RedStone

Stablecoins Report:

The Ultimate **2023** Market Overview

Table of Contents

1. Key Takeaways **3**

- Featured Projects & Stablecoins 3

2. What are Stablecoins? **4**

- Types of Stablecoins 4
- Fiat-backed Stablecoins 5
- CDPs: Collateralized Debt Position Stablecoins 6
- Algorithmic Stablecoins 7
- Which stablecoin should I use? 8

3. Oracles: the backbone of CDPs and algorithmic stablecoins **9**

- Stablecoins x Oracles: MakerDAO and Mento case studies 10

4. CDP Stablecoins: A deep dive **11**

- CDPs: The 2023 Market Overview 12
- LSTs-backed CDP Stablecoins: Future or Fad? 14
- Fresh Stablecoin Giants crvUSD and GHO 15

5. Algo-Stables, the Holy Grail of Web3? **18**

- The Two Successful Use Cases 18
- Algo-issues 19
- UST and Terra Collapse 19

6. What Can We Expect Next in The Stablecoins Space? **21**

- Algorithmic Approach 21
- RWA Approach 21
- Elastic Approach Based on Demand 22

7. Conclusions **23**

References 23

About RedStone Oracles 24

Resources 24

1 Key Takeaways

- Stablecoins are cryptocurrencies whose value is pegged to a fiat currency, commodity, or financial instrument, most commonly the US Dollar.
- There are multiple types of stablecoins, the most popular are Fiat-backed, Collateralized Debt Position (CDP) and Algorithmic versions of stable assets.
- Fiat-backed stablecoins offer greater capital efficiency but are issued by a centralized party, therefore DeFi dApps expand adoption of CDP and algorithmic stablecoins.
- Oracles play a crucial role in decentralized price stability mechanisms. Very often, they are a cornerstone in stablecoin design and their utilization will continue to grow as more stable assets are managed by algorithms and smart contracts.
- Algorithmic stablecoins have massive potential in DeFi, but only very few have found a robust design with security measures and reliance on trusted oracles.
- Stablecoins backed by Liquid Staked Tokens (LSTs) like Lybra, Raft and Gravita are gaining significant traction, being fueled by the growing popularity of tokens like stETH, wstETH, rETH, swETH, frxETH and other LSTs.
- The collateral types for stablecoins are expanding, with the Real World Assets (RWA) tokenization playing an increasingly important role.

Featured Projects & Stablecoins

Fiat-Backed	CDP		Algorithmic	RWA Backed
Tether (USDT)	MakerDAO (DAI)	Lybra (eUSD)	Frax (FRAX)	Ondo Finance (OUSG)
Circle (USDC)	Liquity (LUSD)	Raft (R)	Mento (cUSD, cEUR, cREAL)	Backed Finance (bTokens)
Paxos (BUSD)	QiDao (MAI)	Gravita (GRAI)	OlympusDAO (OHM)	
TrueUSD (TUSD)	Vesta (VST)	Alchemix (alUSD)	Gyroscope (p-GYD)	
	Angle (agEUR)	Aave (GHO)	Terra (UST)	
	Abracadabra (MIM)	Curve (crvUSD)		
	Overnight (USDC+, DAI+, USDT+)			

2 What are Stablecoins?

A stablecoin is a digital asset whose value is price-pegged to another asset class, such as a fiat currency, commodity, or financial instrument. Let us break down key stablecoins characteristics:

1. The vast majority of stablecoins are tied in value to the US Dollar (USD)
2. Stablecoins are issued by a centralized party i.e. a company, or a decentralized party like a DeFi protocol. In both cases, they operate on various blockchains
3. Users should be able to mint stablecoins against provided collateral in the form of fiat or cryptocurrencies and redeem stablecoins back at their will
4. Stablecoins are the backbone of crypto trading and the DeFi ecosystem

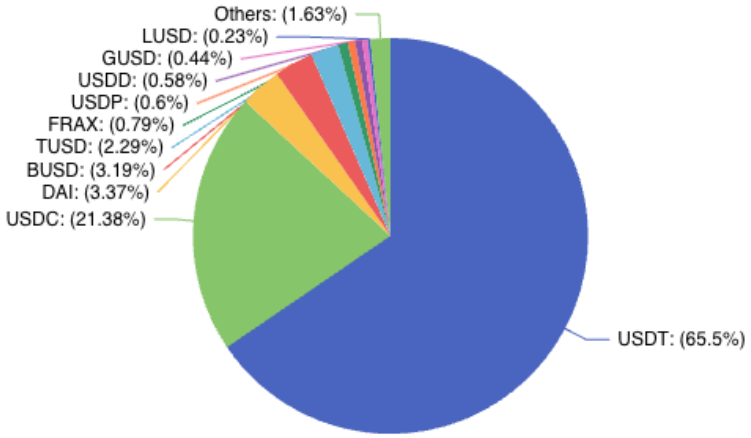
In point III. we specifically use the word should, since in the case of stablecoins issued by centralized entities, they can pause the minting and withdrawal process in turbulent market conditions (i.e. March 2023 USDC periodical depeg). In contrast, decentralized stablecoins operate unless the DAO governance decides to pause it, which is usually a decision tokenholders take upon voting. In the case of centralized issuers, they control fiat currency flow into crypto by storing fiat and minting digital equivalents. In simple words, they convert cash 1:1 into stablecoins. On the other hand, decentralized protocols are permissionless and accept various forms of cryptocurrencies and tokenized assets like ETH, BTC, stETH as collateral. Smart contracts handle funds and execute user actions in an immutable and irreversible way.

Stablecoins are an important link in the trading world, offering constant value (most of the time) and shielding investors from volatile token prices. Stablecoins are for crypto markets what havens are for shipping companies. A safe and stable environment, which allows the explorer to get ready and plan the next marine or investing endeavour. In addition, stablecoins are responsible for the vast majority of digital asset volume. The relationship between stablecoins is crucial for the stability of the whole crypto market, i.e. on Curve 3 Pool with USDT, USDC and DAI, which operates like a sort of on-chain FOREX. Stablecoins serve as an on-ramp for investors to bring assets on-chain and often as an off-ramp to return to the USD or other fiat currency. Moreover, they not only cover the spot market but also serve as a primary settlement option for synthetic markets such as futures, perpetual futures and options.

Types of Stablecoins

Stablecoins are the lifeblood of the crypto landscape. Every cryptocurrency widely adopted on the market is exchangeable in pairs to stablecoins, which helps to limit volatility. As stablecoins aim to maintain a steady value, price fluctuations depend solely on the paired asset. However, it wasn't always this straightforward. In the pre-stablecoin era, most assets were BTC-paired, which led to variable fiat returns due to constant exposure to fluctuations in the crypto market. This often resulted in a challenging trading experience as traders had to constantly calculate volatile returns in fiat terms. The situation used to be quite analogous to the Impermanent Loss dilemma associated with liquidity provision on decentralized exchanges.

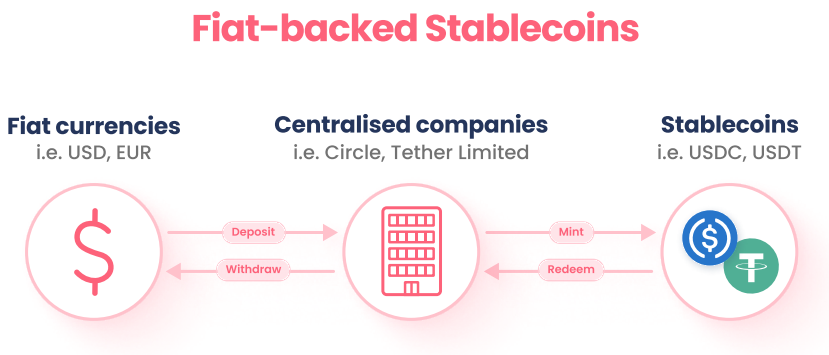
The first stablecoins arrived in 2014. Since then, the stablecoins market share has exponentially grown to a capitalization of $130B and 11% of the total cryptocurrency market cap at the time of writing (Source: Coingecko). The lion's share of stablecoins is pegged 1:1 to the US dollar, but market movements can affect their price performance and trade both over and under the dollar's rate. Theoretically, stablecoins should have a constant value, offering an oasis in the ever-changing cryptocurrency market. That is why they are the preferred means of storing value and are used in DeFi, CeFi, yield-bearing solutions, futures, and more. Nowadays, we have different types of stablecoins with distinct designs and mechanisms.



