Risk Assessment - sdCRV Collateral Asset on FiRM

Useful Links **1**
Background **2**
Protocol Analysis **2**
Org. Structure 2
Multisig Structure 4
Influence, Reputation, and Partnerships 5
Audits & Bug Bounties **6**
Previous and Ongoing 6
Contracts in Scope 6
Collateral Analysis **6**
Oracles 6
Token Statistics 8
Liquidity 9
Volatility 10
Emissions 10
Utility & Use Case 10
Conclusion **11**
Asset Score 11
Parameter Recommendations 12

Useful Links

- Coingecko: https://www.coingecko.com/en/coins/stake-dao-crv
- Website: https://lockers.stakedao.org/
- Holdings: https://lockers.stakedao.org/lockers/crv
- Twitter: https://twitter.com/StakeDAOHQ
- Discord: https://discord.com/invite/stakedaohq
- GitHub: https://github.com/StakeDAO
- Bug Bounty: https://stakedao.gitbook.io/stakedaohq/risks/bug-bounty
- Docs: https://stakedao.gitbook.io/stakedaohq/
- Forum: https://gov.stakedao.org/
- Snapshot: https://snapshot.org/#/stakedao.eth
- Forum: https://gov.stakedao.org/

Background

sdCRV poses another unique opportunity for FiRM to lead the Defi space in CRV wrapper collaterals. As with cvxCRV (and soon yCRV), the newly deployed curve pools with EMA price feed enables a reliable oracle solution for these LP's which was previously not available.

Stake DAO is a non-custodial platform that allows users to stake their CRV tokens to earn rewards. Stake DAO offers a number of features that make it an attractive option for users who want to stake their CRV tokens. These features include:

- No lock-up period: One of the biggest advantages of staking on Stake DAO is that there is no lock-up period. This means that users can unstake their CRV tokens at any time without penalty. This is in contrast to some other staking platforms, which require users to lock up their tokens for a period of time.
- High rewards: Stake DAO offers users a higher yield than other staking options. The current yield on Stake DAO is around 40%. This is significantly higher than the yield offered by many other staking platforms.
- Staking as a service: Stake DAO makes it easy for users to stake their CRV tokens with no technical knowledge required. All users need to do is create an account on Stake DAO and deposit their CRV tokens. Stake DAO will then automatically stake the tokens on the user's behalf.

Some additional details about Stake DAO include:

- Stake DAO was founded in 2021 by Julien Bouteloup.
- … is headquartered in Zug, Switzerland.
- has raised $2 million in funding from investors such as KR1 and Ascensive Assets.
- is currently live on the Ethereum mainnet.

Protocol Analysis

Org. Structure

☐ **Is the Protocol a DAO? How is it governed eg. delegates , snapshot (8)**

Yes, Stake DAO is indeed a DAO. This means that its operation and decision-making processes are largely governed by its community members rather than a centralized authority.

The Stake DAO ecosystem is controlled by holders of its vote-escrowed token, veSDT. These holders vote on off-chain proposals that govern the ecosystem. These proposals are held on Stake DAO's Snapshot page. Proposals that generate majority support, i.e., more than 50% of the votes, are executed by the DAO Multisig, which is a group of individuals that collectively act as the final authority on executing these decisions.

The process for a governance proposal generally follows these steps:

1. Create a proposal using the proposal framework to share on the forum and exchange with the community.
2. Exchange with the community for a minimum of 2 days on the forum, then update the proposal if necessary.
3. Post the proposal on the Stake DAO snapshot by following the proposal framework.
4. If successful, the proposal payload will be executed and implemented by the DAO multisig.

Discussion regarding changes in the protocol happen on various channels, including the Governance Forum, Telegram, and Discord.

The DAO is further protected by multiple multisigs, including the DAO Multisig and the Emergency DAO Multisig. These multisigs play a crucial role in the governance and safeguarding of the Stake DAO ecosystem, controlling the DAO Treasury and providing an additional layer of security against malicious activity, respectively.

