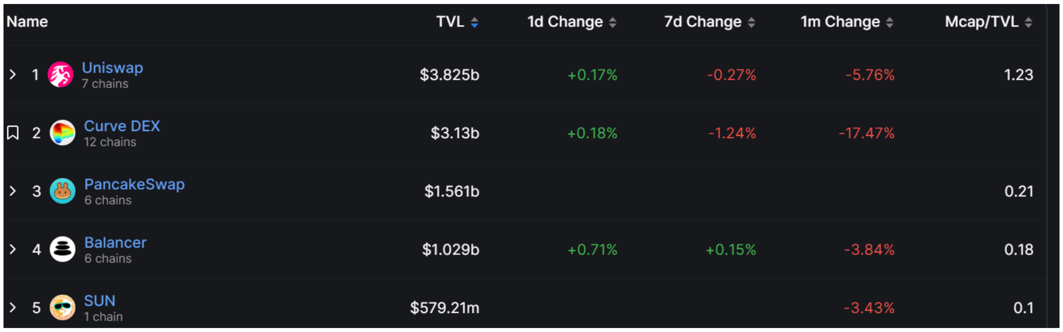
Curve report stage 2

Key Insights

- First to introduce ve(3,3) “locking mechanism” which supposed to represent perfect trilemna between the protocol, the liquidity providers and the traders.
- First Introduction of Stableswap curve mechanism to allow more efficient swaps between stablecoins with the constant product formula curve (x*y=k)
- Extremely efficient AMM for swapping stablecoins and low-volatily tokens
- Integration of Ethereum, Arbitrum, Optimism, Polygon, Avalanche, Fantom, harmony, Aurora, Celo and Moonbeam chains.
- Launch of new innovative stablecoin stablecoin crvUSD which uses the techonoloy LLAMMA for Lending-Liquidating Automated Market Maker Algorithm.
- In July, Curve has suffered from a 52M$ hack on Arbitrums pools that ruined Curve’s image of a bluechip protocol in DeFi
- CEO Michael Egorov not “ethic” OTC CRV transactions regarding a risky loan negatively impacted the Curve’s image.

Analyst sentiment

Curve Finance has been at the forefront of DeFi innovation, introducing groundbreaking features such as the ve(3,3) "locking mechanism or the Stableswap curve mechanism, employing the constant product formula curve (x*y=k), enabling highly efficient swaps between stablecoins and low-volatility tokens. Being pused by bright people like Micheal Egorov and Julien Bouteloup, Curve has know a very fast growth to become a dominant protocol since the DeFi summer in 2020.



	Name	TVL	1d Change	7d Change	1m Change	Mcap/TVL
1	Uniswap 7 chains	$3.825b	+0.17%	-0.27%	-5.76%	1.23
2	Curve DEX 12 chains	$3.13b	+0.18%	-1.24%	-17.47%	
3	PancakeSwap 6 chains	$1.561b				0.21
4	Balancer 6 chains	$1.029b	+0.71%	+0.15%	-3.84%	0.18
5	SUN 1 chain	$579.21m			-3.43%	0.1

Figure1: Snapshot of Defillama the 28th of June 2023 on Dexes ranking

However, Curve suffers from the fact that the CRV’s price is directly correlated to the activity (ie volumes) generated on the platform. Thus, Curve made strides in stablecoin innovation with the launch of crvUSD, featuring LLAMMA technology—an acronym for Lending-Liquidating Automated Market Maker Algorithm. This innovative stablecoin has the primer mission to increase volumes on Curve and then generated a new source of revenue for the treasury.

Despite these achievements, Curve faced a setback in July when a $52 million hack targeted Arbitrum's pools, tarnishing its reputation as a blue-chip protocol in DeFi. This incident underscores the ongoing challenges and security concerns within the decentralized finance space. Furthermore, as bright as Egorov can be, he contracted a loan of 100M$ with 400M CRV tokens that were at risk of liquidation and pushed the Curve’s ecosystem into stress.

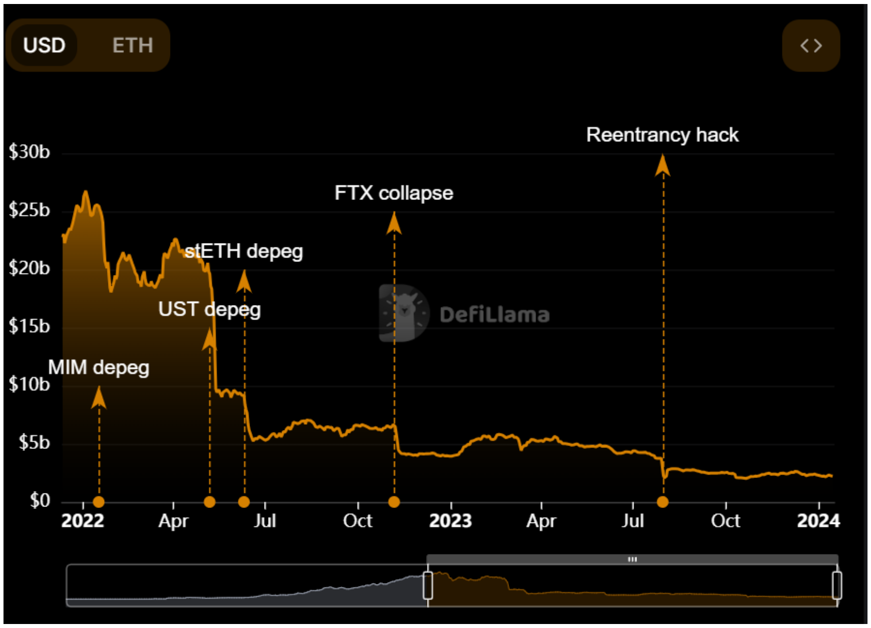


Figure2: TVL drop after FTX and especially Reentrancy hack on Curve

To conclude, Curve's image clearly suffers from the "recent" hack and Egorov's moves which has drastically decreased volumes on platform. Even though Egorov closed OTC trades with other majors figures of DeFi spaces, it will take time for the protocol to recover from this black swan event. I recommend to wait the next 4-6 months to review again the health of the protocol to consider as a potential investment

Project overview

Curve Finance is a protocol for automated market-making that enables low-cost and low-slippage swapping between stablecoins and low volatile assets. It operates as a decentralised liquidity aggregator, where anyone can contribute their assets to various liquidity pools and earn rewards from fees generated by trades.

Users can provide liquidity or use assets in the pool to execute a swap with low slippage. Two types of pools have been introduced since Curve launch:

- Curve v1: Only for stablecoin with the introduction of Stablewap invariant which realize the most efficient swaps.
    - Trade fee: 0.04%

    - Withdraw/deposit fee: [0;0.02%]
  - Curve v2: Introduction of TriCrypto for non-stable assets.
    - Trade fee: [0.04%;0.4%]
    - Withdraw/deposit fee: [0;0.02%]
  - Both Curve v1 and v2 are not relying on external oracles but use directly trading activity inside pools to determine assets' prices.

Key benefits:

- **Very low slippage** – Especially on stablecoin swaps
- **Yield Farming** - Getting rewards by providing liquidity
- **Deep liquidity** – One of the highest TVL among Dexes
- **Innovative** – Responsible for Stableswaps and LLAMMA stablecoin crvUSD.
- **Composability** – Available on more than 15 chains

Project architecture

From an architecture point of vue, Curve Finance is based on four main components: **Base**&**Metapool**, **Gauges**, **Factory, Minter** and **CRV**:

- **Base&Metapool**: Curve pools can be split in 3 categories which are Plain pools, Leading pools and Metapools.
  - Plain pools: the simplest Curve pool is a plain pool, which is an implementation of the StableSwap invariant for two or more tokens. The key characteristic of a plain pool is that the pool contract holds **all** deposited assets at all times.
    - An example of a Curve plain pool is 3pool, which contains the tokens DAI, USDC and USDT.
  - Leading pools: Curve pools may contain lending functionality, whereby the underlying tokens are lent out on other protocols (e.g., Compound or Yearn). Hence, the main difference to a plain pool is that a lending pool does **not** hold the underlying token itself, but a **wrapped** representation of it.

        - An example: Aave pool on Aave or BUSD on YearnFi. The complete list here.

    - Metapools: A metapool is a pool where a stablecoin is paired against the LP token from another pool, a so-called *base pool*. For example, users could seamlessly trade GUSD between the three coins in the 3CRV (DAI/USDC/USDT). This is helpful in multiple ways:
        - Prevents diluting existing pools
        - Allows Curve to list less liquid assets
        - More volume and more trading fees for the DAO.
        - The Metapool in question would take GUSD and 3CRV LP tokens. This means that liquidity providers of the 3CRV pool who do not provide liquidity in the GUSD Metapool are shielded from systemic risks from the Metapool.

- **Gauges**: Curve has a gauge weight mechanism that helps pool operators attract customers. Gauge are determined by a weight and a type:
    - Gauge weight: users can allocate their veCRV towards one or more liquidity gauges ⇒ gauge receive new CRV proportionally to veCRV allocated
    - Gauge type: Gauge are assigned a gauge type according to a chain that is used to calculate the number of CRV to send to liquidity gauge. Ex: Ethereum (stable) = 0, Fantom = 1, Arbitrum = 7, ...

Based on these mechanisms, there are protocols that try to optimize CRV voting power to bribe specific pools. This is called “Curve War” and Convex is the main protocol build on top of Curve.

