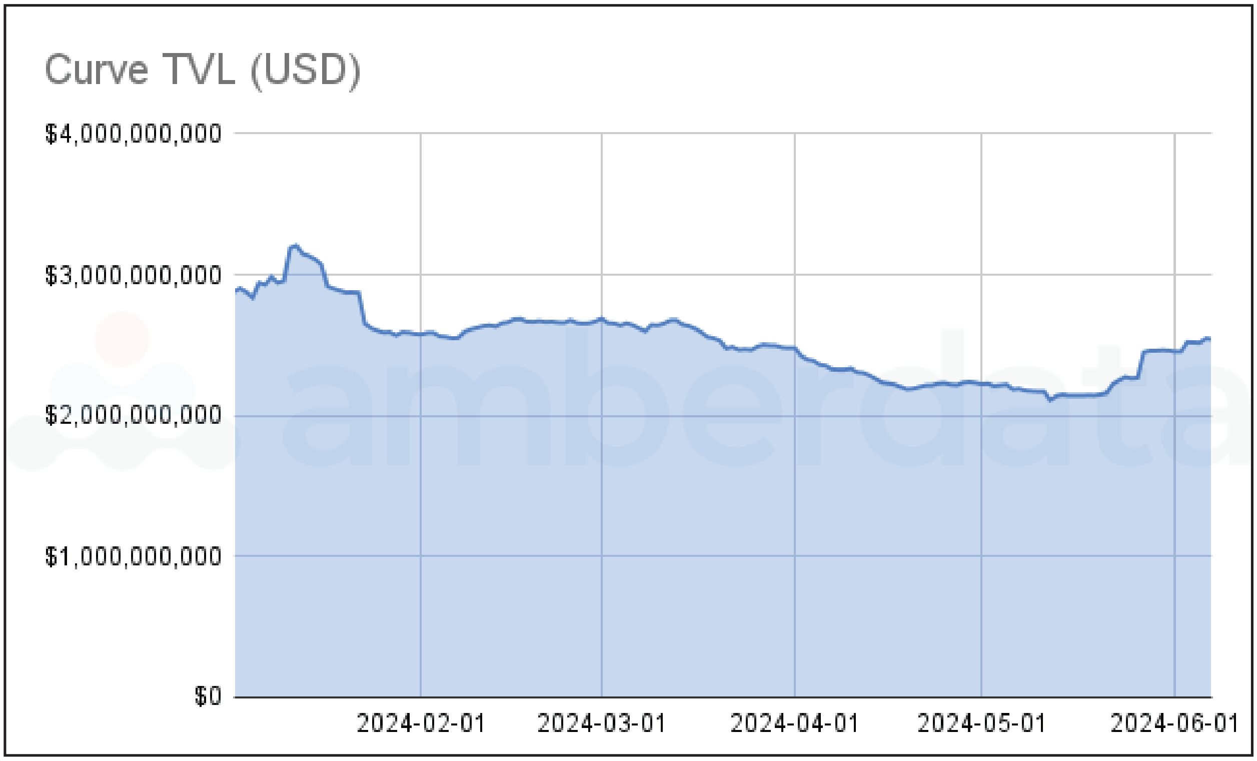
CURVE YOUR ENTHUSIASM: CURVE AND THE CURVE ECOSYSTEM DEFI PRIMER

2024-06-07

CHRISTOPHER MARTIN

amberdata.io

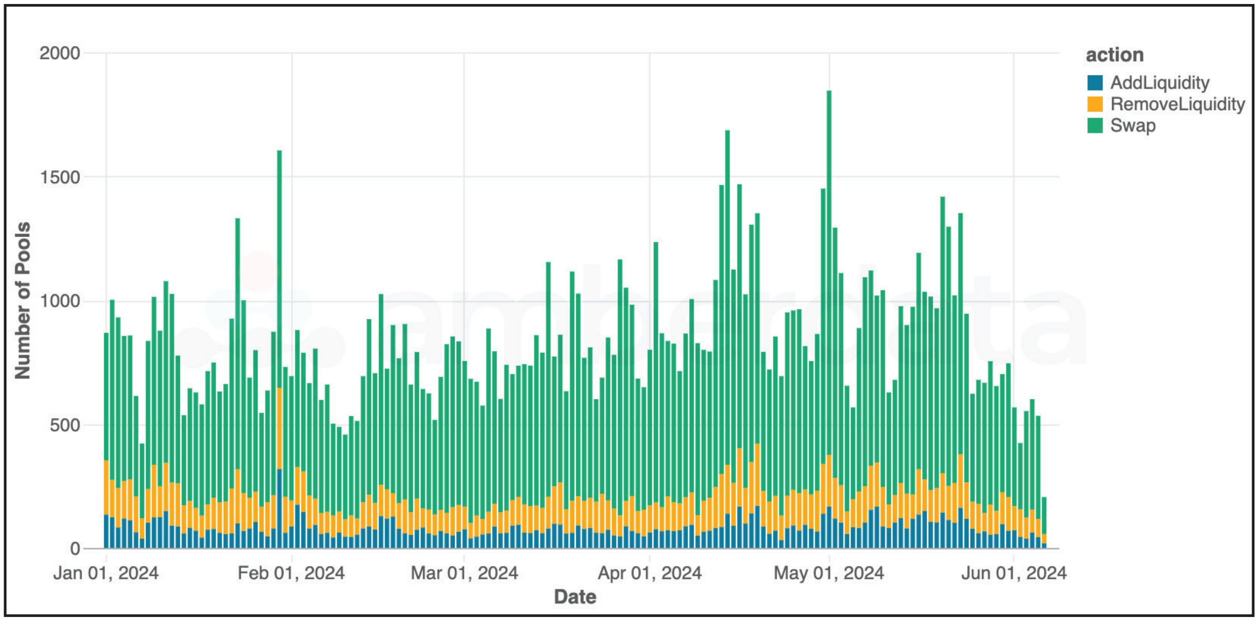
Originating as a stablecoin exchange called Stableswap, Curve has since become one of the biggest protocols on Ethereum due to its high liquidity, low slippage, creative incentive structure, active DAO, and large ecosystem. In this primer, we will explore what sets Curve apart from other protocols.



Curve TVL 2024 YTD

STABLESWAP, AKA CURVE V1

Curve's first protocol (v1) began as an Automated Market Maker (AMM) known as Stableswap. Like other AMMs, the protocol allows traders to swap between currencies in various pools. These pools are funded by liquidity providers (LPs) who earn rewards for providing liquidity in the form of yield. For AMMs, high pool liquidity balanced between the underlying tokens often provides traders with the lowest slippage and fees. As protocols receive more traders (or rather, higher trading volumes), who prefer low fees and low slippage, LPs are incentivized to provide more liquidity, earning more rewards from trading fees.

