Risk Assessment - CRV Collateral Asset on FiRM

Useful Links

- Coingecko: https://www.coingecko.com/en/coins/curve-dao-token
- Website: https://curve.fi/
- Github: https://github.com/curvefi/curve-contract
- Blog: https://curve.substack.com/ (unofficial)
- Twitter: https://twitter.com/CurveFinance
- Main Discord: https://discord.com/invite/9uEHakc
- Bug Bounty: https://classic.curve.fi/bugbounty
- Docs: https://curve.readthedocs.io/
- Resources: https://resources.curve.fi/
- Voting: https://dao.curve.fi/dao
- Forum: https://gov.curve.fi/
- Prime Rating Report: https://www.prime.xyz/ratings/curve-finance

Background

Curve is an AMM exchange protocol with the primary function of allowing for similar-price token transactions with low slippage and handling fees. Curve's AMM model is an engineered version

of Uniswap v2.0's constant product market maker model. Its StableSwap algorithm is explicitly designed to create more market depth by concentrating the liquidity near the ideal price for similar priced assets and minimize slippage when exchanging them, even in large volumes. The Curve DAO token was launched in August 2020 and has achieved great success thanks to its utility. Curve experienced serious growth in the second half of 2020, providing users with low slippage and low fees for exchanging similar stablecoins and ERC-20 tokens. Now, in 2023, it still holds its own in a competitive Defi market with a $714M MC, continuation in community growth and improved voting platform. Curve Pioneered the staking to vote model (veCRV) with many DeFi protocols following behind.

Protocol Analysis

Org. Structure

- ☐ **Is the Protocol a DAO? How is it governed eg. delegates , snapshot**

Curve is fully decentralized with the launch of Curve DAO. There's an Emergency DAO which is able to pause the pools during the first 2 months in existence and Curve DAO can unpause them at any time. Curve Emergency DAO has 9 members and 59.999% support and 51% quorum Curve Emergency DAO can act when there's a danger of loss of funds and call the kill_me function of Curve Pool contracts which disables all functionality except for withdrawals. Curve pools can be reenabled back by either Emergency DAO or Curve DAO. The Emergency DAO is controlled by Curve DAO which can add or remove Emergency members.

Smart contracts CANNOT be upgraded. This limits actions in a case of emergency, but leaves users fully in control of their funds.

Governance is completely in the hands of the user and influences all operations of the protocol as stated above. Details from Curve's gitbook state:

- To vote on the Curve DAO, users need to lock vote lock their CRV. By doing so, participants can earn a boost on their provided liquidity and vote on all DAO proposals. Users who reach a voting power of 2500 veCRV can also create new proposals. There is no minimum voting power required to vote.
- veCRV stands for vote escrowed CRV, it's a locker where users can lock their CRV for different lengths of time to gain voting power. Users can lock their CRV for a minimum of a week and a maximum of four years. As users with long voting escrow have more stake, they receive more voting power.

- ☐ **Does Protocol publish analytics / transparency via Dune or similar?**

Curve hosts analytics of their AMM on two platforms, Llama Airforce, and Dune. Llama Airforce goes into detail of each gauge, pricing, revenue, trading volume, etc. The Dune page consolidates various dashboards made by both Curve team and independent contributors.

☐ **Working group structure**

CRV initial distribution allowed for a community fund of around $151M to be used in cases of emergencies or awarded to community-lead initiatives. In the past Curve utilized this community fund for ecosystem, DAO and community grants. These three types of grants had the common goal of encouraging and developing the Curve ecosystem and empowering the community. They also gave an insight on the early working group structure of the DAO.

- Ecosystem grants aimed at encouraging and developing the Curve, Vyper language and more generally the DeFi ecosystem. They were for individuals, teams of all sizes looking to develop tools, projects that could benefit from grants.
- Community grants aimed at encouraging and developing the Curve community and Curve itself. Those grants were received by users, content creators and projects supporting Curve.
- Proposal grants used to reward users who created successful (non parameter) proposals (CIPs).