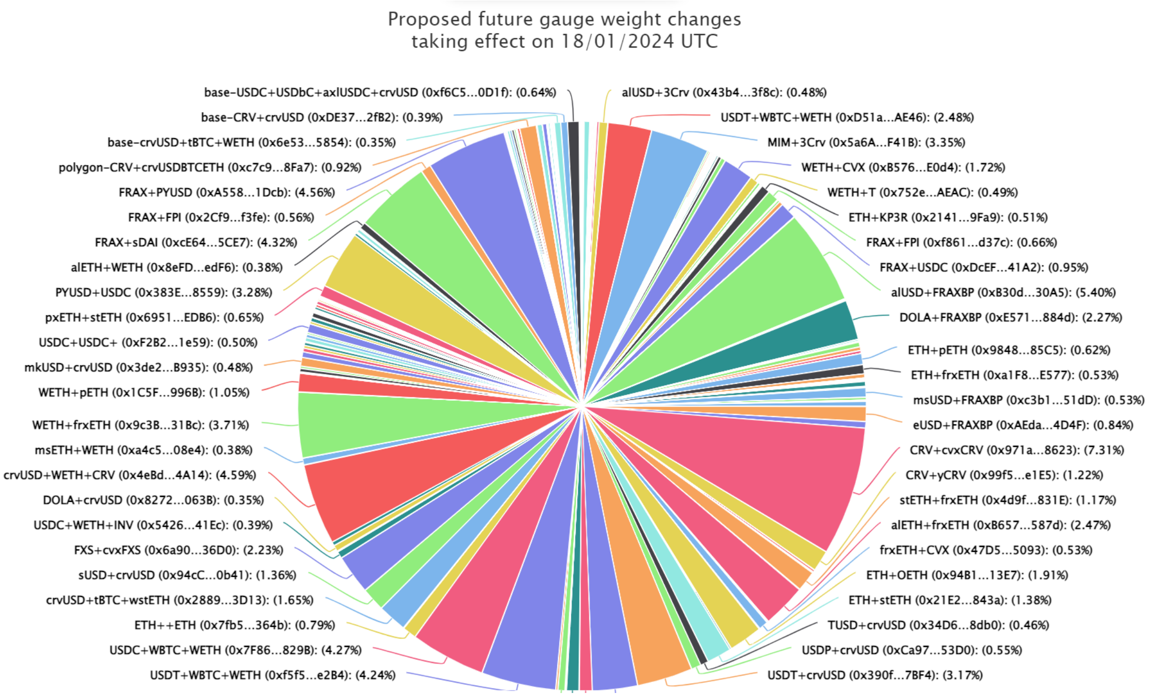


Figure2: State of Gauge weights in Curve ecosystem. (18/01/2024)

There is also an other type of gauges:

- liquidity gauges: CRV inflation is directed to users who provide liquidity within the protocol. This usage is measured via "Liquidity Gauge" contracts. Each pool has an individual liquidity gauge. The *Gauge Controller* maintains a list of gauges and their types, with the weights of each gauge and type. Each pool has a unique liquidity gauge.

- **Factory**: It's where users can create a pool on Curve. Once a pool is displayed on Curve, it cannot be removed.
- **Minter contract**: Minter contract has been deployed to the Ethereum mainnet with the following address: 0xd061D61a4d941c39E5453435B6345Dc261C2fcE0. This is a fixed address, the contract cannot be swapped out or upgraded. This contract mints the correspondant CRV amount for every gauges eligibles.
- **CRV**: ERC-20 token which is the governance token of Curve Finance.

Project Roles

Inside Curve platform, they are several actors that contributes to the activity of the protocol:

- **Liquidity providers**:
  - Provide liquidity to liquidity pools and get yield through the activity in the platform
- **Traders**:
  - Swaps tokens through liquidity pools
- **CRV holders**:
  - Voting power by locking CRV token (veCRV)
  - Stake/Unstake with cooldown of 1 week and 2 days
  - Earn stacking rewards every weeks regarding the time vested.

Governance:

Overview:

Curve is using Aragon, a platform to easily build a DAO, for governance and admin functionalities.

Curve DAO consists of multiple smart contracts connected by Aragon. Interaction with Aragon occurs through a modified implementation of the Aragon Voting App. Aragon’s standard one token, one vote method is replaced with a weighting system based on locking tokens.

Curve DAO has a token (CRV) which is used for both governance and value accrual.

Moreover, there are two DAOs inside Curve’s ecosystem:

- Community DAO: There is a requirement of 2500 veCRV to make a proposal to the DAO. This DAO controls ownership and parameters of admins.
- Emergency DAO: This DAO can kill a gauge/pool in extreme circumstances and with the agreement of the 9 people.

Vote-Escrowed CRV:

Participating in Curve DAO governance requires that an account have a balance of vote-escrowed CRV (veCRV). veCRV is a non-standard ERC20 implementation, used within the Aragon DAO to determine each account’s voting power.

veCRV is represented by the Voting Escrow contract, deployed to the Ethereum mainnet at **0x5f3b5DfEb7B28CDbD7FAba78963EE202a494e2A2**.

veCRV cannot be transferred. The only way to obtain veCRV is by locking CRV. The maximum lock time is four years. One CRV locked for four years provides an initial balance of one veCRV.

Boosting:

In order to incentivize users to participate in governance, and additionally create stickiness for liquidity, we implement the following mechanism. A user’s balance, counted in the liquidity gauge, gets boosted by users locking CRV tokens in Voting Escrow contract, depending on their vote weight

Protocol Ownership:

The Curve DAO controls admin functionality throughout the protocol. Performing calls to to owner/admin-level functions is only possible via a successful DAO vote.

Ownership is handled via a series of proxy contracts. At a high level, the flow of ownership is:

- DAO voting (passed) → Use of Aragon Agent → Call of ownership proxy → Application in contracts

The Curve DAO has a total of three Aragon Agent ownership addresses, which are governed by two independent DAOs:

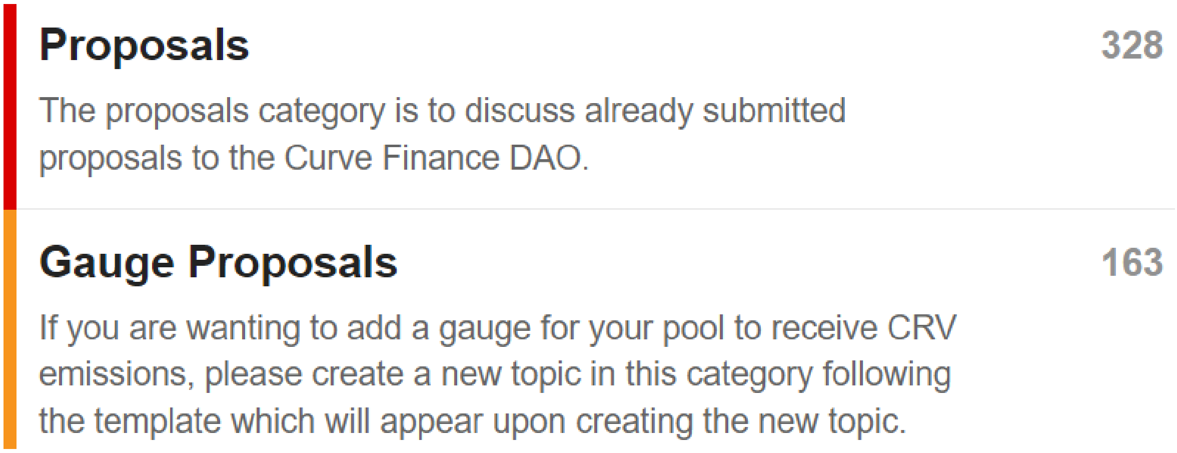
1. The **Community DAO** (or just “the DAO”) governs the day-to-day operation of the protocol. An account must have a minimum balance of 2500 veCRV to make a DAO vote. Each vote lasts for one week. Votes cannot be executed until the entire week has passed. The DAO has ownership of two admin accounts:

   a. The **ownership admin** controls most functionality within the protocol. Performing an action via the ownership admin requires a 30% quorum with 51% support.

   b. The **parameter admin** has authority to modify parameters on pools, such as adjusting the amplification co-efficient. Performing an action via the parameter admin requires a 15% quorum with 51% support.

2. The **Emergency DAO** has limited authority to kill pools and gauges during extraordinary circumstances. The emergency DAO consists of nine members, comprised of a mix of the Curve team and prominent figures within the DeFi community. Each member has one vote. Any member may propose a vote. All members of the emergency DAO may propose new votes. A vote lasts for 24 hours and can be executed immediately once it receives 66% support.

One particularity of Community DAO is that there are 2 types of proposals that can be made:



Proposals 328

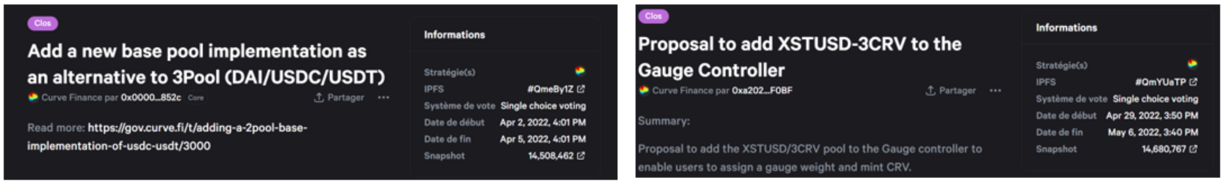
The proposals category is to discuss already submitted proposals to the Curve Finance DAO.

Gauge Proposals 163

If you are wanting to add a gauge for your pool to receive CRV emissions, please create a new topic in this category following the template which will appear upon creating the new topic.

Figure: Two different types of proposals in Curve Community DAO

An other particularity is that the time for voting for the proposal can be chosen by the proposer:



Add a new base pool implementation as an alternative to 3Pool (DAI/USDC/USDT)

Curve Finance par 0x0000...852c Core

Read more: https://gov.curve.fi/t/adding-a-2pool-base-implementation-of-usdc-usdt/3000

Informations

Stratégie(s)	
IPFS	#QmeBy1Z
Système de vote	Single choice voting
Date de début	Apr 2, 2022, 4:01 PM
Date de fin	Apr 5, 2022, 4:01 PM
Snapshot	14,508,462

Proposal to add XSTUSD-3CRV to the Gauge Controller

Curve Finance par 0xa202...F0BF

Summary:

Proposal to add the XSTUSD/3CRV pool to the Gauge controller to enable users to assign a gauge weight and mint CRV.

