSD’s usage primarily in inter-exchange settlements and B2B applications, whereas the other fiat-backed stablecoins have a larger mix of retail usage, especially for DeFi activity.

Usage statistics of fiat-backed stablecoins



	Total Xfer Cnt (in 000s)				Total Xfer'd Value Adj (\$m)				Avg Xfer Size (\$)			
	2019	2020	2021	2022-YTD	2019	2020	2021	2022-YTD	2019	2020	2021	2022-YTD
USDT	14,768	66,087	54,089	14,920	\$104,672	\$596,743	\$1,938,175	\$745,767	\$7,088	\$9,030	\$35,833	\$49,985
USDC	1,083	8,339	22,662	10,806	\$16,516	\$160,429	\$1,395,833	\$1,141,951	\$15,248	\$19,238	\$61,594	\$105,676
BUSD	6	178	665	234	\$630	\$37,132	\$348,333	\$122,890	\$113,353	\$208,293	\$524,192	\$524,142
USDP	388	2,589	254	60	\$8,708	\$14,064	\$32,097	\$6,767	\$22,424	\$5,432	\$126,308	\$111,947
HUSD	5	52	99	6	\$885	\$7,831	\$36,940	\$3,604	\$179,036	\$152,007	\$372,282	\$555,202
GUSD	59	51	261	89	\$509	\$360	\$7,807	\$5,617	\$8,684	\$7,103	\$29,893	\$63,394

	Total Xfer'd by Contract Calls (\$000s)				Total Xfer'd Value - % from Contract Calls			
	2019	2020	2021	2022-YTD	2019	2020	2021	2022-YTD
USDT	\$3,102	\$112,724	\$541,817	\$247,380	3%	19%	28%	33%
USDC	\$2,684	\$113,503	\$914,494	\$725,123	16%	71%	66%	63%
BUSD	\$0	\$1,749	\$36,245	\$16,616	0%	5%	10%	14%
USDP	\$186	\$1,359	\$12,930	\$2,073	2%	10%	40%	31%
HUSD	\$0	\$63	\$3,961	\$31	0%	1%	11%	1%
GUSD	\$57	\$334	\$7,230	\$5,373	11%	93%	93%	96%

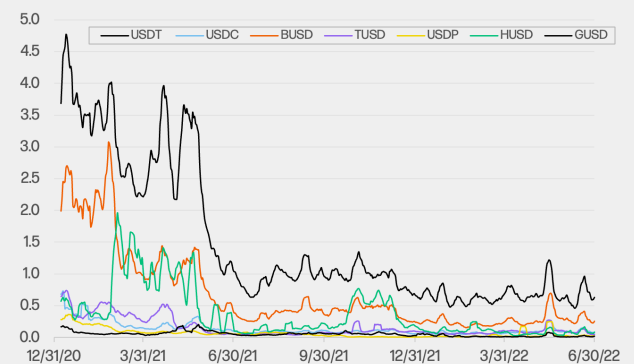
Source: Coin Metrics

Velocity: The velocity of money measures the rate at which money is transacted over a given period of time. We calculate velocity as the 7-day moving average of daily trading volume / supply.

USDT has the highest velocity of the group by a large amount, though its velocity has decreased considerably since May 2021 after China initiated its ban on crypto. For 1H22, the velocity of USDT averaged 0.66–2.5x more than the next closest stablecoin (BUSD @ 0.26). USDC velocity YTD has averaged 0.09 – approximately 1/8th the velocity of USDT, suggesting USDC is used much less as a base currency for active trading.

Fiat-backed Stablecoins - Velocity (7d-MA)

Source: Galaxy Digital Research



Data: CoinGecko



Primary Risks of Fiat-backed Stablecoins

The primary risks associated with fiat-backed stablecoins include run-risk or redeemability of the stablecoin—primarily a function of the composition of reserves—and regulatory uncertainty as a comprehensive regulatory framework has yet to be enacted, which may significantly impact the operations of existing stablecoin issuers. With regards to the rest of the crypto economy, fiat-backed stablecoins are criticized for being custodial (reserves are custodied by the issuer or a trust) and centralization risk (single point of failure, ability to make decisions unilaterally). In addition, due to the lack of transparency around reserve holdings, the demand for specific fiat-backed stablecoins may be influenced by speculation around the quality of collateral (includes credit risk, liquidity risk, rate risk, etc.).

Freezing funds

Fiat-backed stablecoin issuers are subject to compliance with legal obligations regarding KYC/AML and transaction monitoring activities. To remain compliant with these laws, fiat-backed stablecoin issuers may maintain the administrative ability to “freeze” their stablecoins—or prevent a particular address from interacting with their stablecoin—by maintaining a blacklist of these blocked addresses.

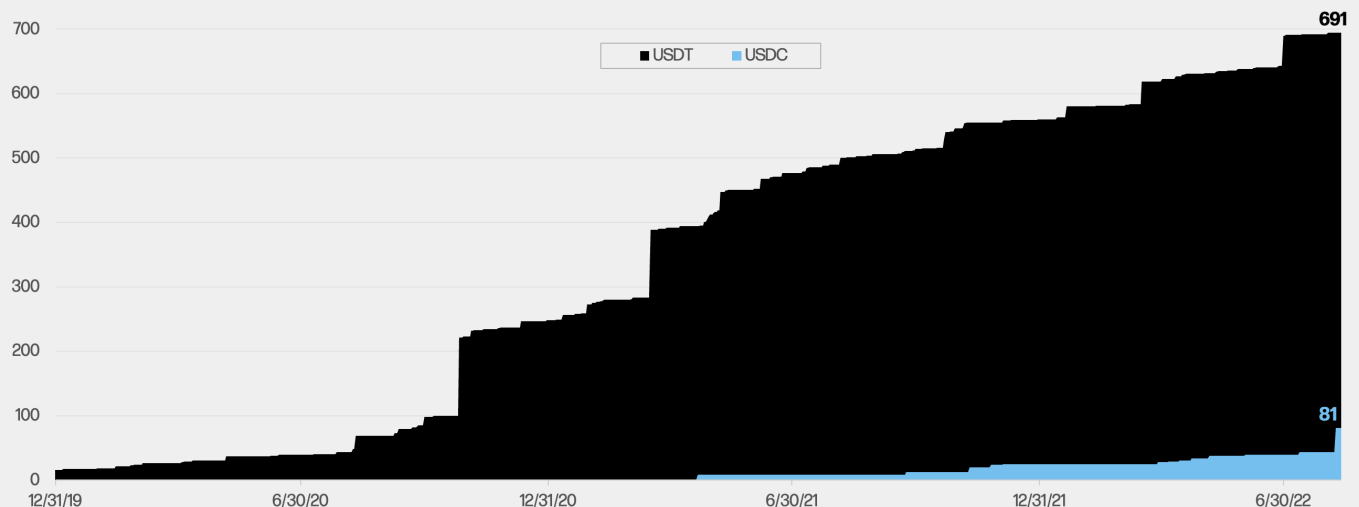
For USDT and USDC, the blacklists are managed by Tether and the Centre consortium (not the individual issuing members), but addresses are typically added at the request of law enforcement. When a transfer function on USDT or USDC is called, the token smart contract queries an off-chain blacklist to ensure that neither the sending nor receiving address is present. If the address

appears on the blacklist, the transaction is blocked. While this authority may not grant the ability to blacklist individual tokens or to seize the tokens from a particular address, it enables the ability to essentially render the tokens useless for blacklisted addresses. This capability is certainly useful for several occasions as we have seen following the Poly Network \$611m exploit in August 2021 when Tether [froze](#) \$33m in USDT on Ethereum before the exploiter was able to transfer the stolen funds. It serves AML and CFT purposes well by restricting sanctioned addresses from redeeming to fiat where illicit funds may be more difficult to trace. In addition, it also may also comfort users knowing that there may be a recovery mechanism in place if sending tokens to the wrong address – once transactions are finalized on-chain, they are typically irreversible, but Tether can recover the funds by freezing the wrongly-sent USDT to then be re-issued to the original sender in certain cases.

As of 7/31/22, Tether has blacklisted a total of 691 addresses on Ethereum – 50 of which were added since 6/30 (does not include banned addresses on other networks). Collectively, there is over \$400m USDT frozen, averaging ~\$580k/wallet and equating to 0.6% of circulating supply. Compared to USDC, there are significantly fewer blacklisted USDC addresses on Ethereum, totaling just 43 as of 7/31/22. “Access denied tokens” totaled 4.0m USDC, averaging ~90k/address per address and equating to 0.007% of total USDC supply. [8/9/22 update: Following Treasury mandated sanctions against Tornado Cash, the Centre consortium blacklisted the 38 related addresses (collectively holding \$149k), bringing its total up to 81. Although complying with the Treasury’s orders, Circle shared in a [blog post](#) that it disagreed with the unprecedented sanctioning against an open-source protocol and would be challenging the logic of the order. For further details, read more about the Tornado Cash update in our [research note](#).]

USDC vs. USDT – Banned Addresses on Ethereum

Source: Galaxy Digital Research



Data: USDC Attestation Reports, Dune



Following UST's collapse in May, Circle [communicated](#) that all of the unique assets blocked to date have been at the direction of law enforcement to comply with OFAC sanctions and court orders, adding that "blocking is never done unilaterally or arbitrarily and follows the highest duty of care." However, this statement is somewhat misleading (perhaps implying Circle doesn't have the unilateral or arbitrary ability, but the Centre consortium does) as addresses can also be blacklisted for protection of user funds or for suspicion that the stablecoin may be associated with illegal activity. In these instances, Tether and Centre technically do have sole discretion to block transactions by certain addresses outside of what law enforcement requires. Per Centre's [blacklisting policy](#), the consortium reserves the ability to add addresses to the blacklist "where Centre determines, in its sole discretion, that failure to grant a blacklisting request presents a threat to the security, integrity, or reliability of the USDC Network, including security breaches that compromise USDC privileged keys (e.g., minter private key) and result in unauthorized USDC being minted from such compromise."

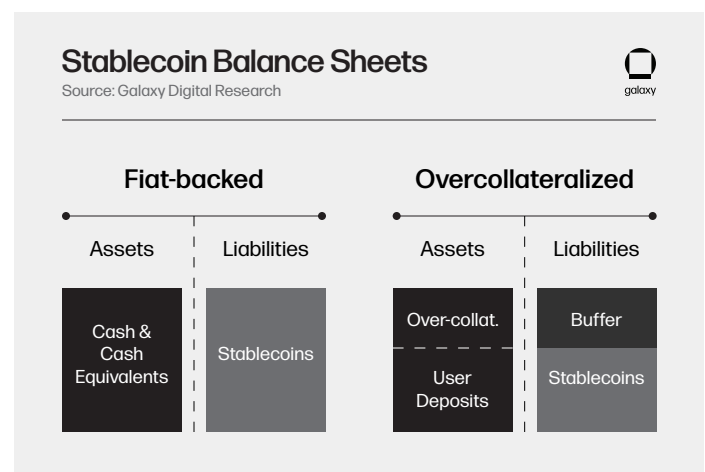
Still, this authority to block transactions reflects some of the limitations of fiat-backed stablecoins especially for on-chain activity like in DeFi applications. Users have little visibility into the decision-making that goes into blacklisting addresses, which contrasts with the (ideally) open, transparent governance processes in crypto networks that puts decision-making in the hands of the community. Fiat-backed token holders must trust that the centralized stablecoin issuers are acting virtuously. It's easy to see how having this blacklisting authority can be easily abused, especially in authoritarian regimes where crypto users stand to benefit the most. While the crypto networks and protocols may be permissionless to interact with, in the case of centralized fiat-backed stablecoins, the underlying assets used may not be. Indeed, this technology could also be used in the reverse—to restrict the transferability of fiat-backed stablecoins to any address that is not *whitelisted*. Were such a restriction to be imposed, it is likely that the majority of stablecoin activity would flow to more decentralized (and less regulated) stablecoin alternatives.

Overcollateralized Stablecoins

While fiat-backed stablecoins are collateralized by off-chain assets, overcollateralized stablecoins typically exist solely on-chain and are explicitly backed by crypto assets. Being entirely on-chain enables anyone to verify the composition of reserves backing the stablecoin, a level of transparency that no fiat-backed stablecoin issuer can offer. Overcollateralized stablecoins are powered by smart contracts and offer a more decentralized alternative to fiat-backed stablecoins, accepting deposits in crypto assets rather than dollars, and they require collateral deposits in excess of \$1 to serve as a buffer against price volatility in the underlying collateral. Given the nature of these types of systems, demand for overcollateralized stablecoins typically comes from demand for leverage as opposed to on- and off-ramps like for fiat-backed stablecoins.

Stability Mechanism of Overcollateralized Stablecoins

Issuance of overcollateralized stablecoins require users to deposit crypto assets (e.g., ETH) into a smart contract to serve as collateral against borrowed assets, which are typically in the form of stablecoins. The borrowed stablecoin is removed from circulation through user repayment, enabling depositors to retrieve their underlying collateral. The rates that borrowers pay and suppliers are paid can be set by variable interest rate models based on the amount of liquidity in the protocol and the utilization of each asset pool.



Like traditional bank balance sheets, users' deposited assets represent assets for lending protocols, while borrowed assets represent liabilities. Compared to fiat-backed stablecoins, where assets (user fiat-deposits that are typically in the form of cash & cash equivalents or Treasuries) are matched 1:1 with liabilities (issued stablecoins), overcollateralized stablecoins require a higher balance of assets than liabilities to provide a safety buffer to help the protocol maintain solvency.



In addition, when assessing the aggregate positions of lending protocols from the top down, it may appear that the entirety of user deposits is used to back the total liabilities, but in most of these systems individual loans are backed by their own collateral positions, meaning the protocol cannot use excess deposits from one user to collateralize certain positions of other users that may failed.

The amount that can be borrowed is set by the Loan to Value Ratio (LTV) or sometimes called the Collateral Ratio (CR), which is the inverse of LTV. Protocols with higher risk tolerance allow higher LTVs upwards of 90%—typically reserved for the safest collateral assets—while more conservative protocols may apply lower LTV of 50-80%. If the LTV falls below its permitted range, then no new borrowings may be taken out, or collateral may be automatically liquidated to cover any imbalance. These parameters, as well as the types of collateral that can be accepted, can be adjusted from time to time via protocol governance, which takes various forms.

Overcollateralized stablecoins also rely on liquidations to ensure the protocol remains fully collateralized. If the value of a depositor's collateral falls below the protocol's LTV threshold or collateralization ratio minimum, then the borrower's position may be liquidated—a process often automated by liquidation bots that involves selling the borrower's collateral deposit to pay off the outstanding debt owed. Many protocols even offer their own off-the-shelf bots to make it easier for users to initiate the liquidation process. Liquidators may be incentivized through a liquidation fee that enables them to purchase the collateral at a discount. Ideally the LTV or CR plus the liquidation fee would be large enough to encourage liquidations to properly function by covering all outstanding debt in a timely manner, though this may not always be the case as protocols can also accumulate bad debt.

While these risk parameters and stability mechanisms can be effective during stable market conditions, they have also faltered during periods of extreme volatility. As a result, these models continue to be enhanced and innovated upon through new mechanisms and features. Below, we compare three of the leading overcollateralized stablecoins: MakerDAO's DAI, Liquity's LUSD, and Abracadabra's Magic Internet Money (MIM).

MakerDAO (DAI)

MakerDAO was founded by Rune Christensen, who laid out the initial ideas for a "stable cryptocurrency" called eDollar in 2015 that drew inspiration from previous stablecoin iterations such as bitUSD and NuBits. The protocol's name, Maker, refers to the importance of needing "Market Makers" to have sufficient liquidity for the protocol to function. In December 2017, the Maker protocol launched DAI on the Ethereum blockchain. MakerDAO initially only accepted ETH as collateral to generate Single-Collateral DAI (now called "SAI") before the protocol was upgraded two years later to allow for multiple collateral asset types with the creation of Multi-Collateral DAI (DAI).

DAI is created and stabilized through Maker Vaults. Users use interfaces such as Oasis Borrow to deposit accepted collateral types and generate DAI. The specific risk parameters, including collateralization requirements and liquidation ratios per asset type, are determined through the Maker governance mechanism, in which MKR holders vote on changes.

Borrowers are charged a stability fee that represent interest on the loan and continuously accrues. Users must pay back the DAI borrowed as well as the stability fee to fully retrieve their deposits. When there is an oversupply of DAI, the stability fee can be increased to encourage borrowers to repay their loans and lessen the supply of DAI. Similarly, when there is excess demand for DAI, the stability fee can be decreased to incentivize borrowers to mint new DAI. Changes to the stability fee are also determined through the Maker governance mechanism.

Liquidations Process

The liquidation process plays an important role in maintaining the integrity of the Maker ecosystem. Protocol participants called *Keepers* are responsible for overseeing the liquidation of vaults that reach their liquidation ratio so that the protocol does not hold bad debt and become undercollateralized. In addition to receiving a liquidation fee, Keepers are incentivized to participate in liquidations through Collateral Auctions. In the first of two phases of Collateral Auctions, Keepers bid the maximum amount of DAI they are willing to pay for the vault's collateral. This first phase enables Keepers to bid less DAI than the amount of collateral outstanding to receive the collateral at a discount. In practice, however, these auctions are normally automated by bots and bid up until the DAI offered is equal to the collateral outstanding.

Once the amount of DAI that will be paid is set, the second phase of the auction begins. During this phase, Keepers bid the minimum amount of collateral they are willing to accept in exchange for the DAI. These two phases create competition between Keepers to try and ensure that the maximum amount of DAI is paid for the collateral. Assuming the underlying collateral does not drastically drop in value, the Keeper that wins a collateral auction is able to purchase the collateral at a discount since all vaults are overcollateralized.

In the case of extreme market conditions, MakerDAO also has an emergency shutdown feature enabling MKR holders to deposit a set amount of MKR in order to freeze the protocol and allow vault creators to recover any collateral not backing outstanding debt.

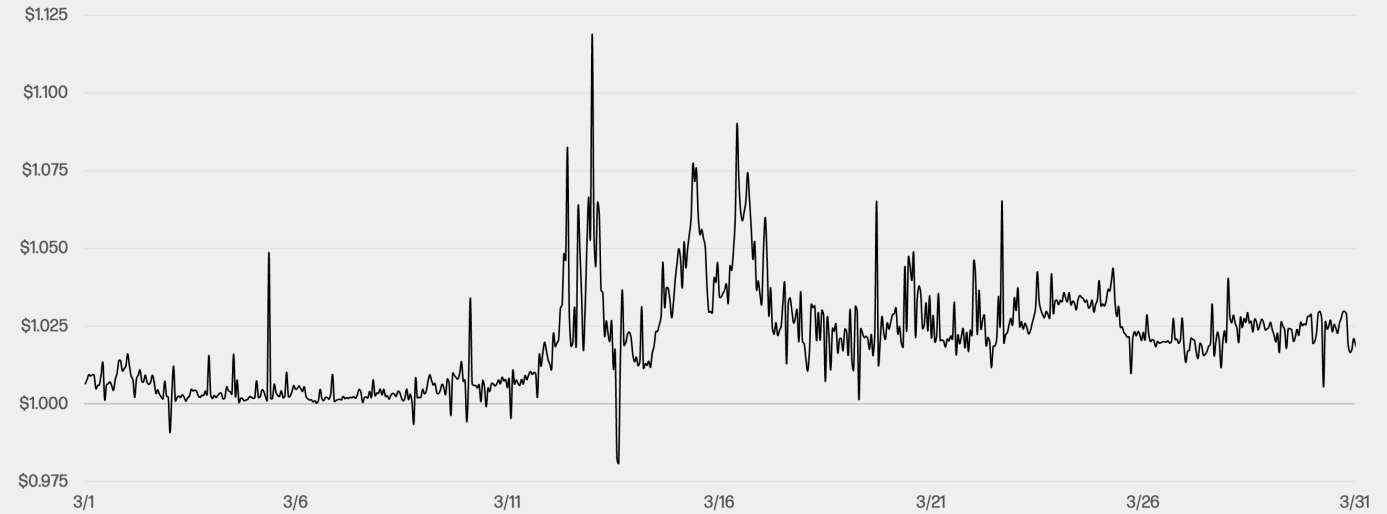
MakerDAO's Black Thursday

On Thursday, March 12, 2020, DAI lost its peg to the dollar in an event referred to as *Black Thursday*. Amidst a broader selloff in digital assets and other risk assets in response to the closing of the global economy in the early days of COVID-19, Ethereum dropped from \$193 to \$95 in less than 24 hours. This dramatic drop in price corresponded with a rapid rise in Ethereum gas fees, resulting in a breakdown in Maker's liquidation process. As users raced to pay back their loans to prevent from being liquidated, demand for DAI surged with the price reaching more than \$1.10 at its peak.