An early (cir. 2020) Curve council that ruled on proposal grants was composed of the following members, split between team and community.

- Curve team members: @angelangel0v, @michwill, @iamdefinitelyahuman, @kendrickllama, @sssschris, @charlie_eth, @JulienBouteloup 9
- Community members: @jiecut, @Julien, @ON-DeFi, @WormholeOracle, @ne1k0, @C2tP, Quentin, Alex, Sebastian, Andre Cronje

The DAO homepage presents Gauge relatives weights and voting power figures, including total veCRV locked and average lock time. Little information is available beyond what's in the subsequent Org. structure answers below.

☐ **Are core contributors compensated / Doxed?**

The founder and CEO of Curve is Michael Egorov, a Russian scientist who has various experience with cryptocurrency-related enterprises. In 2015, he co-founded and became CTO of NuCypher, a cryptocurrency business building privacy-preserving infrastructure and protocols. Egorov is also the founder of decentralised bank and loans network LoanCoin. Other contributors are hard to come by, other than community managers, and two developers from previous reports - Angel Angelov and Ben Hauser (developers), and three community managers, "Charlie," "Kendrick Lama," and "Chris" information on team members seems to be very limited but track record proves a highly skilled and talented team to create one of the biggest DEX's in the DeFi world. CRV initial token allocation includes a portion dedicated to core team as outlined below in tokenomics section.

☐ **Any known controversies in crypto space**

Curve is a staple name in DeFi and has an overall favorable reputation in the crypto space. Some recent controversies include:

- Aug 9th, 2022: A Frontend exploit on the Curve website that resulted in $570k loss in user funds.
- Nov 22th, 2022: Infamous DeFi user Avi Eisenburg opening an $8m short on CRV, trying to liquidate CurveFinance founder Egorov (who at the time had $48m of CRV supplied on Aave with a liquidation price of $0.259)
- Enacting the Emergency DAO to kill previously granted (hastily perhaps) gauges and granting high A params (MIM) indiscriminately.

☐ **Do they have a security or risk management team**

While little is available online on the structure of the various working groups at Curve, there are several, some independent, researchers who are dedicated to Curve risk work. These include Nagaking, chanho, ON-Defi. Curve can also count on LlamaRisk (prev. Curve Risk Team), a team which reviews protocols in the Curve gauge on factors that may constitute a risk to the gauge reward system. Some of these are funded by a Curve grants program mentioned above.

Multisig Structure

☐ **Is protocol transparent of multisigs and signers, List/links of multisigs, purpose, and setup x of x**

Information on Curve multisigs, signers, and purpose is somewhat hard to come by. However, there is a resource that provides sufficient detail titled Curve DAO: Protocol Ownership, from 2020. It is unclear how much of this is still relevant today.

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.

   Voting is based on a user’s holdings of “Vote Escrowed CRV” (veCRV). veCRV is obtained by locking CRV for up to 4 years, with 1 veCRV equal to 1 CRV locked for 4 years. As the lock time decreases, An account’s veCRV balance decreases linearly as the time remaining until unlock decreases. veCRV is non-transferrable.
   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:
   - The ownership admin controls most functionality within the protocol. Performing an action via the ownership admin requires a 30% quorum with 51% support.
   - The parameter admin has authority to modify parameters on pools, such as adjusting the amplification co-efficient. Performing an action via the paramater admin requries 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.

- ☐ **Can multisigs interfere with collateral options? EOA minting**

The Curve DAO controls admin functionality throughout the protocol. Performing calls 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 -> Aragon Agent -> Ownership Proxy -> Contracts

At the ownership proxy level there are two main contracts:
- PoolProxy: Admin functionality for exchange contracts
- GaugeProxy: Admin functionality for liquidity gauges

The DAO is capable of replacing the ownership proxies via a vote.

Influence, Reputation, and Partnerships

- ☐ **How long has the protocol been around , have they endured long bear markets?**

The Curve DAO token was launched in August 2020. This current bear market is their first.