Informations

Stratégie(s)	
IPFS	#QmYUaTP
Système de vote	Single choice voting
Date de début	Apr 29, 2022, 3:50 PM
Date de fin	May 6, 2022, 3:40 PM
Snapshot	14,680,767

Figure: Two different proposals with different voting time

Tokenomics

General metrics: (16/01/2023)

CRV price	$0.5529
Marketcap	$593,702,743
Fully diluted Marketcap	$1,141,640,759
Circulating supply	1,073,853,631
Total supply	3,303,030,299
Volume (24h)	$42,096,397
TVL (Total Value locked)	$1,627,830,019
Market availability	Binance, Coinbase, Kraken, Kucoin, Uniswap, OKX

CRV token is the governance token of the protocol. It has been launched the 13th august 2020. The main purposes of the Curve DAO token are to incentivise liquidity providers on the Curve Finance platform

Currently CRV has three main use cases:

Stacking:

CRV can now be staked (locked) to receive trading fees from the Curve protocol. A community-lead proposal introduced a 50% admin fee on all trading fee. **The lock has to be done on Ethereum.**

Yield farmers will have to constantly monitor their veCRV power to get the maximum payout from the yield farming exercise as veCRV decays with time. There is a **calculator** built that shows this in detail.

Voting:

Once CRV holders vote-lock their veCRV, they can start voting on various DAO proposals and pool parameters.

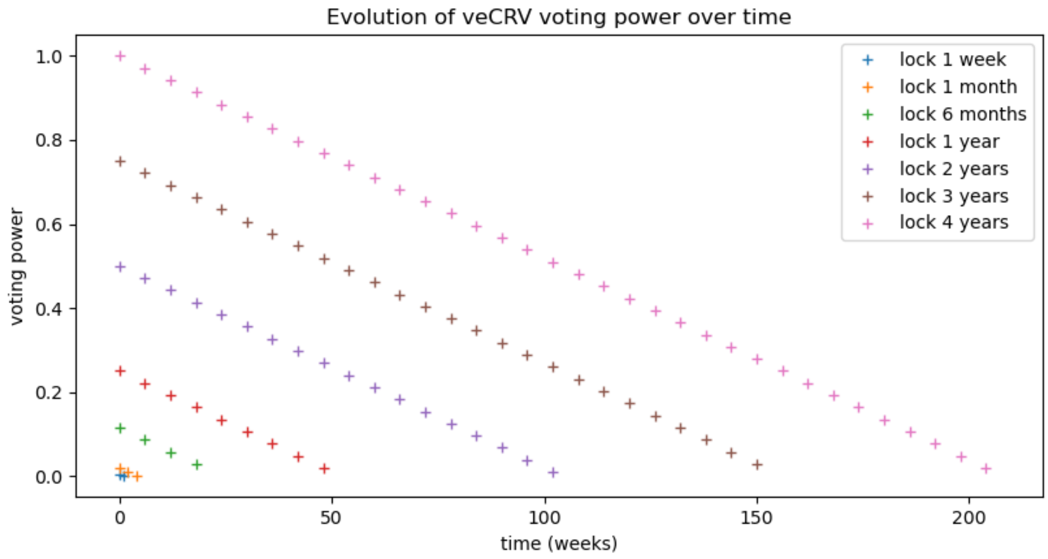


Figure: Evolution of Voting power over time

As it can be seen from above, the voting power is decreasing linearly with time. The more users lock their CRV, the more voting power. Users that locks their get the other 50% admin fee on all trading fee.

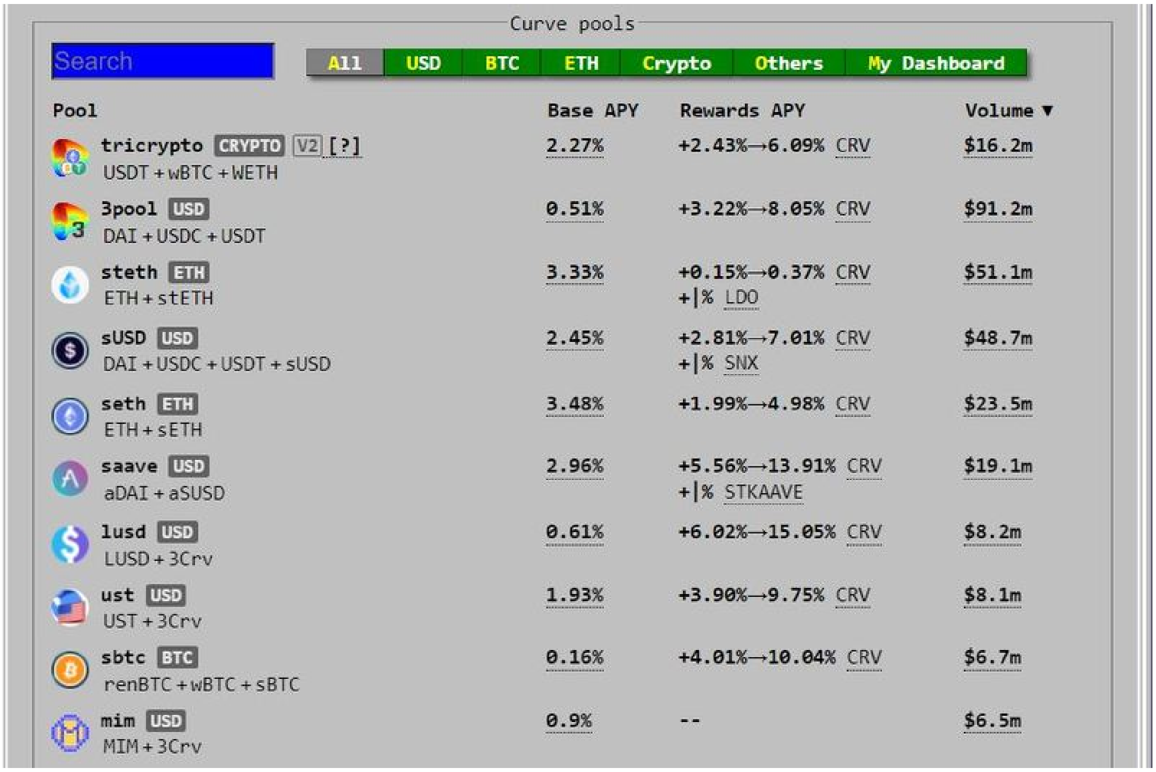
- Example of locking times:
  - 1 CRV locked for 4 years = 1veCRV
  - 1 CRV locked for 3 years = 0.75veCRV
  - 1 CRV locked for 2 years = 0.50veCRV
  - 1 CRV locked for 1 year = 0.25veCRV

Boosting:

Boost your rewards on provided liquidity. Vote locking CRV allows you to acquire voting power to participate in the DAO and earn a boost of up to 2.5x on the liquidity you are providing on Curve.

Application of these mechanisms:

Let’s see all these mechanisms putting in place with one example by looking at stETH pool that provides four sources of yield:



Pool	Base APY	Rewards APY	Volume ▼
tricrypto CRYPTO V2 [?] USDT + wBTC + WETH	2.27%	+2.43%→6.09% CRV	$16.2m
3pool USD DAI + USDC + USDT	0.51%	+3.22%→8.05% CRV	$91.2m
steth ETH ETH + stETH	3.33%	+0.15%→0.37% CRV +|% LDO	$51.1m
sUSD USD DAI + USDC + USDT + sUSD	2.45%	+2.81%→7.01% CRV +|% SNX	$48.7m
seth ETH ETH + sETH	3.48%	+1.99%→4.98% CRV	$23.5m
saave USD aDAI + aSUSD	2.96%	+5.56%→13.91% CRV +|% STKAAVE	$19.1m
lusd USD LUSD + 3Crv	0.61%	+6.02%→15.05% CRV	$8.2m
ust USD UST + 3Crv	1.93%	+3.90%→9.75% CRV	$8.1m
sbtc BTC renBTC + wBTC + sBTC	0.16%	+4.01%→10.04% CRV	$6.7m
mim USD MIM + 3Crv	0.9%	--	$6.5m

Figure: Curve pools with base & rewards APY (screenshot from June 2021)

Looking at the Annual Percentage Yield (APY) figures, it shows that the Liquidity Providers (LPs) can roughly expect 4 types of source of incomes:

- Trading fees: 3.33% APY
- Token rewards: 7.40% APY from LDO token
- CRV token rewards: 0.15% to 0.37% (based on amount of veCRV locked).
- stETH stacking yield: Not shown here.

CRV distribution and token emission schedule:

Here is the details of the distribution and the token release schedule:

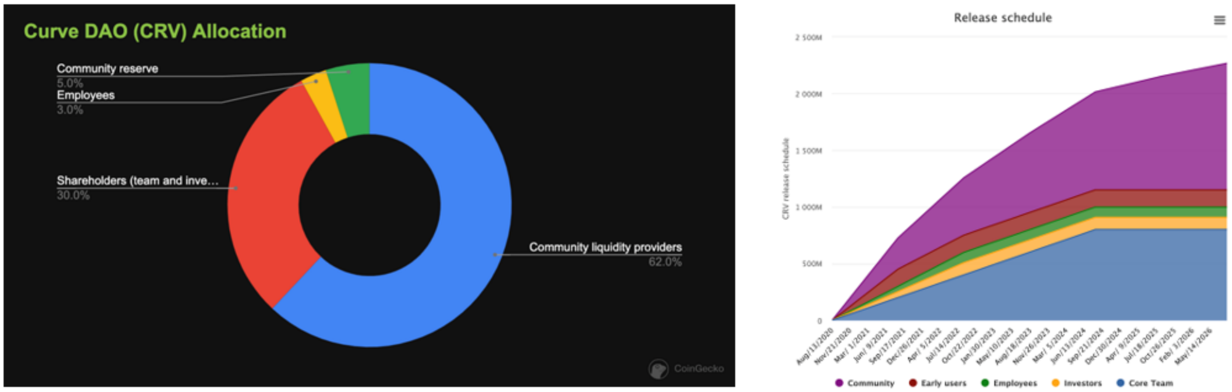


Figure: Token distribution of CRV token on the left and CRV's token emission the right

The distribution of Curve DAO's total supply is as follows:

- 62.00% is allocated to Community liquidity providers
- 30.00% is allocated to Shareholders (team and investors)
- 3.00% is allocated to Employees
- 5.00% is allocated to Community reserves.