Market share of particular stablecoins as of July 2023. (Source: DeFiLlama)

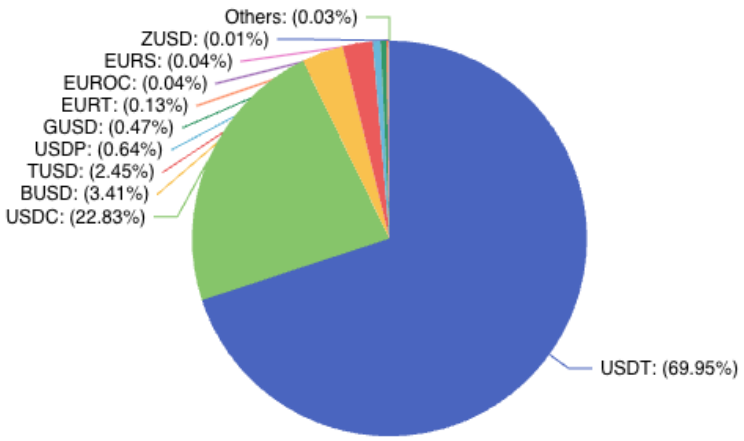
Fiat-backed Stablecoins

The most popular are fiat-backed stablecoins, redeemable to the underlying currencies. The ones with the highest market capitalization are USD Tether (USDT), USD Coin (USDC) issued by Circle, and Paxos's Binance USD (BUSD). These institutions issue and redeem tokens based on their reserves' balance. Without delving into the details of reserve credibility, let us briefly explain the issuance mechanism. Clients deposit fiat currencies, primarily USD, and, in return, they receive an on-chain counterpart of a deposited currency like USDT or USDC, which, in some cases, may be with associated fees. It is worth mentioning that stablecoin issuers are not holding all the assets in cash. They are diversifying portfolios converting funds into other financial instruments such as treasury bills, gold or even Bitcoin.



A simplified flow of funds in Fiat-backed stablecoins.

Every stablecoin comes with its own set of pros and cons. Tether's management history and reserve guarantees have been called into question, although USDT is undoubtedly the biggest player, accounting for 64% of the total market share. The second biggest player, Circle, was tested in March 2023, while over 8% of its reserves were held by the collapsing Silicon Valley Bank (SVB), which led to a temporary de-peg. Admirably, Circle willingly decided to issue balance statements regularly and its monthly flows are positive. Nevertheless, for both Tether and Circle, managing billions of dollars in user funds is an ongoing trade-off in security and capital efficiency. Regulatory uncertainties greatly impact crypto firms like Paxos, which ceased minting new BUSD in early 2023. This event stirred upheaval on Binance, the major BUSD recipient, with almost all of the tokens listed by the exchange being paired to BUSD. In response, Binance reinforced its alliance with TrustToken, the TUSD issuer. However, on June 28th 2023, TUSD depeged at Binance US, which resulted in trust decline and proposals on protocols such as Aave to freeze deposits or borrowing of TUSD. Issues with BUSD have paved the way for decentralized stablecoins as well, particularly Liquity's LUSD. Due to a relatively simple design and widespread adoption among centralized exchanges (CEX), fiat-backed stablecoins are responsible for the industry's liquidity and are the essential medium for assets on and off-ramp in crypto.

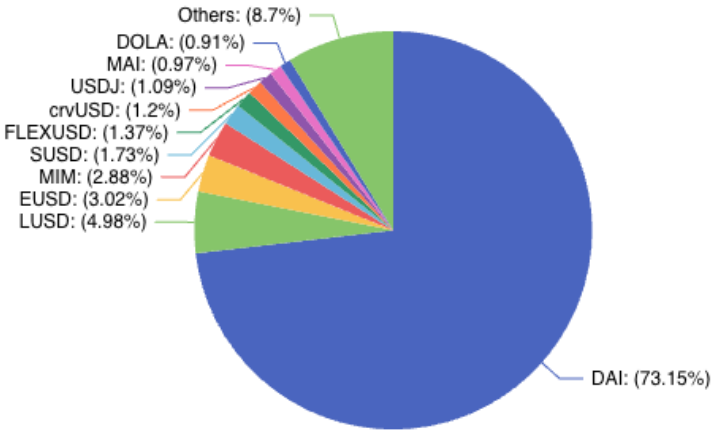


Fiat-backed stablecoins market share as of July 2023. (Source: DeFiLlama)

CDPs: Collateralized Debt Position Stablecoins

Next in line are Collateralized Debt Position (CDP) stablecoins, with a somewhat similar concept to CDOs (The Big Short explainer video). Users wishing to mint CDP coins must provide collateral in the form of other cryptocurrencies. This concept was introduced in 2015 by MakerDAO, who created Dai in 2017, which at the time was a Single Collateral Debt stablecoin (ETH was the only collateral, same as LUSD currently). Later in 2019 the team introduced multi-collateral options, which is Dai as we know it today, and keeping single collateral as Sai. It is the world's first crypto-collateralized and decentralized stablecoin. The collateralized assets backing CDPs are other cryptocurrencies instead of fiat and are held within smart contracts rather than in institutions. Collateralized debt positions are a growing class of stablecoin with a number of innovative projects emerging in recent years. They differ in terms of collateral types and ratios, interest rates, available networks, and safety measures. Regarding Total Value Locked (TVL), the biggest protocols include MakerDAO, Liquity, and Abracadabra. The latter two offer LUSD

and MIM, respectively. Liquity is a single-collateral project with ETH as the only available option. It is straightforward, simple, and immutable since nobody, not even the core team, can upgrade the Liquity smart contract anymore. Abracadabra will suit more advanced DeFi participants by providing diversified cryptocurrencies, including stablecoins, and derivative tokens as collateral. Thanks to CDPs, users can leverage their holdings and gain access to stablecoins without ultimately selling their assets.



CDP stablecoins market share as of July 2023. (Source: DeFiLlama)

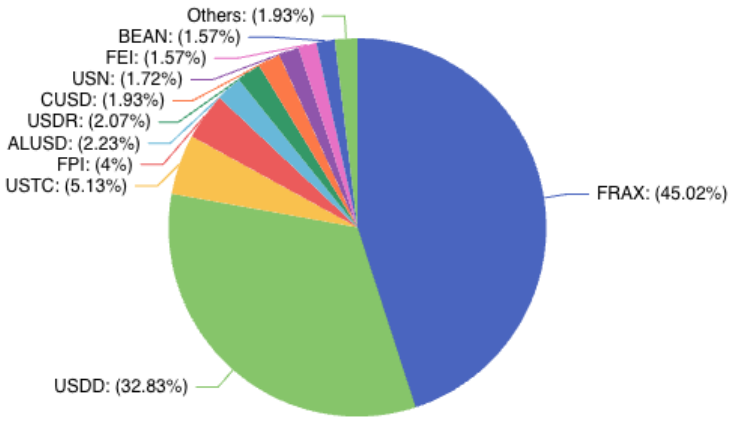
Algorithmic Stablecoins

The algorithmic stablecoin is another variation on a token with a value following the US dollar price. Its design maintains price stability through code and smart contract utilization and automatically adjusts the stablecoin's supply based on market conditions and demand. Usually, algorithmic stablecoins operate in two-coin systems where the first tries to remain pegged, and the other absorbs all the volatility. In simple terms, when a stablecoin's price is higher than $1, the demand is too high and the supply is too low. The algorithm makes adjustments by minting new coins (actual stable or balancing tokens). Steps work in the opposite direction when the peg falls below $1. Such a mechanism works well in theory, but so far hardly any algo-stablecoin has gained enough trust and popularity to be a truly widespread solution, especially after TerraUSD (UST) crash in 2022, which we will discuss later in this report.