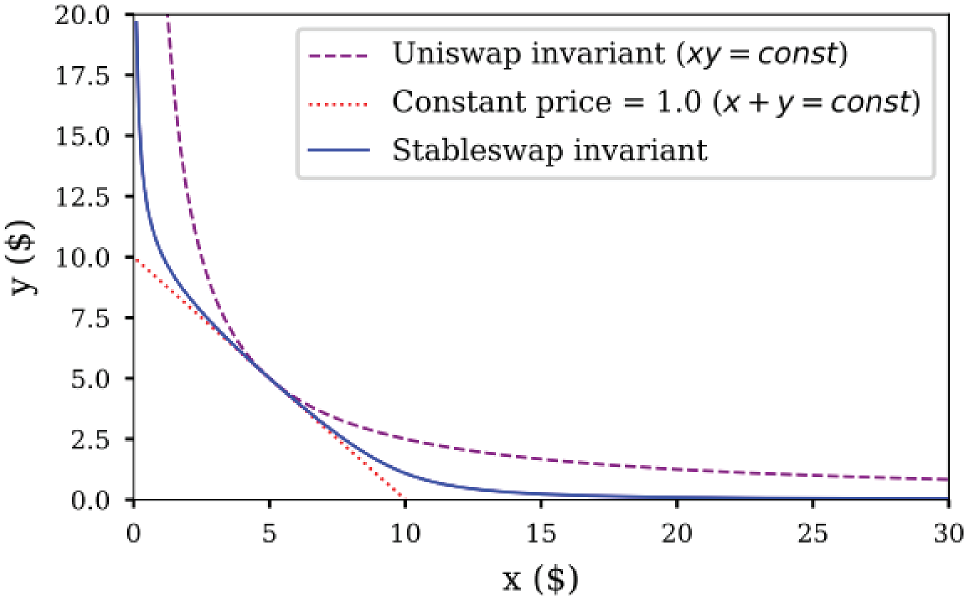


Number of daily Curve v1 pools used for deposits, withdrawals, and swaps

The protocol is decentralized, and many core pool contracts are non-upgradable, which means changes to the contract are prevented after deployment. The protocol is also non-custodial, governed by the Curve DAO and the CRV token. Compared to other DEXs like Uniswap, Curve has a limited number of pools and currently operates across several blockchain networks.

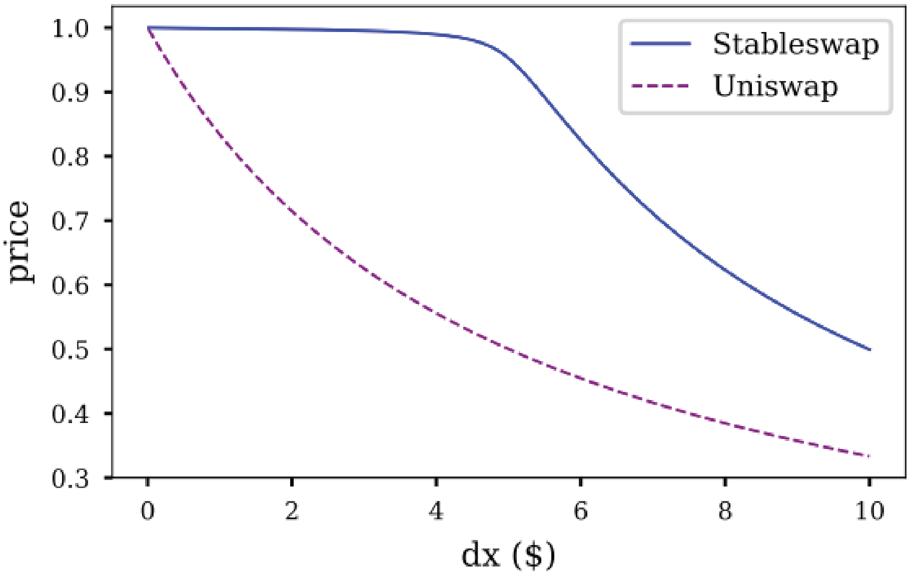
CURVE'S AMM INVARIANT

Curve's AMM differs from other popular AMMs like Uniswap, in which prices are determined by the amount of each token in a pool (x and y) being equal to a constant (k): x * y = k. For Uniswap, as one token (x) is removed from the pool and one token is added to the pool (y) – in other words, a swap of x for y – the balance (k) must be adjusted, changing the underlying token prices. The challenge for Uniswap which Curve set out to solve was that for large token imbalances (for example, a high value of X relative to Y), any minor increase in that imbalance would have a major impact on price.



Comparison of Stableswap (Curve) and Uniswap trading curves. From the ***Stableswap whitepaper****.*

To simplify this explanation: in the case of large transactions in which large amounts of X are traded for large amounts of Y, there can be major price changes for higher tokens. The main factor for this is the Uniswap invariant (k), which remains constant.

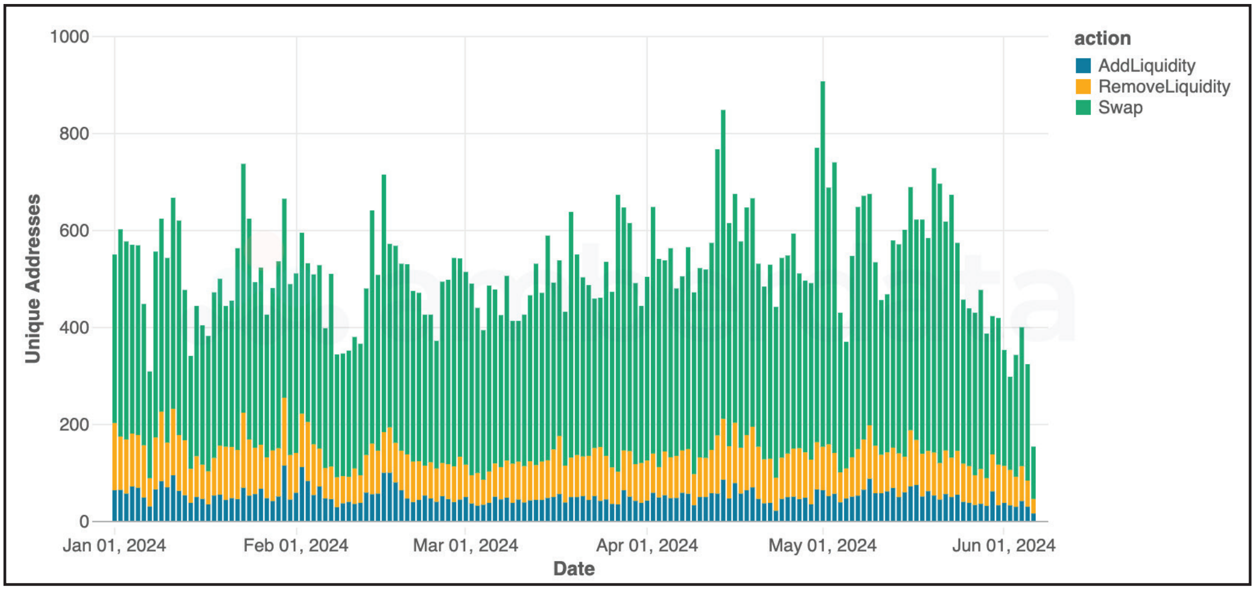


Comparison of slippage between the Stableswap (Curve) invariant and Uniswap invariant

Curve's dynamic invariant attempts to reduce slippage by staying relatively flat when a pool is balanced while shifting towards a constant-product invariant as the pool becomes unbalanced. Given that Curve started as a stablecoin AMM (hence the name "Stableswap"), there is a common assumption that the pools only consist of stablecoins. However, the protocol has since evolved far beyond stablecoins and also holds multi-token pools such as the popular 3pool: DAI/USDC/USDT.