The initial distribution represented 1.3B tokens (~43% of maximum total supply) and was as follow:

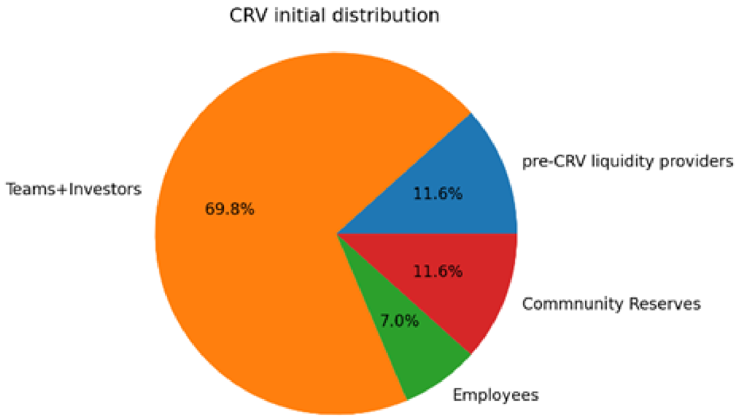


Figure3: Initial distribution of CRV token

- Team and investors have a lock-up vesting between 2 and 4 years.
- Liquidity providers have a lock-up vesting of 1 year
- Employees have a lock-up vesting of 2 years.

Observation: The boosting and stacking aim to reduce sell pressure on CRV token by locking the token over a period of time. The limitation about stacking mechanism is becoming attractive only if there is activity on the platform. Otherwise, fees are low and the APY as well and there is no incentive to lock CRV tokens to get yield.

Curve War:

Because of these locking mechanism to boost rewards for LPs though voting, some entities are trying to dominate the voting power by holding the most of veCRV tokens. It’s a competition amongst several DeFi protocols to get a share of the enormous liquidity in the Curve Finance ecosystem; the hustle to accumulate veCRV, Curve‘s governance token, and decide which pool gets Curve’s reward boost.

Liquidity problem

Why projects would pay to bribes their pools on Curve ?

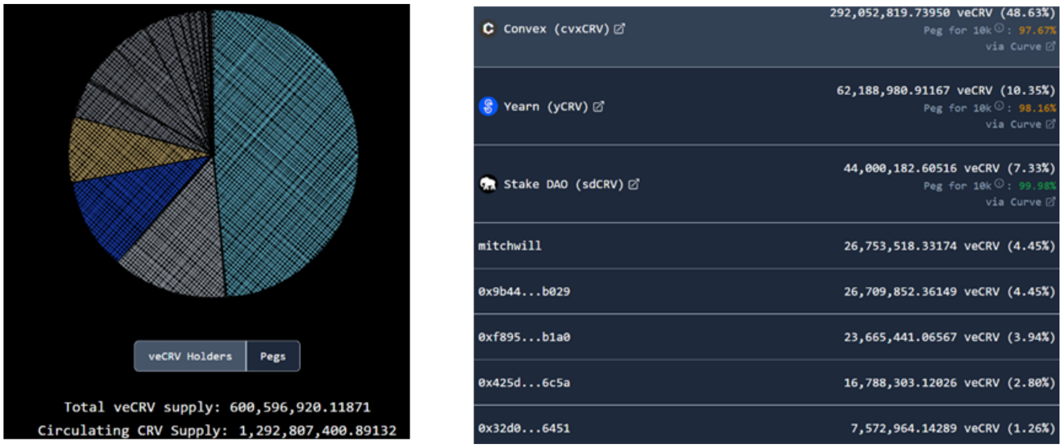
With AMM, the more liquidity in the liquidity pool, the better, as price doesn't slip/rebalance as much. This is important for any crypto asset, as illiquid pairs mean buyers and sellers get a worse deal. With stablecoins, liquidity is even more important, as they need to hold a constant $1 price.

Normally, protocols use the standard model, incentivizing liquidity with their native token.

So if protocols’ pool gets enough votes, they don't have to incentivize liquidity using their own token (less inflation for protocol tokens) by using CRV’s emission. It means the votes by CRV holders allow protocols to save money.

Protocol War

Protocols have realized how vital the control over these votes will be to anyone who wants stablecoin liquidity. So, during the first months, different protocols have tried to accumulate CRV tokens and locked them to get voting power. Here is the current situation:



Total veCRV supply: 600,596,920.11871
Circulating CRV Supply: 1,292,807,400.89132

Convex (cvxCRV)	292,052,819.73950 veCRV (48.63%) Peg for 10k: 97.67% via Curve
Yearn (yCRV)	62,188,980.91167 veCRV (10.35%) Peg for 10k: 98.16% via Curve
Stake DAO (sdCRV)	44,000,182.60516 veCRV (7.33%) Peg for 10k: 99.98% via Curve
mitchwill	26,753,518.33174 veCRV (4.45%)
0x9b44...b029	26,709,852.36149 veCRV (4.45%)
0xf895...b1a0	23,665,441.06567 veCRV (3.94%)
0x425d...6c5a	16,788,303.12026 veCRV (2.80%)
0x32d0...6451	7,572,964.14289 veCRV (1.26%)

Figure: left: Pie chart of veCRV owners / right: list of biggest holders of veCRV

Even though there are some competitors like Yearn.fi and Stake DAO, it can cleary be seen that Convex has won this war by far with barely 50% of the total veCRV locked under Convex protocol. It means that Convex is currently leading the bribes inside Curve pools. Other huge protocols in DeFi are interested in this incentivize process, like FRAX or OHM which have concentrated their effort on having the voting power on Convex instead of Curve.

Ecosystem

As it has been showed in the previous section, Curve Finance is in the middle of several interactions with DeFi protocols because it has been the liquidity hub for more than three years.

Protocols have been building on top Curve for diverse reasons and they can be categorized in four categories: **Core ecosystem, Ecosystem, Cooperative and User projects.**

Categories	Projects	Values for Users	Values for Curve
Core Ecosystem projects	Convex	Revenue aggregation, voting right rent-seeking	Increase subsidies to Curve LP and increase the CRV lockup rate
	Stake DAO	Revenue aggregation, voting right rent-seeking	Increase subsidies to Curve LP and increase the CRV lockup rate

Categories	Projects	Values for Users	Values for Curve
	Votium	Match voting rights rent-seeking	Attract more liquidity purchasers and increase the cash flow of veCRV by matching and optimizing the information on liquidity procurement
Ecosystem projects	Concentrator	Help users optimize Curve's revenue strategy and reduce the wear and tear of Farming	Improve users' willingness to stake and hold CRV\CVX for a long time, thus forming the (3,3) effect
	Clever	Help users optimize CVX proceeds obtained from vote buying, and provide users with a loan limit with future earnings from vote buying as collatera	Improve users' willingness to stake and hold CRV\CVX for a long time, thus forming the (3,3) effect
	Conic	Help users optimize the yield rate of LP in Curve ecosystem	Help Curve raises liquidity
	Pirex	Tokenize voting rights to provide CVX with a derivative trading platform based on proceeds obtained from vote buying	Improve the pricing accuracy of voting rights and enrich the financial instruments for bribing the market
Cooperative projects	Abracadabra	Borrow money with Curve LP	Improve capital efficiency of LP, increase the willingness to make a market, and lower liquidity-raising cost
	MakerDAO	Borrow money with Curve LP	Improve capital efficiency of LP, increase the willingness to make a

Categories	Projects	Values for Users	Values for Curve
			market, and lower liquidity-raising cost
	Yearn	Increase revenue and lower labor losses in Farming	Indirectly help Curve raise liquidity
	Gearbox	Increase revenue and lower labor losses in Farming	Indirectly help Curve raise liquidity
User projects	FRAX	Provide comprehensive DeFi service such as stablecoin, LSD and lending	A liquidity purchaser of Curve, one of the underlying value sources of the entire protocol, and the actual or potential CRV buyer and locker**
	Lido	LSD	**
	Rocketpool	LSD	**
	Liquity	Decentralized over-collateralized stablecoin service	**
	TUSD	Centralized stablecoin	**
	Synthetix	Issue and trade services for synthetic assets, including synthetic stablecoins and other assets	**
	Stargate	Cross-chain bridge	**

Observation:

The above table indicates that the main values protocols built-on Curve are as follows:

- Provide Curve with direct protocol revenue, i.e., liquidity procurement expenses.
- Provide experience optimization or assistance for Curve's core business - liquidity

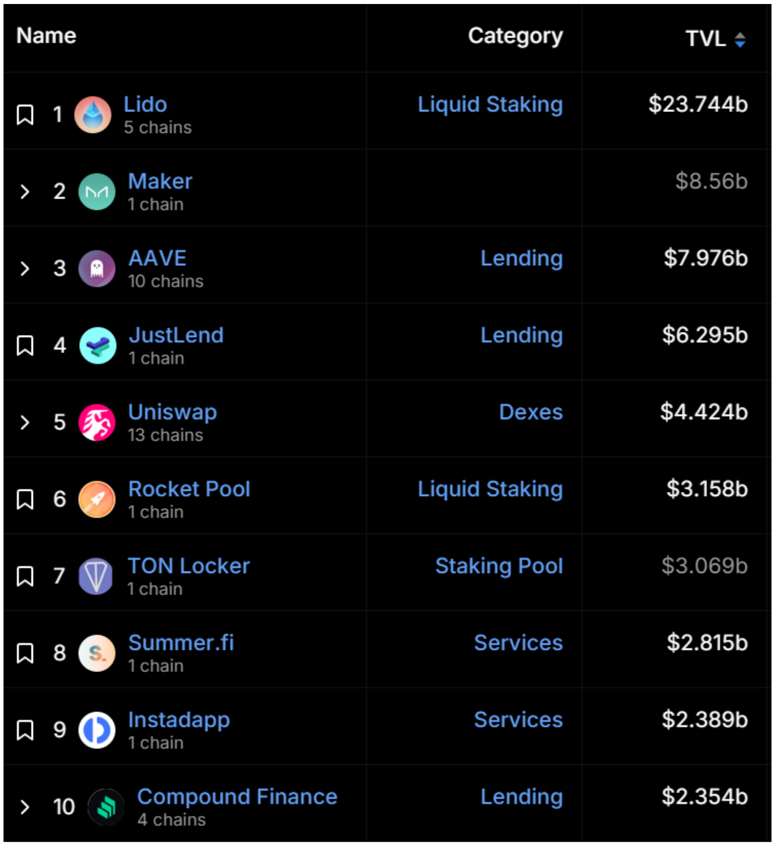
market - in liquidity fundraising or procurement.