Different projects have original approaches to algorithmic stablecoins. A few types have emerged: arbitrage/seigniorage, rebasing, and hybrid (fractional). TerraUSD was (technically still is, renamed as USTC) an arbitrage algo-stablecoin working between two pools of UST and LUNA. Another approach applied by Mento Protocol incorporates arbitrage techniques as a price stability mechanism with no balancing token and a conservative risk approach. Originating on the Celo blockchain, the protocol offers cUSD, cEUR, and cREAL stablecoins and looks to expand cross-chain. Mento holds over 200% collateralization ratio with a 1:1 backing in USDC and DAI and additional assets in CELO tokens and other cryptocurrencies like BTC and ETH.

Ampleforth (AMPL) is pioneering the rebasing stablecoin concept. Its system adjusts supply daily based on deviations from the target price. When it is below the target, additional tokens are distributed to existing holders, diluting the value of each AMPL

token. Conversely, when it is above the target, AMPLs are removed from circulation, reducing the supply and increasing the tokens' value. The last subcategory is fractional-algorithmic stablecoins, like FRAX, that combine elements of collateralization and algorithmic mechanisms to achieve stability. The FRAX token follows USD price, employing re and decollateralization mechanisms in conjunction with FXS token balancing.



Algorithmic stablecoins market share as of July 2023. (Source: DeFiLlama)

Which stablecoin should I use?

There is a variety of stablecoins suited to various users, including individual investors, DeFi users, and institutional clients. Centralized entities are responsible for the issuance, storage, and redemption when it comes to fiat-backed stablecoins. Cash goes in, and coins are issued for a small fee. Smart contracts manage Collateral Debt Position stablecoins where users lock assets as collateral and borrow CDP stablecoins. Service is accessible through decentralized protocols on various Layer 1 and Layer 2 networks. A loan requires monitoring because it depends on deposit value, which can change in the volatile crypto market. Finally, algorithmic stablecoins operate based on the code and relations between demand and supply and usually two-coin architecture. They are an innovative solution to a stable currency but can include new risks. Naturally, each type of stablecoin is available on the market, DeFi and CeFi, where users can purchase or sell them without minting/issuing or burning/redeeming.

The table below provides an overview of the key factors to consider when choosing which stablecoin to use.

	Type of collateral	Collateral ratio	Issuer	Relative Risk
Fiat-backed	Fiat currencies, mostly USD	100%	Centralized entities	Relatively low
CDPs	Cryptocurrencies like ETH, BTC, USDC or other assets like LSTs or RWA	Over 100%, usually between 110% - 150%	Decentralized protocols; some immutable	From low to high, depending on the design
Algorithmic	Usually a mix of stablecoins & cryptocurrencies	Stablecoins below 100%, usually around 90/10 ratio	Decentralized protocols	From low to high, depending on the design

3 Oracles: the backbone of CDPs and algorithmic stablecoins

Due to the fact that fiat-backed stablecoins like USDC or USDT are also fully collateralized with USD, the value of collateral should always be at least equal to the amount of issued stablecoins. In practice, centralized entities invest deposited funds into financial instruments yielding interest like US T-Bills or commodities like gold, in order to accrue excess reserves. For example in May 2023 Tether's CTO Paolo Ardoino announced over 2.5 Billion USD (equivalent) in the company's own excess reserves, which accounted for about 3% of issued stables, resulting in almost a 103% collateral ratio.

The story is quite different in the case of CDPs and Algo-stables. Both types mint stablecoins against deposited reserves in cryptocurrencies, which by nature are volatile. In order to omit bad debt, protocols need a reliable and robust pricing infrastructure of assets they accept as collateral. That is where Oracles play a crucial role and ensure the whole system holds, even during periods of market turbulence and black swan events. Oracles, such as Chainlink, Chronicle or RedStone, aggregate pricing information of assets from multiple sources and provide it to protocols' stability mechanism, which ensures that the health factor for each loan is above a certain threshold. If the oracle reports that the ratio of the user's collateral to loaned stablecoins falls below a certain level depending on the protocol, i.e. 150%, assets locked in the smart contract can be liquidated to pay off minted stablecoins. If your position got fully liquidated, you keep minted stablecoins, but you cannot redeem them for locked assets anymore, meaning you can be left. with, for example, less than 70% of your initial value of locked assets. As one can appreciate, becoming involved in such a flow only makes sense if your collateral holds or appreciates and can be hurtful in the event of a sharp drop in collateral value. Cryptocurrency prices are volatile, and liquidations often happen during market crashes and black swan events. That is why CDPs must be overcollateralized at all times, giving the protocol a safety margin to liquidate a position and repay the loan to keep the system afloat.

CDP and Algorithmic stablecoins utilize oracles to trigger liquidations when needed, which allows for maintaining the 1:1 peg. Therefore it is of utmost importance to choose a robust, secure and suitable provider, as it is the heart making sure the organ works as intended. While choosing an oracle, stablecoins have to consider multiple factors such as, but not limited to:

- Availability of price feeds for accepted collateral types, i.e. ETH, wstETH, USDC
- Presence of oracle feeds on Layer 1 and Layer 2 networks, where the protocol intends to launch, i.e. Arbitrum, zkSync Era, Polygon zkEVM, Scroll
- Price feed update conditions, i.e. seconds/minutes/hours interval, deviation threshold, on-demand/on-chain delivery
- Transparency, security, decentralisation, sources and accuracy of price feeds

Stablecoins x Oracles: MakerDAO and Mento case studies

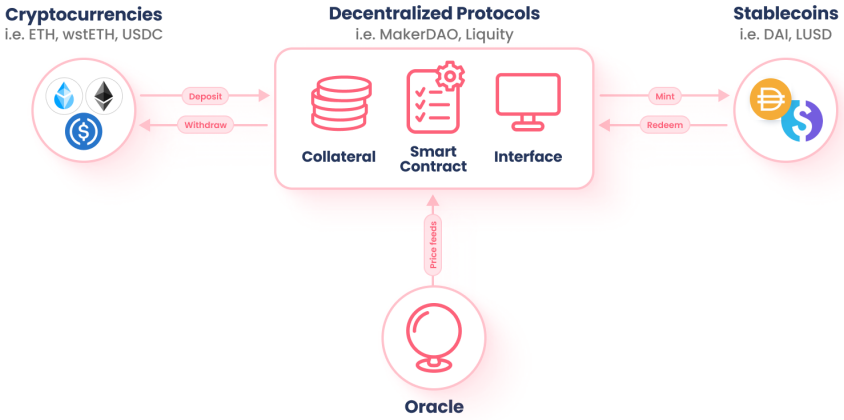
Let's take a look at a specific example of MakerDAO and DAI, the biggest and the oldest CDP stablecoin protocol. Currently, MakerDAO allows multiple collateral options such as ETH, wstETH, rETH, WBTC or USDC. All the following numbers are approximate.

Imagine Anon wants to borrow some DAI, so he opens a Low Fee ETH Vault and locks up 1 ETH as collateral to mint the DAI stablecoin against. At the time of writing, the Chronicle Lab's Oracle would report to MakerDAO the price of ETH at $1,812. The protocol would then calculate the value of the provided assets as 1 * $1,812 = $1,812, allowing the user to mint up to about 58% of that figure. Anon decides to mint 600 DAI worth $600, accounting for 33.11% of the cryptocurrency Anon locked. In the next month, Chronicle Labs reported that the value of both ETH appreciated by 20%, thus Anon's collateral is worth $2,174. Anon did nothing and the loan-to-collateral ratio dropped to 27.59%, making the loan safer. Unfortunately, the next month the market experienced a black swan event. Chronicle Labs reports a 50% drop in ETH, making Anon's locked position priced at $906, bringing the loan-to-value ratio to 66%. The dark scenario becomes a reality, Anon exceeds the 58% threshold and the Vault becomes undercollateralized. The Maker protocol automatically triggers a liquidation of Anon's Vault, transferring the collateral to the protocol and issuing DAO to Anon to cover the debt. An auction is started to sell Anon's collateral for DAI. Other users can participate in the auction using Flash Lending, which allows them to borrow DAI from other protocols to purchase Anon's collateral. The auction settles instantly, so the winning bidder receives the collateral immediately. Anon receives the remaining DAI from the auction after the debt and the liquidation penalty have been paid. Specific numbers vary from liquidation to liquidation, but we can assume that Anon's 1 ETH got liquidated, he keeps 600 DAI plus the liquidation process excess.