PROTOCOL REWARDS

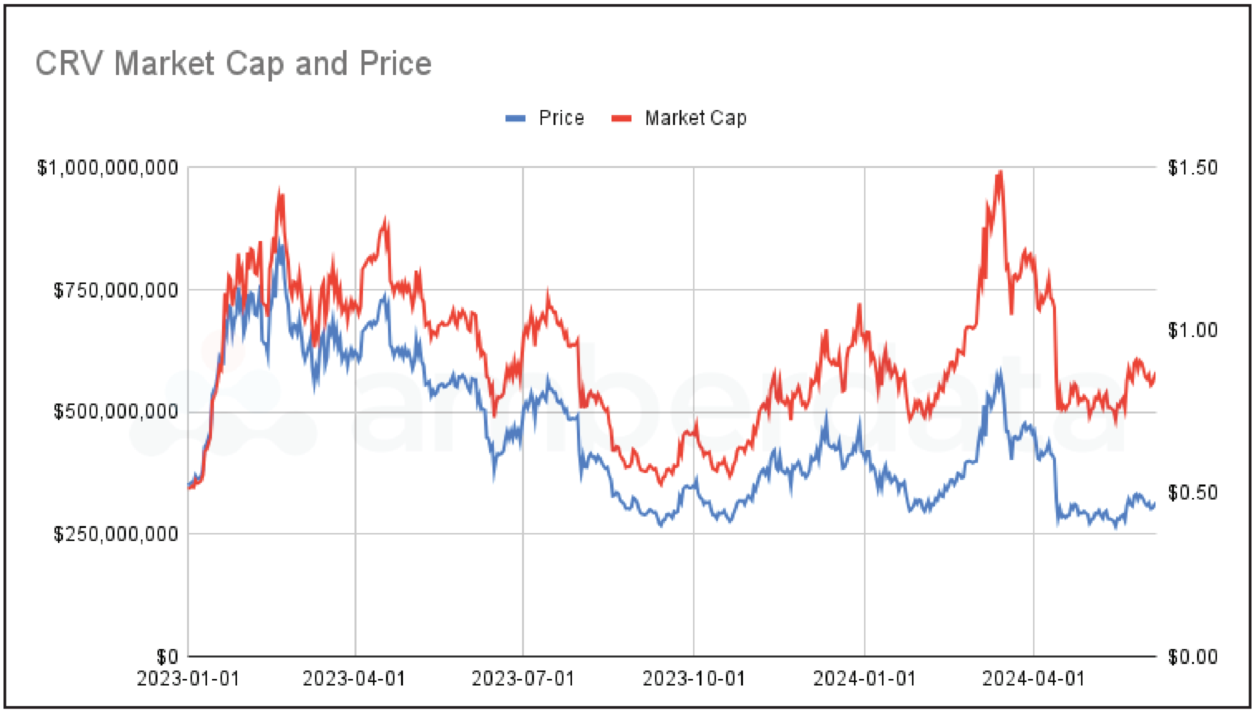
One of the key differentiators of Curve for Liquidity Providers (LPs) is the approach to boosting pools and returns. LPs receive two types of rewards: Base vAPY (variable APY) and Reward tAPR (token APR).



Number of unique daily addresses by action type on Curve v1 pools

Curve's Base vAPY is a variable APY that adjusts automatically with trading volume. For example, as trading volume increases, the vAPY increases as more fees are captured from trades. Swap fees on Curve are generally 0.04%, while some fees for deposits and withdrawals exist for unbalanced pools. Behind the scenes, some pools also lend tokens on lending protocols such as Compound or Aave to generate additional yield for LPs, increasing the pool risks and potentially the withdrawal/deposit fees at the same time. Deposit and withdrawal fees can range from 0% to 0.02% depending on pool imbalances. Balanced deposits or withdrawals have no fee.

Gauges (or liquidity pools) receive CRV emissions depending on their weight and type. Weights represent how much of the daily CRV emissions a gauge receives, with both weights and types dedicated by the Curve DAO. Votes are created using locked CRV tokens, veCRV. Rewards such as CRV emissions are part of Curve's token APR (tAPR) yield.

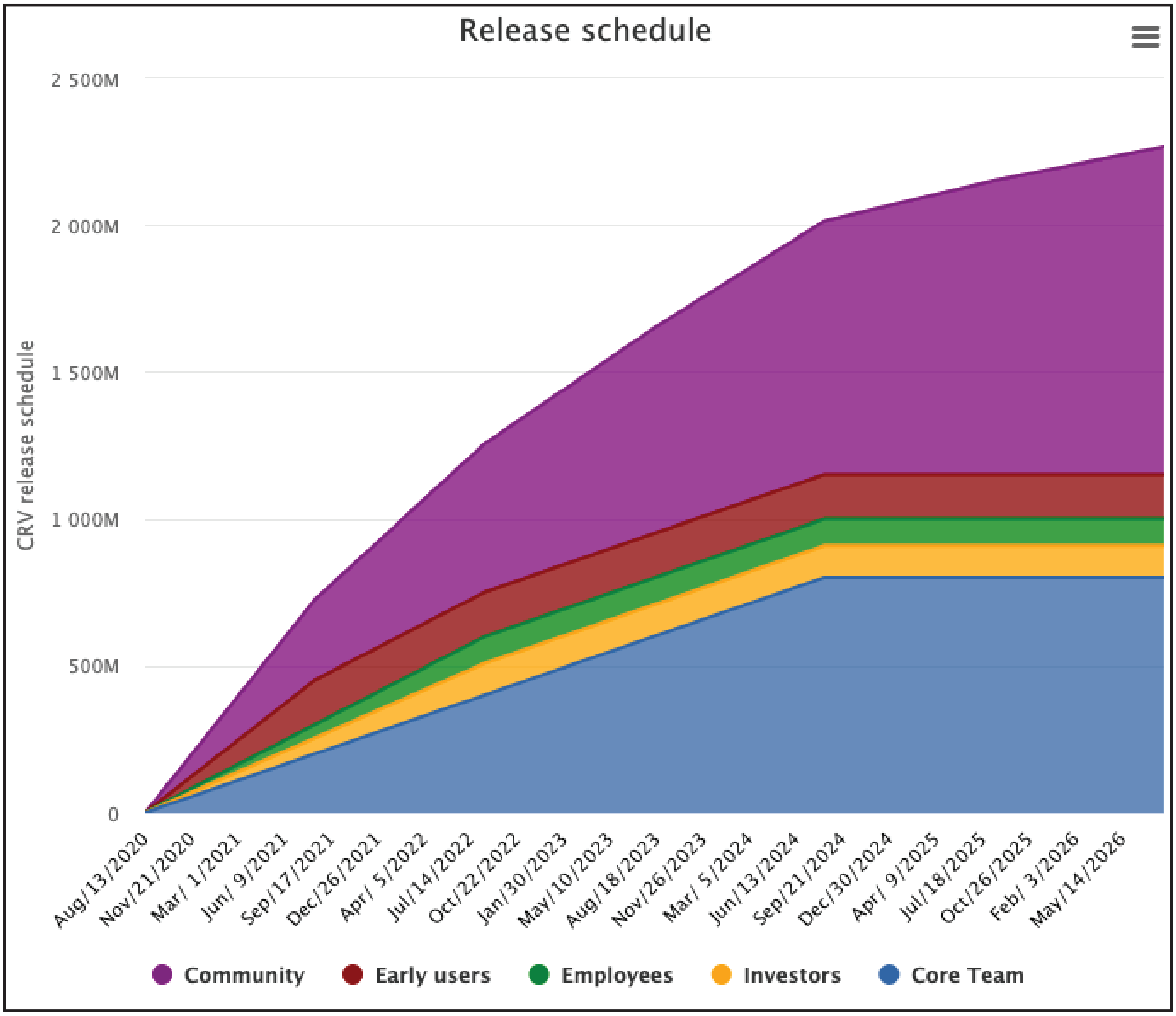


CRV Market Cap and Price

In addition, some pools offer stream rewards that further incentivize LPs. These additional incentive reward tokens are often emissions from token creators or other protocols to incentivize users to hold and lock their tokens, which can be mutually beneficial. One example is the ETH/stETH pool which rewarded LPs with LDO (Lido) tokens. Given Curve's decentralized nature, all Curve pools may permissionless stream other token rewards without approval from the Curve DAO to LPs – this does not limit token issuers or protocols from offering incentives. The combination of incentive rewards and CRV emissions make up the pools' tAPR yield.