- ☐ **Have they been exploited and how was it handled , was value restored to users if affected.**

On August 9th, 2022, Curve Finance's DNS record was compromised and pointed to a cloned malicious site, what is known as DNS Spoofing. The attacker injected malicious code into that site that asked users to give token approvals to an unverified contract. In total, 7 users were affected by the exploit culminating in ~$612k losses. To date, this is their worst recorded exploit.

- ☐ **Current and notable past partnerships , are they a net positive on the DEFI space**

The Curve wars have been ongoing since 2021 and have involved a great number of protocols. By consequence, Curve is very well connected and can count on numerous partners in the space. Major veCRV holders include Convex (who hold 50.7% of supply), Yearn (8.4%), and StakeDAO (4.3%).

The Curve team is one of the multi-sig holders for the Polygon contracts (15-5-2021), as well as a signer on the YFI admin key (07-21-2020).

The Swiss Stake GmbH is the legal entity of the Curve team, with the principal Michael Egorov, incorporated in Zug, Switzerland. Source - Cointelegraph. Framework and jurisdiction falls under Switzerland - Top tier.

Audits & Bug Bounties

*Previous and Ongoing

- ☐ **Audits & Bounties**

Curve has been audited three times, two of which were pre-launch. Curve Bug Bounty program offers up to $250K in rewards, their program is rather unimpressive.

Reward Payouts

- ☐ **Rewards paid, vulnerabilities found with severity**

Rewards have been paid out in the past.

Collateral Analysis

Oracles

- ☐ **Available Chainlink Oracles**

Curve Protocol uses TWAP oracles. Curve details front-running mitigation in their docs. Flashloan countermeasures are implemented.

CRV has chainlink oracles on mainnet. Price Feed CRV/USD and CRV/ETH.

- ☐ **Does the asset have a backup oracle**

No

- ☐ **Any advanced oracle implementation required**

No

Liquidity, and Liquidations

- ☐ **AMM liquidity, (pools over 100k)**

Asset	# Markets on Ethereum	# CEX	Primary Liquidity ($)	Secondary Liquidity ($)	Alerternative Liquidity ($)
CRV	many	many	Curve: CRV/ETH ($67M TVL)	UniV2: CRV/wETH ($2M TVL)	Sushi: CRV/wETH ($480k)

- ☐ **CEX markets with depth if available**

Curve DAO is available on the top 187 platforms providing ample liquidity to trade. Main centralized exchanges, Binance, Coinbase, OKX.

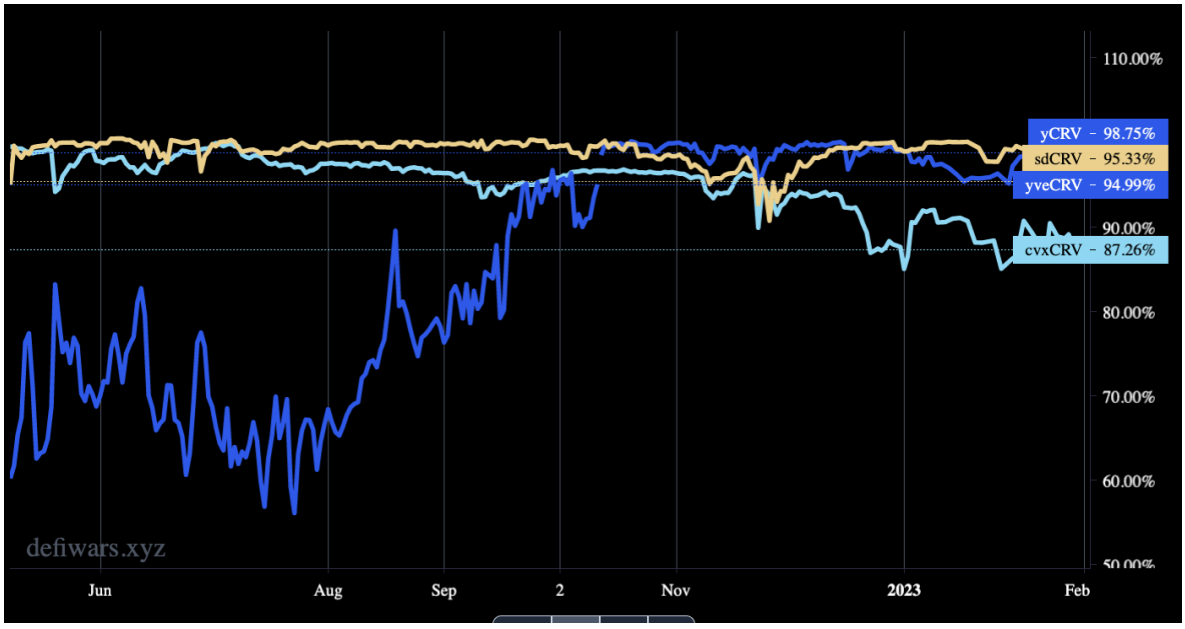
- ☐ **Liquidation Routing, Do liquidations require a wrapper?, accessibility**