DAI - Price (March 2020)

Source: Galaxy Digital Research

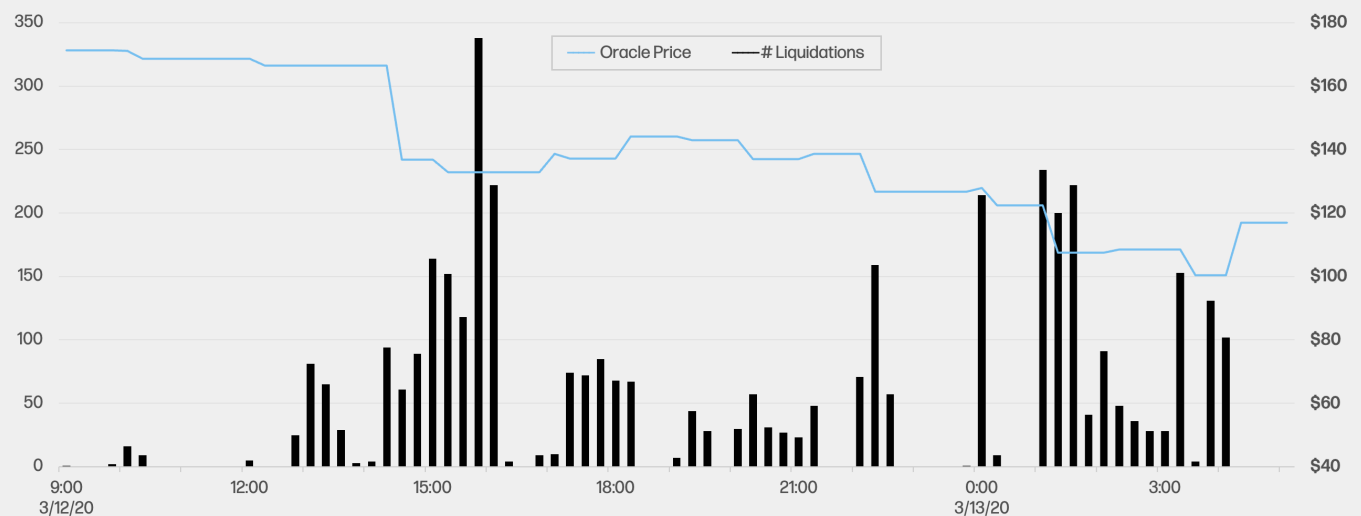


Data: AmberData

However, the rise in Ethereum gas fees and long transaction queues also prevented Maker price oracles from updating in a timely manner. By the time the oracles' transactions could go through, the price of Ethereum had dropped significantly, leading to the liquidations of several Maker vaults that saw LTVs fall below the liquidation threshold. Rather than pay the normal 13% liquidation penalty and lose a portion of their collateral, 320 vault owners lost 100% of their collateral.

DAI - Oracle Price vs. # Liquidations (March 12-13, 2020)

Source: Galaxy Digital Research



Data: @whiterabbit_hq



Compounding the issue, Keepers that normally would have participated in collateral auctions to pay back the debts were unable to get their transactions through without paying exorbitant gas fees. This enabled other bidders to step in with higher gas fees to bid on liquidated vaults with no competition. As a result, 36% of all vault liquidation auctions were won with zero bids. A single liquidator won 1,461 auctions and more than 62k ETH for close to zero DAI, resulting in 6.65m of unbacked DAI. To re-collateralize the protocol, the Maker community opted to print additional MKR governance tokens and auction them off for DAI (Maker calls this a debt auction).

Improvements to the protocol after Black Thursday

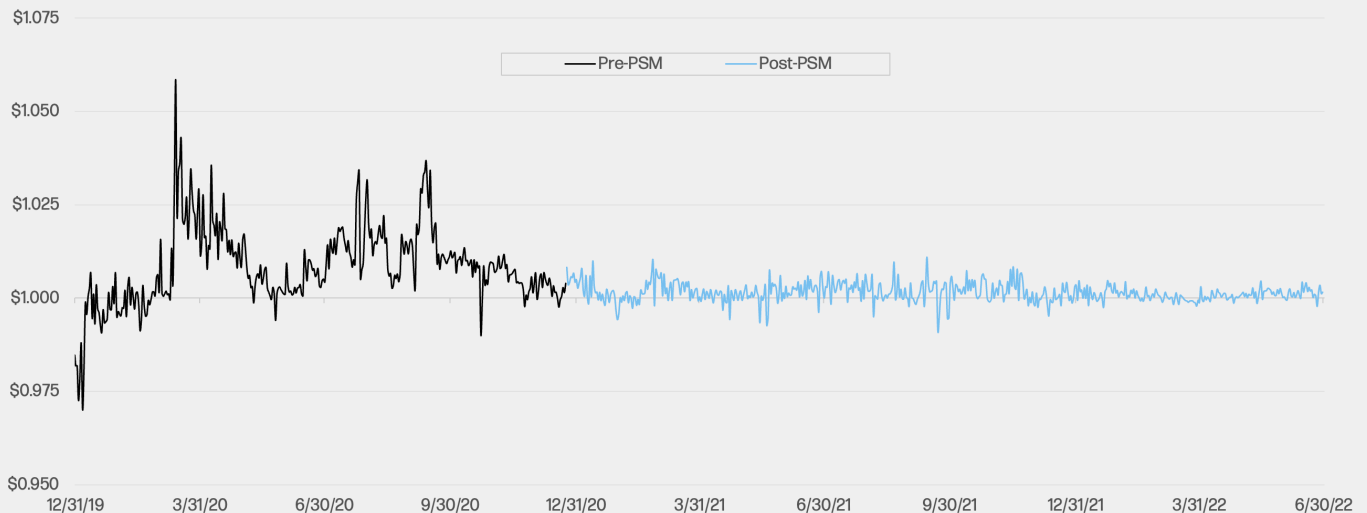
To prevent a similar event from re-occurring, Maker implemented several changes to the protocol. The most significant improvement introduced an arbitrage facility called the **Peg Stability Module (PSM)**, a DEX through Maker which enables users to mint new DAI against stablecoins (incl. USDC, USDP, or GUSD) at a 1:1 rate. The PSM enables users to instantly swap US-pegged stable coins for

DAI at a 1:1 rate (less a small fee). This mechanism has the benefit of enabling arbitrageurs to buy and sell DAI for a profit when the peg deviates from \$1 without needing to open a vault and overcollateralize a position. It also increases the amount of DAI in circulation that is backed 1:1 with other reliable stablecoins (as opposed to volatile cryptoassets). Since its introduction, the PSM has led to a significant reduction in DAI volatility, accounting for a 70 basis points decline in intra-day volatility.

Maker also implemented a **surplus buffer**, a pool of excess capital to ensure the protocol's ability to cover any accumulated bad debt. Once that buffer is met, any surplus DAI the protocol earns is auctioned to MKR holders. MKR tokens are then burned in exchange for the surplus DAI, simultaneously rewarding MKR holders by decreasing its outstanding supply. Other improvements following Black Thursday included the addition of USDC as an approved collateral and safeguards to prevent auctions with only single bidders from closing.

DAI - PSM Impact on DAI Price

Source: Galaxy Digital Research



Data: AmberData



Other key MakerDAO initiatives

- **DAI Direct Deposit Module (D3M):** In November 2021, Maker launched the D3M to expand DAI's presence outside of just Maker by providing DAI to other lending protocols. To date, D3M has only been implemented on Aave, but Maker has begun [exploring the possibility](#) of implementing D3Ms on Compound, TrueFi, and Maple Finance. Collateral deposits on Aave that are used to borrow DAI are indirectly used to maintain DAI's backing in the Maker Protocol. Maker benefits by earning additional income that's earned on the deposited DAI on these protocols and because DAI remains competitive with centralized stablecoins (e.g. USDT and USDC) through lower borrow rates. Following a collapse in the stETH-Eth peg in June, MakerDAO voted to [temporarily suspend](#) its Aave D3M initiative as \$100m in DAI had been borrowed using stETH as collateral.
- **Multi-Chain:** Maker has also begun to enable DAI's use on other Ethereum Layer 2 protocols. To date, DAI token bridges have been deployed for Optimism, Arbitrum, and Starknet. Maker's multi-chain strategy is aimed at growing DAI's overall capture of the stablecoin market-share by enabling users on L2s to seamlessly use DAI.
- **Real World Assets (RWA) Initiative:** In 2021, Maker began accepting RWA—or off-chain assets—as collateral to borrow DAI. The primary motivation of the RWA initiative is to build integrations between DeFi and TradFi to help scale DAI and improve the reserve composition of Maker with longer duration

assets. They require complex legal agreements that are subject to regulation, the use of third parties that introduce counterparty risk, and extensive due diligence that cannot completely mitigate factors like credit and liquidity risk. A secured deal with [Centrifuge](#), for example, enables RWAs to be securitized as NFTs to then used as collateral against DAI borrowings. Other deals have been with companies including [Tesla](#) and banks [Huntingdon Valley Bank](#) and [Societe Generale](#).

Reserve Composition

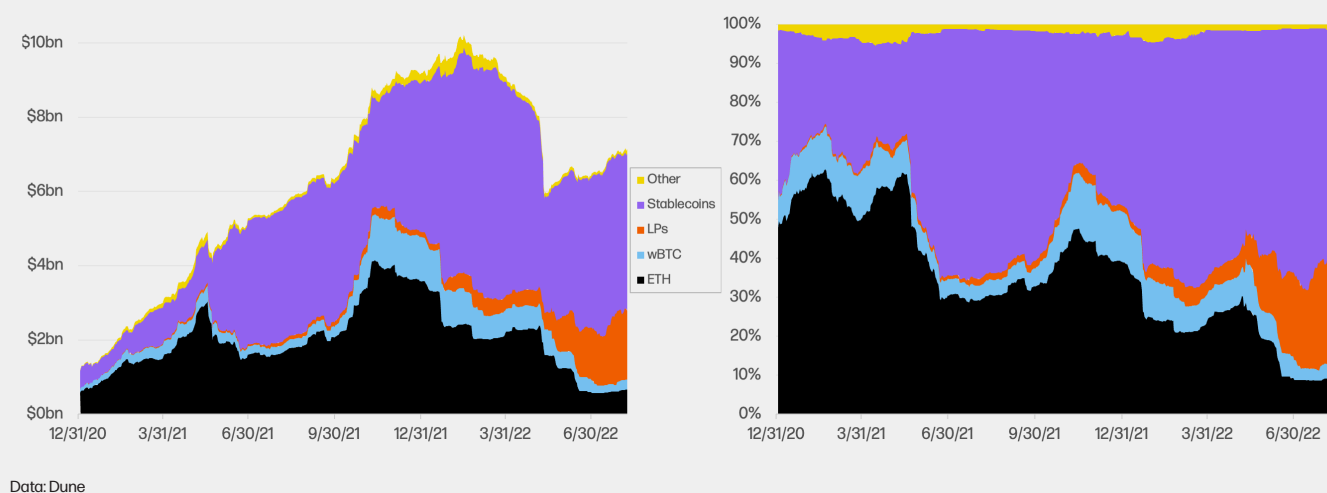
As of July 31, 2022, MakerDAO had 7.5bn DAI in circulation with \$10.4bn in TVL, representing a collateralization ratio of ~140% and having a debt ceiling of 9.3bn DAI - meaning an additional 1.8bn DAI could be minted across all vaults based on the prevailing risk parameters.

Over time, Maker's reserve composition has shifted from only ETH to acceptance of a variety of assets including wBTC, UNI, LINK, YFI, MANA, MATIC, and even UNI LP tokens (i.e. DAI/USDC LP). Through stablecoin vaults and the PSM, Maker also accepts USDC, USDP, and GUSD.

According to [DaiStats](#), as of July 31, USDC directly accounted for 50% of total DAI collateral, though this figure may be understated though given USDC is also present in several LPs such as Uniswap DAI-USDC LPs. When taking these into account, USDC either directly or indirectly backs ~65% of DAI.

MakerDAO – Assets by Type and % Share

Source: Galaxy Digital Research





Criticisms of DAI

While the PSM has succeeded in strengthening DAI's peg and reducing its volatility, it has faced some criticisms for leading to DAI's outsized backing by USDC and fiat-backed stablecoins. Since the introduction of the PSM, DAI's collateral mix has increasingly shifted to centralized stablecoins. The risks of the centralized stablecoins as it relates to freezing assets or potential censorship are extended to DAI with Maker's acceptance of centralized stablecoins as collateral deposits. Some critics argue that MakerDAO and DAI are facing an existential risk posed by the PSM and USDC – if regulators potentially demand significantly increased blacklisting or freezing of USDC, or if they force an actual whitelist that inhibits free transferability of USDC, then the majority of DAI's backing would be unavailable to cover Maker's liabilities, leading the system to become insolvent. Said another way, MakerDAO was created to function as a decentralized stablecoin system, and relying on centrally-issued assets for collateral undermines the system's stated purpose and core value proposition.

Other Overcollateralized Stablecoins

Liquity (LUSD)

Liquity is a decentralized borrowing protocol that enables users to take **interest-free loans** denominated in its stablecoin LUSD using ETH as collateral. By removing a variable interest rate, users have more certainty over their future borrowing costs. Liquity compensates for a lack of an interest rate by charging dynamic borrowing and redemption fees ranging from 0.5% to 5% depending on the rate of issuance/redemptions during a given time period. These dynamic fees influence the level of borrowing activity. The one-time fee model can be beneficial for long-term borrowing as the fee is amortized over time, but it can be less-than-ideal for extremely short-term loans. Liquity's founder has previously stated that LUSD is “not optimized for maintaining absolute price stability. Its main purpose is to offer sufficient stability to borrowers while serving as a base currency in other DeFi applications.” Instead, the protocol focuses on enhancing user's ability to set their own risk parameters without having to abide by a broader protocol monetary policy (i.e. DAI's stability fee).

Liquity relies upon the Stability Pool to ensure the protocol remains solvent. The Stability Pool takes LUSD deposits to repay undercollateralized debts, acting as the first line of defense for maintaining system solvency. When a trove, or a vault, is liquidated, LUSD is burned from the stability pool to repay the debt, then the entire ETH collateral from the trove is transferred to the Stability Pool to be split among pool depositors. In effect, Stability Pool depositors lose a portion of their LUSD deposits in exchange for a pro-rata share of the liquidated ETH collateral. Because collateral pools are liquidated just below 110%, stability pool depositors should receive more collateral (in \$ value) than the portion of their LUSD burned.

The stability pool enables any depositor to assume some of the credit risk typically borne by the protocol from trove owners that take out LUSD loans. Stability pool depositors also directly benefit from liquidations across the protocol – rewards that typically would go entirely to liquidation bots on other protocols. These rewards can be especially rewarding during steep market selloffs when multiple troves are liquidated. Trove owners may also assume default risk even if their individual trove is far from liquidation – in the event the stability pool runs out of funds, then the protocol will utilize a secondary liquidation mechanism that redistributes the debt and collateral from liquidated troves to all other troves.

Magic Internet Money (MIM)

Abracadabra.money is a cross-chain DeFi lending protocol founded by Daniele Sestagalli. Abracadabra uses Sushi's Kashi Lending Technology to enable users to borrow stablecoin Magic Internet Money (MIM) against interest-bearing tokens issued by third-party protocols, such as tokens representing deposits into Yearn Finance or Curve. Interest-bearing tokens allow the value of the underlying collateral in the protocol to continue to increase over time as they earn yield.

Abracadabra.money provides borrowers with a user-friendly interface to isolated lending markets, charging a fixed interest rate and displaying the liquidation price of their collateral deposits. Abracadabra.money supports leveraged yield farming strategies for its borrowers, including features such as a built-in leverage option which utilizes flash loans to replicate the repetitive process of using borrowed funds as deposits to enable more borrowings – all in one easy step for users. Abracadabra also accepts non-interest-bearing collateral to be used in automated yield-enhancing strategies through Degenbox. As the name indicates, the strategy was especially attractive to *degen yield farmers* looking to earn yield by leveraging their UST. It attracted significant liquidity, but also increased the protocol's exposure to risk.

During the collapse of UST, the price of MIM fell as low as \$0.91 as the rapid drop of UST prevented the protocol from liquidating UST collateral fast enough, leading to an accumulation of \$12m in bad debt. MIM had also previously lost its peg in January 2022 after it was revealed that Daniele Sestagalli was working with Michael Patryn, founder of fraudulent Canadian exchange Quadriga CX, on another DeFi project Wonderland. This news concerned MIM holders and led many to exit their positions, including Alameda Research, which withdrew more than \$500m worth of MIM from a Curve pool. The sudden withdraw of liquidity led MIM to drop to \$0.97 for several days in May before it eventually returned to \$1.



Overcollateralized Stablecoins (data as of 6/30/22)



	 Dai	 Magic Internet Money	 Liquidity USD	 Alchemix USD	 sUSD
Stablecoin	DAI	MIM	LUSD	alUSD	sUSD
Stablecoin Market Cap	\$7.0bn	\$229m	\$178m	\$186m	\$198m
Launch Date	Dec-17	Oct-21	Apr-21	Mar-21	Jul-18
Borrow/Lend Platform	MakerDAO	Abracadabra	Liquity	Alchemix	Synthetix
Governance Token	MKR	SPELL	LQTY (non-gov)	ALCX	SNX
Governance Token Market Cap	\$1.0bn	\$93m	\$73m	\$55m	\$839m
Collateral Accepted	ETH, stables, wBTC, LPs	Interest bearing tokens (ibTKNs)	ETH	DAI, USDC, USDT	SNX
Available Networks	Eth, Starknet, Optimism, Arbitrum	ETH, BSC, Ftm, Avax, Matic, Arb	Ethereum	Ethereum	Ethereum, Optimism
Reserves Size or TVL	\$10.5bn	\$369m*	\$563m	\$133m	\$m
Reserves - % ETH	9%	20%*	100%	alETH is separate from alUSD	0%
Reserves - % stables	84%	19%*	0%	100%	0%
Collateral Ratio	139%	154%*	328%	304%	499%
Liquidation Mechanism	Auctions (liquidation bots)	Auctions (liquidation bots)	Stability Pool	Self-Liquidations	Liquidation bots, self-liquidations
Peg Mechanisms	PSM/Stability Fee/ Arbitrage (anyone)	Arbitrage (debt holders)	Redemptions + Arbitrage (anyone)	Transmuter (PSM), Elixir (AMO)	Arbitrage (stakers)
Oracle	Oracle Security Module (OSM) using whitelisted feed providers	Multiple oracles for different assets	Chainlink + Tellor Oracles	Chainlink	Chainlink

Source: Protocol websites, Dune, third-party dashboards, Coingecko, etc. Note: Reserve and Collateral metrics for MIM are as of 6/30/22.