CURVE DAO AND CRV

The Curve DAO operates the Curve ecosystem through its governance systems, using the CRV token. CRV was launched on August 13, 2020.



CRV emissions schedule, from the official Curve DAO release schedule.

The CRV token is supply capped to 3.03 billion, having launched with 1.3 billion tokens and a token schedule for the remaining 1.73 billion being minted over 355 years. The token was created for four main use cases: incentivizing LPs, allowing LPs to boost their CRV rewards, voting in governance proposals, and collecting a portion of the swap/loan fees.

The total token supply is broken down into:

- 57% for the community (through LP emissions)
- 26.5% for the Core Team
- 5% for early users (LPs on Curve before CRV emissions)
- 5% for the community reserve
- 3% to Curve employees

THE CURVE LOCKER: VECRV

Curve also introduced the veCRV token, meaning: vote-escrowed CRV. veCRV represents a non-transferrable locked CRV, with the timeframe chosen by the CRV holder. Using the Curve Locker, users can lock CRV for a given timeframe (such as 1 year or 4 years) and receive veCRV in return with the amount of veCRV returned influenced by the time frame selected. The longer the time frame a user selects to lock their CRV, the more veCRV they get in return.

By locking CRV, Curve prevents a form of governance vote manipulation in which an individual buys or borrows a token to influence a governance vote, and sells or repays the tokens immediately after the vote closes. In terms of governance, the veCRV community regularly votes on how emissions, or rewards, are distributed.

According to **Curve**: "After 2 community-led proposals and subsequent governance votes in September 2020[...], the admin fees of Curve pools were set to 50%, this means 50% of all trading fees are distributed to veCRV holders, while the remaining 50% goes to the respective liquidity providers of the pools. This distribution was implemented to align the incentives between liquidity providers and governance participants (veCRV holders). Additionally, since the launch of Curve's own stablecoin (crvUSD), 100% of the accrued interest from crvUSD markets also goes to veCRV holders. veCRV holders don't receive any direct value from lending markets, but they do receive indirect value from increasing crvUSD supply. All collected fees are converted to 3CRV (the LP token for 3Pool) and distributed among veCRV holders."

Another incentive for CRV mentioned earlier, vote-locking also enables boosted returns. "Users who provide liquidity to a swap pool and/or lending market with a reward gauge and have some vote-locked CRV receive boosted CRV rewards."

SWAPS BEYOND V1

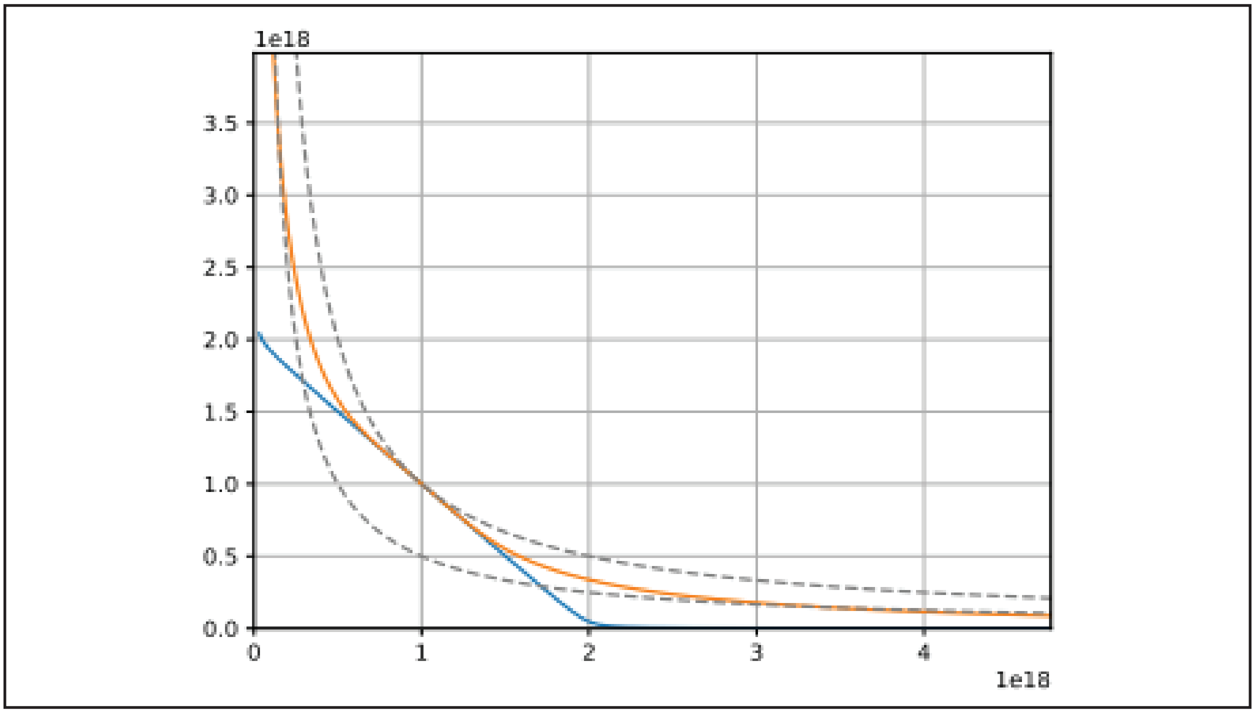
CURVE WARS

The "Curve Wars" began in 2020 and refer to escalating competition among DeFi protocols to attract users and liquidity within the Curve ecosystem. Given Curve's high TVL, the incentives to users became extremely competitive with significant benefits being given to LPs accumulating veCRV (locking CRV) to encourage them to vote on specific gauges and pools. As users voted to increase emissions on specific pools (increasing the CRV rewards for LPs in that pool) using their veCRV, protocols would provide an additional reward to those voters (such as tokens from their protocol).

As expected, the Curve Wars was hugely successful for the protocol, which became one of the most popular DEXs due to this design. The success of the v1 DEX brought about Curve v2 and Curve Factory.

CURVE V2, AKA CRYPTOPOOLS

Curve's second iteration, known as CryptoPools, brought forward pools that, unlike Curve v1 Stableswap pools, are not pegged to each other.



Comparison of AMM invariants: constant-product (dashed line), stableswap (blue), and CurvePools (orange). From the *CurvePools whitepaper*.

By pairing non-pegged assets, Curve was able to introduce new pools such as the Tri-Crypto Pool: consisting of BTC, ETH, and USDT. Given the price variability of these tokens (as compared to a stablecoin pool like USDC/USDT), liquidity concentration and management are far more important.