Liquidity is sufficiently available for liquidators on Curve in the form of two pools for high efficiency. CRV/WETH. While wETH and DOLA don't have a sufficiently deep pairing it can easily be routed WETH > USDC > DOLA to repay loans.

- ☐ **Peg Risk if any**

For CRV, NA.

Wrappers -



Tokenomics

- [ ] **Contracts, are they upgradable?**

Admin controls are easy to find. Relevant contracts are clearly labelled as upgradeable or immutable in the various sections of their technical documentation. Ownership is in the hands of the DAO, as stated. Information regarding admin control and its relation to user funds' safety is clearly described at https://resources.curve.fi/faq/security. No timelock documentation is detailed. However, their DAO structure fundamentally operates like a timelock due to admin's giving up ownership to the DAO, and every vote on contract changes has to go through a lengthy voting process. In addition, Curve has clearly stated that the only contract that the DAO does not have full ownership of is the CRV DAO token. Regardless, the token contract restricts all admin access and external call possibilities. This renders the need for a timelock effectively useless for any Curve contract.

- [ ] **Market Cap History , Price History , Volatility**

Current Mcap: $745,487,313 (-71% from ATH), FDV $3.3B, TVL: $4.7B

Token Supply:

Circulating: 726,303,518
Total: 1,894,093,270
Max: 3,303,030,299

- [ ] **Coingecko / Coinmarket cap**

Coingecko // CoinMarketCap

- [ ] **Emissions Policy, what are emissions used for?**

Curve has a total amount of 3.03 billion CRV tokens and has the following token distribution: - 62% will be distributed to liquidity providers - 30% to shareholders (linearly unlocked within 2-4 years) - 3% to team members (linearly unlocked within 2 years) - 5% as a community reserve. The initial release distributed around 43% of the total CRV supply, Individuals that stake their CRV in the voting contract will receive a greater portion of the inflation; the longer one locks their CRV for, the more they receive in liquidity pool fees as well as the veCRV voting token. The 2-4 year unlock period increases the shareholder distribution credibility, yet 30% of the supply being distributed to shareholders is relatively high. The top non-exchange CRV holding wallet now holds around 4% of the supply and all others hold less than 1% of the supply. All in all, the metrics indicate a somewhat even distribution among holders Curve DAO currently has 90,376 holders and a circulating supply of 726,303,518. Full release schedule found https://dao.curve.fi/inflation. Distribution has been well executed to follow appropriate vesting periods for longevity.