- Absorb and increase the lockup rate of CRV (or CVX) to avoid the flow of CRV to the secondary market.

Apart from direct client-oriented projects that provide a source of underlying value to the protocol, other projects in the ecosystem play a major role in:

- Subcontracting tools and product innovation for Curve’s ecosystem. Functional innovation and continuous upgrade of experience are important conditions for Curve to maintain its phased leadership.
- Locking CRVs, Curve's high liquidity cryptocurrency, layer by layer, to avoid selling them into the secondary market to trigger a negative spiral in Curve's overall business.

To get a better understanding of the importance of the projects linked with Curve Finance, here is the list of top 10 TVL in DeFi ecosystem:



Name	Category	TVL
1 Lido 5 chains	Liquid Staking	$23.744b
2 Maker 1 chain		$8.56b
3 AAVE 10 chains	Lending	$7.976b
4 JustLend 1 chain	Lending	$6.295b
5 Uniswap 13 chains	Dexes	$4.424b
6 Rocket Pool 1 chain	Liquid Staking	$3.158b
7 TON Locker 1 chain	Staking Pool	$3.069b
8 Summer.fi 1 chain	Services	$2.815b
9 Instadapp 1 chain	Services	$2.389b
10 Compound Finance 4 chains	Lending	$2.354b

Figure: Top 10 TVL in DeFi ecosytem

As it shown, there are 5 out of 10 protocols and 3 out of top 5 that are directly "linked" with Curve protocol. For example, we could add instadapp which is built-on Compound which means that the protocol is indirectly linked to Curve. Curve is at the backbone of a lot of ramifications inside DeFi legos.

crvUSD innovative feature:

Base Curve Problem

Creating your own stablecoin is basically free money for a protocol. Just allow users to borrow against their own or external positions and charge a few % annually and/or minting/repayment fee and the protocol get new revenue stream.

But Curve had to deal with specific isssue. A negative loop in 5 steps:

1. With less liquidity swaps become less efficient
2. Which means less trading volume

3. Then less fees generated
4. Which means CRV becomes less attractive
5. To finally less TVL

To solve these problems, Curve has announced a new feature called crvUSD: a new type of stablecoin mechanism.

crvUSD solution

On May 3rd, Curve's teams announced its deployment on the Ethereum mainnet. (https://twitter.com/CurveFinance/status/1653872243556986880)

CrvUSD is a collateralized-debt protocol (CDP) stablecoin by design. While not specified yet, crvUSD will likely start by accepting ETH as collateral, similar to DAI by MakerDAO. Eventually, collateral options might include liquidity pool (LP) positions as well.

So Curve had to solve the problems of get more liquidity, Increase trading volume and Increase revenue for veCRV holders.

Get more liquidity:

Introducing a CDP stablecoin with liquidation-deliquidation mechanism creates a strong crypto/stable liquidity by itself. Additionally, allowing liquidity providers to borrow against their positions will attract even more TVL to Curve liquidity pools.

Increase trading volume:

The unique lending-liquidating AMM algorithm (LLAMMA) allows users to borrow against collateral without the risk of liquidation. At the same time, constant rebalancing is increasing trading volume in the pools and fees generated.

Increase revenue of veCRV holders:

With the introduction of crvUSD there will be new sources of fees for veCRV holders:

- crvUSD borrowing fee
- Increased trading volume due to LLAMMA

More in depth crvUSD mechanism

Curve showcases their innovation with their proprietary Lending-Liquidating AMM Algorithm (LLAMMA). Let’s look how it works:

- Price bands: LLAMA fixes specific price bands to liquidate portions of the collateral rather than liquidating fully at a specific liquidation price.
- liquidation process: when the collateral value supposedly hits the liquidation point, there will already be enough crvUSD to cover the loan value, averting a typical liquidation scenario. Conversely, as the price of collateral recovers, crvUSD is converted back to the collateral posted.

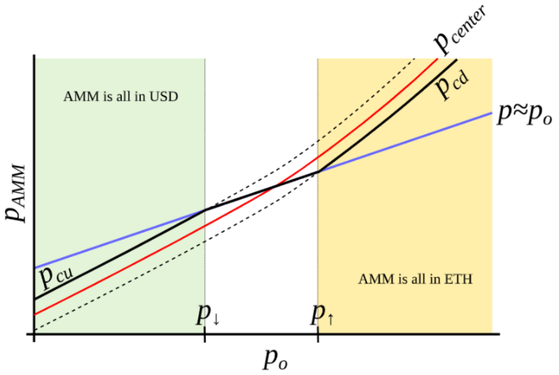


Figure 4: AMM which we search for. We seek to construct an AMM where p_{cd} and p_{cu} are such functions of p_o that when p_o grows, they grow even faster. In this case, this AMM will be all in ETH when ETH is expensive, and all in USD when ETH is cheap.

Figure: crvUSD scheme mechanism

LLAMMA solves the liquidation problem by gradually liquidating/deliquidating users' collateral, converting between collateral and a stablecoin:

- as collateral’s price goes down, LLAMMA sells it and buys crvUSD
- as collateral’s price goes up again, LLAMMA buys back collateral

This mechanism is very different from from traditional liquidation engines (aave, compound, maker, etc):

- if collateral’s price goes up, collateral gets sold
  - With LLAMMA: your collateral gets sold
- if collateral’s price goes down, bagholding USD at the bottom
  - With LLAMMA: your collateral gets buy

crvUSD is currrently available for 6 collaterals: sfrxETH, wstETH, tBTC, WBTC, WETH and crvUSD:

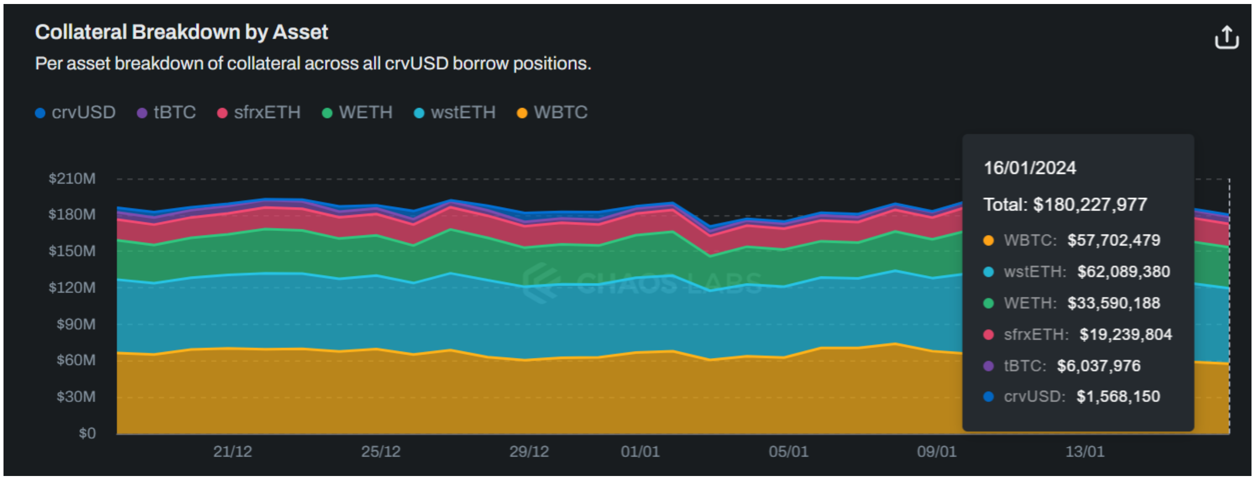


Figure: Collateral situation of crvUSD stablecoin

Currently, there are $180.23M$ backing crvUSD. The major backers are WBTC, wstETH, WETH and sfrxETH with respectively 57.7M$, 62.1M$, 33.6M$ and 19.2M$. This collateralization has been the last month.