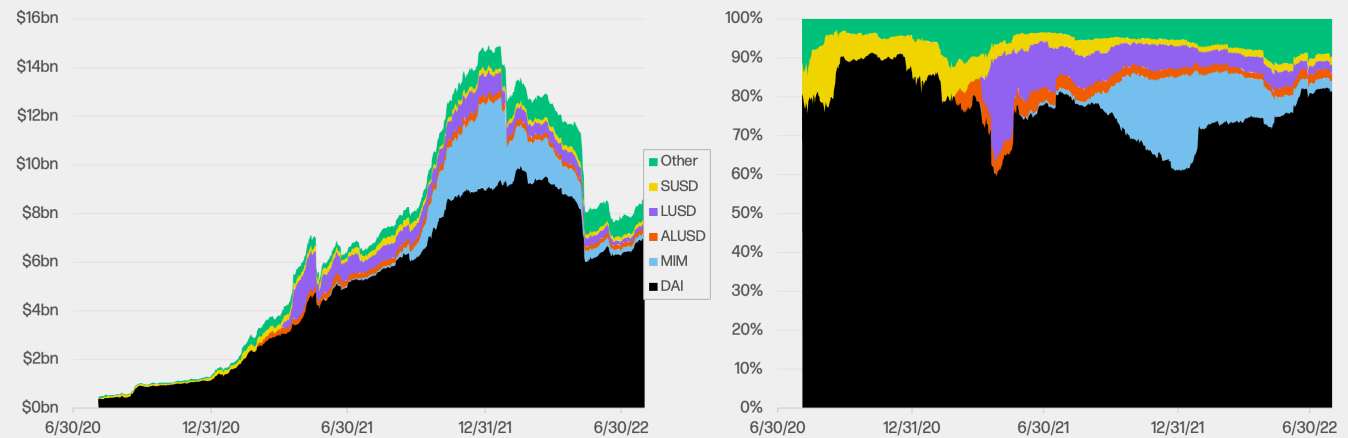
Others

- alUSD (Alchemix).** Launched in February 2021, Alchemix is a lending protocol that offers its borrowers self-repaying loans that are paid down over time. Asset deposits on Alchemix are then deposited in Yearn vaults and the total accumulated yield can be harvested periodically to proportionally pay down depositors' loans (with 10% of generated yield going to Alchemix as a service fee). Borrowers take out loans in the form of synthetic tokens (alAssets) such as alUSD, which can be minted against DAI, USDC, and USDT deposits. alUSD loans require a 200% collateralization ratio on stablecoins (i.e. max LTV ratio of 50%). The protocol targets a minimum 0.998 ratio for alUSD and alETH pegs, which is maintained through Alchemix Transmuter, a backstop for the peg (similar to Maker's PSM) that enables alUSD deposits to be converted to DAI.
- sUSD (Synthetix).** Built on Ethereum and Optimism, the optimistic rollup layer 2 built on Ethereum, Synthetix is a derivatives platform that enables the issuance of synthetic assets, including its dollar-based stablecoin Synthetix USD (sUSD). Borrowers can mint sUSD or other "synths" by staking Synthetix's SNX token as collateral. Synths are backed by a 400% collateralization ratio (borrowers will be unable to claim rewards on staked assets if the collateralization ratio falls below 400%). If the collateralization ratio falls below 200%, the accounts are flagged for liquidation. Synthetix has a liquidation timer of 72 hours to permit borrowers to improve their positions back above 400% before liquidations are initiated.



Overcollateralized Stablecoins – Market Cap and % Share

Source: Galaxy Digital Research



Data: DeFi Llama

Competitive Dynamics of Overcollateralized Stablecoins

So far, overcollateralized stablecoins have failed to see the same level of adoption or competition seen among fiat-backed stablecoins. Maker is currently the most popular DeFi protocol as ranked by TVL, but it has faced heavy competition from other long-standing borrow/lend platforms including Aave and Compound. Up until now, Maker has been the only one in that group to launch its own stablecoin, but that may soon change following a new [governance proposal](#) in July for Aave to launch its own stablecoin, GHO. And, to date, no decentralized over-collateralized stablecoin has seriously challenged Maker's dominance on that product.

Compared to fiat-backed stablecoins, which have much less flexibility to differentiate themselves, overcollateralized stablecoins compete not just on price stability and liquidity, but also on specific features of the stablecoin asset, including yield, rates, accepted collateral types, and the entire user experience of the borrow/lend platform.

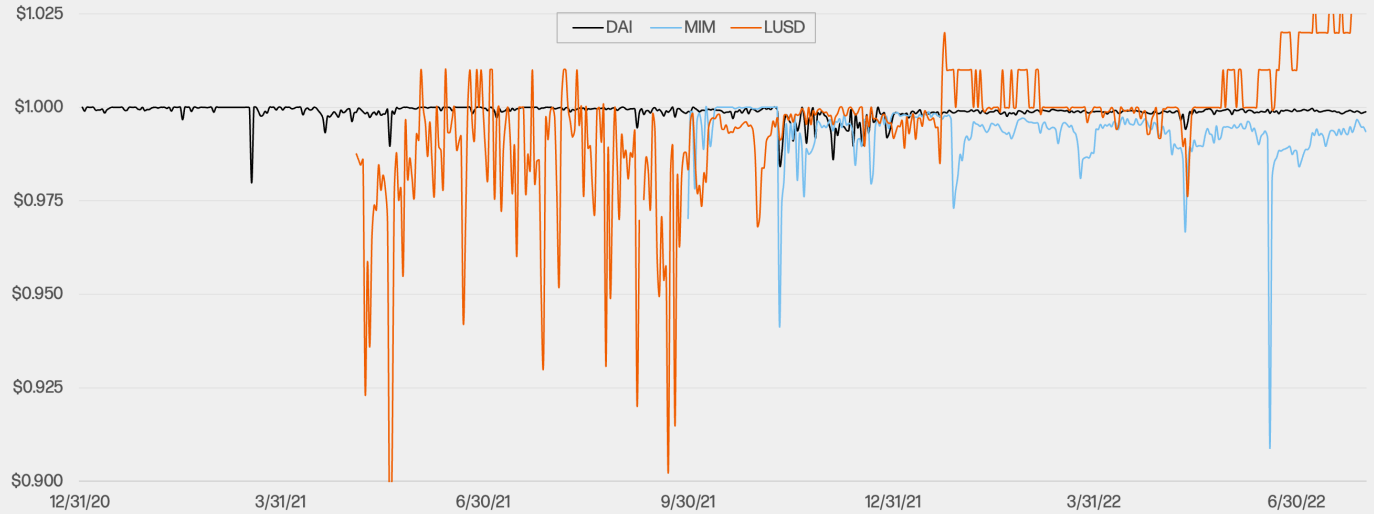
Depositors into overcollateralized stablecoins may see a varying range of acceptance of multiple asset types with varying deposit rates offered between platforms. Borrowers of stablecoins through lending protocols may be charged interest rates that are variable, high-fixed, low-flat, zero, or even negative and self-repaying interest depending on the deposited collateral and lending platform. These platforms can also integrate varying levels of yield, which can come directly from protocol revenues or from other platforms that integrate the asset.

To influence the overall reserve profile behind overcollateralized stablecoins or to affect their prices in the event of de-peggings, lending protocols typically implement changes to incentives structures. The most common strategy is to influence interest rates. Higher interest rates can be implemented to attract more liquidity from depositors (which usually comes at the expense of borrowers). Interest rates are typically based on preset parameters such as the availability of liquidity and utilization rates, but they can be adjusted through governance changes. Overcollateralized stablecoins ideally would have deep enough liquidity to maintain price stability through preset limits and rate structures, but changes to risk parameters are often necessary. In these cases, openness in communication behind protocol changes are important or else overcollateralized stablecoins may lose their benefits of transparency over fiat-backed stablecoins.



Overcollateralized Stablecoins - Daily Low Prices

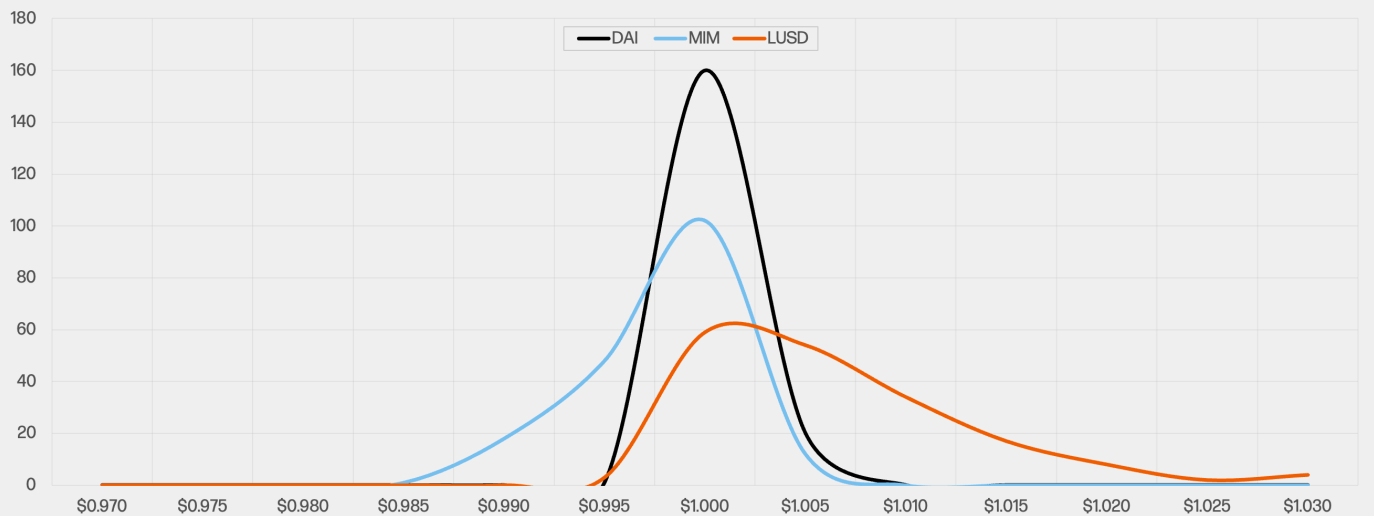
Source: Galaxy Digital Research



Data: CoinMarketCap

Overcollat. Stablecoins - # Days Daily Close Price Ended Within Each Range (1/1/22-6/30/22)

Source: Galaxy Digital Research



Data: CoinGecko



Financial Analysis of Overcollateralized Stablecoins



Peg Stability

DAI has been the most stable in its select peer group over 1H22 with 160 out of the 181 days that its closing price fell between \$0.9975-\$1.0025 and 20 days that its price closed in the \$1.0025-1.0075. The daily closing prices of MIM has been skewed more negatively with 67 days out of 181 days that it has closed below \$0.9975. Since launching in October 2021, MIM has consistently experienced price volatility with periodic de-pegging events occurring almost monthly, including its most significant de-pegging experienced in June. On the other hand, the daily closing prices of LUSD has been positively skewed with 119 days in 1H22 that it has closed above \$1.0025. LUSD has improved its price stability significantly since launching in April 2021, though it does not prioritize stability for upside deviations to the same degree as downside deviations. Notably, overcollateralized stablecoins have almost all experienced significant volatility early in their launches (DAI is no exception here). Those that survive, though, have tended to level out over time.

Usage

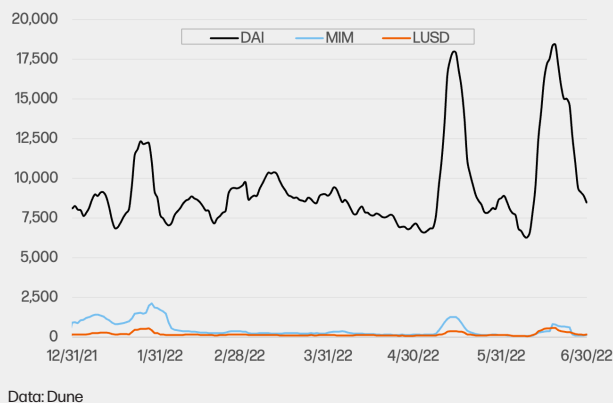
DAI stands well above MIM and LUSD in both transaction count and volume. MIM and LUSD come in at approximately 5% and 2% of the transaction count of DAI. Activity levels with DAI and LUSD have generally been increasing throughout 1H22 seemingly at the expense of MIM, whose activity levels have peaked early this year and have been sliding since.

Days daily low price traded at or below (1/1/21-6/30/22)	DAI	MIM	LUSD
\$0.925	0	1	0
\$0.930	0	0	0
\$0.935	0	0	0
\$0.940	0	0	0
\$0.945	0	0	0
\$0.950	0	0	0
\$0.955	0	0	0
\$0.960	0	0	0
\$0.965	0	0	0
\$0.970	0	1	0
\$0.975	0	1	0
\$0.980	0	1	1
\$0.985	0	4	0
\$0.990	0	32	4
\$0.995	1	67	15
>\$0.995	180	74	161
Total Days	181	181	181
Average Daily Low Price	\$0.9987	\$0.9930	\$0.9935
Standard Deviation	\$0.0020	\$0.0080	\$0.0167

Source: CoinMarketCap

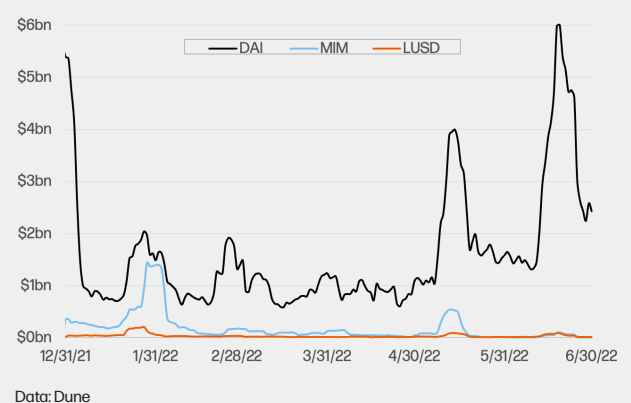
Overcollat. Stablecoins – Daily Tx Count (7d-MA)

Source: Galaxy Digital Research



Overcollat. Stablecoins – Daily Tx Value (7d-MA)

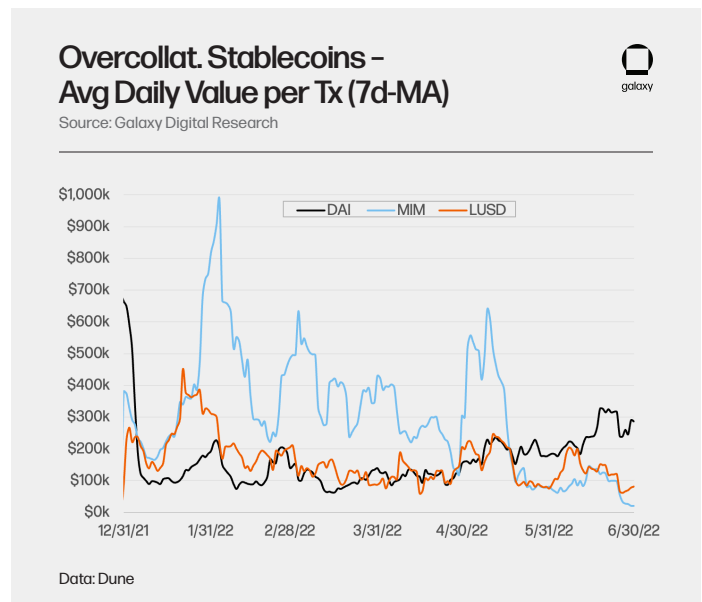
Source: Galaxy Digital Research





DAI's average transaction value was \$164k/tx during 1H22 as it consistently increased since March. MIM started out the year with a much higher average transaction value than DAI, though it has experienced a downward trend since. LUSD saw either higher or comparable average transaction values with DAI through the first 4.5 months of 1H22 though it has since trended in the opposite direction.

During 1H22, DAI experienced higher velocity than MIM and LUSD, averaging 0.049 vs. 0.042 and 0.030, respectively. DAI experienced the highest spike in velocity in the group following the collapse of UST, though MIM has experienced several periods of high velocity related to its de-pegging events with Danielle Sesta's association with Michael Patryn in late January and then Abracadabra's accumulation of \$12m in bad debt.



Usage statistics for Overcollateralized Stablecoins



Total Tx Cnt - 1H22								
		<u>Jan</u>	<u>Feb</u>	<u>Mar</u>	<u>Apr</u>	<u>May</u>	<u>Jun</u>	<u>1H22</u>
DAI		275,801	235,740	285,210	229,597	325,328	343,345	1,695,021
	ΔMoM		-15%	21%	-19%	42%	6%	
MIM		41,277	9,103	7,728	5,807	13,295	8,575	85,785
	ΔMoM		-78%	-15%	-25%	129%	-36%	
LUSD		8,534	3,978	3,834	3,250	5,512	7,774	32,882
	ΔMoM		-53%	-4%	-15%	70%	41%	

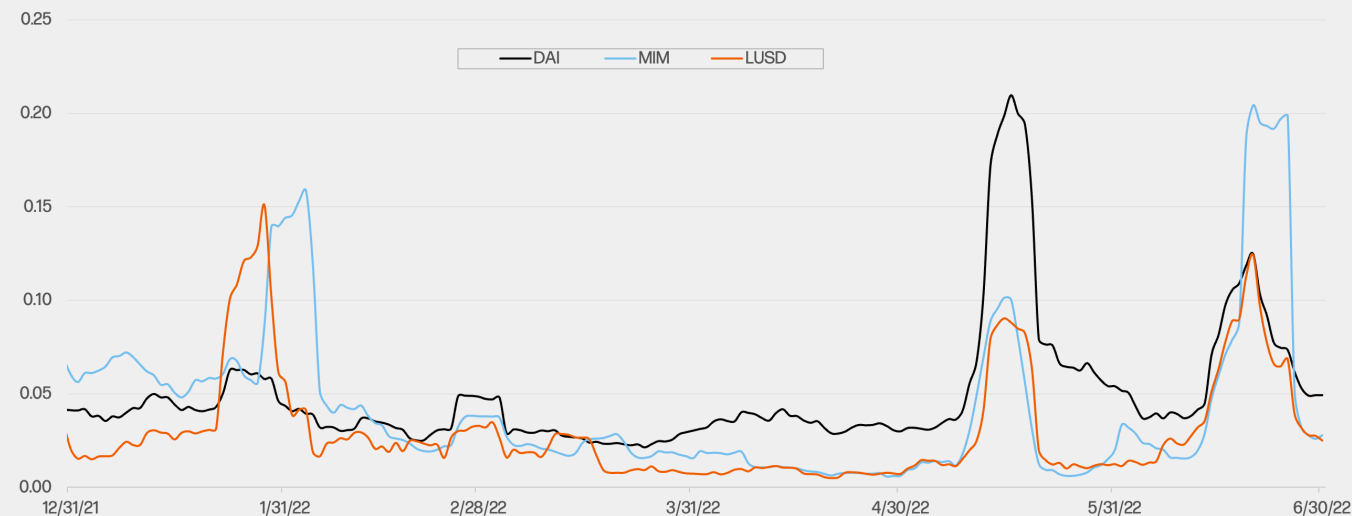
Total Tx Volume (\$m) - 1H22								
		Jan	Feb	Mar	Apr	May	Jun	1H22
DAI		\$36,520	\$29,692	\$29,678	\$27,319	\$63,221	\$92,069	\$278,500
	ΔMoM		-19%	0%	-8%	131%	46%	
MIM		\$17,543	\$4,136	\$3,055	\$1,673	\$4,504	\$863	\$31,774
	ΔMoM		-76%	-26%	-45%	169%	-81%	
LUSD		\$2,456	\$712	\$472	\$436	\$885	\$984	\$5,946
	ΔMoM		-71%	-34%	-8%	103%	11%	

Avg Tx Volume - 1H22								
		<u>Jan</u>	<u>Feb</u>	<u>Mar</u>	<u>Apr</u>	<u>May</u>	<u>Jun</u>	<u>1H22</u>
DAI		\$132,416	\$125,952	\$104,055	\$118,989	\$194,331	\$268,154	\$164,305
	ΔMoM		-5%	-17%	14%	63%	38%	
MIM		\$425,014	\$454,335	\$395,277	\$288,107	\$338,745	\$100,673	\$370,388
	ΔMoM		7%	-13%	-27%	18%	-70%	
LUSD		\$287,834	\$179,067	\$123,129	\$134,021	\$160,535	\$126,626	\$180,816
	ΔMoM		-38%	-31%	9%	20%	-21%	



Overcollateralized Stablecoins - Velocity (7d-MA)

Source: Galaxy Digital Research



Data: CoinGecko

Main Concerns with Overcollateralized Stablecoins

- **Reserves backed by centralized, censorable assets (e.g., USDC and USDT).** Overcollateralized stablecoins take on some of the risks of the collateral assets that they accept. For example, the risks of the centralized stablecoins as it relates to freezing assets or potential censorship are extended to DAI with Maker's acceptance of USDC for the PSM. This may be beneficial for maintaining price stability, but it limits the level of decentralization that overcollateralized stablecoins can achieve, reducing their overall value proposition.
- **Technical Risk.** A failure of a protocol's smart contracts, either through exploitation or design flaws, could disrupt the protocol's ability to adhere to its risk parameters, leading to peg failures. Protocols are reliant on oracles to ensure accurate reference prices for the underlying collateral to feed into smart contracts.
 - Price oracles may face risk of manipulation or infrequent updates that can cause reporting to be lagged. Protocols often rely upon Chainlink price feeds for ETH and can rely upon other oracles for other collateral assets including Uniswap v3 TWAP oracles or oracles operated by the asset team.
- **Capital inefficiency.** Overcollateralized stablecoins are capital inefficient as they require a greater amount of collateral deposits for each issued token (vs. 1:1 for fiat-backed stablecoins). Maker recommends users in certain ETH vaults to maintain collateralization ratios above 200% with liquidation thresholds set at 150%. This would imply that users take out a maximum of 66% of their collateral value in DAI, which limits the speed at which these stablecoins can grow. The supply of overcollateralized stablecoins is heavily dependent on borrowing activity, which can quickly dry up in a downturn as it is highly correlated to traders seeking leveraged long positions, limiting their utility for other applications looking to integrate the stablecoin.