Utility & Use Case

- ☐ **Does the Token have utility, Can it retain the utility while supplied to FiRM?**

The main purposes of the Curve DAO token are to incentivise liquidity providers on the Curve Finance platform as well as getting as many users involved as possible in the governance of the protocol. Governance is heavily weighted to a handful of whale's currently, but that still allows high APY liquidity pools to benefit all relevant stakeholders involved. CRV has 3 main utilities - voting, staking and boosting. Those three things will require you to vote lock your CRV and acquire veCRV. Fees are charged for swaps and shared between LPs and the protocol. The fees accrued by the protocol are shared among the veCRV token holders, (i.e. CRV holders which committed their CRV tokens for a certain amount of time). All together, this is a solid value capture model which ensures participation in governance and long term alignment of token holders with the protocol. The CRV boost feature is the ability to 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. The table below can help you understand the value add of veCRV:

	Liq in pool No veCRV	Liq in pool Has veCRV	Liq in pool & gauge No veCRV	Liq in pool & gauge Has veCRV	No liq No veCRV	No liq Has veCRV
Earns lending & trading fees	Yes	Yes	Yes	Yes	No	No
Earns CRV	No	No	Yes	Yes	No	No
Earns more CRV (boost)	No	No	No	Yes	No	No
Can vote on DAO proposals	No	Yes	No	Yes	No	Yes
Can vote on gauge weights	No	Yes	No	Yes	No	Yes
Earns gov fees	No	Yes	No	Yes	No	Yes

- ☐ **Liquid or locking feature**

The token enables its holder to participate in Curve DAO proposals and incentivises holders through staking in protocol revenue. By locking the tokens for a certain amount of time, the token holder gains voting power and revenue participation rights that are correlated to the length of the commitment. This ensures a long term alignment between token holders and protocol. Lock up times include - 1 week, 1 month, 3 months, 6 months, 1 year and 4 years for maximum voting power. This voting token allows the community/ liquidity providers to decide each week where the CRV emission incentive rewards for liquidity pools are distributed. This is decided on a Gauge vote every week. Simply put, a gauge weight translates into how much of the daily CRV inflation it receives. the more VeCRV tokens you have, the more voting power you can use to boost liquidity pool earnings. This proves absolutely vital to keeping the Curve economy circulating.

- ☐ **Goal of the token, where is value derived from?**

The main purposes of the Curve DAO token are to incentivise liquidity providers on the Curve Finance platform as well as getting as many users involved as possible in the governance of the protocol. Governance is heavily weighted to a handful of whale's currently, but that still allows high APY liquidity pools to benefit all relevant stakeholders involved.

Outside of the Curve ecosystem, the main protocol to make use of CRV is AAVE. AAVE holds $110M in liquidity and allows CRV to be used as collateral against other borrowing loans and yields.

Curve Liquid Wrappers

CurveFinance veToken model allows users to lock $crv for up to 4 years and receive admin fees (paid in stables) and allows them to vote for CRV emissions for the pools. Protocols seeking liquidity have the option to bribe veCRV holders to stream CRV emissions to their pools. But locking CRV for 4 years is not a very attractive option for the holders. What's the solution? Liquid wrappers.

- **cvxCRV** from ConvexFinance
- **sdCRV** from StakeDAO
- **yCRV** from Yearn Finance

Liquid wrappers allow CRV holders to receive fees and/or bribes without locking it for 4 years and provide a chance to exit the position. What is the difference between each of them?

- **cvxCRV**: By staking cvxCRV, you're earning 3crv fees plus a share of 10% of the Convex LPs' boosted CRV earnings and CVX tokens on top of that. This is another source of revenue besides admin fees for veCRV holders. While the bribe revenue (voting power which can be sold) is distributed among vote-locked CVX. So the normal revenue from veCRV (fees+bribes) is split between cvxCRV and CVX.

- **sdCRV**: sdCRV is distributing 3crv fees and keeping voting power with the stakers. Voting power can be delegated to the StakeDAO, it combines market and OTC bribes in order to get the best return. Or users can access the bribes from Paladin Vote or Votium directly on Stake DAO.Since StakeDAO is not splitting the bribes and admin fees between sdCRV and native token, staking APR is notably higher. Stakers are getting 3CRV, CRV and bribes are converted into SDT rewards. However to get the highest APR users have to boost it by locking the native token SDT.