However, the collateralization ratio has drastically increased the last week t reach 264.2%:

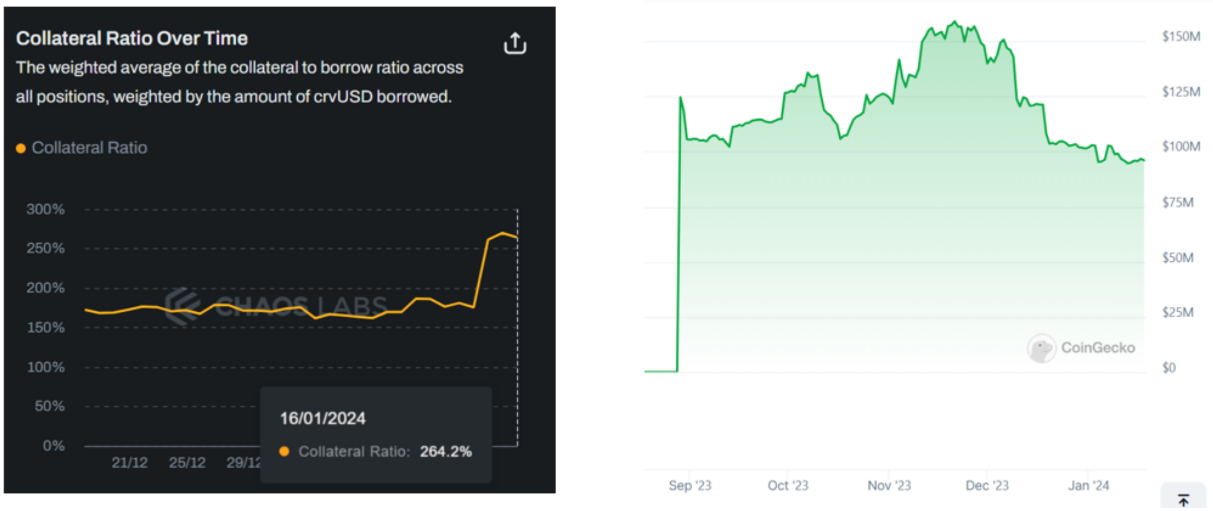


Figure: On the left, the evolution of the collateralization ratio and on the right the evolution of circulating supply

This increased was from 175.2% to 264.2%, which represent an increase of 50%. It means that huge part of crvUSD has been burnt at the beginning of this year. Effectively, crvUSD has been reduced from 150M tokens to approximativaly 100M tokens in circulation.

Drawback

However LLAMMA also has its drawbacks:

Auto-rebalancing systems are subject to permanent loss. In simple words, LLAMMA will be selling low and buying high every time when rebalancing happens.

This is a trade-off for not losing the whole collateral instead:

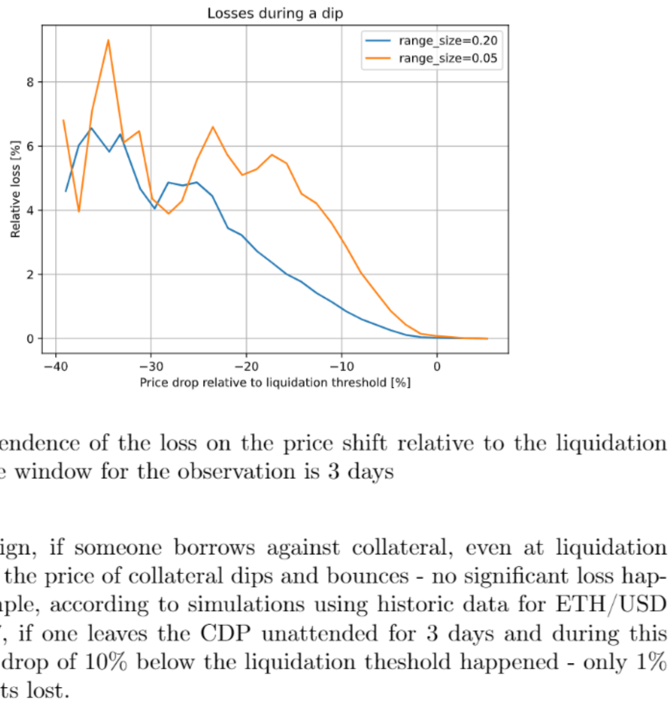


Figure 2: Dependence of the loss on the price shift relative to the liquidation theshold. Time window for the observation is 3 days

In this design, if someone borrows against collateral, even at liquidation threshold, and the price of collateral dips and bounces - no significant loss happen. For example, according to simulations using historic data for ETH/USD since Sep 2017, if one leaves the CDP unattended for 3 days and during this time the price drop of 10% below the liquidation theshold happened - only 1% of collateral gets lost.

Figure: Graph of the relative loss regarding the price drop

As per crvUSD whitepaper these losses are relatively low - only 1% of collateral gets lost (range_size=0.05) at a price drop of 10% below the liquidation threshold during 3 days period.

crvUSD and its peg

Theoretically

crvUSD is algorithmically expanding the supply (minting without collateral) when the peg is > 1$ and reducing the supply (burning) when peg is < 1$. Here is the architecture of the stabelcoin:

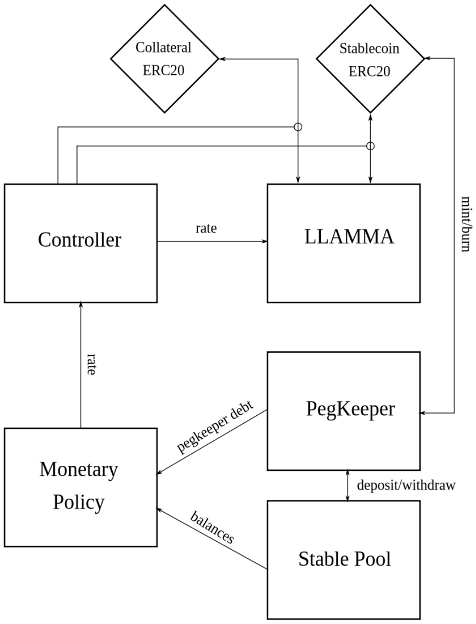


Figure: crvUSD's architecture

This way *Monetary Policy* allows keeping the peg without big PSM, reliance on third-party arbitrageurs, credit, fractional reserves, etc. Indeed *Monetary policy* contracts are integrated into the crvUSD system and are responsible for the interest rate of crvUSD markets. It is directly communicating with *PegKeeper*, *StablePool* and *Controller*.

The *PegKeeper* are contracts that help stabilize the peg of crvUSD. They are allocated a specific amount of crvUSD to secure the peg.

The *Controller* is the contract the user interacts with to create a loan and further manage the position. It holds all user debt information. External liquidations are also done through it.

In practice

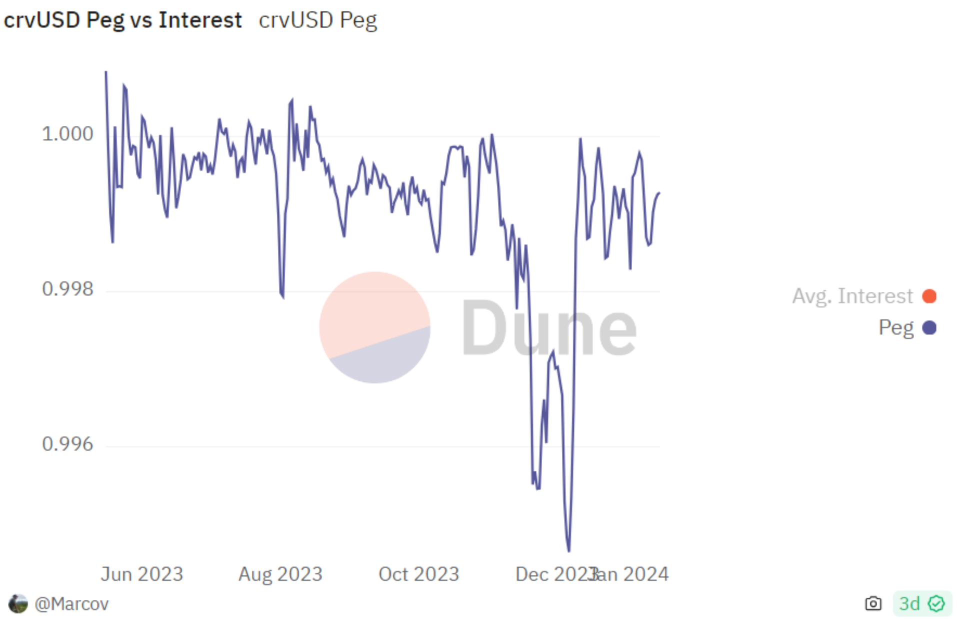


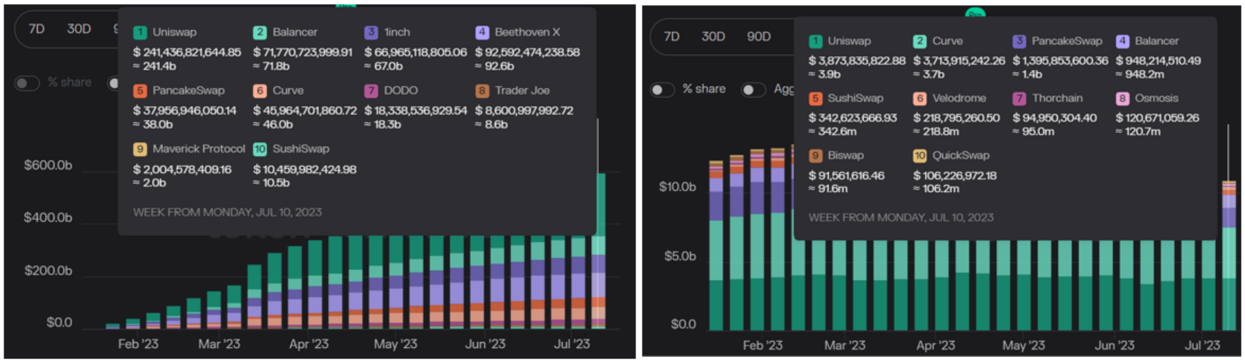
Figure: Evolution of crvUSD's peg over the last 8 months

As it can be seen, crvUSD's peg has suffered from a little drawdown during the end of the last year (surely due to the retrieve of collateral seen before). However, this drop only was only to 0.9955 which represent a depeg of 0.5% which means that crvUSD respects its peg since the launch of the stablecoin.