The second example of a quite different flow is implemented by Mento Labs, the issuer of cUSD, cEUR and cREAL algorithmic stablecoins on the Celo blockchain. Mento implements a stablecoin infrastructure that is monitored by RedStone Oracles, ensuring the stability of the system. By design, Mento holds a conservative +200% collateralization ratio, priced by RedStone data feeds, making their design highly secure in comparison to regular algo-stables.

Imagine Anon exchanges 100,000 USDC for cUSD stablecoin on Mento. At the time of writing, the RedStone Oracles would report to Mento Protocol the price of USDC at $0.99923. The circuit breaker smart contracts would verify that the price is within an acceptable price range. Next, the minting contracts would calculate the value of the provided assets as 100,000 * $0.99923 = $99,923. In the next month, USDC stabilised to $1 and CELO appreciates 20%, hence the value of the Mento reserves increases and creates an additional collateralization buffer. Unfortunately, the next month the market experienced a black swan event and CELO drops 60% and USDC de-pegged slightly to 0.9899. The total value of the reserve decreases but all outstanding stablecoins are still backed 1:1 by USDC, thanks to Mento stability mechanisms. Mento protocol does not have liquidation architecture and Anon will be able to exchange his cUSD back to the equivalent in USDC or CELO at any given time unless the stability mechanism goes down. Arbitrageurs ensure that cUSD market prices will revert towards 1 USD by trading with the Mento reserves at USDC and Celo price constantly delivered via price feeds by RedStone Oracles.

4 CDP Stablecoins: A deep dive



A simplified flow of funds in CDP stablecoins.

Stablecoins have emerged as an essential component of the cryptocurrency ecosystem, offering stability and mitigating the volatility commonly associated with digital assets. While they differ in their underlying mechanics, they share certain similarities. The fundamental goal for fiat-backed, CDP, and algorithmic stablecoins is the same – issuing stable tokens in exchange for deposited assets. Secondly, they strive to maintain a stable value relative to a specific benchmark where a majority is pegged 1:1 to the US dollar. But that is as far as the similarities go. While fiat-backed stablecoins rely on direct fiat currency reserves, collateral debt position stablecoins leverage collateral health factor mechanisms to maintain stability. Both types offer stability with diverse underlying mechanisms and cater to different use cases within the broader cryptocurrency space.

First and foremost, the differences between fiat-backed and CDP stablecoins are more noticeable and start at the core assumptions. CDPs only operate in DeFi and utilize other cryptocurrencies as collateral, whereas USDT and USDC are issued based on fiat currency deposits stored by institutions. Although the situation is changing as we speak with real-world assets (RWA) becoming collateral for some CDPs like MakerDAO.

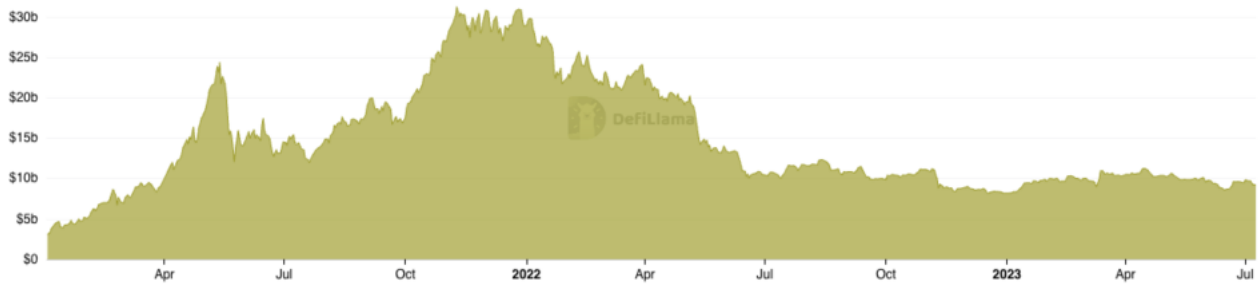
An important differentiator is that there is no third-party while using CDP protocols, contrary to fiat-backed stablecoins. Fiat-backed stablecoins are centralized, as they are released and managed by single entities. It introduces counterparty risk as users must trust the issuing entity to maintain the backing reserves. CDP stablecoins, however, are mainly distributed by decentralized protocols, often operating as decentralized autonomous organizations (DAOs). Protocols govern stability mechanisms, reducing reliance on a central entity while aiming for increased transparency.

Protocols issuing CDP stablecoins are a specific type of lending platform, like Aave, but one borrows newly minted stablecoins instead of other crypto assets. Users are responsible for monitoring the required collateral ratio for their positions with the help of monitoring dashboards. Because smart contracts execute and operate autonomously, borrowers must keep track of their positions' health factors, especially in turbulent market conditions. To avoid liquidation, users always have two options to boost their health factor: either repay part of the loan or add more collateral assets.

Overcollateralization is often cited as one of the most substantial drawbacks of CDP. Such a design is capital-inefficient since you need more collateral than you can borrow, and users who wish to obtain stablecoins must deposit the excess value of assets. The collateralization ratio (CR) is typically above 100%. For example, the CR of 150% means users must provide 1.5x the borrowed amount. Many projects fight this issue with lower CRs, more collateral options, and clever loan designs. Critics call this flow inefficient, compared to traditional finance (TradFi) design, where banks offer loans to individuals, who can ultimately default, whereas such a scenario is unacceptable in DeFi. Moreover, many juxtapose mortgage loans with DeFi, which require i.e. only a 25% collateral ratio in a scenario of a $200,000 down payment for an $800,000 loan to purchase a house, but the house is the asset that can be liquidated in case of default. But it's a whole other story, so we should investigate specific CDPs, shall we?

CDPs: The 2023 Market Overview

DeFi Llama lists over 25 CDP projects with TVL above $20M, but that metric changes rapidly over time. Let's take a look at a few projects that are renowned for their robustness, design, and market reputation.



CDP stablecoins cumulative TVL between Jan 2021 - July 2023 (Source: DeFiLlama)

Liquity, QiDao, and Vesta are decentralized and permissionless borrowing platforms, all offering collateral debt position stablecoins and CR for selected, usually highly liquid, assets as low as 110%. Liquity is the most conservative protocol, with ETH as the only collateral option. However, the more moderate approach lets the team focus on delivering the best single-asset borrowing solution. Liquity is simple and easy to use, utilizing ETH CDPs on the Ethereum blockchain. Loans are paid out in LUSD pegged to USD, however, the upcoming V2 could include other types of collateral, especially popular ETH LSTs.

"Liquity is a flagship example that a CDP stablecoin can work reliably – in a fully decentralized and autonomous way – without human governance. While such an approach has scalability limitations due to borrowing demand, our team is confident that we can eventually overcome them by pushing the boundaries even further," said Robert Lauko, Liquity Founder.

QiDao is a CDP stablecoin protocol. Users can access QiDao's solution via Mai Finance. Principle rules are the same as for every other non-custodial platform. Users' assets go in, and stablecoins go out. QiDao allows users to mint MAI. It is an overcollatralized stablecoin designed to match the US dollar price. The main distinguishing advantages

of QiDao are multiple collateral tokens and the variety of available blockchains. This diversity makes it suitable for DeFi users to always find something for their bespoke needs.