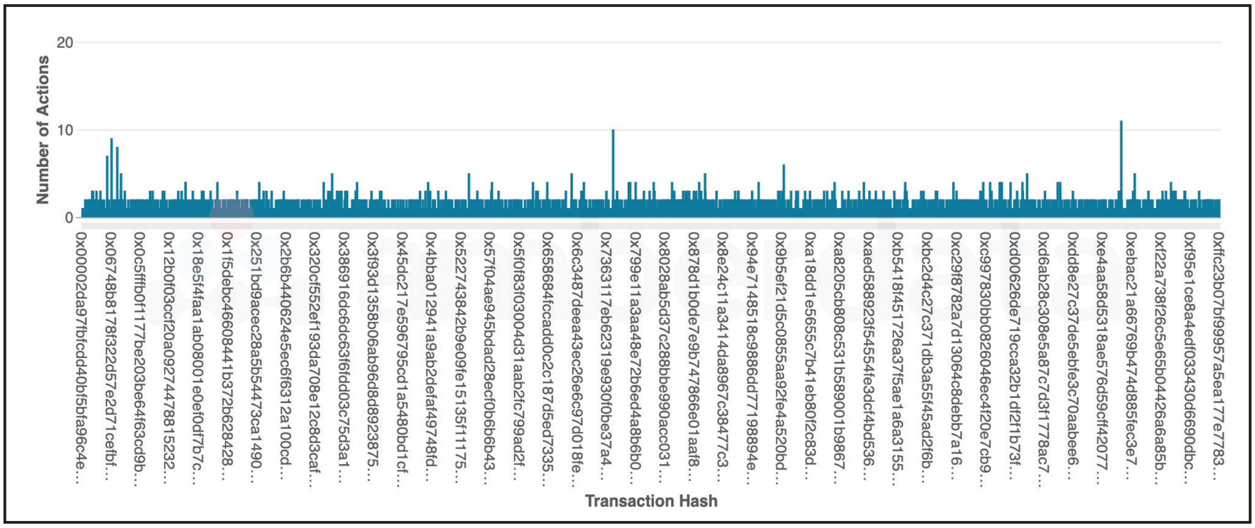
CURVE FACTORY

The Curve Factory was launched in 2021 allowing anyone to launch a Curve pool. Just one and a half months later, Curve Factory v2 was launched with several upgrades such as TWAP (time-weighted price average) oracles and gas efficiencies. Another major update included a path to become an officially recognized Curve pool by hitting key milestones such as audits and liquidity thresholds.

In July 2023, Curve Factory pools were hit with a major attack caused by an exploit against pool contracts known as a reentrancy vulnerability as a result of a faulty compiler version of Vyper – the smart contract programming language used to write the factory pools. The exploit caused over $70 million of losses from Curve pools and the draining of CRV tokens. Several other DEXs were exploited via the same vulnerability. Curve has since patched this vulnerability but the exploit brought forward significant fear across DeFi given Vyper's popularity among developers, and shed light on this relatively unknown exploit path.

FARTHER ALONG THE CURVE ECOSYSTEM

As Curve evolved and grew into the DeFi behemoth it is today, the ecosystem has expanded far beyond a stablecoin AMM. Many aspects of the expanded ecosystem leverage veCRV's non-transferable token structure. Multiple protocols (some highlighted below) have been able to use it to their advantage by incentivizing veCRV holders beyond the DAO governance structure. These external incentives have been so popular that even **Curve's documentation** has a section outlining how they work.

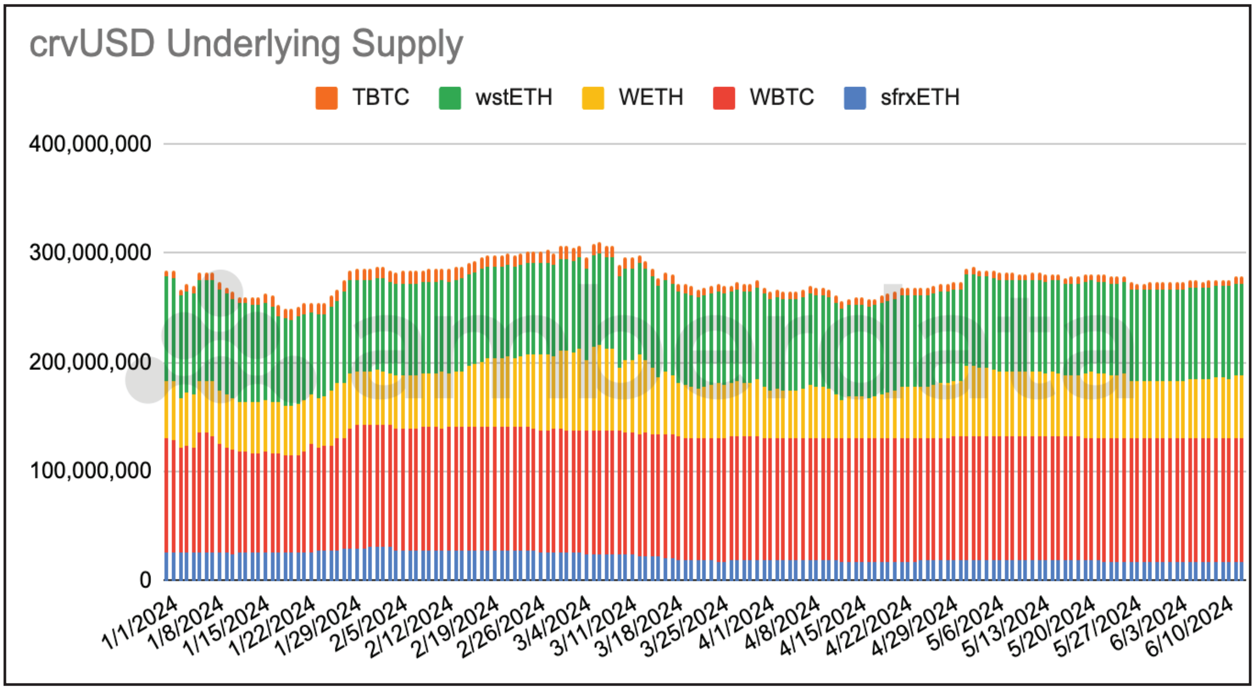


Sample of transaction hashes and the number of actions per hash (Curve v1)

Another interesting aspect of Curve is the way it has been adopted by MEV bots and contract calls – making transaction events a complicated process to analyze. Several MEV bots and sophisticated traders use the protocol due to its favorable treatment of slippage, token emissions, and portability. As such, many transactions (defined here as a single transaction hash) can have multiple actions wrapped into one. An example of this would be a contract-initiated transaction swapping token X for token Y (creating a single "Swap" transaction) and then depositing token Y into the X/Y pool to LP. Below, we outline a few Curve ecosystem projects, including some other key Curve Finance projects.

crvUSD

crvUSD (Curve USD) is Curve's USD stablecoin first launched on Ethereum Mainnet on May 3, 2023, with the official public launch on May 17.



crvUSD's underlying token supply since March 2024

Originally, the stablecoin was launched with Frax's liquid staking token (LST), frxETH, as the only supported asset and has since grown to support multiple tokens for supply: WBTC, ETH, wstETH, sfrxETH v2 (with v1 currently being phased out), and tBTC. The protocol's support for LSTs as a base token is a notable approach and gives credence to their support of decentralization.

As is the case with many over-collateralized USD stablecoins, token supply has generally been equivalent to the borrowed amount. In other words: the amount of crvUSD borrowed against collateral is roughly equal to the token's supply. Collateral in the form of the tokens previously mentioned is deposited into one of the crvUSD markets and can be borrowed against crvUSD, increasing the tokens' supply.

Rather than instantly liquidating users, the protocol uses a liquidation process in which a user's collateral is converted into stablecoins. As Curve has found: "Simulations suggest most price drops would result in the loss of just a few percentage points worth of collateral value, instead of the instant and total loss implemented by the liquidation process common to most debt-based stablecoins."

As collateral prices increase, the process reverses. The user's position undergoes trading through the AMM and crvUSD is transitioned back to the original collateral, minus any trading fees.