Algorithmic Stablecoins

Algorithmic stablecoins attempt to address the centralization concerns of fiat-backed stablecoins and the capital-inefficiency concerns of overcollateralized stablecoins. Rather than being explicitly backed or fully collateralized, algorithmic stablecoins are designed to maintain price parity with a certain asset through market forces via smart contracts to increase/decrease supply.

In some ways, the concept of an algorithmic stablecoin can be thought of as a “Holy Grail” in that achieving stable value purely through engineering has been a goal of financial planners for thousands of years but has yet to be achieved in a durable way. The closest examples of successful implementation of an algorithmic currency with no backing is probably the U.S. dollar but, notably, USD began as a fully collateralized currency, backed and convertible at various times by gold or other hard assets. The success of shifting to a fully fiat model (uncollateralized), as occurred in 1971 when President Richard Nixon suspended the dollar’s conversion to gold, has mostly relied on other currencies following suit and was done so from a position of immense economic and military strength. Further, the prevailing use of the dollar in commerce in trade has helped maintain demand for USD outside of its use as a note convertible for hard assets. While the dollar has remained intact for the 50 years since the end of the gold standard, whether its position remains durable in the future remains to be seen. A longer view of history suggests that global reserve currencies routinely rise and fall. Whether the dollar is replaced by a competitor fiat currency or a harder currency, such as commodity linked currency as supposed by Credit Suisse’s Zoltan Pozsar or even Bitcoin, or whether the dollar remains hegemonic forever, remains to be seen.

But, like the dollar and fiat currencies, the success of algorithmic stablecoins has hinged on several factors including supply dynamics and demand. Within the world of cryptocurrencies, Ampleforth (AMPL) is an example of one of the first attempts at an algorithmic stablecoin. As a rebasing currency, AMPL used a single-token model in which holders shared in the benefits of the growing supply, which itself was due to increasing demand for the token. Token holders in this model bore the responsibility of financing its re-pegging to stable value in the event of shrinking demand. Another coming attempt at designing algorithmic stablecoins involved a two-token model, with Luna’s TerraUSD (UST). Rather than using any exogenous collateral like fiat or crypto assets for its backing, algorithmic stablecoins maintain their price stability through the use of a separate asset to absorb volatility, and through market incentives that increase/decrease the circulating supply of the stablecoin via smart contracts. With TerraUSD, one volatility-absorbing token (LUNA) is burned to create new units of the stablecoin (UST). To redeem UST, an equivalent dollar amount of LUNA is newly minted. The model only functioned properly if, upon demand to redeem UST, the market price of Luna was

durable enough to absorb its own inflation. Importantly, algorithmic stablecoins are not explicitly backed by the volatility-absorbing asset, so they are technically undercollateralized; instead, they are reliant on faith and demand in the paired asset.

There are several examples of algorithmic stablecoins, including UST and AMPL, but the concept at its core is one of decentralization. Achieving stable value without involving the use of exogenous collateral or government decree could create the world’s first stable, censorship resistant currency. Overcollateralized stablecoins, as described in the previous section, were one answer to this problem, but, in times of extreme market volatility impacting the underlying collateral, they have historically failed to maintain their pegs for a variety of reasons. So far, the primary mechanism by which overcollateralized stablecoins have mitigated this issue has been to diversify their collateral types to include centrally-issued assets, thereby undermining the vision of decentralization and censorship resistance. Because of these prior failures, as well as the remaining urge to achieve a truly decentralized stablecoin, we expect there will be further attempts at finding the algorithmic stablecoin “Holy Grail” going forward, despite the number of failures that this adventure has left in its wake over the years.

Stability Mechanism of Algorithmic Stablecoins

Just like any asset, the price of an algorithmic stablecoin may fluctuate due to changes in its supply and demand. In response to these changes, an algorithmic stablecoin system will adjust the supply of the stablecoin through minting new tokens or by burning them and taking them out of circulation.

One of the first algorithmic stablecoins was Ampleforth (AMPL), which used an approach called **rebasing** – a supply-regulating mechanism that automatically adjusted the circulating supply of the asset based on its current price to return its value to one inflation-adjusted US dollar (based on the CPI). Ampleforth rebased every 24 hours, which resulted in non-dilutive supply changes of AMPL tokens held in users’ wallets. However, AMPL and other rebase stablecoins experienced frequent deviations between rebases, preventing them from being widely adopted.

While Ampleforth relied upon a single-token model, other attempts at algorithmic stablecoins include **Seigniorage** models, which introduce one or two additional tokens to absorb the volatility in the stablecoin by changing its supply. Three-token systems consisted of the stablecoin, share, and bond tokens. When the price of the stablecoin was above \$1.00, the share token holders would receive newly minted stablecoins to sell, diluting the price back down to \$1.00; if the stablecoin was below \$1.00, bond tokens would be sold



Different Algorithmic Stablecoin Approaches



Algorithmic Stablecoin Types	Examples	Stability Mechanism
Rebase	AMPL, BASE	The total supply of the stablecoin is automatically adjusted within holders' wallets depending on the price of the stablecoin at fixed periodic intervals.
Seignorage - 2-token	UST, ESD, BAS	Follows a multi-coin structure that mints/burns volatility absorbing tokens to control supply of the stablecoin to maintain its price peg.
Seignorage - 3-token	Basis	A 3-token structure introduces another incentive token - a redeemable bond token that burns the stablecoin's when price falls below peg.

at a discount for the stablecoin with the opposite impact on the price. However, the incentives behind the bonding mechanism in seignorage models have failed to prevent runs as seen with Basis Cash and Empty Set Dollar.

Two-token algorithmic stablecoin systems were designed to enable users to swap the algorithmic stablecoin for its paired volatility-absorbing asset always at the price of \$1 – regardless of the market price of the other token at the time. The redemption mechanism creates incentives for market participants to step in whenever the price deviates from its peg.

For example, if the price of the algorithmic stablecoin trades above \$1.00 due to increased demand, users will mint more of the stablecoin at the lower fixed price through the redemption mechanism, thereby diluting its supply and bringing the overall market price back down to \$1. This process requires sending the paired volatility-absorbing asset to an inaccessible address, effectively taking it out of circulation and contracting its supply. Similarly, if the algorithmic stablecoin is trading below \$1.00, then users could redeem the stablecoin by burning it through the market module for \$1.00-worth of the paired asset. This mechanism presents a constant arbitrage opportunity designed to keep the price of the stablecoin equal to \$1.00.

How the mechanism fails (i.e. “death spirals”)

Without explicit backing from other assets, the stability mechanisms behind algorithmic stablecoins are subject to breaking down in “death spiral” scenarios. Death spirals occur in scenarios where algorithmic stablecoin holders look to exit their positions, but there is not enough demand to hold the volatility-absorbing token. This would cause users to redeem their stablecoins and then immediately market sell the newly minted coins on third party exchanges, which puts even further downward pressure on the price of the volatility-absorbing token. This can cause limitless

printing of the volatility-absorbing token that sends its price to zero. With the volatility absorbing token inflating continuously and its price declining, each additional stablecoin redemption accelerates the process, causing the so-called “death spiral.”

There are multiple ways that stability mechanisms can fail for algorithmic stablecoins, including: the parameters set for the redemption mechanism prevent it from being fully utilized; there is insufficient liquidity across exchanges or liquidity pools to meet exit demand; or there are technical exploits of the protocol, smart contracts, oracles, or bridges. Catalysts can also be driven by broader market risk or by events impacting the underlying platform upon which the stablecoin relies. But ultimately, these events unfold when the incentives for arbitrageurs to restore the peg evaporate, causing investors lose faith in both the stablecoin and the volatility absorbing token.

The most prominent demonstration of this failure is TerraUSD (UST).

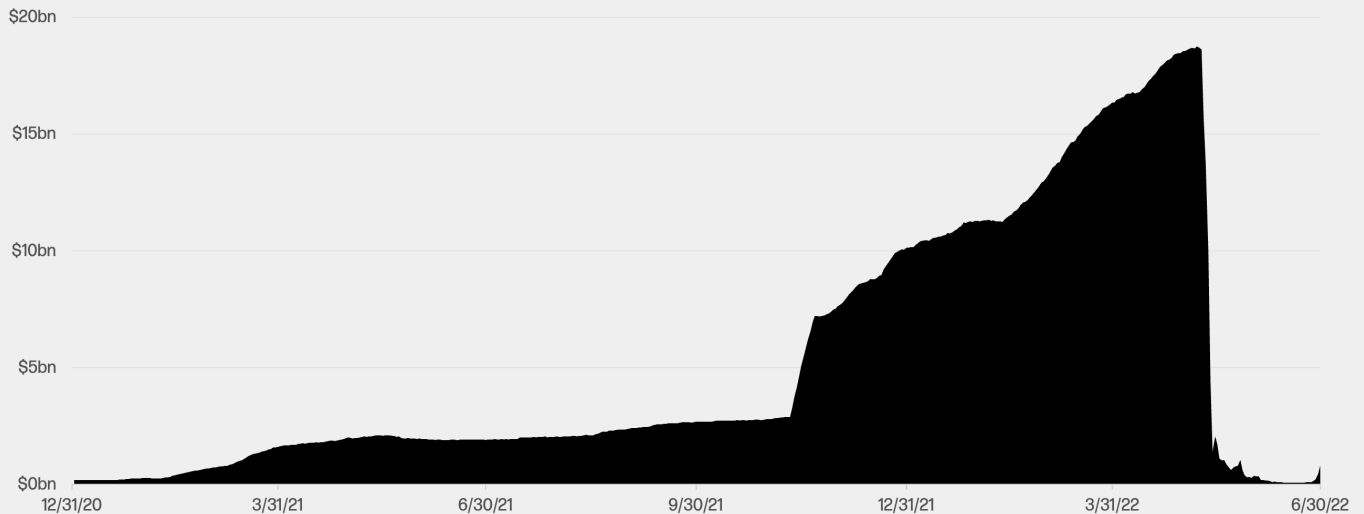
TerraUSD (UST)

TerraUSD (UST) was developed by **Terraform Labs (TFL)**, co-founded in 2018 by Do Kwon and Daniel Shin, and originally issued on the Terra blockchain, a Tendermint chain in the Cosmos ecosystem. Luna and UST were originally known for being used in Chai, a South Korean payments application, but became prominent for having a long track record of providing some of the highest fixed yields on a stablecoin at ~20% through Anchor, a lending protocol built on the Terra blockchain. Towards the end of its run, TFL further expanded its strategy for UST's growth, attempting to expand its use across other chains. These efforts helped drive UST to become the 3rd largest stablecoin behind USDT and USDC and lift Terra (LUNA) to become the 2nd largest blockchain by TVL.



UST Market Cap

Source: Galaxy Digital Research



Data: CoinGecko

UST's Market Module

LUNA is the governance token of Terra. UST was designed to maintain its price stability through the mint/burn function of Terra's market module. By design, on-chain users could redeem their LUNA for UST (or vice versa) at a \$1:1 ratio regardless of the market price of UST at the time. Recognizing the risks of its design from seeing past failures of other algorithmic stablecoins, TFL sought to mitigate the risk of a UST death spiral by building enduring demand to hold both the stablecoin and the volatility-absorbing token. With Terra, an entire economy of use cases was built around UST, including retail spending, savings, credit, and investing.

Beyond the stability mechanism and an ecosystem of demand for UST, TFL looked to add another layer of security and build confidence in UST by setting aside several billion dollars' worth of funds to establish a reserve with external currencies like BTC and AVAX to be managed by the **Luna Foundation Guard ("LFG")**, which was overseen by 6 industry experts. The reasons for creating the reserve included: (i) reducing UST's reliance on LUNA and providing diversification benefits by enabling redemptions in BTC or other assets at the choice of the user, and (ii) support TFL's plans to expand UST to other chains, which required establishing confidence in the stability of UST for users outside the Terra ecosystem. The LFG had accumulated over 80k BTC (worth around ~\$3bn in early May) and ~\$200m of AVAX in reserves before Terra collapsed.

The Collapse of UST

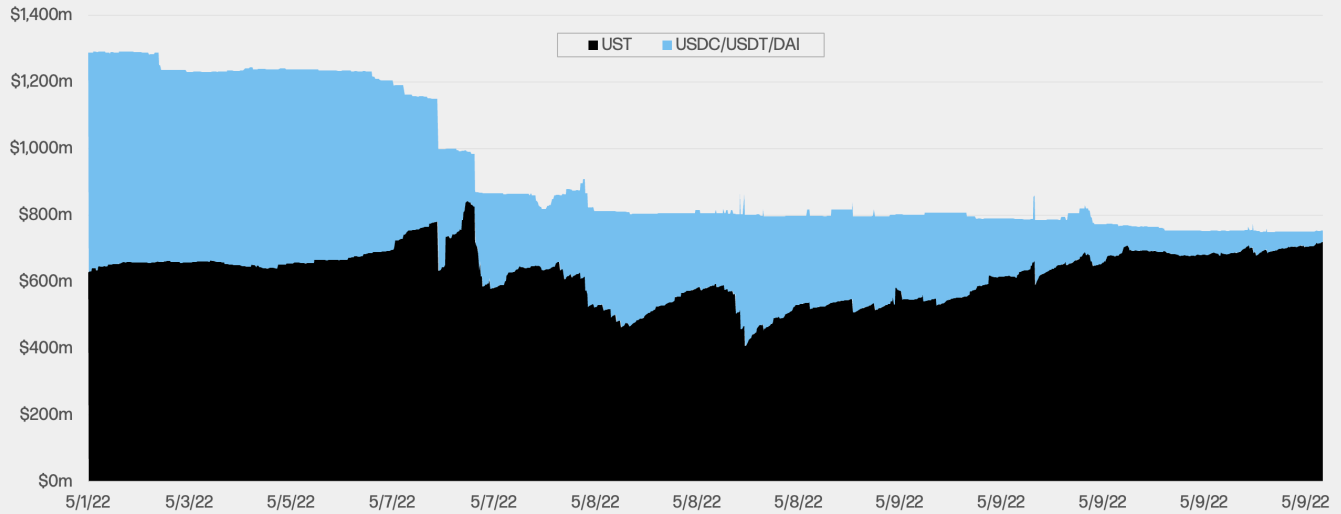
Despite all the efforts to help sustain the peg beyond just its stability mechanism, UST did indeed experience a death spiral in May 2022. The peg first began to break as few large wallets initiated large withdrawals of UST from Anchor, bridging to Ethereum, then selling UST for other stablecoins on external decentralized exchanges like Curve and centralized exchanges like Binance. These actions quickly diminished UST's liquidity in the order books and liquidity pools, causing others to panic and exit their positions, resulting in a bank run on UST.

The Luna Foundation Guard put its bitcoin reserves to work, trying to restore UST's peg alongside many other members of the Terra community such as Terraform Labs. Overall, at least \$500m was added to Curve pools or swapped to rebalance the pool. These actions helped stabilize UST prices a bit but eventually, these efforts proved insufficient in restoring the faith needed to stabilize UST. The inability to restore confidence in the algorithmic stablecoin resulted in continued downward pressure on the stablecoin and on LUNA as users continued to exit their UST positions.



Curve - UST-3pool Balance (May 2022)

Source: Galaxy Digital Research



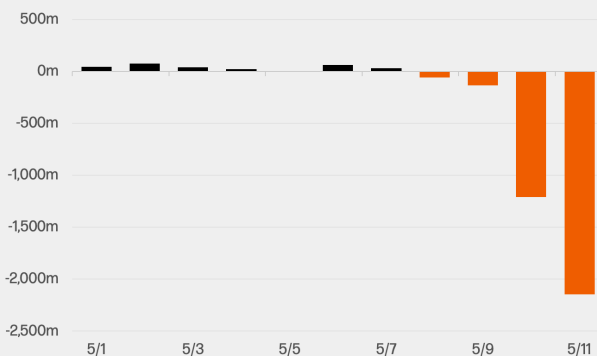
Data: Dune (note: x-axis is not scaled linearly)

Initially, UST's on-chain market module was not being utilized to its full extent for several reasons, including spam overwhelming the network as well as existing set parameters around the daily redemption limits and the fee structure which inhibited orderly redemptions. As TFL loosened some of those controls to meet demand for UST redemptions, UST holders raced for the exit, causing LUNA to be minted at an exponential rate. This inflation

crashed LUNA's price, further accelerating the downfall. This dynamic continued for several days until Thursday, May 12, 2022, when Terra validators elected to halt the chain and restrict new delegations to preserve the security of Terra. By then, over 6 trillion LUNA tokens had been minted while the algorithmic design of UST had effectively failed.