Vesta focuses on the Arbitrum network by providing users with loans and collateral debt position stablecoins. With Arbitrum being, at the time of writing, the largest Ethereum layer-2 scaling solution, Vesta aims to capitalize on the increasing popularity of the L2 by providing additional earning opportunities and leverage. The primary product of Vesta is VST, an overcollateralized stablecoin pegged to USD. Importantly, VST is backed by a variety of crypto assets, including ETH, wstETH, and GLP (liquidity token from GMX protocol). By providing stable liquidity pools and innovative interest/staking infrastructure, Vesta allows users to leverage their assets to earn additional yield or to increase their exposure to the crypto market. Another mutual characteristic these protocols share is an incentive mechanism, harnessing the power of the DeFi community. Liquity, QiDao, and Vesta created a token respectively: LQTY, Qi, and VSTA, to boost protocol usability. These tokens are associated with additional utilities such as governance or revenue capturing.

Abracadabra is a collateral debt position protocol that offers the ability to borrow a USD-pegged stablecoin called MIM (Magic Internet Money). It operates as a lending platform and introduces a unique feature wherein interest-bearing tokens, like yvWETH or xSUSHI, can be utilized as collateral. This characteristic makes it particularly attractive for participants in DeFi activities like liquidity provision, yield generation (on Yearn Finance) and staking. Leveraging the yield generated by interest-bearing tokens as collateral allows the protocol to increase the overall gains. An illustration of this capability is the magicGLP market, where an asset generating a 60% APY at the time of writing, can be further amplified to reach an APY of up to 250% using the MIM leverage engine. Nevertheless, as in the overall DeFi market, novel design and higher yield in the long term might result in additional risk and exposure to market turbulence.

Alchemix, on the other hand, offers a completely new paradigm of self-repaying loans with deposited cryptocurrencies working double shifts in DeFi to automatically pay them off. In the process, the protocol issues alUSD tokens that represent the self-repaying loans and keep an approximate peg to the USD. Alchemix introduces a fascinating mechanism of self-repayment, which is unseen in traditional finance. Users can borrow up to 50% of deposited assets and, in return, receive synthetic tokens (alAssets). The collateral works in the DeFi economy and earns a yield, which is used to pay off the loan automatically. Protocol's stablecoin is the alUSD, and in comparison to other stable cryptocurrencies, it is not pegged directly to the US dollar but to DAI, USDC, USDT, and FRAX.

Angle, providing a stablecoin pegged to EUR, is an especially interesting project for European users. The protocol is based on two smart contract modules, which operate on multiple chains. The first one, Angle Core, allows three actions: minting agEUR stablecoin from multiple collateral tokens at face value, open perpetuals on collateral or stablecoin pairs, or depositing tokens to earn yield. The second module, Angle Borrowing, allows borrowing or getting leverage with the agEUR from tokens deposited as collateral. Angle utilizes a designated module designed to withstand black swan events like the USDC depeg and diversifying agEUR backing among multiple Euro stablecoins and other € assets. Interestingly, Angle is pioneering the implementation of

US and European bonds as collateral together with the Backed Finance team, which is an issuer of bIB01 and bHIGH.

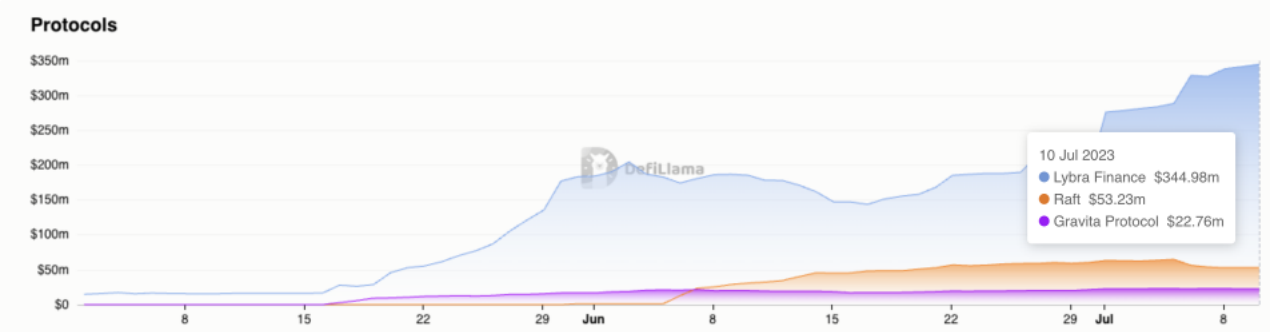
Overnight, a relatively fresh protocol, allows users to mint USD+ assets against their USDC. What is important in that case, is that USD+ is pegged to USDC, not USD itself, so the relationship gets complicated at large sums with small deviations of USDC from USD (like in March 2023). Overnight generates profits/losses from the users' collateral via delta-neutral strategies and every 24 hours the yield/loss is redistributed to USD+ holders in the form of additional tokens. We can illustrate that with an example. You mint 100 USD+ with your 100 USDC. After the first yield redistribution, your position could be charged or substracted with 0.5 USD+, so your balance will be 100.5 USD+ or 99.5 USD+, which you can redeem for 100.5 USDC or 99.5 USDC respectively and the process goes on like that.

Collateral debt position projects accumulate almost $10B in TVL and rank in the top five among decentralized finance categories, according to DefiLlama. Some of the biggest CDP projects by TVL are MakerDAO, Liquity, Abracadabra, Lybra Finance, crvUSD, Raft, and QiDAO. We specifically omit USDJ here, due to the questionable market approach towards the TRON ecosystem. Each protocol aims to fill the void in the market, focusing on specific problems and needs, whether it is integrated blockchains, available deposit cryptocurrencies, or stability mechanisms. The current stagnating crypto ecosystem affects every sector with no exceptions, but CDP protocols can still thrive and grow during the bear market. A certain category of CDP projects gained incomparable momentum. They are LST-backed stablecoins. Lybra Finance is among the top performers in recent weeks, gathering $190M in TVL and reporting a growth of 760% in May. Another one is Raft and their R stablecoin with TVL increasing over 26x times in June to over $57M.

LSTs-backed CDP Stablecoins: Future or Fad?

Liquid staking tokens (LSTs) are derivatives of staked assets, which maintain liquidity and tradeability while underlying cryptocurrencies are locked in smart contracts. LSTs are powerful instruments within DeFi utilized by more and more protocols. Many platforms support LSTs, and users can supply and borrow these assets. The biggest platforms offer liquid staking tokens for ETH, leaders in the category include Lido (stETH), Coinbase (cbETH), RocketPool (rETH), and Frax (frxETH). But the LST space is not cemented, with newcomers such as Swell and ether.fi gaining adoption in DeFi and the recent launch of Eigenlayer will only boost that vertical.

Protocols have already emerged utilizing LSTs as collateral for stablecoins. The most popular are Lybra Finance, Raft, and Gravita Protocol. Lybra Finance allows for ETH and stETH deposits, and users can mint/borrow eUSD against provided collateral. The stability of eUSD is upheld by a blend of over-collateralization, liquidation mechanisms, and arbitrage opportunities. These elements collaboratively ensure the proximity of eUSD's value to its 1 USD peg.



TVL growth for Lybra, Raft and Gravita between May - June 2023 (Source: DeFiLlama)

It feels like the DeFi summer all over again, and LST protocols are trending. Raft is riding this wave, recently growing its TVL significantly. Raft introduces a stablecoin called R, pegged to $1. Platform users can deposit stETH or wstETH and generate R tokens. The collateralization ratio is as low as 120% and can be adjusted depending on users' risk exposure. Raft and R stablecoins offer enhanced capital efficiency, adaptable fees, streamlined and immediate liquidations, and a resilient incentive and soft peg mechanism.

"There's a growing demand for CDP stablecoins and new protocols have room to grow. Yet, the long-term winners will be the ones that manage to take in protocol fees rather than merely attracting LPs in the short term. Raft for example is leaning on the leverage use case," said David Garai, Raft Founder.