Market Analysis

This market analysis will be in two steps: Before and after the hack that occurs the 30th July 2023. The hack will discussed in an other section

Before hack



1	Uniswap	$ 241,436,821,644.85	≈ 241.4b
2	Balancer	$ 71,770,723,999.91	≈ 71.8b
3	1inch	$ 66,965,118,805.06	≈ 67.0b
4	Beethoven X	$ 92,592,474,238.58	≈ 92.6b
5	PancakeSwap	$ 37,956,946,050.14	≈ 38.0b
6	Curve	$ 45,964,701,860.72	≈ 46.0b
7	DODO	$ 18,338,536,929.54	≈ 18.3b
8	Trader Joe	$ 8,600,997,992.72	≈ 8.6b
9	Maverick Protocol	$ 2,004,578,409.16	≈ 2.0b
10	SushiSwap	$ 10,459,982,424.98	≈ 10.5b

WEEK FROM MONDAY, JUL 10, 2023

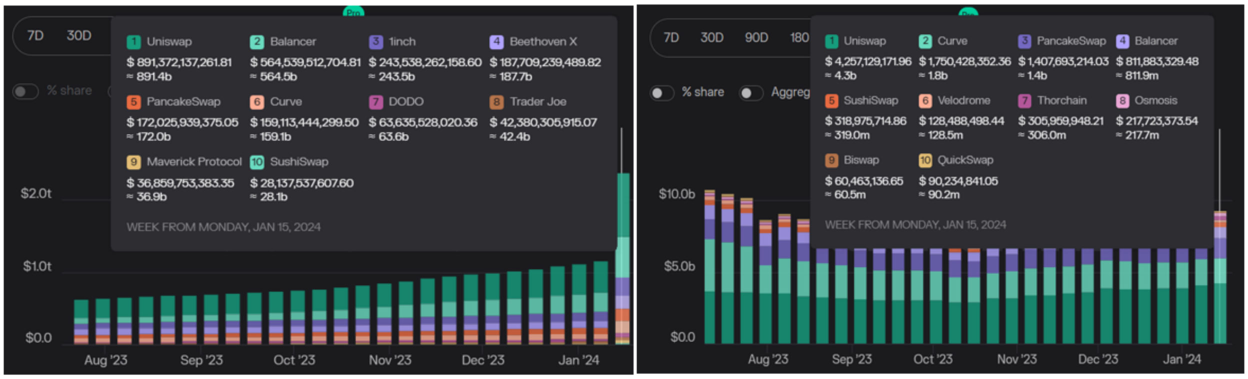
1	Uniswap	$ 3,873,835,822.88	≈ 3.9b
2	Curve	$ 3,713,915,242.26	≈ 3.7b
3	PancakeSwap	$ 1,395,853,600.36	≈ 1.4b
4	Balancer	$ 948,214,510.49	≈ 948.2m
5	SushiSwap	$ 342,623,666.93	≈ 342.6m
6	Velodrome	$ 218,795,260.50	≈ 218.8m
7	Thorchain	$ 94,950,304.40	≈ 95.0m
8	Osmosis	$ 120,671,059.26	≈ 120.7m
9	Biswap	$ 91,561,616.46	≈ 91.6m
10	QuickSwap	$ 106,226,972.18	≈ 106.2m

WEEK FROM MONDAY, JUL 10, 2023

Figure: On the left, DEX volumes ranking and the right the DEX TVL ranking (top 10) before hack

During the first part of the year 2023, Curve were standing at the second largest DeFi in TVL with around 3.7B$ and sixth largest protocol in trading volume with 46.0B$ traded on the platform. Regarding TVL, there were two DeFi protocols with more than 3.5B$ in TVL and the rest were lagging far away with 3rd protocol (Pancakeswap) at 1.4B$. Curve were clearly part of the top DeFi protocol at that time.

After hack



1	Uniswap	$ 891,372,137,261.81	≈ 891.4b
2	Balancer	$ 564,539,512,704.81	≈ 564.5b
3	1inch	$ 243,538,262,158.60	≈ 243.5b
4	Beethoven X	$ 187,709,239,489.82	≈ 187.7b
5	PancakeSwap	$ 172,025,939,375.05	≈ 172.0b
6	Curve	$ 159,113,444,299.50	≈ 159.1b
7	DODO	$ 63,635,528,020.36	≈ 63.6b
8	Trader Joe	$ 42,380,305,915.07	≈ 42.4b
9	Maverick Protocol	$ 36,859,753,383.35	≈ 36.9b
10	SushiSwap	$ 28,137,537,607.60	≈ 28.1b

WEEK FROM MONDAY, JAN 15, 2024

1	Uniswap	$ 4,257,129,171.96	≈ 4.3b
2	Curve	$ 1,750,428,352.36	≈ 1.8b
3	PancakeSwap	$ 1,407,693,214.03	≈ 1.4b
4	Balancer	$ 811,883,329.48	≈ 811.9m
5	SushiSwap	$ 318,975,714.86	≈ 319.0m
6	Velodrome	$ 128,488,498.44	≈ 128.5m
7	Thorchain	$ 305,959,948.21	≈ 306.0m
8	Osmosis	$ 217,723,373.54	≈ 217.7m
9	Biswap	$ 60,463,136.65	≈ 60.5m
10	QuickSwap	$ 90,234,841.05	≈ 90.2m

WEEK FROM MONDAY, JAN 15, 2024

Figure: On the left, DEX volumes ranking and the right the DEX TVL ranking (top 10) after hack

As it can be surprising, Curve didn’t loose its second place in TVL after the hack. However, the TVL drastically decrease to be closer to Pancakeswap’s TVL around 1.8B$. It represents a drop of 52% of the liquidity inside Curve Finance.

Observation: Liquidity retrieved hasn’t been flowing into other DeFi protocols as a diversification but direcly been taking out of the part. As a mentionne, Uniswap increased its TVL by 400M$ during the last part of the year, which could be link to Curve's hack.

Also, regarding the trading volume on the platform, Curve has kept its sixth place which means that the activity on the platform is still following the pace of the DeFi market and users are trading on the platform.

Observation: With a drop in TVL but with quite constant (slow growth) of trading volume, APY available on Curve's pools should have been increasing during the last part of the year 2023.

Let's take the example of 3crypto pool (DAI/USDT/USDC) which is the most used pool on Curve (Ethereum):

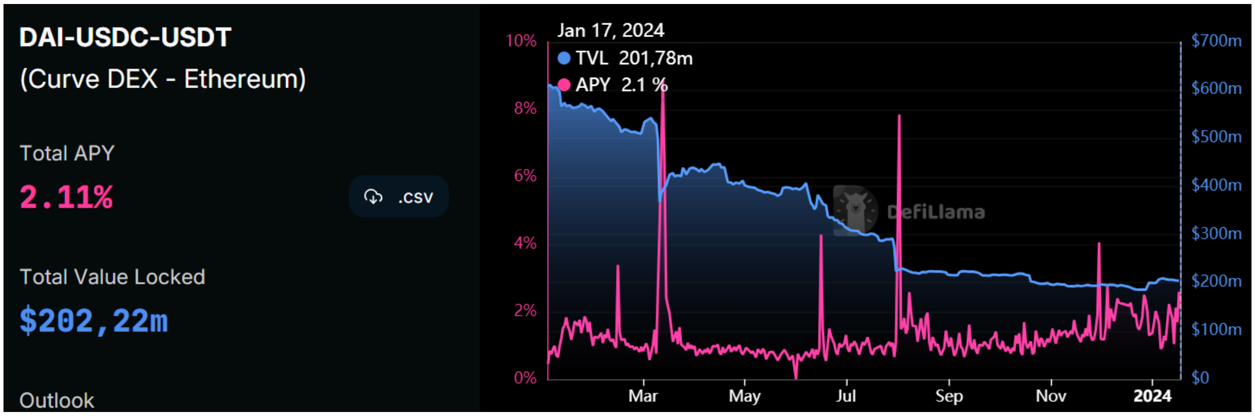


Figure: Graph representating the evolution of TVL and APY of the 3crypto pool on Curve

As it has been mentionned in the last obersvation, we can see that with the drop of TVL in end of July, the APY of the 3pool has been increased until today to reach 2.11% APY. This situation could attract more Liquidity providers who are seeking for high yields.

KPI:

Now let's look to some catching value parameters to understand where Curve stands inside Liquidity providing market. We will look at two different ratios in both circulating and fully diluted conditions:

- **P/F** = supply/fees where fees represent the aggregate fees paid by end users, source from on-chain data.

- **P/S** = supply/revenue where revenue represents the value kept by the protocol, source from on-chain data.

Protocol	Curve	Balancer	Uniswap
P/S (circulating)	**51.07x**	**20.37x**	**N/A**
P/S (fully diluted)	**157.04x**	**35.99x**	**N/A**

Protocol	Curve	Balancer	Uniswap
P/F (circulating)	**25.44x**	**10.67x**	**6.59x**
P/F (fully diluted)	**78.21x**	**18.85x**	**7.28x**

In direct comparison, Curve is clearly not the best regarding P/F and P/S ratios. Indeed, with its direct concurrent Balancer, Curve has at least the double of the ratios (max 5 times more) than Balancer has. This is due to the low circulating supply that CRV token is going through. Indeed, only half of the total supply has been minted and put in circulation. For CRV holders, it means that their holdingbags will suffer from dilution of the token.

So from a revenue over token supply point of vue, Curve is clearly not the best protocol to be out there in the DeFi space.

Hack of Curve pools - 30/07/2023

Overview

On July 30, 2023, several liquidity pools on Curve were exploited, resulting in approximately $70 million in losses and triggering panic within the DeFi ecosystem. These hacks occurred due to a vulnerability in Vyper, a third-party Pythonic programming language for Ethereum smart contracts used by Curve and other decentralized protocols. Since then, several white hackers and MEV bot operators have helped recover some of the funds, which means the actual value lost may end up being lower than the total currently reported. Below, we'll share what we know so far about the hack.

How did the exploit occur?

Vyper, a language similar to Python, has attracted developers to the DeFi ecosystem. Versions 0.2.15, 0.2.16, and 0.3.0 of Vyper revealed vulnerabilities, exposing smart contracts to re-entrancy attacks. These attacks exploit contract miscalculations, enabling theft of funds. The hacking incident commenced with a $12 million exploit on JPEG'd's pETH-ETH pool, followed by attacks on Alchemix DAO's alETH-ETH ($20 million), Metronome DAO's sETH-ETH ($1.6 million), and Curve's CRV/ETH pool ($18 million). Curve's CEO confirmed a $22 million CRV token drain from the swap pool.