UST Daily Supply Change (May 2022)

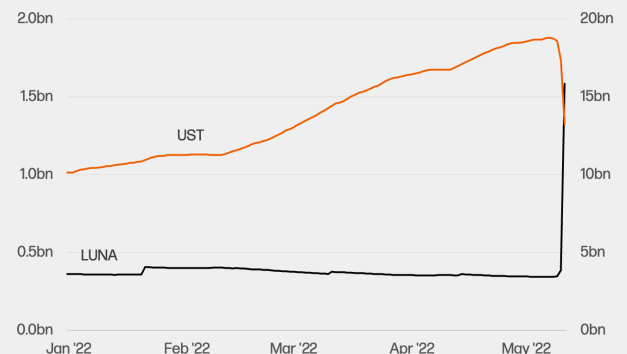
Source: Galaxy Digital Research



Data: terra.smartstake.io

UST + LUNA Circulating Supply (5/11/22 YTD) (in native units)

Source: Galaxy Digital Research



Data: terra.smartstake.io



Main takeaways from the unwinding of UST

Key flaws were uncovered as UST de-pegged:

- The main stability mechanism was not utilized to its full extent.**
 There were several parameters as part of the market module that prevented arbitrage opportunities from forming as UST fell below \$1. There was a variable spread fee that was added to any swap between UST and LUNA based on the volume of mint/burn activity. The rapid spike in the fee made it uneconomical for many UST holders to redeem for LUNA, leading them to instead opt for swapping on external venues. Also, the daily redemption capacity was set at \$293m, a limit that had been periodically adjusted through governance proposals as the system continued to scale (it was updated 4 times since 2021). Had the redemption limit and spread fee been designed to adjust dynamically based on the supply of UST, the system could have been more resilient during the run. Instead, these safety parameters intended to limit volatility in supply changes had backfired by slowing the peg recovery process.
- Cross-chain ambitions come with liquidity risk.** It's well-known in the cryptocurrency ecosystem that operating across multiple chains entails "bridging risk," the risk that the mechanism that supports moving assets from one chain to another can fail or be exploited. But operating across multiple systems can also cause liquidity imbalances that create or exacerbate other risks. One of the necessary components for UST to expand to other blockchains was through using external exchanges (e.g., Curve on Ethereum) where UST's on-chain market module was unavailable. As seen in the chart of the UST Curve pool balance, UST's supply became extremely imbalanced which put downward pressure on its price. If everything was on-chain on Terra, the stabilizing mechanisms would have had greater control over the fluctuation of UST, and if the pool had more liquidity, the

supply imbalance and the price impact would have been less severe, so that a rebalancing could have been possible.

- Stablecoins backed by endogenous assets can scale quickly but can unwind even faster.** Algorithmic stablecoins are primarily backed by an endogenous asset—an asset that sits within its own system—so the volatility absorbing token may also operate as the governance token and the value accrual token. This contrasts with exogenous assets, such as Ethereum or Bitcoin, which exist outside of the stablecoin system and are not directly influenced by the protocol behind the algorithmic stablecoin. UST's design relied entirely on LUNA—a fully endogenous asset—until the addition of exogenous assets like Bitcoin and Avalanche managed by the LFG. Endogenous assets enable protocols behind algorithmic stablecoins with more control over their implementation, but they come with greater reflexivity, which means that they can unwind quickly in death spiral scenarios. Building the entire Terra ecosystem around LUNA/UST also put each of the projects at risk while the assets collapsed. Adding BTC and AVAX as exogenous assets was an attempt by LFG to mitigate this risk, but the mechanism to incorporate their position as redemption assets had not materialized by the time the bank run occurred.

We describe how UST collapsed in more detail in our report ["Examining UST's Collapse"](#).

Algo Stables Competitive Landscape

Today, there are few true algorithmic stablecoins that are still operating, though several hybrid models exist that use a combination of an algorithmic stability mechanism as well as a partial collateral backing.

Algorithmic Stablecoins



Data as of 7/31/2022	 TerraUSD	 Neutrino Dollar	 Tron USDD	 Frax	 Fei
Stablecoin	UST (USTC)	USDN	USDD	FRAX	FEI
Launch Date	Sep-20	Feb-20	May-22	Dec-20	Apr-21
Stablecoin Market Cap	\$344m	\$731m	\$725m	\$1,466m	\$200m
Primary Volatility Absorbing Asset	LUNA (LUNC)	WAVES	TRX	FXS	TRIBE
Vol Absorbing Asset MCap	nm	\$565m	\$6.4bn	\$521m	\$74m
Available Platforms	Terra	Waves	Tron	ETH, BSC, Polygon, Avalanche, others	Ethereum
Exogenous Reserve Assets?	BTC, AVAX	n/a	BTC, USDC, USDT	USDC	PCV Deposits (ETH, stETH, DAI)
Size of Exogenous Reserves	nm	n/a	\$1.4bn	\$1,327m	\$220m
Collateral Ratio (\$ reserves / \$ stable)	n/a	n/a	202%*	90.5%	191%

Source: CoinGecko, protocol websites, Dune *CR calculation excludes TRX + burnt TRX unlike what is reported by USDD.io



- **Neutrino USD (USDN).** After UST's collapse, the largest algorithmic stablecoin is **Neutrino USD (USDN)**. USDN is a stablecoin built upon the Waves blockchain that relies upon the platform token WAVES as its volatility-absorbing token. It employs similar mechanics to UST but differs in some of its redemption parameters that impact how many redemptions are processed each day. In April, USDN experienced a partial spiraling event after Twitter user [0xHamz](#) had accused the Waves team of manipulating the price of its native token through the platform's lending app Vires.finance. This sparked fear and drove many users to exit, leading USDN to lose its peg, falling below \$0.70 as the price of WAVES fell from a high of \$60 to nearly \$20 in a few short days. USDN had partially recovered to trade back above \$0.96 until the collapse of UST, which caused USDN to fall back below \$0.75. Since then, the Waves team released a [DeFi Revival Plan](#), which involves several improvements to harden the defense of the peg, including dynamic daily borrow and withdraw limits, dynamic limits based on utilization, and liquidity locks to prevent bank runs, among several others. Through the month of July, the price of USDN averaged \$0.989 as it traded at a slight, persistent discount.
- **USDD.** USDD was launched in May 2022 on Tron, employing both an on-chain mechanism (using Tron's platform token TRX as the volatility-absorbing token) as well as a pool of collateralized assets that includes BTC, TRX, USDT, and USDC. USDD is also available on BNB Chain and Ethereum. USDD initially offered a 30% fixed rate yield (most likely as an attempt to compete with Anchor's rates on UST at the time) and has grown its market cap to over \$700m. Compared to UST, USDD has a few notable differences aside from the exogenous reserve assets, including permissioned access to access the on-chain mechanism to mint/burn USDD—a function controlled by the Tron DAO—which makes it more of a centralized stablecoin that is not as reliant on arbitrageurs and market forces to maintain its peg. Since June 13, USDD lost its peg, falling to below \$0.93 amid broader market concerns, and has continued to trade below \$1 for over a month before recovering back to \$1 late July.
- **Market Operator (AMO)** that enables the protocol to expand/contract the supply of FRAX in LP pools to support the peg of FRAX.
- **Celo Dollar (cUSD).** Celo Dollar (cUSD) is a collateral-algorithmic stablecoin that is platform-native to Celo, the mobile-first EVM blockchain. Celo Dollar's main purpose is P2P payments, leveraging Celo's mobile-first payment infrastructure, as well as to support the overall Celo ecosystem. cUSD can be minted and redeemed at a value of \$1 in CELO tokens. cUSD is backed by a large reserve that is mostly in CELO and DAI but also includes BTC and ETH (though the reserve assets are not incorporated into the redemption function). As of August 8, 2022, all Celo stablecoins (incl. cUSD, cEUR, and cREAL) have a reserve ratio of 2.97x (or 1.33x when excluding CELO tokens from the calculation).

Other notable stablecoin designs that don't quite fit the stablecoin categories above include:

- **Fei.** The FEI stablecoin was launched in April 2021 by Fei Protocol. In January 2022, Fei merged with Rari Capital to become part of the Tribe DAO that includes other products including Volt (inflation-pegged stablecoin) and Midas Capital. Fei enables users to mint/redeem FEI for \$1 of collateral (either DAI, ETH, RAI, or LUSD) using PSMs. To support direct redemption of FEI at \$1, the Protocol introduced the concept of Protocol Controlled Value (PCV) – rather than having collateral deposits sit idle in contracts, PCV brings liquidity to deposits to be actively managed to support the protocol with yield generation and to defend the \$1 peg. As a backstop, FEI may be redeemed for newly minted TRIBE if PCV ever drops below the target reserve ratio. With the PCV model, FEI is less subject to runaway inflation since redemption of FEI would improve the collateralization ratio of PCV / Fei liabilities. In Fei v2, if the collateralization ratio moves downwards towards 100%, then PCV weights would be adjusted algorithmically towards more stable assets (e.g., DAI and RAI) using risk curves.
- **UXD.** UXD Protocol on Solana uses a delta-neutral stability design for its stablecoin, UXD. UXD was created with the primary goal of solving for a decentralized, scalable stablecoin. By accepting BTC, SOL, or other assets as collateral, UXD Protocol creates delta-neutral positions by balancing long and short positions using perpetual futures contracts, which would imply that the value of the overall position would not depend on the value of the deposited assets. UXD works best when funding rates for perpetual futures positions remain positive – delta-neutral strategies are created by shorting perps so any interest paid on these positions would be partly distributed to UXD Protocol stakers with the remainder going towards an insurance fund. UXD Protocol also enables redemptions of its stablecoin for \$1-worth of collateral, which presents opportunities for arbitrageurs to support UXD's peg. The primary risk behind UXD's delta-neutral stability model is if perp funding rates are negative for an extended period of time. The insurance fund exists to pay the negative funding rate on behalf of UXD holders. In the event that the insurance fund is depleted, UXD has several backstops including auctioning off UXP tokens to replenish the insurance fund, or temporarily enabling redemptions of UXD for USDC through a stablecoin pool. UXD (currently restricted in the US) utilizes derivatives exchange Mango Markets and is integrated with Saber, Solana's Curve-like stablecoin exchange.

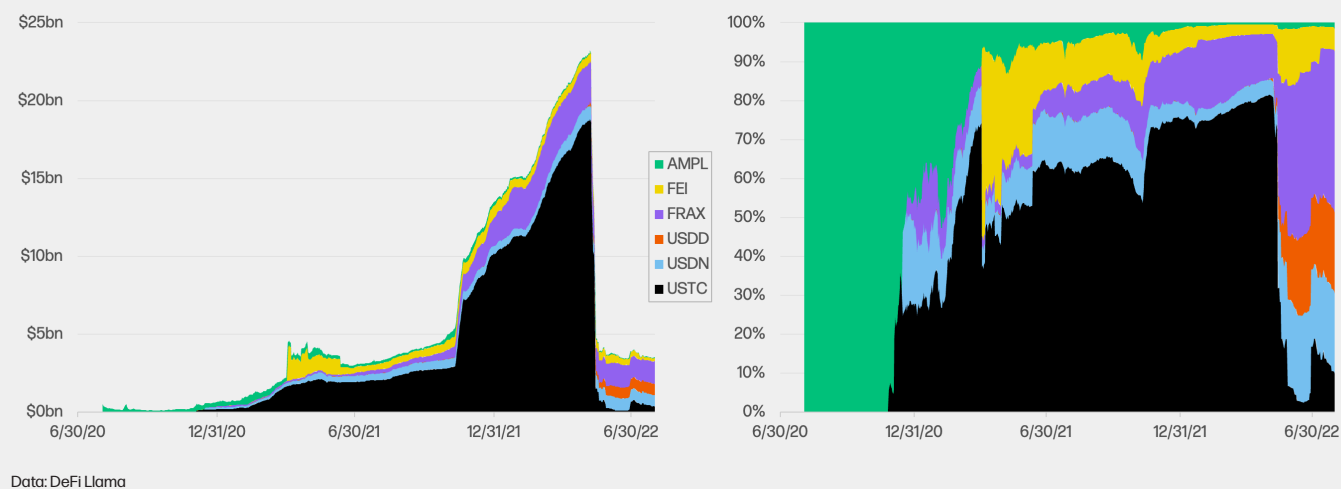
Stablecoins that follow a hybrid model—employing both a stability module and backed by collateral—include:

- **Frax (FRAX).** FRAX is a fractional-algorithmic stablecoin that combines both on-chain collateral backing (partial backing vs. overcollateralized) and a price-stability algorithm. FRAX launched in November 2020 and was the first stablecoin to incorporate the fractional-algorithmic hybrid design at the time. FRAX can be minted/redeemed from the system for \$1 of value; users can mint FRAX by depositing \$1 of value into the system. When FRAX is at 100% collateral, then the entire deposit is kept as collateral. If FRAX is in a fractional state (collateral ratio is <100%), then a portion of the deposit is swapped for the platform governance token FXS and then burned. Redeeming FRAX works the opposite way: if the CR is 98%, for example, then every FRAX can be redeemed for \$0.98 of USDC and \$0.02 of newly minted FXS. This system creates arbitrage opportunities whenever the price of FRAX deviates from \$1. In addition, the protocol may adjust the collateral ratio every hour by increments of 0.25% depending on whether the price of FRAX is above or below \$1. Frax also provides an Algorithmic



Algorithmic Stablecoins – Market Cap and % Share

Source: Galaxy Digital Research



Competitive Dynamics of Algo Stables

Algorithmic stablecoins generally compete on stability, utility, and yield.

- **Trust (faith in stability mechanism).** Since algorithmic stablecoins are uncollateralized with relatively novel and experimental designs, they are heavily reliant on faith in the underlying system, as well as trust from its holders that the stablecoin can maintain its value. Trust and faith can be established through proper communication from the team, building a community, and demonstrating resilience through market cycles and stress tests. A longer operating history paired with a well-understood stability mechanism will build more trust, which enables continual growth that fuels the yield opportunities.
- **Utility.** Algorithmic stablecoins compete on utility which means building integrations and forming use cases around the stablecoin. It is crucial for algorithmic stablecoins to build demand outside of speculative use cases—this utility serves as both a growth and defense mechanism. Compared to past algorithmic stablecoins issued by independent projects, UST was relatively unique because it was the platform stablecoin for the Terra blockchain, enabling it to easily build an ecosystem around it and create utility for the token. Still, building more integrations with protocols and other blockchains come with their own set of risks, including liquidity and bridging risks associated with existing cross-chain, a heightened contagion risk, and more.

- **Yield.** Algorithmic stablecoins, like most DeFi protocols, have typically relied upon massive incentives programs to put the stablecoin in the hands of users. Before its collapse, UST set a high bar at ~20% interest rate through Anchor for other algorithmic stablecoins to compete. New stablecoins like Tron's USDD employed a similar fixed rate model that offered an even more competitive 30% yield since launching in May. Though unsustainable, these offerings used a depositor-friendly model that paid out rewards in stables rather than through a different token, enticing users to expand the algorithmic stablecoin's supply.

Primary Risks with Algorithmic Stables

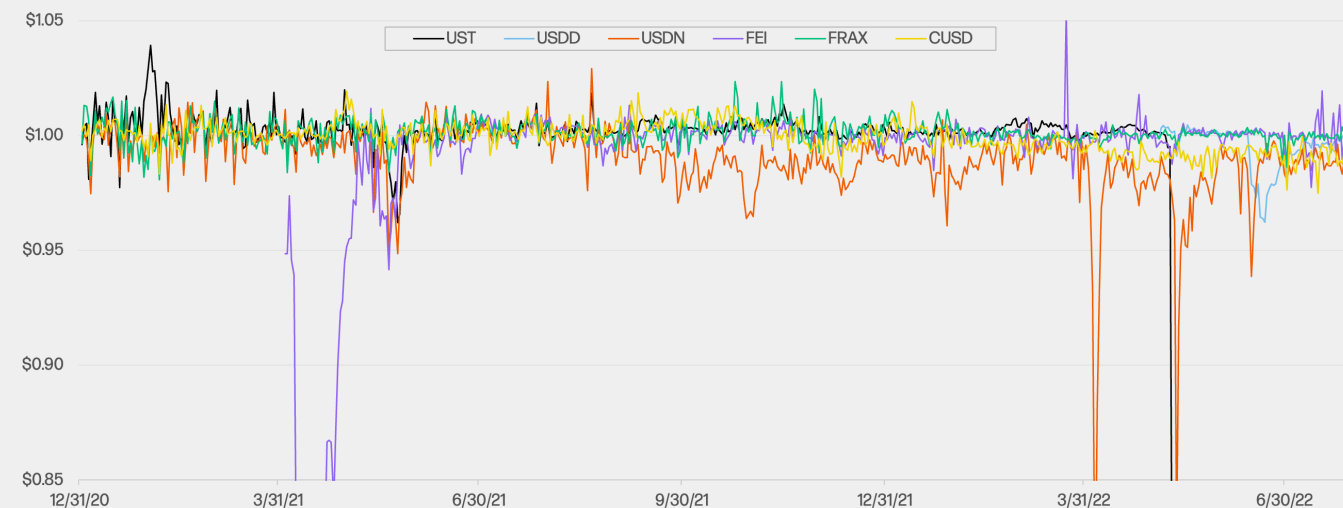
The main concern with algorithmic stablecoins is simply proving that they work. To date, nearly every algorithmic stablecoin has either faced a major de-pegging event or failed.

Without a long operating history that shows resilience through adversarial conditions, it is difficult to build confidence in a stablecoin, particularly if it is using a novel stability mechanism. The problem is that there have been somewhat infrequent stressed market conditions over the past five years to expose weaknesses in algorithmic stablecoin designs and incentive structures to learn from. Dai was only launched about 4.5 years ago, while essentially all of today's relevant algorithmic stablecoins have been launched since 2020. Algorithmic stablecoins need time to build trust and confidence, and they must weather some demanding, challenging periods to demonstrate resilience.



Algo/Hybrid Stablecoins - Daily Closing Prices

Source: Galaxy Digital Research



Data: CoinGecko

However, with a growing graveyard of past algorithmic stablecoins, it becomes harder for each new issuer to gain acceptance among users. Following UST's collapse, many now wonder whether algorithmic stablecoins are a fundamentally flawed concept. As a result, some algorithmic stablecoins underwent changes to their operating structures to strengthen their pegs by improving their parameters around their algorithms, or moving more towards collateralized models and/or higher stablecoin backings:

- **USDD:** Early June, just one month after launching, TRON DAO [announced](#) that USDD—initially designed as an algorithmic stablecoin with a design similar to TerraUSD—had undergone a major upgrade to transition into an overcollateralized model. Moving forward, USDD would have a minimum collateral ratio of 130% backed by reserve assets including BTC, TRX, and stablecoins (incl. USDC, USDT, TUSD, and USDJ) – all held under the TRON DAO Reserve.
- **Neutrino Dollar (USDN):** In addition to a new action plan to recover USDN's peg in May, Waves protocol [published](#) a longer-term improvement plan for its stablecoin that includes: (i) improving demand for USDN through incentivizing the USDN 3-pool on Curve, (ii) liquidating large accounts and taking control over their collateral to enable larger user withdrawals, and (iii) improving USDN architecture with “a new recap token that recapitalizes Neutrino with new Waves Tokens when under-collateralized.”
- **Sperax USD (USDs):** Sperax, built on Arbitrum, [announced](#) mid-May that its yield-bearing stablecoin, Sperax USD, would be undergoing a structural change from its previously hybrid

90-10 algorithmic-overcollateralized stablecoin model to a 100% collateralized model with the new collateral provided by Sperax Foundation. Over time, USDs will move back towards a hybrid model with the collateral target is set to decrease by 1% each year, meaning USDs will move back towards a hybrid maims to become more algorithmic at a rate of 1% per year.

- **Celo USD (CUSD):** A governance proposal published on May 13th ([CGP-56](#)) was passed to increase the CUSD reserve mix of low-volatility assets (i.e. stablecoins like DAI) from 5% to 30%. A month later, another governance proposal ([CGP-62](#)) was passed – this time, community members voted to diversify its stablecoin allocation from DAI-only to a 50-50 split between DAI-USDC in the stable asset basket, citing the need for “maximum protection of cStable holders during these extreme market conditions.”