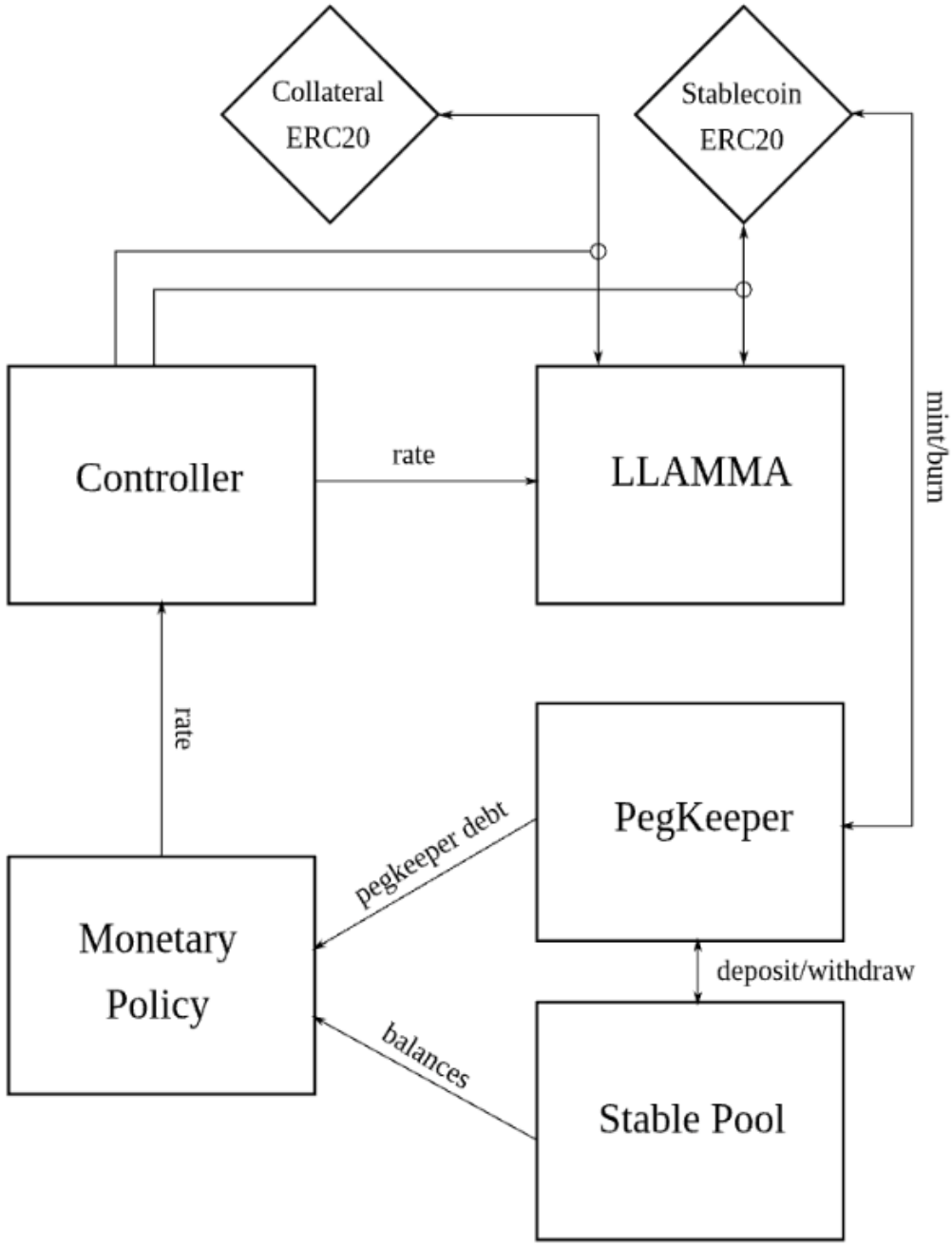
Gravita Protocol, a friendly fork of Liquity, is in the same boat as Lybra and Raft. It is a non-custodial and decentralized way to maximize staked tokens rewards. Borrowers can supply LSTs, including rETH, wstETH, bLUSD, plus WETH. In return, they receive GRAI stablecoins. Users mint GRAI against the value of their collateral. GRAI is an over-collateralized debt token, mimicking standard CDP stablecoins architecture. Gravita offers more collateral options than the competition incentivizing more people to use the platform.

As you can see, the LST-backed stablecoin landscape is doing well, and is one of a few sectors recording growth regarding TVL and users. Are LST-backed stablecoins the future? Probably not, they will work as an important cog in maximizing capital efficiency. As it goes with everything in DeFi, leveraging the use of derivative tokens and other platforms increases the risk. Each participant needs to determine their risk levels.

Fresh Stablecoin Giants crvUSD and GHO

Curve Finance, the leader in automated market making (AMM), entered the stablecoin space with its crvUSD in May 2023. Curve provides over a hundred liquidity pools, which in the design represent cryptocurrency trading pairs. The majority of pools incorporate stablecoins creating a substantial market for crvUSD. The Curve stablecoin infrastructure empowers users to generate crvUSD by utilizing a variety of crypto-tokenized collateral options. This innovative system provides flexibility and accessibility. crvUSD represents the overcollateralized CDP stablecoin category and other cryptocurrencies serve as collateral for its issuance. New collateral options will be introduced through proposals since Curve is managed by a DAO. The community will

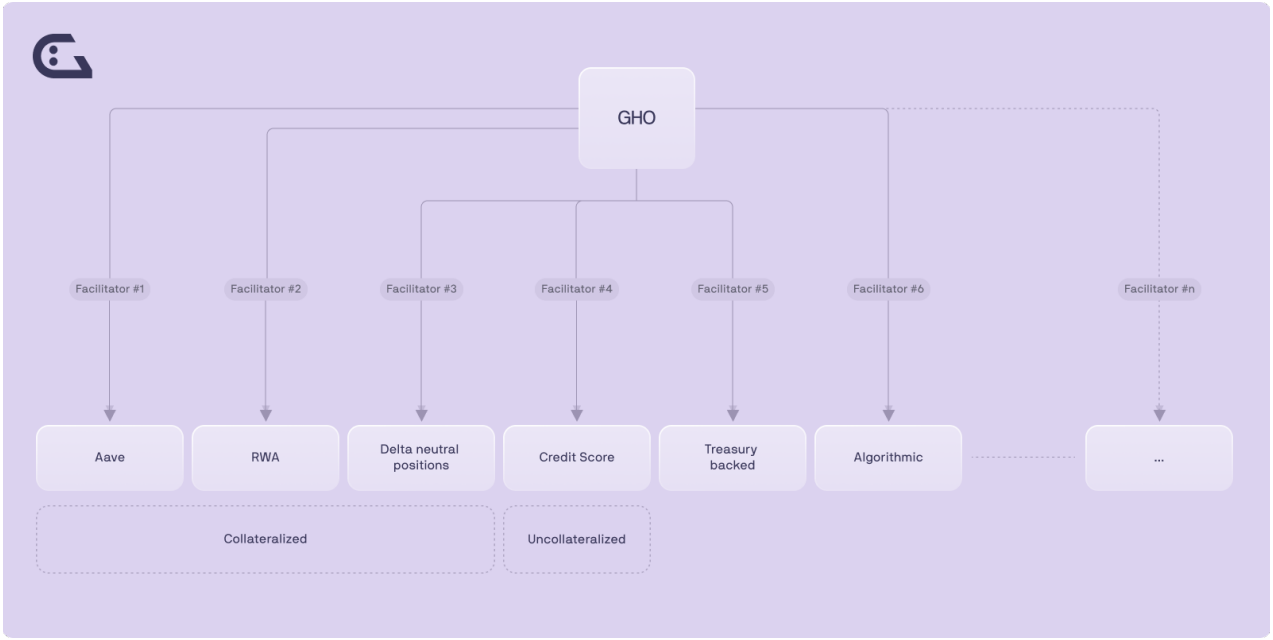
vote on the next available assets. Initially, only two ETH liquid tokens, sfrxETH and wstETH, were in the set, but wBTC and ETH have been added already. Although crvUSD launched recently and is still in the testing phase with limited collateral assets, the demand for Curve's stablecoin can be considerable taking into account Curve's status in DeFi and its position as the biggest DEX in TVL, according to DeFiLlama.