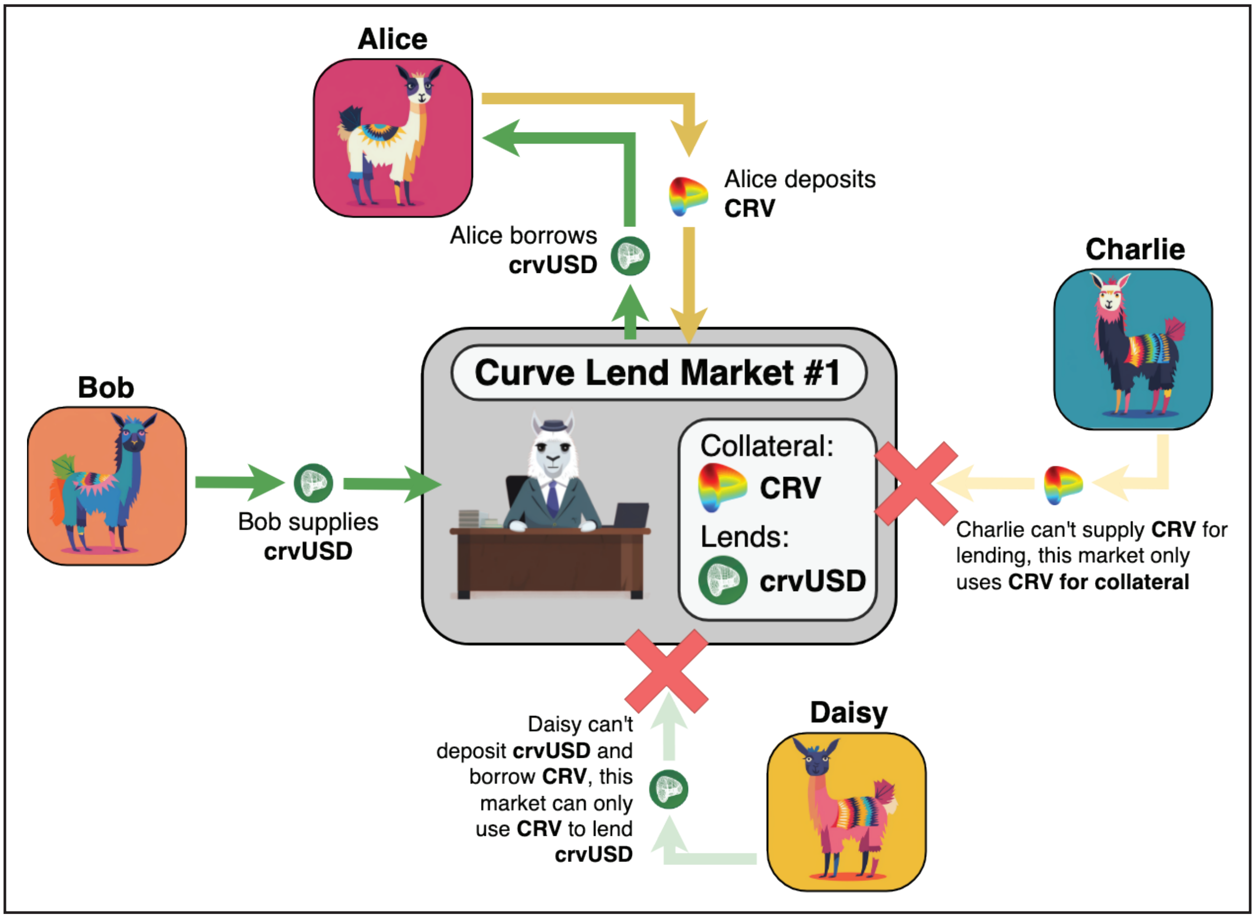
However, Curve's approach to maintaining the USD peg differs from other over-collateralized USD stablecoins. The protocols' primary stability mechanism is common: supply and demand are adjusted through borrow rate fluctuations. However, Curve also relies on "Peg Keepers" (contracts) authorized to mint or burn crvUSD.

Peg Keepers are contracts specifically designed to balance crvUSD with other stablecoins (USDC, USDT, TUSD, and USDP) by trading crvUSD with stablecoins and attempting to profit from these trades (assuming the stablecoins can return to their peg). For example, when the balance of crvUSD is too low in a given pool (such as the crvUSD/USDC pool), the Peg Keeper can mint crvUSD to trade and maintain the peg between the two stablecoins. When the pool has an oversupply of crvUSD, the Peg Keeper can repurchase crvUSD and burn.

crvUSD plays a key role in Curve Lending.

CURVE LEND (LLAMMALEND)

Curve Lend is Curve Finance's DeFi Lending protocol allowing users to borrow crvUSD against any collateral token – or borrow any token against crvUSD. The protocol uses the "soft-liquidation" mechanism LLAMMA.


Alice
Alice deposits CRV
Alice borrows crvUSD
Charlie
Bob
Curve Lend Market #1
Collateral: CRV
Lends: crvUSD
Bob supplies crvUSD
Charlie can't supply **CRV** for lending, this market only uses **CRV for collateral**
Daisy
Daisy can't deposit **crvUSD** and borrow **CRV**, this market can only use **CRV** to lend **crvUSD**

Curve Lend Market flow diagram. From Curve's lending overview.

As Curve describes in their documentation: "In simple words: LLAMMA automatically converts collateral into crvUSD as the collateral price decreases, and vice versa, converts crvUSD back into the collateral asset when prices rise. Due to this, there is no instant hard-liquidation when certain collateral prices are reached, but during the soft-liquidation process, losses occur and consequently decrease the health of a loan. When the health drops below 0%, the user is eligible for hard-liquidation. The user's collateral can be sold off, and the position will be closed (just as in regular liquidations)."

Curve Lending allows users to borrow crvUSD against any collateral token or to borrow any token against crvUSD while benefiting from the soft-liquidation mechanism provided by LLAMMA. This innovative approach to over-collateralized loans enhances risk management and user experience for borrowers. Additionally, Curve Lending allows users to generate interest through lending (supplying) their assets to be borrowed by others.

EXTERNAL PROTOCOLS

As previously mentioned, the Curve ecosystem has expanded far beyond the protocol's domain and a wide variety of external protocols have developed on top of Curve. Perhaps the most well-known of these is Convex.

Convex Finance

Convex Finance is perhaps the largest external Curve ecosystem protocol, with a reported TVL as of June 2024 of $1.74 billion. The protocol provides LPs with boosted Curve rewards as well as supporting Prisma, Frax, and f(x) Protocol.