Peg Breaks and Failures of Stablecoins

It's important that we learn from the past mistakes of other stablecoins and iterate on their designs. When looking at the list of peg breaks and failed stablecoin designs, it's important to assess why the stability mechanism failed and whether it was: (i) a fundamental flaw in its design that could impact other stablecoins that have similar designs or, (ii) if it was a more idiosyncratic failure due to the specific implementation of the stablecoin.



De-peggings and Failures of Stablecoins



Stablecoin	Ticker	Stablecoin Type	Date Failure	Failure Description	Dead?
Tether	\$USDT	Fiat-backed	Apr 18	Tether announces international transfers to move funds to move outside Taiwan were blocked	No
Tether	\$USDT	Fiat-backed	Oct 18	Loss of faith - lack of transparency over reserves and rumored issues at Bitfinex	No
Basis (fka Basecoin)	n/a	Algorithmic - Seignorage	Dec 18	US securities regulation prevented ability to launch Basis	Yes
Libra (Diem)	n/a	Fiat-backed	Jun 19	Regulators prevented Facebook's ability to launch Diem (Silvergate has since acquired Diem tech/assets)	Kinda
MakerDAO	\$DAI	Overcollateralized	Mar 20	Black Thursday - Oracle not updating fast enough, manipulations of liquidators	No
Empty Set Dollar	\$ESD	Algorithmic - Seignorage	Dec 20	Loss of faith, bad bonding and coupon mechanics that led to exploitation	Yes
Dynamic Set Dollar	\$DSD	Algorithmic - Seignorage	Dec 20	Loss of faith, bad bonding and coupon mechanics that led to exploitation	Yes
Basis Cash	\$BAC	Algorithmic	Jan 21	Death spiral - lack of demand to hold volatility-absorbing asset \$BAS and slow emissions schedule	Yes
Fei	\$FEI	Hybrid: algo / collat	Apr 21	Bug - blocked purchase of Fei tokens from incentivized pool; inability to burn FEI tokens to rebalance	No
TerraUSD	\$UST	Algorithmic	May 21	Decoupling - oracle problems	No
TITAN / Iron Finance	\$IRON	Algorithmic	Jun 21	First large-scale crypto bank run leading to death spiral, oracle not updating fast enough	Yes
Abracadabra	\$MIM	Overcollateralized	Jan 22	Faith - Danielle Sesta, investors rushed to exit - cap dropped from \$4.6B to \$2.8B in 3 days	No
Waves	\$USDN	Algorithmic	Apr 22	Loss of faith - Oxhamz alleged Waves team manipulated WAVES price through Vires.finance	No
TerraUSD	\$USDT	Algorithmic	May 22	Death spiral from rapid growth strategy and lack of liquidity/financial support to restore faith	Yes
Tether	\$USDT	Fiat-backed	May 22	Loss of faith - broader market risk concerns following UST collapse	No
Tron USDD	\$USDD	Algorithmic	Jun 22	Loss of faith - broader market risk concerns following UST collapse	No
Waves	\$USDN	Algorithmic	Jun 22	Loss of faith - broader market risk concerns following UST collapse	No
Magic Internet Money	\$MIM	Overcollateralized	Jun 22	Accumulation of bad debt from liquidation mechanism	No

Most of these incidents belong to algorithmic stablecoins due to their experimental designs. So far, it appears that many have given up on rebase and seignorage designs due to their fundamental design flaws or are at least proceeding with new designs more cautiously by adding in more protections and mitigations.

But even with “fully-backed” stablecoins, we have also seen flaws with fiat-backed currencies and overcollateralized stablecoins that cause them to break their peg. We have learned that no stablecoin is immune from the following risks:

- **Price risk.** There is no guarantee of price stability on external exchanges. A stablecoin may always be redeemable for \$1 through the issuer, but there may be limits to how accessible the redemption option may be or there may be alternative channels where price deviations can occur.

- **Smart contract risk.** Protocols rely on self-executing code in smart contracts, which may be vulnerable to exploits and technology failures. Smart contracts require sufficient testing and auditing to mitigate potential exploits.
- **Oracle risk.** Oracles are relied upon for accurate and timely reference prices for stablecoins and their underlying collateral – including off-chain deposits. Manipulation of oracles or failure for oracles to provide accurate data can result in stability mechanism failures or unexpected liquidations.

Failures can and will continue to happen. User perceptions change after a de-pegging event, but among the non “full-backed” stablecoins, Maker has proven that trust can be recovered through transparency, speedy communication and owning responsibility to the community.



Analysis of the Different Categories of Stablecoins

Trade-offs

Similar to the [scaling trilemma](#) (where blockchains often make trade-offs between decentralization, scalability, and security), stablecoins have had to make trade-offs along three factors:

- **Price stability.** This refers to how well a stablecoin maintains its peg and the strength of its redemption procedures and guarantees. With stronger reserve guarantees, fiat-backed stablecoins generally maintain better peg stability to the dollar than crypto-backed stablecoins. However, the reserves backing certain “fiat-backed” stablecoins do often comprise assets other than fiat currency, at the discretion of the issuer, that may be less liquid in a mass redemption scenario. Both fiat-backed and overcollateralized stablecoins tend to provide stronger redemption guarantees than algorithmic stablecoins due to their more robust reserves.
 - Depending on their designs, some stablecoins may not be designed to stay exactly at \$1.00, so the baseline for “failures” can be different for each type of stablecoin. Some may have fees in place or arbitrage mechanisms that may not activate until the stablecoin trades outside of a certain range. Others have redemption limits which can delay how quickly a stablecoin can recover after price deviations occur. For example, due to a redemption fee of 0.1%, arbitrage opportunities may not be presented for USDT until it trades outside of \$0.999 – \$1.001 range. Alternatively, USDC charges no fees for issuance/redemptions and has a narrower arbitrage range, while Liquity’s dynamic fee model can charge issuance/redemption fees of up to 5% (depending on the rate of issuance/ redemptions), preventing arbitrageurs from stepping in until LUSD trades outside of \$0.95 - \$1.05 in some cases.
- **Scalability or capital efficiency.** This includes factors like how quickly stablecoin supply can expand, which is linked with its capital efficiency and how capital efficient it is. Both fiat-backed and over-collateralized stablecoins are constrained by their capital deposits and reserves. Fiat-backed stablecoins require 1:1 backing for users and are more capital efficient than overcollateralized types which require a greater amount of deposits for each issued stablecoin. Because they may not be collateralized by fiat currency or user deposits, algorithmic stablecoins can theoretically scale to meet higher levels of demand without being constrained by the amount of collateral they can obtain.
- **Decentralization.** The goal of decentralization in stablecoins generally refers to being un-censorable or seizure-resistant first and foremost, followed by reduced reliance on a centralized entity to properly function. Fiat backed or asset backed stables will require regulated intermediaries to issue the coin, manage collateral and govern the ecosystem whereas crypto or algo backed lack the centralized intermediary, which can make the stablecoin less prone to censorship—and this is one of the demand drivers for more decentralized stables. However, “decentralized” stablecoins may also suffer from these same risks if they rely upon these centralized stablecoins for their backings, and many are also heavily reliant on centralized teams for growth or governance to quickly implement changes for safety in response to changes in operating conditions.

Trade-offs Between Stablecoin Designs



Stablecoin Approaches	Pros / Advantages	Risks / Limitations	Competitive Dynamics
Fiat-backed or “Off-chain”	Strong redemption guarantees, simplest, less vulnerable to hacks with no collateral on-chain, not forkable (likely to require banking licenses for issuance), ability to freeze funds	Centralized - need trusted custodian, not scalable, slow liquidation into fiat, need for regular audits, lack of verifiable reserves so reliance on attestations, relatively low-yielding, ability to freeze funds	Compete on transparency, cash backings, and issuance licenses
Crypto-backed or “Overcollateralized”	Strong redemption guarantees, relatively long track record, more decentralized, can liquidate quickly, transparent (see collateralization ratio), used to lever up	Capital inefficiency, mostly backed by centralized coins, users face liquidation risk based on normal currency risk (price risk), more (less) price instability than fiat-backed (algos), more complex, faces oracle risk	Demand comes from leverage, typically more cyclical, compete on collateralization, collateral types
Algorithmic	Scalable (hypothetical infinite liquidity), decentralized, capital efficient (no collateral required), most decentralized and independent (not tied to other centralized stables like USDC,DAI)	Reliance on external data for peg (subject to poor quality data, reporting delays, data errors). Smart contract risk. Reflexivity (i.e. death spiral) - needs trust/faith in redeemability, no liquidations, complex - difficult to analyze safety bounds or health	Requires continual growth (reliant on platform growth, integrations). Uncollateralized so it’s heavily reliant on faith in the underlying system but enables higher yield opportunities



The trade-offs along these factors between various stablecoin designs are not always evident until a stress-testing event occurs. Compared to overcollateralized stablecoins, algorithmic stablecoins have prioritized growth and capital efficiency at the expense of price stability—they have always been subject to the risk of reflexivity and potential death spirals. Most algorithmic stablecoins have not been sufficiently stress tested in adversarial market conditions, and most that have been stress tested have not fared well, historically. Peg stability may be easier to maintain during a bull market, which can create a sense of false confidence with longer operating histories. But against a weak macro backdrop (e.g., a rising interest rate environment), liquidity can quickly dry up and the capacity for outside peg defenders to act as a backstop weakens.

Even within each of the categories described above, stablecoins can have very different degrees of risk. For example, USDT employs less conservative reserve practices than USDC or BUSD, which can potentially generate higher amounts of yield that theoretically

could benefit depositors through a larger equity buffer, though fiat-backed stablecoins depositors usually do not directly receive any yield benefits. The same applies to the use of stablecoins in DeFi, as issuers do not bake in any native yields, though some applications that integrate the stablecoins may offer rewards separately. Among overcollateralized stablecoins, DAI prioritizes peg stability and safety but provides lower yields, whereas MIM caters towards a more risk-tolerant audience with greater availability to take on leverage and access high-yield opportunities.

Adding to the complexity of this landscape, as previously mentioned, there is a growing class of hybrid stablecoins that seek to combine the benefits of algorithmic stablecoins (e.g., decentralization and capital efficiency) with the safety and price stability benefits of overcollateralized stablecoins. The trade-offs described in this section are only meant to describe the general dynamics between the different types of stablecoins, but each stablecoin deserves its own risk assessment.



Financial Analysis of All Stablecoins

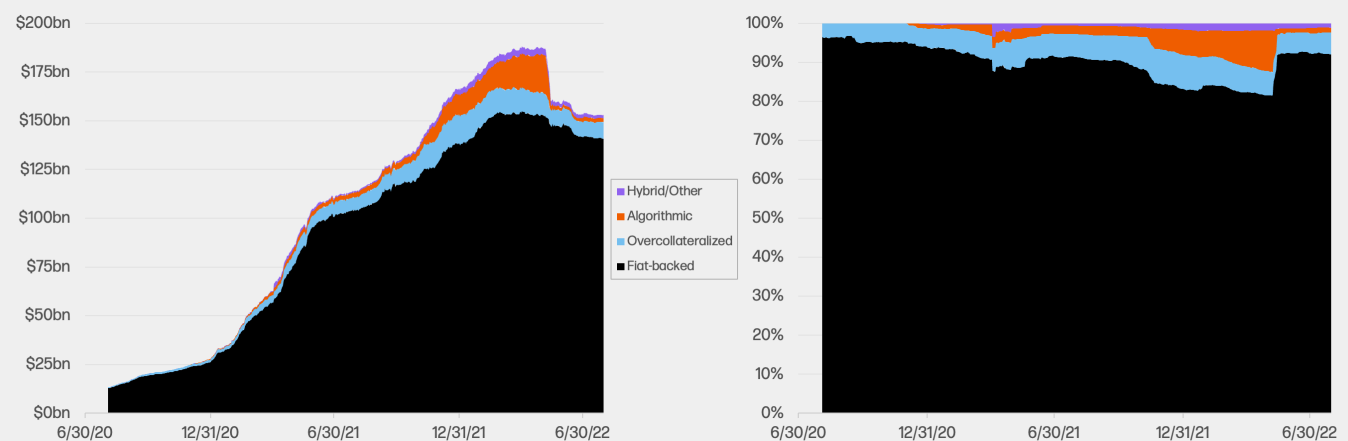
Stablecoin Market Cap by Design



Stablecoin Mcap (in \$m)		9/30/20	12/31/20	3/31/21	6/30/21	9/30/21	12/31/21	3/31/22	6/30/22
Fiat-backed	USDT	\$15,466	20,921	\$40,730	\$62,663	\$69,575	\$78,442	\$81,930	\$66,464
	USDC	\$2,538	\$3,705	\$10,904	\$25,227	\$31,496	\$42,429	\$52,132	\$54,865
	BUSD	\$476	\$896	\$3,585	\$10,128	\$13,451	\$14,720	\$17,464	\$17,634
	TUSD	\$396	\$273	\$330	\$1,497	\$1,405	\$1,293	\$1,368	\$1,235
	USDP	\$292	\$303	\$945	\$836	\$923	\$1,037	\$965	\$857
	Others	\$37	\$49	\$158	\$259	\$297	\$220	\$285	\$505
	Total	\$19,205	\$26,146	\$56,652	\$100,610	\$117,148	\$138,140	\$154,144	\$141,560
	% Share	95%	94%	91%	92%	90%	83%	82%	92%
Overcollateralized	DAI	\$912	\$1,158	\$3,014	\$4,961	\$6,191	\$8,940	\$9,225	\$6,326
	MIM	\$-	\$-	\$-	\$-	\$882	\$4,533	\$2,759	\$192
	ALUSD	\$-	\$-	\$-	\$233	\$238	\$295	\$185	\$185
	LUSD	\$-	\$-	\$-	\$748	\$590	\$869	\$477	\$159
	SUSD	\$73	\$130	\$216	\$154	\$205	\$225	\$217	\$150
	Others	\$30	\$56	\$259	\$199	\$318	\$697	\$871	\$788
	Total	\$1,015	\$1,343	\$3,489	\$6,296	\$8,425	\$15,559	\$13,734	\$7,800
	% Share	5%	5%	6%	6%	6%	9%	7%	5%
Algo	USDN	\$-	\$134	\$218	\$392	\$539	\$536	\$839	\$776
	USDD	\$-	\$-	\$-	\$-	\$-	\$-	\$-	\$718
	USTC	\$-	\$182	\$1,600	\$1,910	\$2,686	\$10,128	\$16,355	\$657
	Total	\$-	\$317	\$1,818	\$2,302	\$3,226	\$10,664	\$17,193	\$2,175
	% Share	0%	1%	3%	2%	2%	6%	9%	1%
Hybrid/Other	FRAX	\$-	\$57	\$111	\$181	\$352	\$1,770	\$2,693	\$1,366
	FEI	\$-	\$-	\$-	\$363	\$501	\$813	\$559	\$360
	CUSD	\$-	\$19	\$43	\$51	\$86	\$98	\$79	\$56
	Others	\$-	\$-	\$-	\$-	\$-	\$-	\$107	\$22
	Total	\$-	\$75	\$154	\$596	\$939	\$2,682	\$3,438	\$1,804
	% Share	0%	0%	0%	1%	1%	2%	2%	1%
Total Stablecoin Mcap		\$20,220	\$27,882	\$62,113	\$109,803	\$129,737	\$167,044	\$188,510	\$153,339

Stablecoin Market Cap and % Share by Type

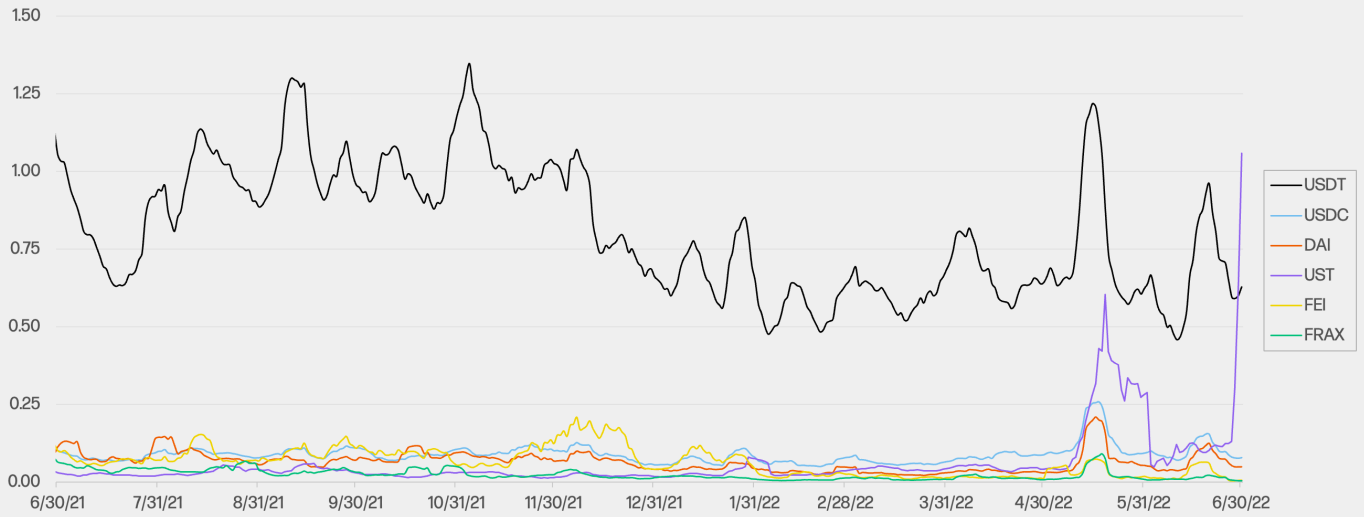
Source: Galaxy Digital Research





Velocity of Select Stablecoins (7d-MA)

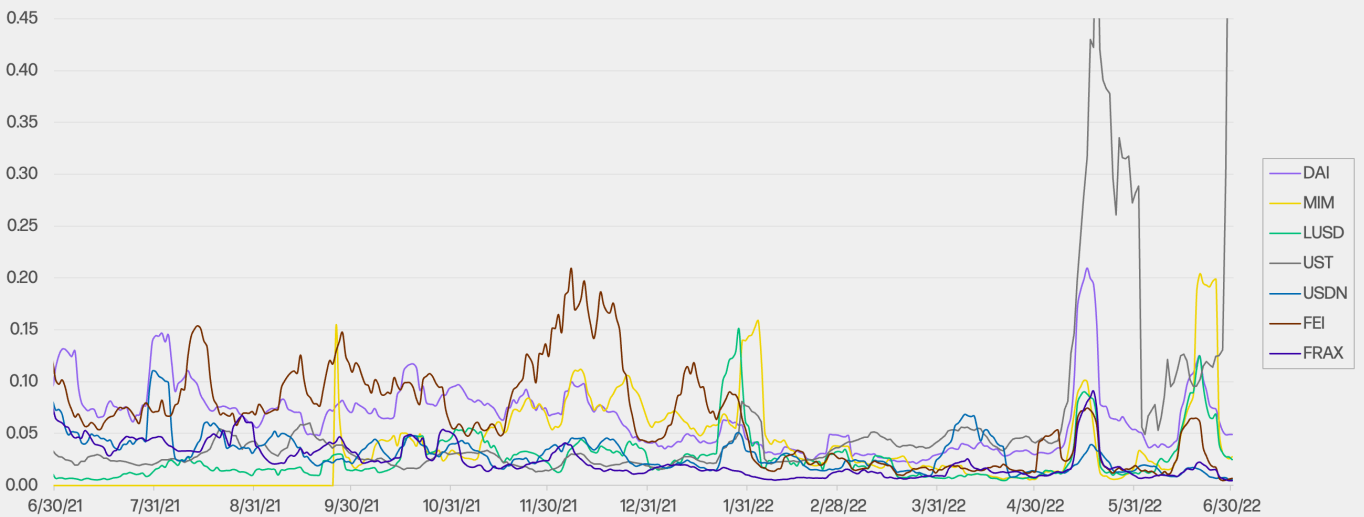
Source: Galaxy Digital Research



Data: CoinGecko

Velocity of Select Stablecoins (7d-MA)

Source: Galaxy Digital Research



Data: CoinGecko



Risk Assessment Framework for Stablecoins

Due Diligence of Risks

When performing due diligence of stablecoins, questions to consider asking include the following (note this is not a complete list and is intended to be a starting point for diligence):

Stablecoins Due Diligence Questions



Operational Assessment

- 1 How strong is the team / governance?
 - Are they anonymous or public? Do they have a strong track record?
 - Is there a governance token? How distributed is its ownership? Is there any systemic risk or concentration of economic power?
 - How strong is the community? Is the success of the protocol dependent on the team? Is there key-man risk?
 - Does the team communicate properly with the community regarding how and why business changes are made?
- 2 What is the revenue model of the issuer?
 - What fees are users paying and when are they paid (e.g. on deposits/withdrawals, new issuance/redemptions, liquidations, etc.)?
- 3 What is the governance token used for? Are token holders compensated? How?
- 4 How much transparency do they provide into their reserves and operations? Is there proper management and auditing of reserves?
- 5 How is the stablecoin typically used?
 - What does the stablecoin aim to do? What problems does it aim to solve? What is the potential for adoption?
 - Who is the target user - institutions, yield farmers, enterprises, retail users? Is it primarily used as an on- or off-ramp? In DeFi?
 - Where does supply and demand come from? What is the underlying blockchain that it operates? What integrations does it have with other projects?
- 6 Are there regulations that govern the use of the stablecoin or the operation of its issuer? Is the issuer in compliance?