☐ **Does Protocol publish analytics / transparency via Dune or similar (2)**

StakeDAO has an in-house analytics page at https://analytics.stakedao.org/. However, this page appears to be outdated. There are a handful of unofficial community-created Stake DAO dashboards on Dune, including for SDT as well as sdTokens such as sdCRV.

☐ **working group structure (10)**

Since the inception of Stake DAO, the multisig has fostered a ‘sub-unit structure’ by encouraging the development of autonomous sub-units consisting of freelance contributors.

The DAO now has multiple sub-units or working groups specialized in different functions that help to make Stake DAO what it is. These sub-units execute day-to-day tasks as set out in the guidelines in various SDIP’s approved by the community.

The sub-units comprise various independent freelancers that execute tasks for the DAO based on the instructions or laws specified in SDIPs and voted on by the DAO community via snapshot voting in SDT/xSDT.

Some of these Sub-units and their purpose is as follows:

Engineering - Build and maintain all code.
DevOps - Run validators, build and sustain DevOps architecture.
Analytics - Provide platform and user analytics to inform policy decisions.
Policy - Determine policies for emissions, fees, etc.
Marketing - Share the message of Stake DAO, cultivate community and attract freelancers.

Multisig - Ratify decisions and execute SDIP alterations to the protocol.

☐ **are core contributors compensated / Doxed (10)**

https://stakedao.org/contributors

Many of the StakeDAO contributors are doxed and compensated.

☐ **Any known controversies in crypto space (e.g. Sifu) (10)**

There are no known controversies specifically related to Stake DAO in the crypto space.

☐ **do they have a security or risk management team (0)**

There is not a defined sub-unit at StakeDAO for Risk Management

Multisig Structure

☐ **Is protocol transparent of multisigs and signers, List/links of multisigs, purpose, and setup x of x (10)**

Stake DAO Multisigs can be accessed here. There are 2/9 multisig which has the following main powers:

1.) Deploy treasury funds

The threshold of the multisig is currently set low to speed up developments at the initial stages of the DAO. We plan to increase it as we move further right in the decentralization spectrum.

Multisigs

Ethereum multisig : link
Polygon multisig : link
Avalanche multisig : link
Harmony multisig : link
Arbitrum multisig: link

Emergency DAO Multisigs
In order to address the community's concerns, and to reduce all risks as much as possible, Stake DAO has put in place various preventative measures that have been discussed and voted on by the DAO.
These measures include, among others, the veSDT veto right, the time-weighted average voting power mechanism, and the creation of an Emergency DAO. Presented as an additional means of guarding against malicious voting, the emergency DAO will be a further bulwark against

malicious or suspicious voting. A malicious vote can be defined as « any governance vote which puts the underlying protocol at risk ».
Therefore, Stake DAO has agreed with Frax, Angle, Curve, Balancer and Convex to create an Emergency DAO, which will be able to close any vote that seems malicious and disregard the final result.
The idea of the Emergency DAO was pioneered by Curve, serving to empower a small trusted group to “kill” pools and gauges in the event of malicious activity and/or potential loss of funds. In this case, it will be used to veto any suspicious votes in the 3 Liquid Lockers. sdAngle/Angle, sdFXS/FXS, sdCRV/CRV and sdBAL,BAL. It should also be noted that, in the medium term, as with Curve, the Emergency DAO will have the power to kill a gauge if necessary.
Each of the Liquid Lockers will have its own Emergency DAO. This Emergency DAO will comprise of two members from each of the underlying protocols; two members from Stake DAO, and two independent members from the ecosystem, to be chosen by the four other members. An emergency DAO vote would require at least four votes to pass, each member has one vote. Any member may propose a vote. All members of the emergency DAO are entitled to raise their concerns if they deem a vote to be malicious.

There are currently 4 Emergency DAO Multisigs deployed:

- Curve Liquid Locker Emergency DAO
- Angle Liquid Locker Emergency DAO
- Frax Liquid Locker Emergency DAO
- Balancer Liquid Locker Emergency DAO

☐ **Can multisigs interfere with collateral options? EOA minting (10)**

An issue was raised by the Inverse Finance Risk team surrounding Governance Guardian EOA in January 2023. The StakeDao team quickly mitigated the issue by updating Governance to a 4 of 7 Multisig which was confirmed by the Inverse Finance Team. This has mitigated EOA risk associated with the protocol and products.