crvUSD stablecoin's design scheme (Source: GitHub)

The largest lending protocol, Aave, has unveiled its plans to launch a stablecoin called GHO. It is described as a decentralized, collateral-backed stablecoin, pegged to USD. The Aave DAO manages GHO characteristics and design from the supply of GHO to the interest and risk parameters. Initially, GHO will launch on the Ethereum blockchain, while the potential path for cross-chain bridging versus minting on multiple ecosystems is still

ongoing. Aave DAO implemented a discount rate when borrowing GHO. Users staking AAVE tokens will be eligible for a discount. It is a disruptive mechanism in CDP stablecoin's architecture and improves cryptocurrency use cases (stkAAVE in particular). Because GHO is decentralized, just like crvUSD, it is transparent and all the details can be found in the documentation and on-chain governance. As the protocol and demand grow, GHO can adjust its architecture to market conditions and user experience. GHO introduces the concept of Facilitators who can mint and burn GHO tokens permissionlessly, utilizing various strategies. Different collateral exposure will help maintain the GHO peg. This way GHO incorporates multiple stability mechanisms, improving the overall security.



GHO stablecoin's design scheme (Source: GHO Docs)

5 Algo-Stables, the Holy Grail of Web3?

Algorithmic stablecoins are a song about a decentralized future. Existing solutions play second fiddle to fiat-backed and CDP stablecoins so far. Unfortunately, many users and investors got burned by the UST and the Terra ecosystem collapse. Many algo-stable architectures are not bulletproof (yet), and the next generation must learn from the mistakes made in the past to make technology resilient. The UST de-peg and Terra ecosystem crash serves as the biggest lesson for this type of stablecoins. On the flip side, the benefits gained through a working algo-stables system could be enormous in comparison to other types, from accessibility and worldwide availability to on-chain transparency and reserve monitoring. Hence the stakes and possible rewards are high.

The Two Successful Use Cases

Algo-stables are hard to design robustly, especially when the market crashes. Despite failures, new teams and projects try to create secure and stable algorithmic coins. They build on past misfires as they follow the path of templars to the promised land.

So far two stars shine on the market. FRAX is the biggest algo-stablecoin with a market capitalization of $1B. It is a fractional-algorithmic, open-source, permissionless, and entirely on-chain stablecoin utilized in various DeFi protocols. It is the first stablecoin with parts of its supply backed by collateral and an algorithmic price stability mechanism. The proportion of collateralized and algorithmic components in FRAX stablecoin is contingent upon the market's valuation. If the trading price of FRAX exceeds $1, the protocol reduces the collateral ratio. Conversely, if 1 FRAX falls below $1, the CR is raised. Frax Protocol uses Algorithmic Market Operations Controller (AMO), autonomously implementing arbitrary monetary policy.

Historical Collateralization Ratio for FRAX stablecoin (Source: FRAX dApp)

The second standing algo-stable giant is Mento Protocol, which brings another variation to decentralized algorithmic stablecoins. The protocol manages stables in the Celo blockchain. The coins they issue track fiat currencies such as the US dollar, Euro, and Brazilian Real. Users can exchange CELO tokens for cUSD, cEUR, and cREAL. The reserve consists of the deposited CELO and additional diversified crypto-assets, allowing the Mento Protocol to expand and contract the supply of stablecoins. Mento falls into the category of overcollateralized stablecoins with over 2x reserve ratio. The issuance and redemption process is similar to fiat-backed solutions but requires precise Celo-Fiat and USDC-Fiat price data that in Mento's case is delivered by RedStone Oracles. Asset pools are recalibrated every time the reported oracle value is updated, preventing manipulation, attacks, and limiting depletion of reserves, however, arbitrage opportunities may still occur.

Algo-issues

Many algo-stables failed and did not withstand periods of market turmoil. Hence, users should be cautious and verify novel approaches. UST is a great example, showing how untested architecture can destroy an entire ecosystem in days. Victorious projects would be stablecoins surviving crashes and bear markets, and currently, there are not many of those. The matter is not only to verify designs when the crypto market is going up and new funds are pumped into protocols but also when investors run and leave the market.

Automatic smart contract-based operations are concurrently algo-stables' strengths and weaknesses. Their design must be indestructible and impenetrable to gain mass adoption. Unfortunately, there is no shortage of hackers. Every month the crypto market witnesses precedents regarding stolen funds, hacked protocols, and exploited smart contracts. Incidents like this must be eradicated for algorithmic stablecoins to become the dominant choice.

Algorithmic stablecoins have often been hailed as the "Holy Grail" of decentralized finance due to their potential for exceptional capital efficiency. However, despite their immense potential, algorithmic stablecoins have faced persistent challenges in maintaining price stability, as mentioned earlier. Nonetheless, they hold the greatest promise in achieving all three aspects of the stablecoin trilemma. In contrast, fiat collateralized stablecoins inherently rely on centralization, as a central entity must control fiat reserves. Likewise, crypto-collateralized stablecoins suffer from capital inefficiency, necessitating over-collateralization due to the volatility of the crypto market.

UST and Terra Collapse

This story is so renowned (in the worst way) because it involved the collapse of a blockchain with multi-billion dollar TVL – around $30B days before the earthquake. The algorithm within the market module of the Terra protocol allowed users to consistently exchange 1 USD worth of Luna for 1 UST, and vice versa, incentivizing users to maintain the price of TerraUSD. The arbitrage happened based on two pools: UST and LUNA. May 2022 de-peg was not the first one of many. Exactly a year earlier, in April and May 2021,

UST lost its 1:1 ratio to USD, but the price recovered shortly thereafter. It was not a surprise that an algo-stable is not steadily maintaining the peg. It has happened to every algorithmic stablecoin before. The beginning of the end for UST and LUNA stemmed from a few events and poor design practices. First, there was a massive concentration of UST in the top Terra protocol Anchor, making it an enormous failure point in the event of trouble. Secondly, the UST peg was supposed to be protected by Luna Foundation Guard (LFG), which had BTC as reserves. Saving UST led to the selling of BTC and a decrease in its price, affecting the overall reserve's asset value.

Moreover, a few high-calibre trades on key platforms exposed vulnerabilities within the Terra ecosystem. The TerraUSD collapse unfolded in three phases. Initially, two traders compromised UST's peg on Curve Finance. Subsequently, Terraform Labs and three supporters intervened by acquiring $2 billion worth of UST to restore its stability. According to the stablecoin's governing algorithm, any UST holder could exchange 1 UST for one dollar's worth of LUNA, regardless of the current LUNA price. Consequently, holders collectively engaged in the burning process of their UST, leading to the hyperinflation of LUNA. However, the prolonged sell-off exerted pressure causing prices to decline significantly.

TerraUSD was an undercollateralized algorithmic stablecoin. Just reading this gives you chills. Instead of relying on asset reserves to maintain its peg, Terraform Labs employed a sister token, LUNA, to absorb the price volatility of UST. Non or undercollateralized algorithmic stablecoins are intrinsically vulnerable as their peg is solely reliant on an algorithm. Market demand and volatility, independent actors, and price information heavily influence such stables. It is impossible to forecast the full spectrum of responses the algorithm could have under various market conditions. Individuals require prompt, dependable, and current price data to take advantage of stablecoin arbitrage opportunities. Oracles play a vital role in delivering trusted information fast. Importantly, a somewhat similar story can be followed on the Titan Token panic-selling collapse.

Terra chain TVL between Jan 2021 - July 2023 with May 2022 crash. (Source: DeFiLlama)

6 What Can We Expect Next in The Stablecoins Space?

Stablecoins are an area of ongoing development and innovation in the cryptocurrency space. Fiat-backed stables currently lead the race since they are a natural choice for CEXes. However, stablecoins' future leans towards decentralized solutions. While it is challenging to predict future directions with certainty, we can speculate on some potential trends and possibilities.