Technological Assessment

- 7 How does the stablecoin maintain its price? What is the stability mechanism?
 - How strong are the redemption guarantees? If not fully collateralized, then what incentives (i.e. arbitrage) are relied upon for price stability?
 - Is it modeled after another protocol? What innovations does it introduce?
 - How accessible are these mechanisms?
 - How long has the stablecoin been around - has it experienced or endured any adversarial market conditions or stress testing events?
- 8 Does the token smart contract allow governance to mint new tokens? Is the token contract upgradable? Can user collateral positions be seized through governance or at will?
- 9 Can tokens be frozen in-flight? Addresses blacklisted?
- 10 If a borrow/lend protocol, are the incentives targeted at borrowers or lenders? How is risk split between the participants?
- 11 How does it prepare for black swan events?
 - What are the scenarios that the stablecoin may fail?
 - If primary stability mechanism fails, what safety mechanisms do they have to defend the peg?
 - How much excess capital is needed to remain solvent if the collateral is not sufficient?
 - Are there any other backstops or potential lenders of last resort?
 - In a bank run, can the stablecoin safely wind down? What are the most illiquid assets and who would be expected to take on that exposure (e.g. the protocol, the depositor, liquidation bots, etc)
 - Is there a recovery or resolution plan in place? Are there admin privileges that can be abused?
- 12 For borrow/lend protocols, what are the risk parameters in place?
 - This includes what collateral assets are accepted and what collateral ratios are applied. Higher collateral ratios should be applied to higher risk assets, which can be assessed by evaluating the volatility of the collateral asset, its liquidity (e.g. available exchanges and the depth of the liquidity), its token holder distribution (e.g. can one person dump), governance risk, team risk. Those accepting yield-bearing assets like liquid staking derivatives as collateral must consider the redemption/unlock periods and the issuing protocol behind the yield-bearing asset. What is the stability fee? Are the incentives high enough for liquidation bots to step in if prices fall steeply?
- 13 Has there been proper auditing and review of technical risks (e.g. oracle risk, smart contract risk)?
- 14 What price oracles are used? Is the price feed provided by a reputable entity? At what rate does the oracle update? Are there sanity backup checks for the main oracle?
- 15 What is the tech stack? What infrastructure does it rely upon? What platform does it operate on? What are the platform risks and how resilient is the underlying technology?
- 16 Is the stablecoin canonical (issued natively on the network) or is it wrapped (i.e., bridged by locking the canonical token on native chain to mint a synthetic token on destination chain)?
- 17 Are all collateral reserves cross-margined or are the individual loans backed by their own collateral in isolated vaults?

Market Risk

- 18 What collateral assets are accepted and what is their individual level of risk? How much correlation risk? Are the reserves diversified? What collateral ratios are applied?
- 19 How much risk is in the reserves? What is the level of credit risk, how much volatility and liquidity is available, is there concentrated exposure to one counterparty or asset type, is there correlation risk? What is the level of collateralization and is it sufficient?
- 20 How much liquidity is available on external exchanges? How many available exchanges and what is the depth of the liquidity and how much trading volume?
- 21 How is the quality of on-chain liquidity? What is the distribution of liquidity contributors? Is the liquidity growth organic or heavily incentivized?

As noted above, this is not an exhaustive list of questions but serves instead to stimulate our readers to think deeply about stablecoins and evaluate the many types of competitors in the market.



Best Practices for Stablecoin Issuers

- **Provide radical transparency / proper management and auditing of centralized/decentralized reserves.** Providing full transparency to users over reserve compositions is needed so that users can assess the risks. For fiat-backed stablecoins, solutions such as Armanino and Chainlink's Proof of Reserves (utilized by True USD and Kraken) can be utilized to provide more frequent updates on the health of reserves relative to the issuer's liabilities. It's also important to actively communicate with community to keep them aware of any changes and to build trust in their product. Trust among community members can be destroyed by not fully transparent governance changes.
- **Adopt additional forms of defense.** Since UST's collapse, many algorithmic stablecoin models have adopted have added reserves with exogenous collateral to defend their peg during tail risk events. Others have explored risk parameters that can be tuned (e.g., target debt ratio, debt ceilings) or set aside liquidity backstops to defend their pegs. Issuers would be prudent to start with lower limits during the early stages of the project and then gradually increasing over time with greater understanding of market mechanics.
- **Balance the ability to react quickly to changes with trust minimized DAO governance.** For more decentralized stablecoins, in the case of stress changes should be implemented quickly through governance in response to new market developments. Ideally, there would be dynamic risk parameters set so that there may be more trust minimized governance.
- **Do not overextend credit and do not overspend on marketing in search of growth.** Product market fit is often perverted by over-incentivizing adoption. All protocols incentivize usage initially to bootstrap its network, even bitcoin (with higher initial block subsidy). But some have overextended the use of incentivization and attracted irresponsible or less-than-ideal users (e.g., yield farmers or mercenary capital) that would be the first to leave once incentives dry up. Furthermore, the growth of highly-incentivized protocols leads less-sophisticated users to overestimate the adoption and, therefore, resilience of the protocol. For more responsible and organic growth, a stablecoin must be clearly understood by its users so that want to continuing using the product regardless of the incentives attached to it.
- **Diversify reserves and reduce dependence on volatile assets for collateral.** Higher volatility assets deserve higher safety margins. Though each new accepted collateral asset comes with its own set of risks, having a reserve of diversified assets can potentially mitigate some of the price risks with single-asset reserves. Ideally, the asset would be low in volatility to prevent from having unintended effects from sharp price changes.
- **Adopt controls to limit exposure to a single counterparty.** Having large concentration with a single counterparty can create systemic risk and could possibly make redemptions/withdrawals inaccessible to other users depending on the parameters in place. Having utilization limits in place for large whales can prevent concentration risk. Additionally, liquidation of large collateral positions will likely result in high slippage costs that can prevent flash arbitrage from occurring, depending on the available market liquidity. Enabling execution of partial liquidation and selling of collateral can prevent the price pressure on assets during times of crisis, as well as improve the borrower experience.
- **Attract sticky demand for leverage with longer duration.** Implementing a delay in withdrawals from safety liquidity or having strong incentives for users to contribute to the safety liquidity during times of crisis provides stronger protections to stablecoins. During non-crisis times, it is important to build non-speculative demand for the stablecoin to limit redemption requests and to reduce the price volatility of the stablecoin. The Terra ecosystem attempted to do this by promoting UST for payments and other applications. Tether has notably expanded the use of USDT for payments widely across Africa and Asia. MakerDAO has targeted real estate borrowers as part of its Real World Assets initiative due to the longer duration of the asset, which could improve the health of the protocol's balance sheet if properly managed.



Regulation

Regulators, lawmakers, and policymakers largely started paying close attention to stablecoins when Facebook announced plans to launch Libra (later rebranded to Diem) in the summer of 2019. Even though USDT and USDC had been in existence for several years, Facebook's announcement seemingly caught lawmakers and regulators off-guard as they viewed a stablecoin issued by the social media giant—whose reputation had already taken a hit over privacy practices and its role in the 2016 American election—as having a particularly disruptive impact on the role of the dollar and on the fractional reserve banking system. At the time, USDT and USDC were used primarily as on/off-ramps and as trading instruments, but Facebook's stablecoin project had the capability to reach billions of users and transforming commerce and the broader payments system. Furthermore, Libra's initial proposed design suggested collateral composed of multiple fiat currencies, not just the U.S. dollar, which frightened policymakers who worried Facebook's coin could become a supra-national currency and ultimately exact undue influence on the governments, central banks, and economies of the underlying currencies.

These concerns ultimately prevented Facebook from launching its stablecoin. Several reasons for the regulatory headwinds included Facebook's history and poor communication with Congress regarding its plans and the design of the product. Despite failing to ever launch, Diem still had a lasting impact on the space as it forced lawmakers and regulators to think about the risks of stablecoins and how they are used. Today, the Diem team at Facebook has mostly dissolved, with some assets sold to Silvergate Bank, David Marcus (its leader) leaving to create a new startup focused on Bitcoin's Lightning Network, and various others working on two new alternative Layer 1 blockchains based on the tech behind Libra (Aptos & Sui).

Multi-year blockchain research efforts at global central banks to create *central bank digital currencies* (CBDC) have also accelerated since the failed launch of Libra. While several CBDCs already launched in smaller jurisdictions (e.g., the Bahamian Sand Dollar, Jamaica's JAM-DEX, and Nigeria's eNaira), major central banks including the Federal Reserve, Bank of England, European Central Bank, and People's Bank of China are in various stages of research or implementation. To some extent, the heightened awareness of stablecoins issued by private companies or decentralized protocols has led to increased urgency by the world's fiat currency issuers to either act against, compete with, or regulate stablecoins.

Other meaningful regulatory catalysts for regulating stablecoins come from the Financial Action Task Force (FATF)—an international body that includes 37 member countries to set global AML standards—and its recommendations for the **Travel Rule**. The Travel Rule (TR) puts customer due diligence requirements on regulated financial services companies to collect and store identifying information on their customers for certain transfers of funds. It has been in effect for financial institutions (e.g., banks

& payment service providers) but in 2019, FATF elected to extend AML requirements to virtual asset service providers (VASPs). FATF recommendations are non-binding, meaning they are not legal obligations – they merely outline AML standards and policies and promotes collaboration between member states.

Regulation in the US

In November 2021, the Treasury-led President's Working Group on Financial Markets (PWG), which includes members from the Fed, SEC, and CFTC, along with participation from the FDIC and OCC, issued a [22-page report](#) on stablecoins that explores risks associated with stablecoins and makes recommendations on how to best mitigate those risks. The report identified several key risks posed by stablecoins including:

- **Stablecoin runs (contagion risk).** The first—and likely primary—risk concerning the PWG is that a sudden loss of confidence in stablecoins could result in a “fire sale” of reserve assets which “could disrupt critical funding markets, depending on the type of and volume of reserve assets involved.” Given the size of major stablecoins, the PWG worries that sudden redemption demand could require a stablecoin issuer to sell its reserve assets on the open financial markets quickly, which could allow a crypto-native loss of confidence to spill into the broader economy. This risk has become more acute as fiat-backed stablecoins have become larger.
- **Systemic risk and concentration of economic power.** The PWG argues that, as stablecoins scale quickly, the intermediary service providers (e.g., wallet providers, custodians, or other commercial firms) could become excessively powerful, which “could have detrimental effects on competition and lead to market concentration in sectors of the real economy.”
- **Regulatory gaps.** Broadly, the PWG argues that stablecoins currently fall through the regulatory cracks, subject only to a loose patchwork of oversight that is insufficient to create a “consistent and comprehensive regulatory framework.”

Recommendations in the report called for Congress to “act promptly to ensure that payment stablecoins are subject to appropriate federal prudential oversight on a consistent and comprehensive basis”. Specifically, and importantly, the report calls for: “Stablecoin issuance, and related activities of redemption and maintenance of reserve assets, [to be limited] to entities that are insured depository institutions (IDIs).” Essentially, the PWG is calling for legislation to limit stablecoin issuance to banks, or at least a new type of institution that closely resembles a bank. The report also suggests that “custodial wallet providers” come under regulation due to “the central role that custodial wallet providers play within a stablecoin arrangement.” At the time of writing, there are bipartisan efforts to propose legislation along these lines in



both chambers of the U.S. Congress—though the path forward for such legislation, once introduced, is subject to significant headwinds during the balance of this congressional session.

Requiring stablecoin issuers to become FDIC-insured would bring significant transparency and user protections, and would bring the nascent industry into conformity with existing and familiar rules governing banks. Users would be more protected in the event of a “run” on the stablecoin issuer, have more confidence in the solvency and operational procedures of stablecoin issuers, and bring comfort to skeptics of the technology. For issuers, the bank-like capital and liquidity requirements may even mean that reserves may not be required to be 100% backed by cash or cash equivalents, presenting an opportunity for them to invest in higher yielding alternatives, in contrast to recent moves by Circle and Paxos to commit their reserves entirely to the least risky assets. But the current process for crypto companies to obtain banking charters has been lengthy, burdensome, and subject to significant policy changes between presidential administrations.

SEC Chairman Gary Gensler has called on Congress to grant the regulatory agency specific authority to regulate cryptocurrency exchanges. And the OCC, prior to the start of the Biden Administration, had begun issuing bank charters to crypto custodians and issued guidance to its covered banking institutions clarifying that they could operate public blockchain nodes and participate in public blockchain networks. Taken together, and adding the PWG recommendations, a picture of a privately issued, distinctly American digital dollar comes into focus: commercial banks, whether crypto-native or traditional, operating in concert with regulated custodians and distributors, could issue stablecoins if they are sufficiently overseen by existing regulators of insured depository institutions, such as the Fed, FDIC, OCC, and state banking regulators.

Since the issuance of the report, there have been several stablecoin congressional hearings, including two major hearings in February with Nellie Liang, the Treasury’s undersecretary for Domestic Finance, serving as witness and making the case to limit stablecoin issuance to insured depository institutions (IDIs). Congressmembers during both the House Financial Services Committee and the Senate Banking, Housing, and Urban Affairs Committee at the time expressed support for new legislation to oversee stablecoins, particularly as it related to reserve practices and reporting and disclosure requirements. However, many congressional members were opposed to limiting stablecoin issuance to IDIs with some members reasoning that the crypto ecosystem deserved its own regulatory framework rather than applying existing banking regulations onto stablecoin issuers.

In addition to Congress, stablecoins have also been called out by the Fed and the White House. In March, the Biden Administration issued an [Executive Order](#) to oversee the development of digital assets across six key priorities: (i) consumer and investor protection, (ii) financial stability, (iii) illicit finance, (iv) U.S. leadership in the global financial system and economic competitiveness, (v) financial inclusion, and (vi) responsible innovation. The Fed noted in its semi-annual [Monetary Policy Report](#) to Congress: “Stablecoins that are not backed by safe and sufficiently liquid assets and are

not subject to appropriate regulatory standards create risks to investors and potentially to the financial system.”

Calls for federal regulation of stablecoins were re-ignited following the collapse of UST and Tether’s brief de-pegging in May. Treasury Secretary Janet Yellen took notice, saying, “A stablecoin known as TerraUSD experienced a run and declined in value. I think that this simply illustrates that this is a rapidly growing product and there are rapidly growing risks.” Yellen also pushed for Congress to approve federal regulation of stablecoins by the end of the year.

Proposed legislation in the US for regulating digital assets and stablecoins include:

- [The Stablecoin TRUST Act](#) – proposed by Senate Banking Committee Ranking Member Pat Toomey (R-Pa.)
- [Stablecoin Innovation and Protection Act of 2022](#) – proposed by Congressman Josh Gotthiemer (NJ-5)
- [Responsible Financial Innovation Act](#) – proposed by Senators Cynthia Lummis (R-WY) and Kirsten Gillibrand (D-NY)
- Bipartisan Stablecoin Bill from the House Financial Services Committee [draft now expected in September]

The Responsible Financial Innovation Act by Senators Lummis and Gillibrand provides a blueprint for a more comprehensive regulatory framework to oversee the broader crypto industry, including stablecoins. Given competing priorities for Congressional attention and a looming mid-term election in November, it is unlikely that these or any other proposals will become law this year. However, whatever legislation is ultimately signed into law will likely contain elements from each of these bills.

If we do see a comprehensive regulatory regime take hold, we’re likely also to see a bifurcation of the stablecoin markets, with US-regulated stablecoins on one side and offshore stablecoins and those issued in a decentralized manner on-chain on the other. While the PWG and legislators have acknowledged the importance of stablecoins to the DeFi ecosystem, decentralized stablecoins like DAI and TerraUSD are only briefly mentioned. Whether the enactment of a comprehensive stablecoin regulatory regime would be accompanied by a prohibition on the use of algorithmic stablecoins remains to be seen, but typically these frameworks come with enforcement of those who exist outside them.

CBDCs vs. Stablecoins

Central bank digital currencies (CBDC) are also being explored as an alternative solution to a privately issued digital currency tied to a fiat currency. The Bank of International Settlements (BIS) published a [report](#) in October 2020 laying out foundational principles and core features of potential CBDCs, listing unique advantages of central bank money including stability, traceability, and better control on monetary supply. In a [follow-up report](#) in September 2021, the BIS laid out some of the practical policy and implementation issues of CBDCs. Other major central banks are in various stages of researching and implementing CBDCs, including the Federal Reserve, European Central Bank, Bank of England, and People’s Bank of China.