Influence, Reputation, and Partnerships

☐ **How long has the protocol been around , have they endured long bear markets (8)**

The SDT token was launched on January 20th, 2021 beginning StakeDAO governance.

☐ **Have they been exploited and how was it handled , was value restored to users (10)**

None

☐ **Current and notable past partnerships , are they a net positive on the DEFI space (10)**

https://stakedao.org/partners

StakeDAO has maintained great relationships in the Defi space, including a working relationship with the Inverse Finance TWG dating back to October 5, 2022. Their partners page appears to be out of date.

Audits & Bug Bounties

Previous and Ongoing

☐ **Previous and Ongoing audits & bounties with links (3)**

https://stakedao.gitbook.io/stakedaohq/risks/bug-bounty

The StakeDAO team runs a bug bounty program with rewards paid out in USDC ranging up to $100,000 for High Severity.

Stake DAO also offers users purchase protection through Nexus Mutual

☐ **Are Rewards paid ? Were vulnerabilities found with severity level? (10)**

Unclear. None that have been made publicly available

Contracts in Scope

☐ **Is the scope a comprehensive list of contracts including collateral and wrappers**

All Stake DAO smart contracts

Collateral Analysis

Oracles

☐ **EMA vs TWAP**

The EMA oracle (Exponential Moving Average oracle) is a type of oracle called "exponential" because it uses a weighting factor that exponentially decreases the influence of older data points on the moving average. The EMA oracle works by taking a series of recent prices for a

particular asset and calculating an average price, giving more weight to the more recent prices. The result is a moving average price that is updated over time.

Whereas EMA calculates the average price based on a weighting factor that exponentially decreases the influence of older data points on the moving average; TWAP, on the other hand, calculates the average price based on the time-weighted average of prices over a specific period of time. This means that each price is given equal weight in the calculation, regardless of when it was recorded. The main difference between EMA and TWAP is in their responsiveness to changes in market conditions. EMA is more responsive to changes in market conditions (depending on half-life setting), while TWAP provides a more stable and predictable reference price over a longer period of time.

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

There is a MA Price built into the LP as well.

☐ **Any advanced oracle implementation required**

In our oracle implementation for sdCRV, we'd rely on the same mechanism of our cvxCRV and yCRV oracle implementation (recently audited by Nomoi). That is, we cap the max price using the CRV chainlink price feed, and use the EMA reading from the new sdCRV/CRV LP when it reads prices below 1 CRV.

Using the chainlink price feed for CRV as a "price ceiling" for sdCRV makes sense since there are no scenarios aside from malicious ones where the price of sdCRV would ever be greater than CRV. Together with FiRM's PPO safety feature, we believe these measures are enough to protect against upward price manipulation of the sdCRV asset.

As for downward price manipulation, something to consider is the EMA half-life. The new Curve stablepools are deployed by default (using the UI) with an EMA Half-Life of 10 minutes. For our intents and purposes, a half-life of 30 minutes would result in a more resilient EMA price reading in the context of a malicious actor trying to manipulate the price downwards (in order to profit from liquidations). EMA Half-Line can be adjusted by Curve gov after deployment, or it can be set on deployment using this proxy admin contract.

Other safety measures (that carry obvious cons) the PWG might consider here are:

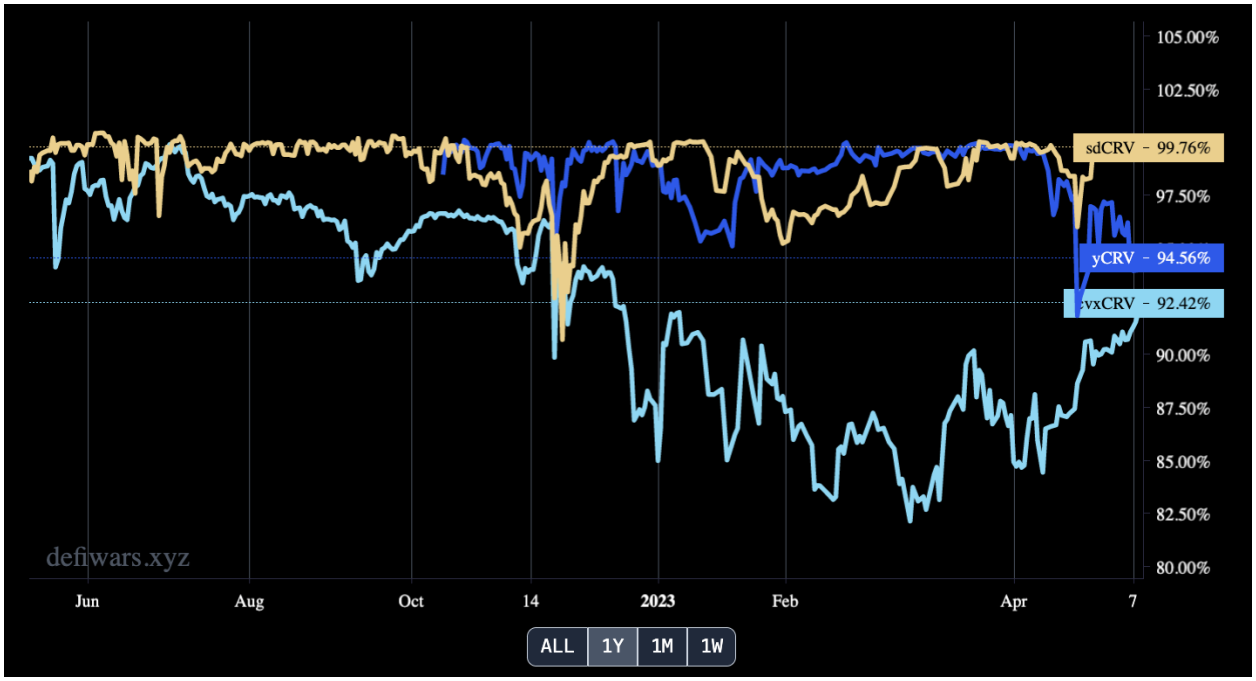
- Using an EMA that gives more weight to older price readings.
- Using a consensus mechanism though this would require multiple trusted oracles.
- Implementing a circuit breaker though inefficient as it would require governance to intervene and 5+ days to reactivate the market (especially a problem if triggered incorrectly)
- Exploring the use of comparing last used price with EMA price, and causing reverts if the difference is too large.

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

sdCRV>CRV>USDC>DOLA
sdCRV>USDC>DOLA

☐ **Peg Risk if any**

sdCRV's peg, while volatile, is often very close to 1:1 with CRV. One can assume healthy use of the sdCRV market on FiRM will positively affect the peg.



Token Statistics

☐ **Contracts**

sdCRV
SDT (Governance)

☐ **Price / Market Cap / Circulating Supply / Locked Supply / True Circulating / Total / Max**