- **yCRV**: Staked yCRV offers the highest yield among all wrappers. However, the yield will go down, as there are remaining rewards coming from the legacy yvBOOST donator contract. Also, 1/4 of all yCrv is owned by the treasury boosting yield for all yCRV stakers. st-yCRV offers "set & forget" UX where the source of yield comes from two places:
    - Admin Fees: 100% of admin fees earned are auto-compounded into more yCRV

- Bribes: 1 st-yCRV = 1 veCRV worth of vote power which will be sold on the bribes market to further increase yield Unlike sdCRV, st-yCRV holders are giving up their voting power, so protocols can't use it to cast votes for Curve gauges.

However, vl-yCRV is in the final stages of development, which will give the voting power but remove fees and bribes in favor of st-yCRV.

What are the tradeoffs with liquid wrappers?

1. Protocol fees are charged by the protocol for the service they provide (they are deducted from the displayed APR)
    - cvxCRV 0% fee
    - sdCRV 16% fee
    - yCRV 10% fee

2. Voting power
    - cvxCRV doesn't offer voting power nor does share bribe revenue
    - yCRV doesn't offer voting power, but shares the bribe revenue
    - sdCRV offers voting power and bribe revenue, but they are reduced in favor of veSDT stakers

3. For the peg maintenance all the protocols are directing CRV emissions to their respective LPs. But Stakedao is buying sdCRV with the bribe revenue when the peg is below 0.99 and distributing to the stakers (otherwise they pay with SDT tokens bought from the market).

Conclusion

In conclusion, the due diligence conducted by Inverse Finance's Risk Working Group on CRV by Curve Finance has determined that CRV is a suitable collateral for the fixed-rate lending market, FiRM. Curve is a staple name in the Cryptocurrency space and we have little reason to believe this won’t continue being the case.

The CRV token has demonstrated a strong track record of interest from other protocols (re: Curve Wars) and has the necessary infrastructure in place to support its use as collateral on the platform. We can safely assume that the Curve team, however little can be found on them, has a clear understanding of the lending market landscape and has implemented appropriate risk management measures to ensure the safety and security of user funds. The Bug Bounty program is somewhat lacking compared to peers in the space with similar TVL, with only a maximum payout of $250k and unclear amounts of total available rewards.

The Risk Working Group has evaluated CRV technical and economic characteristics and has determined that it possesses the necessary attributes to be used as collateral on the FiRM platform. The token is liquid, is paired with other reliable tokens (mainly wETH on mainnet) in

deep LPs on several chains (Ethereum, Arbitrum, Fantom, Polygon), thus addressing most SPOFs. CRV also has an elegant oracle solution, making use of a Chainlink oracle for both CRV/USD and CRV/ETH feeds.

Naked CRV is subject to strong dilution from emissions. This hasn't stopped over $110M in CRV to be deposited as collateral on Aave. Given FiRM's target audience and "long-term" horizon, a liquid wrapper such as yCRV might make a more appropriate collateral option. However it must be stated that heavy CRV emissions pose a long-term feasibility issue for CRV or any liquid wrapper on FiRM. Emissions have been greater than rewards for veCRV holders historically, which would "down only" price action for CRV in the long term. This all can change with the launch of Curve' own stablecoin, crvUSD. Launch is imminent, and adoption and value-add to veCRV remains to be seen.

Overall, the Risk Working Group is satisfied with the findings of this due diligence report and is confident in the ability of CRV to serve as a reliable collateral on the FiRM platform. The Risk Team recommends we also consider liquid wrappers for alternate collaterals. While liquidity for these is thin, this might soon change and eventually qualify them as suitable options.

CRV is presently an available collateral asset on Aave's Ethereum v2 market, CF is set at 52%, and TVL is $110M. Based on these findings, the Risk Working Group recommends CRV be made available as collateral on FiRM with an initial Collateral Factor (CF) of 50%. Setting a low CF, along with general supply caps, and daily limits, will limit overall risk exposure.