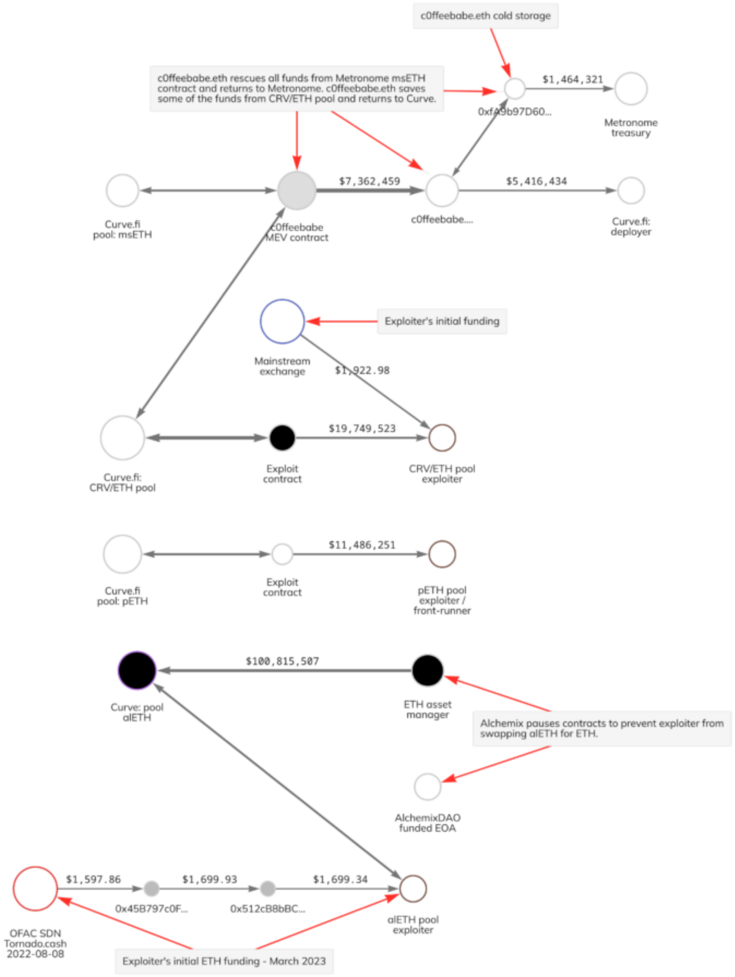


Figure: Scheme explaining how hackers drained Curve pools

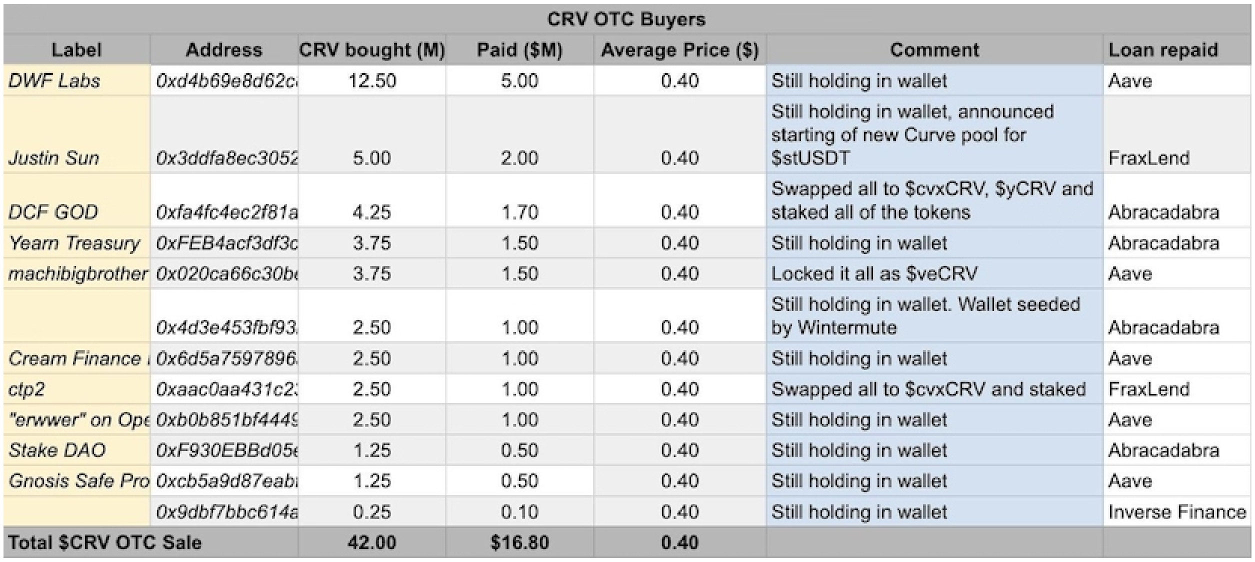
Aftermaths of the hack

After news broke of the hacks, CRV dropped in price. This decline, along with the risk that malicious hackers in possession of millions' worth of CRV could sell into the token's now-illiquid market. In particular, the lending protocol AAVE appears to be at risk of incurring debt due to Egorov's massive and well-known borrow position secured by CRV token collateral.

On Aug. 1, Egorov made headlines for his $100 million DeFi debt on Aave by collateralizing 400M$ in CRV token, as reports showed that further drops in the price of Curve DAO (CRV) tokens could potentially trigger liquidations and could have started a DeFi implosion. Seeing the risks, the Curve founder made some moves to lower his debt and utilization rate back then.

He settled his loans on the lending platform Aave, reducing his debt to $42.7 million across other DeFi protocols. According to the on-chain analytics platform Lookonchain, the Curve founder deposited 68 million CRV tokens, worth $35.5 million, to lending protocol Silo and borrowed 10.77 million in crvUSD stablecoin in the last two days. Following this, Egorov swapped the crvUSD into Tether USDT and paid all his debt on Aave.

However, this settlement hasn't been done without sacrifices. Indeed, Egorov has accepted OTC deals with several partners:



CRV OTC Buyers						
Label	Address	CRV bought (M)	Paid ($M)	Average Price ($)	Comment	Loan repaid
DWF Labs	0xd4b69e8d62c	12.50	5.00	0.40	Still holding in wallet	Aave
Justin Sun	0x3ddfa8ec3052	5.00	2.00	0.40	Still holding in wallet, announced starting of new Curve pool for $stUSDT	FraxLend
DCF GOD	0xfa4fc4ec2f81a	4.25	1.70	0.40	Swapped all to $cvxCRV, $yCRV and staked all of the tokens	Abracadabra
Yearn Treasury	0xFEB4acf3df3c	3.75	1.50	0.40	Still holding in wallet	Abracadabra
machibigbrother	0x020ca66c30b	3.75	1.50	0.40	Locked it all as $veCRV	Aave
	0x4d3e453fbf93	2.50	1.00	0.40	Still holding in wallet. Wallet seeded by Wintermute	Abracadabra
Cream Finance	0x6d5a7597896	2.50	1.00	0.40	Still holding in wallet	Aave
ctp2	0xaac0aa431c2	2.50	1.00	0.40	Swapped all to $cvxCRV and staked	FraxLend
"erwwer" on Op	0xb0b851bf444	2.50	1.00	0.40	Still holding in wallet	Aave
Stake DAO	0xF930EBBd05	1.25	0.50	0.40	Still holding in wallet	Abracadabra
Gnosis Safe Pro	0xcb5a9d87eab	1.25	0.50	0.40	Still holding in wallet	Aave
	0x9dbf7bbc614a	0.25	0.10	0.40	Still holding in wallet	Inverse Finance
Total $CRV OTC Sale		42.00	$16.80	0.40		

At the end, around 42M CRV has been dealed with an average price of 0.4$ for every participants. We could for example mentionned Justin Sun, he founder of the blockchain network Tron that bought around 5M of CRV. This partnership could explained why it can be seen that tBTC is a collateral of crvUSD.

All this drama haven't been well accepted by the Curve's community that consider this move from Egorov has a betrayal and not respecting Curve DAO ethos

Teams

Michael Egorov:

He is known to be the Founder and CEO of Curve which has garnered a ton of attention in the space as a new type of decentralized stablecoin exchange which also features yield farming and more, he was also the Co-founder and CTO of NuCypher, an encryption company, from Y Combinator. Before that, Egorov worked on infrastructure tools at LinkedIn, where he faced scaling challenges. He has experience as a scientist and physicist, where he worked in an area closely related to quantum computing and cryptography. Egorov was a bronze medalist in the 2003 International Physics Olympiad and graduated from the Moscow Institute of Physics and Technology. Linkedin: https://www.linkedin.com/in/michael-egorov/

Julien Bouteloup:

He is the co-founder of Curve Finance. He is also the Founder and CEO at Stake Capital Group. Julien previously worked at The British Blockchain Association as a Information Technology Advisor.

Julien Bouteloup is a serial entrepreneur and inventor addicted to crazy innovative ideas. He has started his entrepreneurial career building websites and selling hardware technologies atage 14. He holds a Master's degree in Electrical Engineering from Union Graduate College (USA) and a Master's degree in Computer Science and Electrical Engineering from GEM (France), specializing in Artificial Intelligence.
He started working in the research sector in USA and then went back to Europe where he started freelancing full-time and consulting in the IT sector for Security & Defence. After 2 years, he quit his freelance position to become a full-time entrepreneur and left to Asia. He has helped and started multiple tech startups in different locations: NYC, Paris, London, Hong-Kong, Brussels and Singapore.
Linkedin: https://www.linkedin.com/in/jbouteloup/

Audits

Curve DAO smart contracts were audited by Trail of Bits, MixedBytes and Quantstamp.

Curve's smart contracts have also been "tested in prod." That is, you may consider Curve contracts to have been essentially audited in public by virtue of the fact the contracts have successfully managed billions of dollars in funds for several years without any loss of funds.

Current state & Roadmap

There is no roadmap per se as all the development of the project is coordinated through the Curve community. (https://dao.curve.fi/)

However, they are currently working on a stablecoin, crvUSD, which is based on a novel mechanism called “LLAMMA” and will be normally launched this year on mainnet.