The primary differences between a fiat-backed stablecoin and a CBDC are:

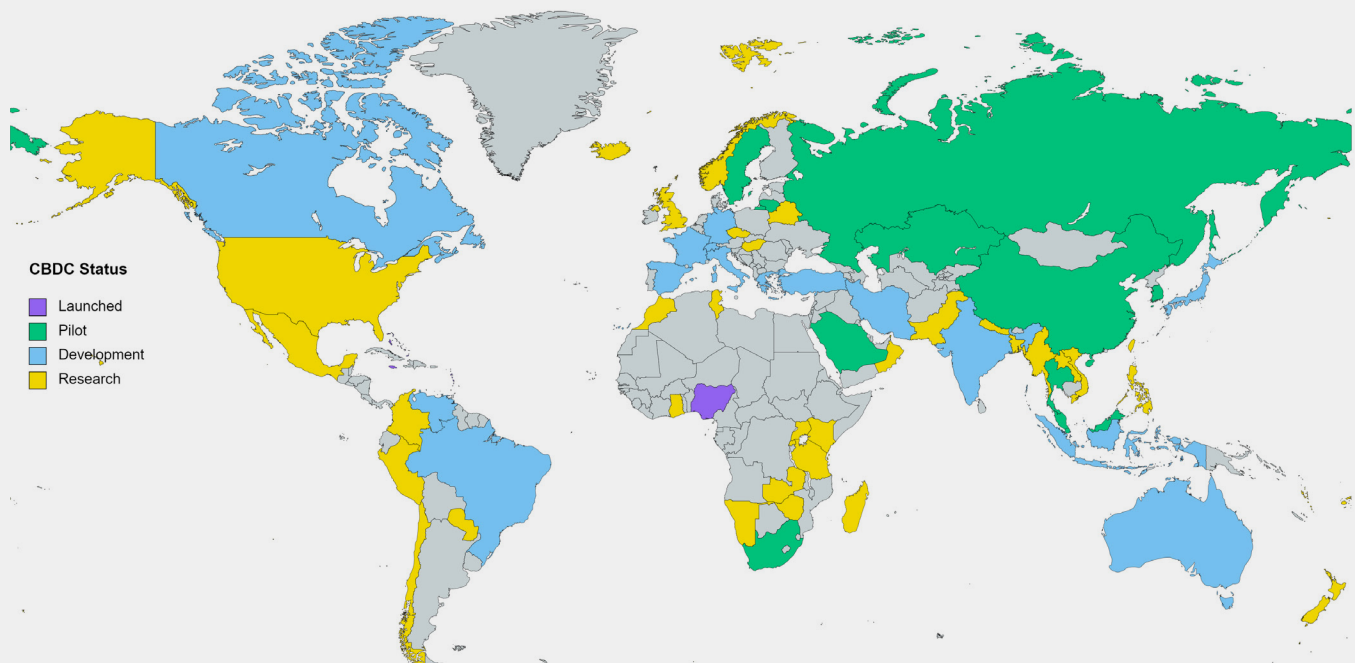
- **The issuer.** Currently, fiat-backed stablecoins are issued by private enterprises, whereas CBDCs would be issued by a government entity or a central bank.
- **The type of reserves backing the token.** Fiat-backed stablecoins require full backing of the stablecoin. For CBDCs, there are 2 main designs being explored: (i) insured deposits – the conventional method used by commercial banks in fractional reserve banking systems where deposits for the token may be partially backed by cash and the rest of it backed with risk assets including bank loans, treasuries and securities, or (ii) narrow banking, a “safer” alternative to insured deposits where reserves for the token would be backed solely by the good faith of the central bank and its reserves. This would require central banks to hold user accounts.
- **The distribution of the token.** The type of reserves used to back the token would also influence the distribution of the token. Under the narrow banking model, distribution of the token would likely result in the central bank directly distributing digital currencies to financial institutions and individual citizens. The insured deposits model would likely rely upon the two-tiered banking system, where CBDCs would issue digital currencies to commercial banks, which would then distribute them to businesses and consumers.

Another consideration for a CBDC not mentioned above is the technology stack upon which the CBDC is built. Stablecoins are already a form of programmable, composable digital currency that developers can build upon. Given that central banks and governments appear to be seeking to utilize blockchain technology to augment, rather than replace, their national currencies, it is almost certain that CBDCs will be issued on their own permissioned technical network. Building CBDCs in a closed system would create headwinds for integrating with existing systems and infrastructure, which would represent a big disadvantage to existing stablecoins. And regardless of which type of technical architecture is chosen, successfully building it out will be a major lift with technical and financial risks for central banks in seeking to provide a useful tool for interbank settlements (wholesale), or for businesses & consumers (retail).

Multiple CBDC designs are being explored by central banks across the globe. China is the furthest along in the deployment of a CBDC among major economies with its Digital Currency Electronic Payment (DCEP), also known as the “digital yuan.” The US is also exploring a CBDC, though its efforts to date have been more tenuous than those of other central banks. In January 2022, the Federal Reserve released a paper titled [“Money and Payments: The U.S. Dollar in the Age of Digital Transformation,”](#) intended to start a public discussion on the pros/cons of a potential US CBDC. Importantly, the Fed’s paper does not commit the Fed to issuing a

CBDC Global Tracker

Source: Galaxy Digital Research



Source: Atlantic Council CBDC Tracker (created with mapchart.net)



Fed Dollar nor does it commit the Fed to any specific design. The paper also notes: “The Federal Reserve’s initial analysis suggests that a potential U.S. CBDC, if one were created, would best serve the needs of the United States by being privacy-protected, intermediated, widely transferable, and identity-verified.” Ultimately, the paper doesn’t convincingly make the case that there exists any problem requiring a solution, nor that a CBDC would be the appropriate solution even if there was one.

Fed Chair Jerome Powell has [stated](#) in the past that in creating a CBDC (which would likely require new legislative authority to do so), it would not preclude “well-regulated, privately-issued stablecoins” from co-existing and that the Fed would not seek to undermine the two-tiered banking system: “We don’t want to destabilize the two tiered system... Central banks interface with banks, banks interface with the public, and we do not want to destabilize that, and therefore we don’t want to compete with banks for funding.” Yet, many share concerns over the implications that a CBDC may have on privacy and on the dollar’s global competitiveness. A CBDC could potentially enable the Fed to monitor every digital transaction made, implement burdensome KYC/AML registration and reporting requirements that could prohibit financial inclusion and slow the pace of innovation, and possibly deter digital financial services firms, particularly those abroad, from using the dollar. Rep. Tom Emmer (MN-06) introduced a [bill](#) prohibiting the Fed from issuing a CBDC directly to individuals, warning of a slippery slope that would be akin to “digital authoritarianism.”

The Fed is still studying whether a privacy preserving CBDC is possible and what could be the potential design of a Fed CBDC based on the potential risks/benefits of each design consideration. In May 2022, Fed Vice Chair Lael Brainard wrote in her [testimony](#) in front of the House Financial Services Committee that a CBDC would not be mutually exclusive to privately-issued stablecoins: private stablecoins from existing: “[CBDC could coexist with and be complementary to stablecoins and commercial bank money](#) by providing a safe central bank liability in the digital financial ecosystem, much like cash currently coexists with commercial bank money.”

Regulation Outside the US

The EU

In July, the EU reached agreement on Travel Rule and MiCA as part of comprehensive regulatory framework for cryptoassets. After months of deliberations between the EU Parliament and Council, an agreement was reached on: (i) the implementation of the **Transfer Funds Regulation (TFR)**, and on (ii) **Markets in Crypto-assets (MiCA) Regulation**. With regards to MiCA, the EU’s first attempt at a comprehensive regulatory framework for cryptoassets (and the first for a major global economy), more authority is granted to ESMA (European Securities & Markets Authority) to oversee crypto activity. As it relates specifically to stablecoins, MiCA puts in place new stricter standards for stablecoin issuers – per [Ernest Urtasun](#), an EU lawmaker involved in the negotiation:

“Large stablecoins will be subject to strict operational and prudential rules, with restrictions if they are used widely as a means of payment, and a cap of 200€millions in transactions/day. Stablecoins will have to maintain reserves to cover all claims and provide redemption rights of the holders. The reserves will have to be legally and operationally segregated and insulated in the interest of the holder, and will be fully protected in case of insolvency.”

At the time of writing, the new agreements must receive formal votes in the Parliament before the TFR and MiCA come into force. Impacted crypto entities under MiCA and the TFR will have a transition period to implement the new rules, which will be 18 months after the entry into force (~early 2024). At that time, legislators will review the regulation and assess whether fewer/more measures are needed.

Europe is taking the global lead when it comes to regulating cryptoassets, which will certainly influence how other economies shape their regulatory frameworks to oversee the industry. Part of this accelerated legislation may have been influenced by crypto’s usage in the Ukraine conflict (even though top US officials from the White House and Treasury Department have asserted that crypto would be ineffective for Russia to circumvent sanctions). The EU’s lead on crypto regulation may encourage some crypto-related business to migrate to less restrictive jurisdictions, but its policy framework also serves as a form of quality control that provides assurances for market participants to interact with licensed tokens and licensed crypto intermediaries. Whether or not the EU’s lead on regulating crypto ends up benefitting its global competitiveness will depend on how other policymakers around the globe react.

The UK

The United Kingdom has announced legislation to regulate stablecoins that are used as a means of payment. The regulation will be included in the more comprehensive Financial Services and Market Bill, which aims to “strengthen the United Kingdom’s financial services industry” by “seizing the benefits of Brexit.”

In May 2022, HM Treasury released a 40-page report outlining their recommendations for stablecoin and crypto regulation, stating that fiat-backed stablecoins “have the capacity to potentially become a widespread means of payment.” HM Treasury is currently in an [open consultation period](#) for “Managing the failure of systemic Digital Settlement Asset (including stablecoin) firms,” set to close by August 2nd.

The UK will likely mirror the EU in many aspects of regulation including AML/CFT and stablecoin issuance; however, it appears that overall, the UK has a more favorable view of stablecoin potential and will perhaps will more approach the industry with more leniency. Tether, citing the U.K.’s aim to make stablecoins a valid form of payment and the U.K a global hub for crypto, has already launched a stablecoin pegged to the British Pound Sterling (GBPT) in July.



Later in July, the UK Parliament introduced the [Financial Services and Markets Bill \(FSMB\)](#)—the first and primary legislation to regulate financial services and crypto-related activities in the UK post-Brexit. The FSMB intends to create a new regulatory framework separate from existing EU legislation that will improve the global competitiveness of the UK and establish the UK as an open financial

hub. The Bill introduces new rules overseeing digital settlement assets (including crypto) as it relates to payments, transfers, and storage, though the Bill does not specifically mention “stablecoins.” Under HMG’s plans, issuers of in-scope stablecoins would need to seek a license from the FCA under the Electronic Money Regulations and apply prudential and conduct of business standards.

Outlook

Stablecoins, along with their underlying blockchains, have come a long way since their early days when they were only used for transacting to and from centralized exchanges that lacked access to bank accounts. Today, stablecoins have clearly become one of blockchains’ breakthrough applications. Stablecoins continue to find adoption in real-world use cases like treasury management, international B2B, cross-border remittances, and e-commerce, among other payment flows. These integrations will continue as the underlying infrastructure continues to mature. And the market for bridging between fiat and crypto not just confined to issuers like Circle and Paxos. Indeed, DeFi integrations, led by MakerDAO’s real-world asset initiative, is also beginning to capture new sources of payments and money movements between institutions and individuals.

In the wake of Terra USD’s collapse, market participants have given preference to the safer, “stabler” stablecoins. This includes a general decline in Tether’s market share, which will continue eroding unless it repairs its long-standing trust problem and manages to preserve its competitive moat that separates on- and off-shore issuers in the absence of regulation. But efforts to build a comprehensive regulatory framework have been progressing rapidly as seen with Europe’s finalized MiCA bill and the on-going conversations among US legislators. These regulatory efforts will likely drive fiat-backed stablecoins to converge on a common model, eventually forcing them into a winner-take-all market.

Despite the likelihood that fiat-backed stablecoins become codified and converge, however, the crypto backed stablecoins seen today are not necessarily redundant products as they can serve many different purposes than their fiat-backed brethren. While fiat-backed stablecoins are subject to stringent regulation and are much less flexible in their designs, crypto-backed stablecoins have more room to experiment and iterate on UX and safety. Crypto users deserve to have a choice between which stablecoins they use, but it’s important that they are made aware of the risks and trade-offs inherent in each of the designs.

DAI’s growth in recent months demonstrates that radical transparency in operations and communications, conservative design, and an established history go a long way in building the trust that is needed for stablecoins to succeed as money. Yet, DAI’s current title as the leading “decentralized stablecoin” leaves much to be desired. MakerDAO’s PSM mechanism was successful in stabilizing DAI, but it has led to USDC becoming the dominant asset in its reserves, undermining the system’s decentralization. Overcollateralized stablecoins can only be as decentralized as assets held in their reserves just as DeFi applications can only be as decentralized as the underlying platforms upon which they are built. With such a heavy reliance on centralized technology, trustless transparency and protection against extraordinary disruptions is not guaranteed for DAI.

Recent events from this year have demonstrated the problems with centralized, trusted set-ups (e.g., the [Canadian trucker protest](#) in February, the unraveling of major CeFi lenders and funds, and [protests in China](#) over bank scams & frozen assets). Each of these incidents leads to increasing public appreciation of decentralization and censorship-resistance. These incidents will likely continue to occur, along with more de-pegs of stablecoins, as we navigate the challenging macro environment. While some of the attention following these centralized failures goes and will continue to go to native digital assets like Bitcoin and Ether, we expect significant interest to flow to censorship-resistant stablecoins, if they exist. And while some stablecoin failures may overshadow the hard work of builders and slow the pace of experimentation for algorithmic designs, the evolution of stablecoins certainly isn’t going to stop at USDC and DAI. Hard times build hard money, and the stablecoins that endure the toughest challenges are likely to gain share and thrive.



Predictions

- **Fiat-backed stablecoins will lead in finding real world adoption compared to other types.** When it comes to business development and driving stablecoin integrations, fiat-backed issuers have an advantage of operating more closely with traditional enterprises and regulators. They also have more physical resources and employees, enabling them to drive more face-to-face discussions to onboard adopters and to support them on an on-going basis. In contrast to fiat-backed issuers, crypto-native stablecoin protocols have small employee bases, opting to drive labor efficiencies through smart contracts – which will still take time to fully realize those benefits. Having greater employee level of support is important especially when education remains one of the primary headwinds for expanding acceptance points and capture new sources of money movements. Maker has made some impressive progress on its RWA initiative, but any further RWA adoption for Maker will likely be outpaced by fiat-backed issuers.
- **Stablecoins will be used more for commerce payments, which will be led by new ecosystem players.** Traditional banks are expected to eventually launch their own stablecoins but have yet to enter the stablecoin arena. However, when it comes to development of new digital payment rails, banks will be hindered by their existing financial relationships with the card networks, payment processors, merchant acquirers, and central banks. As it relates to commerce adoption, Coinbase has long offered Coinbase Commerce, Block (fka Square) has adopted LN to facilitate bitcoin payments, PayPal has offered crypto-funded payments through its closed-loop payment network and [confirmed](#) it was exploring its own stablecoin product. Fintechs that own relationships with both merchants and consumers can innovate faster than banks as they are more unencumbered in banking relationships and can leverage open monetary networks (such as Lightning Network or Solana Pay integrations) to deliver the cost and speed efficiencies of stablecoin payments to consumers and merchants.
- **Interest-bearing fiat-backed, custodial stablecoins to emerge.** Among the fiat-backed stablecoins, there is a market opportunity for an issuer to develop a coin that pays users all or a portion of the interest generated by the underlying collateral. Several decentralized stablecoins have experimented or enacted this feature, but we expect to see this model attempted with centrally issued stablecoins. The success of these digital dollars has reinvigorated institutional interest in other bespoke financial use cases for blockchain technology, and we expect an institutional-grade, interest-bearing stablecoin to be one of the big projects that emerges in the next few years.
- **Each platform will establish its own preferential, native stablecoin.** Utility of stablecoins comes from integrations in the banking and DeFi ecosystems. Without any integrations, the only use of a stablecoin may be to swap for more useful stablecoins – which is hardly a productive use case. Stablecoins are a network effect business and forming these types of integrations with outside parties first requires building trust or strong financial incentives to drive adoption. More ecosystems will select a preferred native-stablecoin option to support its adoption by facilitating integrations and dedicating ecosystem resources to build trust in the stablecoin (already starting to take hold on several emerging ecosystems such as Polkadot-Acala USD, Fantom-fUSD, Optimism-sUSD).
- **DeFi protocols with their own stablecoin products will evolve into super dApps.** As we have mentioned, building out non-speculative demand for the stablecoin is necessary for the stablecoin to be competitive. Lending protocols with stablecoins must constantly devote financial resources for peg support – most have been utilizing native token emissions or other non-native owned assets which is value extractive for the protocol and token holders (this includes Curve bribes). Platforms have been adding to their product offerings to generate additional revenues to cover their expenses (e.g., DEXes, AMOs, yield, bridging, payments, NFTs) – this evolution towards super dApps forms a competitive moat that will benefit protocols that aggregate the widest product offerings.
- **Solving for capital efficiency: rather than starting uncollateralized, new algorithmic stablecoins will mostly start collateralized and become more undercollateralized over time.** Having sufficient collateral and liquidity backing is a key determinant for the success of algo stablecoins. New emergent algo stablecoins solving for capital efficiency will not be uncollateralized at issuance; instead, they will start collateralized and gradually become more undercollateralized over time.
- **Noncustodial stablecoins will aim to be less reliant on USDC for stability.** The top crypto-native stablecoins—DAI and FRAX—are heavily reliant on USDC for explicit backing, and many more may be indirectly reliant on USDC for stability in arbitrage structures. Establishing a separate reserve of exogenous assets to support price stability will become more standard and there will be greater emphasis on reducing reliance upon custodial stablecoins (i.e., USDC and USDT) in favor of more decentralized reserve assets (e.g., BTC and ETH).
- **Third-party risk management services will be increasingly relied upon.** Longer operating histories of stablecoins and lending protocols provides better understanding of credit positions and risk parameters. Third-party risk management services such as auditors, consultants, simulation & testing, and insurance providers already exist, but their modeling and underwriting practices will continue to improve and will be increasingly relied upon for noncustodial stablecoins. Specialized credit scoring providers will create real-time risk dashboards to flag any key risks for both protocols and users as they arise.



Contact Us

■ galaxy.com/research

For all inquiries, please email
charles.yu@galaxy.com or research@galaxy.com.

Legal Disclosure

■ This document, and the information contained herein, has been provided to you by Galaxy Digital Holdings LP and its affiliates ("Galaxy Digital") solely for informational purposes. This document may not be reproduced or redistributed in whole or in part, in any format, without the express written approval of Galaxy Digital. Neither the information, nor any opinion contained in this document, constitutes an offer to buy or sell, or a solicitation of an offer to buy or sell, any advisory services, securities, futures, options or other financial instruments or to participate in any advisory services or trading strategy. Nothing contained in this document constitutes investment, legal or tax advice or is an endorsement of any of the stablecoins mentioned herein. You should make your own investigations and evaluations of the information herein. Any decisions based on information contained in this document are the sole responsibility of the reader. Certain statements in this document reflect Galaxy Digital's views, estimates, opinions or predictions (which may be based on proprietary models and assumptions, including, in particular, Galaxy Digital's views on the current and future market for certain digital assets), and there is no guarantee that these views, estimates, opinions or predictions are currently accurate or that they will be ultimately realized. To the extent these assumptions or models are not correct or circumstances change, the actual performance may vary substantially from, and be less than, the estimates included herein. None of Galaxy Digital nor any of its affiliates, shareholders, partners, members, directors, officers, management, employees or representatives makes any representation or warranty, express or implied, as to the accuracy or completeness of any of the information or any other information (whether communicated in written or oral form) transmitted or made available to you. Each of the aforementioned parties expressly disclaims any and all liability relating to or resulting from the use of this information. Certain information contained herein (including financial information) has been obtained from published and non-published sources. Such information has not been independently verified by Galaxy Digital and, Galaxy Digital, does not assume responsibility for the accuracy of such information. Affiliates of Galaxy Digital own investments in some of the digital assets and protocols discussed in this document. Except where otherwise indicated, the information in this document is based on matters as they exist as of the date of preparation and not as of any future date, and will not be updated or otherwise revised to reflect information that subsequently becomes available, or circumstances existing or changes occurring after the date hereof. This document provides links to other Websites that we think might be of interest to you. Please note that when you click on one of these links, you may be moving to a provider's website that is not associated with Galaxy Digital. These linked sites and their providers are not controlled by us, and we are not responsible for the contents or the proper operation of any linked site. The inclusion of any link does not imply our endorsement or our adoption of the statements therein. We encourage you to read the terms of use and privacy statements of these linked sites as their policies may differ from ours. The foregoing does not constitute a "research report" as defined by FINRA Rule 2241 or a "debt research report" as defined by FINRA Rule 2242 and was not prepared by Galaxy Digital Partners LLC. For all inquiries, please email contact@galaxydigital.io.

©Copyright Galaxy Digital Holdings LP 2022. All rights reserved.