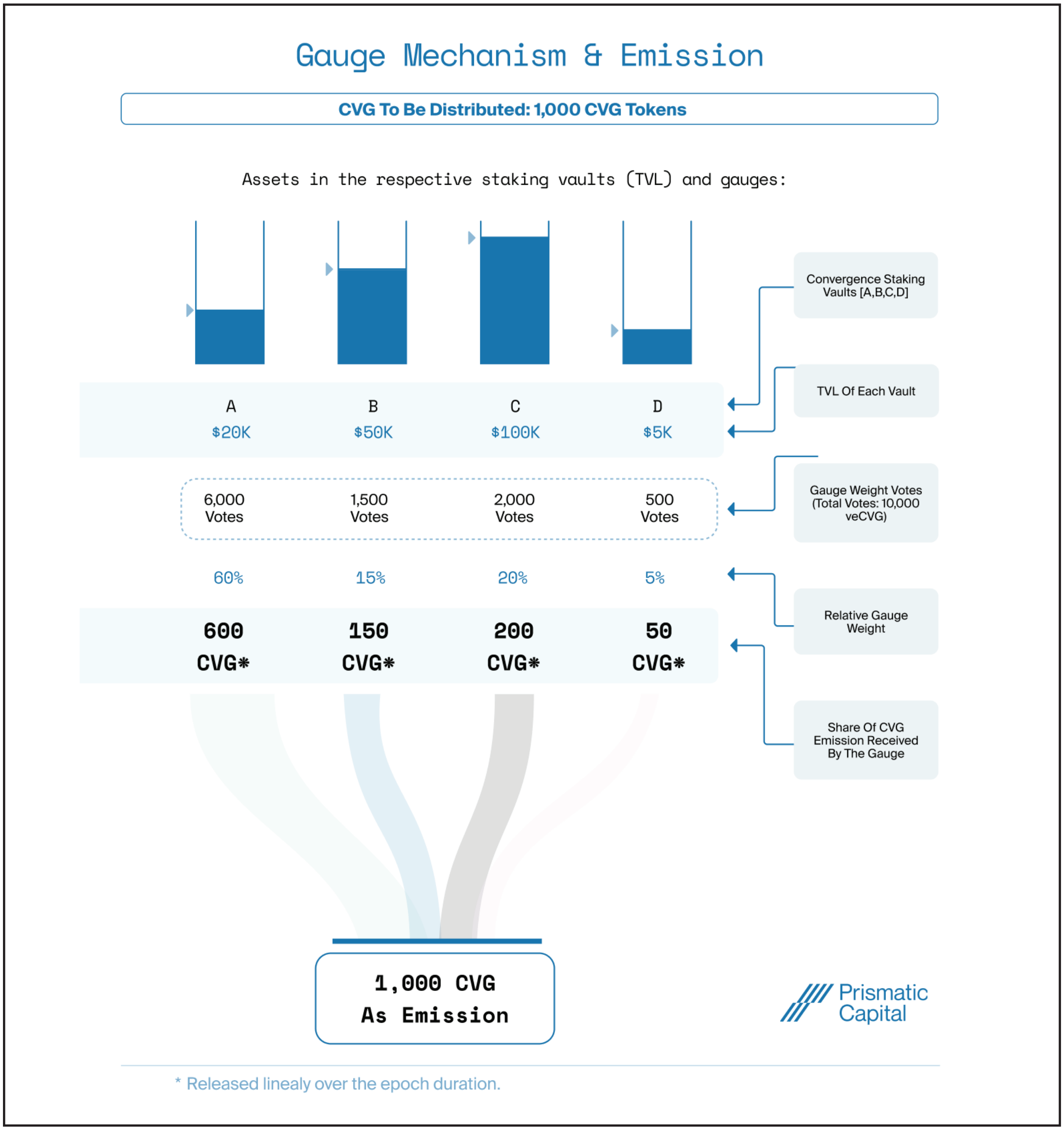
Curve LP tokens, representing stake in a Curve pool, can be re-deposited on Convex spreading yields across a larger group of LPs which boost pools through Curve boosting. By using Convex, CRV held by Curve LPs do not need to be staked into vote-locked veCRV, giving users benefits of additional yield but at the cost of governance benefits. The protocol also boosts CRV rewards and provides LPs with CVX (Convex tokens).

To do this, Convex provides Curve LP token depositors with Convex LP tokens, which can be then staked into a Convex rewards contract earning them CVX and boosted CRV. CRV deposited into Convex is locked forever as veCRV but returned to the user as cvxCRV and can be swapped on external liquidity pools back for CRV. cvxCRV can then be staked on Curve, returning 3CRV, or Curve admin fees.

Convex uses veCRV to vote on Curve liquidity pool gauges, which dictate how Curve distributes CRV to Curve liquidity pools). CVX holders can vote on Convex governance votes.

Convergence

Convergence is a governance aggregator, incentivizing liquidity across multiple protocols – as they mention in their white paper: “One could describe Convergence as a ‘decentralized governance hedge fund’ as well as a ‘sustainable liquidity providing incentivizer,’ built on top of DeFi2.0 protocols.”

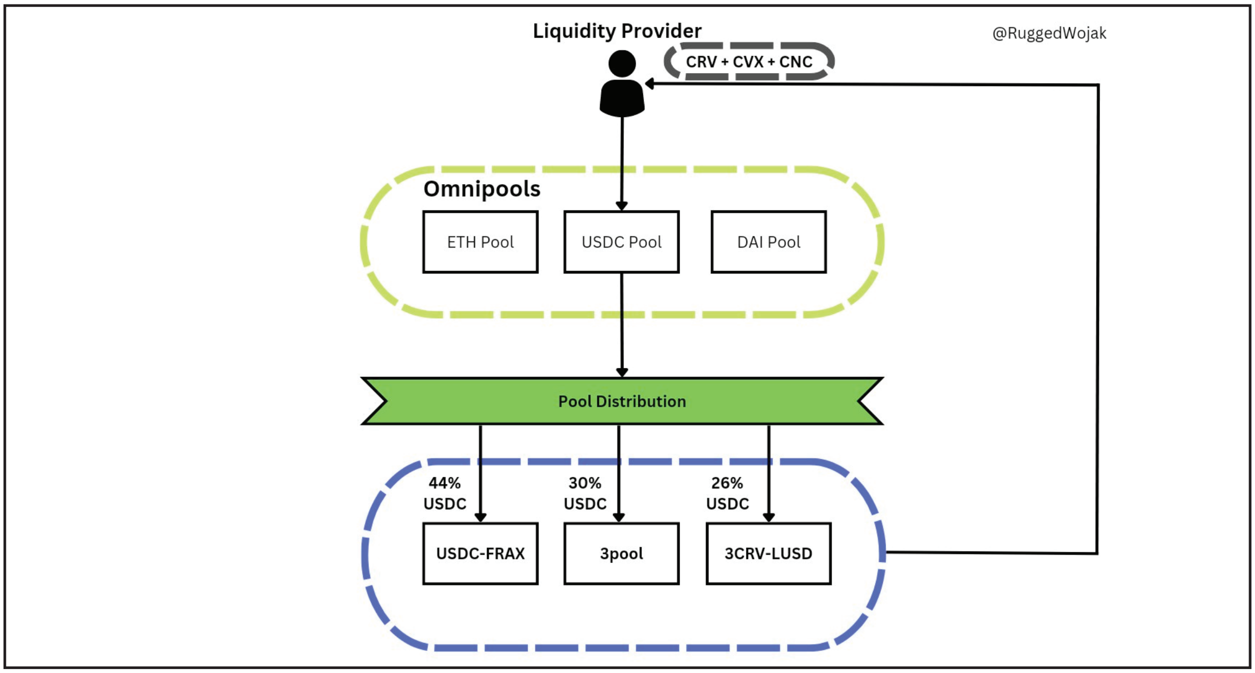

Gauge Mechanism & Emission
CVG To Be Distributed: 1,000 CVG Tokens
Assets in the respective staking vaults (TVL) and gauges:
A
$20K
B
$50K
C
$100K
D
$5K
6,000 Votes
1,500 Votes
2,000 Votes
500 Votes
60%
15%
20%
5%
600 CVG*
150 CVG*
200 CVG*
50 CVG*
Convergence Staking Vaults [A,B,C,D]
TVL Of Each Vault
Gauge Weight Votes (Total Votes: 10,000 veCVG)
Relative Gauge Weight
Share Of CVG Emission Received By The Gauge
1,000 CVG As Emission
Prismatic Capital
* Released linealy over the epoch duration.

Convergence gauge mechanism and emissions example. From Prismatic Capital.

Convergence is similar to Convex in many ways by participating in Curve (as well as other protocols) governance for the benefit of optimizing their LP’s yields across multiple protocols such as Curve, Convex, and OlympusDAO. The Convergence governance token CVG allows the protocol to have a decentralized governance structure while redistributing rewards to token holders and stakers.

Conic Finance

Conic Finance may be a familiar name. The protocol lost $3.2 million in July 2023 after a re-entrance exploit but has since made a huge comeback after raising $1 million from Curve founder Michael Egorov weeks after the incident. The protocol continues to rebuild and has even introduced Conic v2 in January 2024.



Conic Finance Omnipool diagram. From @RuggedWojak.

Conic allows Curve LPs to earn yield through "Omnipools," or liquidity pools in which deposits of a single asset are spread across several different Curve pools. LPs of an Omnipool gain exposure to multiple Curve pools through Omnipool LP tokens, and receive CNC (Conic token) emissions when staking Omnipool LP tokens. Curve liquidity is then staked on Convex.