Algorithmic Approach

Algorithmic stablecoins will continue to evolve as developers refine their mechanisms and learn from past experiences. As technology advances and new economic models emerge, algo-stables have the potential to become more robust and effective in maintaining price stability. However, they may still face challenges in achieving long-term stability due to their reliance on complex algorithms and market dynamics. On the other hand, CDP stablecoins are already an attractive solution for everyone who wishes to unlock additional assets' liquidity and obtain extra leverage. Maybe they are not as capital efficient as algo-stablecoins can be, but collateral debt positions endured market downturns and black swan events.

New ideas upgrading stablecoin standards make this space very exciting. Gyroscope Protocol builds on previous experiences and combines an algorithmic pricing mechanism with a fully-collateralized design. In that sense, Gyroscope is focused on the use of algorithms to automate monetary policy and not as a replacement for asset-backing. Such architecture aims for a long-term reserve ratio of 100%, where every unit of stablecoin is backed by 1 USD worth of collateral. The Gyroscope team also published a technical paper specifically about the price feeds consolidation and circuit breakers.

RWA Approach

Stablecoins backed by real-world assets (RWA) collateral are also gaining attention. These stablecoins aim to provide stability by utilizing tangible assets such as commodities, real estate, or other forms of value. RWA-backed stablecoins present challenges, such as ensuring proper valuation, custody, and regulatory compliance. In addition to algorithmic and RWA-backed stablecoins, further innovation in hybrid models can combine different collateral types, algorithms, or governance mechanisms.

Backed Finance is a practical example of a company tapping into RWA-backed assets. Flow is very similar to Circle and USDC issuance, where Backed Finance issues bTokens. They offer fully backed, tokenized real-world assets. Tokens track the value of RWAs, such as stocks or ETFs, and can be freely transferable across wallets bridging Web3 with traditional finance. Bringing RWAs on-chain creates strong fundamentals for stablecoins collateralized with a bigger range of assets. It can spur greater interest among institutions and companies regarding blockchain technology.

Another fascinating protocol that tokenizes tangible world assets is Ondo Finance. Ondo brings institutional-grade finance to DeFi and creates quality security assets. They tokenize US Money Market (OMMF), US Treasuries (OUSG), Short Term Bonds (OSTB), and High Yield Corporate Bonds (OHYG). These represent major US asset classes known to every traditional investor. Ondo's solutions improve liquidity and accessibility for investment vehicles. Each product can be treated as a fund, giving familiar vibes to investors regarding management, fees, and risk exposure. Apart from tokenizing RWAs, Ondo creates and helps set up decentralized protocols to utilize the power of high-class security tokens. The first one of them is a lending platform called Flux Protocol. Flux uses OUSG as loan collateral, making it a valuable RWA use case. Lending and borrowing are supported with derivative stable fTokens representing loan positions. Ondo and Flux technology can play a significant role in RWA-backed stablecoins, merging quality TradFi securities with blockchain. It is expected that Traditional Finance (TradFi) and DeFi will intertwine more and more.

Elastic Approach Based on Demand

A stablecoin's purpose is to track the value of a fiat currency, but even fiat currencies are not maintaining value concerning products and services. Increasing monetary supply and inflation affect purchasing power of fiat currencies since they are only backed by the trust in the governments. Assets like Bitcoin and Ethereum have been referred to as stores of value to combat this dynamic, but are too volatile due to fixed or deflationary monetary policy that encourages hoarding. OlympusDAO presents a slightly different approach to stable cryptocurrencies. They created OHM, a decentralized reserve currency designed to be elastic based on market demand. Interestingly, OHM is not pegged to any asset but achieves its stability via a combination of Protocol Owned Liquidity (POL) and a large treasury supporting a monetary policy mechanism called Range Bound Stability (RBS). The RBS system maintains a moving average price, calculates upper and lower bounds for OHM price, and allows users to swap OHM for reserves at specific prices up to the capacity of the current walls. The mechanism also deploys treasury reserves in a downward-trending market and sells OHM for reserves in an upward-trending market to stabilize the price. The system aims to neuter periods of "panic selling". The treasury assets supporting RBS include other cryptocurrencies, i.e. DAI and LUSD, as well as derivatives LP and liquid staked tokens (LSTs). If these assets appreciate, the RBS system defends higher price-moving averages with an increased liquid backing, allowing OHM to appreciate. OlympusDAO offers a unique alternative to traditional fiat currencies and stable cryptocurrencies. The project is highly complex and innovative, but only time will tell if that is a viable long-term solution.

The stablecoin regulatory landscape is still very much a work in progress. Governments closely monitor the crypto ecosystem, but regulatory bodies must provide clear guidelines for global adoption. The oversight and regulatory requirements imposed on stablecoin projects may impact their adoption and development. Unless restraining regulations are established, collateral debt position, algorithmic, and LST-backed stablecoins might flourish once Central Bank Digital Currencies (CBDCs) are introduced.

7 Conclusions

Stablecoins have become a foundational layer of the cryptocurrency ecosystem, providing stability and mitigating volatility. There are diverse stablecoins available, each with a distinct design, mechanism, advantages, and associated risks. Fiat-backed stablecoins, such as USDT, USDC, and BUSD, are the most popular, relying on reserves of fiat currencies held by centralized institutions.

Collateralized Debt Position (CDP) stablecoins, like DAI and LUSD, utilize the collateral in the form of cryptocurrencies and are governed by decentralized protocols. Algorithmic stablecoins have currently just two solid representatives with Frax and Mento Protocol proving to be robust protocols. Although other projects from this category have promising concepts, they still need to gain widespread trust and adoption. These systems function solely on code, auto-adjusting the stablecoin supply in line with market conditions. However, TerraUSD's (UST) 2022 collapse reminds us that algorithmic stablecoins still grapple with notable challenges, and need to learn from past missteps to bolster resilience and reliability. On the other hand, RWA-backed stablecoins present an innovative approach with the potential to claim a large portion of the future stablecoin market. These could truly propel the global adoption of blockchain technology and DeFi to new heights. Finally, the role of oracles is crucial for stablecoins, providing real-time price data to maintain collateral health, guaranteeing transparency and integrity.

So, what are we most excited about in the space? In our view, the most critical aspect of the stablecoin is stability in the volatile market, since market crashes are the real litmus tests for a specific design. The publishing team follows the expansion of recently launched CDP stablecoins such as Lybra Finance, Raft, Gravita Protocol, and crvUSD. Naturally, we are looking forward to GHO's launch, which has huge potential but will also face fierce competition in the market.

References

1. https://defillama.com/protocols/CDP
2. https://defillama.com/protocols/Algo-Stables
3. https://www.coingecko.com/en/categories/stablecoins
4. https://dune.com/hagaetc/stablecoins
5. https://tokenterminal.com/
6. https://makerdao.com/
7. https://www.mento.org/
8. https://blog.chainalysis.com/reports/how-terrausd-collapsed
9. https://medium.com/stablecorp/a-brief-history-of-algorithmic-stablecoins-6974dd5bff5e
10. https://www.tradingview.com/

About RedStone Oracles

RedStone is a modular oracle delivering diverse, high-frequency, data feeds to all EVM L1 and L2 networks and beyond, i.e. Starknet, Fuel Network or TON. By responding to market trends and developer needs, RedStone is capable of supporting assets not available elsewhere. The modular design allows for data consumption models adjusted to specific use cases, i.e. CDP stablecoins and algorithmic stablecoins. RedStone raised almost $8M from Lemniscap, Blockchain Capital, Maven11, Coinbase Ventures, Stani Kulechov, Sandeep Nailwal, Alex Gluchovski, Emin Gun Sirer and other top VCs & Angels.

Core contributors to the report:

- **Kamil Zawieja**, Independent Technical Researcher
- **Marcin Kazmierczak**, Co-Founder of RedStone Oracles

Resources

If you'd like to partner with the RedStone team on the next research pieces let us know in the form below. If you like the report or have any comments share your feedback in the form too!

https://forms.gle/wuih7AyiP42qi4xS7