Similar to Curve's governance structure, CNC holders can lock their tokens and receive vlCNC (vote-locked CNC) in return. Vote-locked token holders can take part in bi-weekly liquidity allocation votes to determine the distribution of LP tokens to Curve pools, vote on assets to add or propose protocol changes, vote on Omnipool rebalancing rewards, and vote on whitelisting/blacklisting Curve pools for Omnipool liquidity.

Conic v2 introduces "liquidity allocation modules" (LAMs) providing Omnipools with more optionality including non-Convex-based rewards, Omnipool support for multiple LAMs, and the ability to support more features like crvUSD Peg Keeping.

CortexDAO

Cortex provides simplified participation in Curve and Convex governance systems while providing diversified exposure to a portfolio of yield-generating strategies. The DAO created the Convex Index to provide single token holders of the Index (idxCVX) exposure to a variety of liquidity pools.

The protocol operates by pooling deposits created by purchases of the index/index token and deploying capital across active Curve LP pools within the index. The governance token CXD votes on the tokens underlying the index and balancing. Representing liquidity provided on a liquidity pool, the Curve LP pool tokens are then staked on Convex to generate additional rewards. The CortexDAO claims CRV/CRX and any other token rewards generated from the liquidity provided, and swap these rewards for stablecoins that can be re-deployed into active index strategies. Finally, the CortexDAO rebalances positions to target weights.

The Cortex Index represents one of many interesting protocols creating a diversification strategy to simplify user experiences on top of several other DeFi protocols. By leveraging Curve and Convex, the DAO has found value in supporting other protocols while providing a service that also benefits users.

Napier Finance

Napier Finance aims to provide yield management strategies and fix-term assets to the Curve ecosystem. Leveraging incentives from Curve and Convex, Napier provides LPs with token rewards (CRV, CVX, and Napier's native token) on top of staking/lending yields. The protocol consists of two main parts: minting and AMM.

The "Napier Minting System" is designed to take any yield-bearing token (such as liquid staking derivatives) and create a fixed-income equivalent by separating it into a principal token and the yield token, which represents the yield generated by the target asset. For example, rETH (Rocketpool-staked ETH) can be split into a token representing the underlying ETH asset (principal token) and the rETH yield (yield token). The Napier AMM facilitates trading between principal and yield tokens.

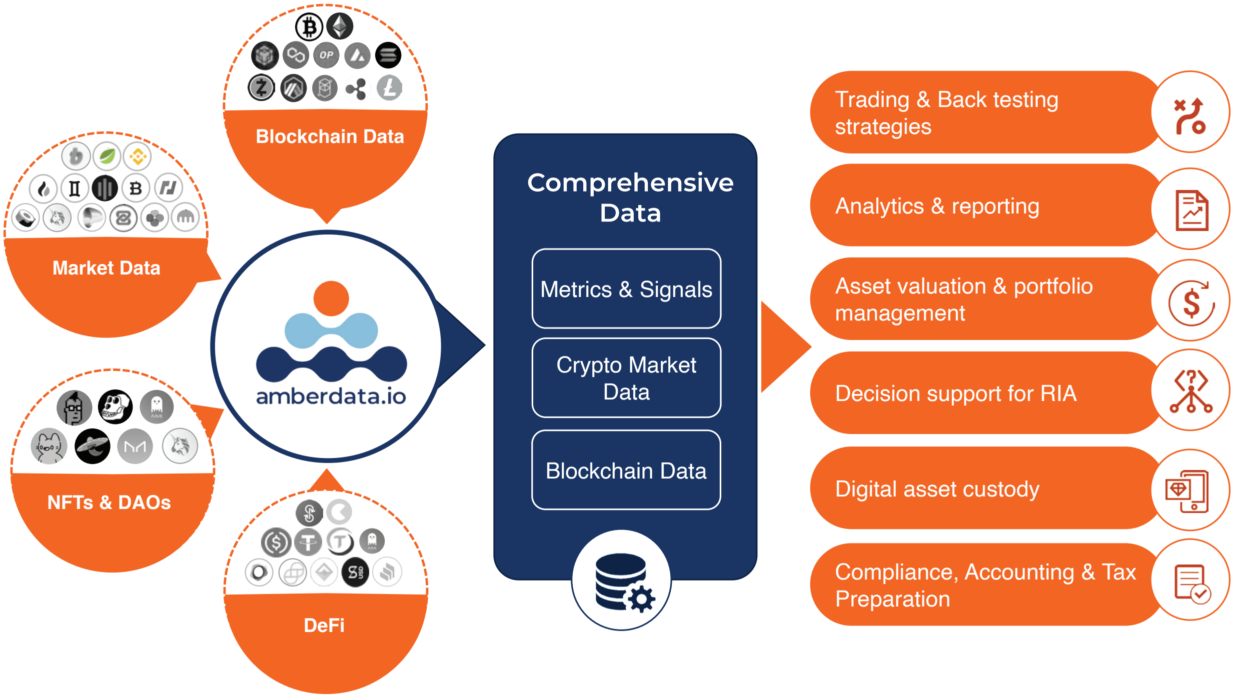
Similar to Curve, Convex, Conic, Convergence, and more, Napier plans to use the veToken model (i.e., veCRV, vlCNC, etc.) for governance as token holders lock their tokens to receive a vote-locked equivalent and participate in governance votes on protocol fees, pool durations and parameters, and emissions schedules.

The protocol is currently running "Llama Race" (launched April 10, 2024) – a point tracking system counting contributions to the Napier and Curve ecosystems. Campaigns called "quests" are designed to reward users for taking part in various activities such as connecting their accounts with Twitter and spreading tweets or referrals. This type of user bootstrapping is not uncommon in the DeFi landscape and has been a popular source of income for airdrop hunters for several years now.

CONCLUSION

Curve's initial launch as a stablecoin DEX has proven hugely successful for its innovative approach to rewards, multi-token liquidity pools, and low slippage. The protocol has since launched into lending, crvUSD, and factory pools but the culture of the protocol has largely remained unchanged. As stablecoins continue to evolve in the DeFi landscape and as adoption grows on both custodial platforms like centralized exchanges and decentralized wallets, Curve has cemented a place in the DeFi world. The long-term question is: will it be enough for them?

LOOKING TO ENTER DIGITAL ASSETS?



If you're looking to enter the digital asset space, you need Amberdata.

Our platform connects to all the blockchains and markets that matter today, allowing a comprehensive view of crypto markets, blockchain networks, NFTs, DAOs, and DeFi. We provide real-time and historical transparency into markets and price discovery across spot, derivative and decentralized exchanges, as well as on-chain data from the most active cryptocurrency networks and protocols.

Our data solutions support all pre- and post-trade functions. We provide deep market data, down to Level 2 order books, facilitating backtesting of quant trading strategies. And our blockchain data provides transparency not seen with other asset classes, allowing you to track pending transactions and wallet balances over time across various blockchain networks, as well as market cap and total value locked. You can also create analytics dashboards with fundamental data to track network health and understand DeFi data like liquidity and lending rates. For fund accounting and administration, you'll know what was in a wallet at any time and what it was worth in any currency. For institutions that want to do custody themselves rather than outsource it, we provide the on-chain data needed.

With Amberdata, you get a single integration point for market and on-chain data, eliminating the need to integrate offerings from multiple vendors and allowing you to accelerate time to market for your digital asset products. We've built our data sets with institutional use cases in mind, providing the easy to consume formats and reliability you receive with traditional asset classes.

Request a demo to find out how the Amberdata platform solves digital asset data challenges and enables institutions to enter the digital asset space quickly, easily, and reliably. amberdata.io/demo

amberdata

amberdata.io
docs.amberdata.io
hello@amberdata.io