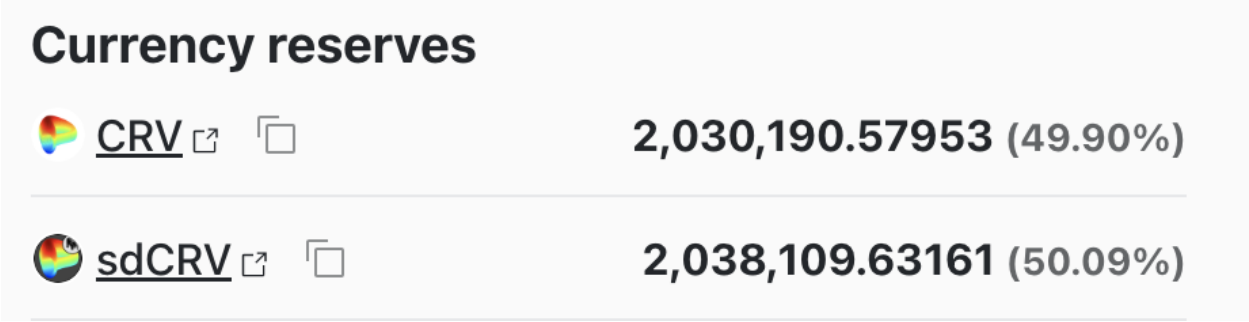
*As of May 10th

Price	Market Cap	Circulating Supply
$0.817051	$23,888,293	29,237,212.50

Liquidity

☐ **Mainnet Dex Liquidity**

LP	Protocol	Liquidity	24 Hour Volume
sdCRV/CRV	Curve	$3,110,756	$136,451



☐ **On-Chain Slippage**

*Cowswap is the only aggregator indexing sdCRV on llamaswap. This results in potentially inaccurate price impacts due to high gas costs included in the swapout.

Initial ->	sdCRV ->	CRV ->	USDC ->	DOLA	Slippage (%)	Price Impact (%)
$5,000	6088	6083	4990	4999	0	0.08
$10,000	12177	12167	9980	9998	0	0.11
$20,000	24354	24329	20001	20054	0	0.15
$50,000	60886	60782	49923	50056	0	0.29
$100,000	121772	121455	99432	99694	0.31	0.52
$200,000	243524	242258	197933	198442	0.78	1.00
$500,000	608812	600929	490482	491660	1.67	2.72
$1,000,000	1217624	1177218	950309	952348	4.77	9.09
$2,000,000	2435249	1906014	1513971	1516862	24.16	80.18
$5,000,000	6088124	2019397	1601013	1604014	67.92	99.63

☐ **Token Holders**

Holders

Volatility

☐ Price Log Return Volatility

Emissions

☐ **Token Emissions schedule**

For *CRV* - Please refer to Emissions section in Risk Assessment CRV Collateral on FiRM
For sdCRV - N/A

☐ **Emissions Policy**

For *CRV* - Please refer to Emissions section in Risk Assessment CRV Collateral on FiRM
For *sdCRV* - N/A

☐ **What are emissions used for**

For *CRV* - Please refer to Emissions section in Risk Assessment CRV Collateral on FiRM
For *yCRV* - N/A

Utility & Use Case

☐ **Does the Token have utility (10)**

The main purposes of CRV is 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. 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. All together, this is a solid value capture model which ensures participation in governance and long term alignment of token holders with the protocol.

sdCRV offers the highest yield among all wrappers (if boosted). 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.

What are the tradeoffs with sdCRV?

1. Protocol fees (16%) are charged by the protocol for the service they provide (they are deducted from the displayed APR). In comparison yCRV has 10% fee, and cvxCRV has 0%.

2. Voting power
    - 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).

☐ **Liquid or locking feature (10)**

sdCRV is tokenized veCRV. If a user deposits CRV into StakeDAO, that CRV is locked forever on the platform as veCRV. A tokenized version of veCRV, sdCRV, is returned to the user at a 1:1 rate. sdCRV conversion is 1-way. One liquidity pool exists that allows users to swap sdCRV for CRV tokens. StakeDAO has recently surpassed 30,000,000 veCRV.

☐ **Goal of the token, where is value derived from (10)**

One of Stake DAO's purposes is to scoop up as much CRV as possible. Consequently, sdCRV value is derived by how much CRV StakeDAO hold and the future prospects of them increasing their bag.
Outside of the Curve ecosystem, there is no other protocol making use of sdCRV. This makes it an appealing proposal for Inverse Finance. allowing sdCRV to be used as collateral against other borrowing loans and yields will draw much attention from the Yearn Finance community.

Conclusion

Asset Score

As we build out a registry of TAS for a variety of collateral options and match them with findings from other risk profiling frameworks and methodologies, the RWG will be able to rely more and more on the Asset Scoring Model. As of now, our data indicates the following:

- Any asset with TAS > 7.5 can be deemed an asset carrying a low risk profile.
- 5 > TAS > 7.5 warrants caution, and, if approved, a "guarded" launch on FiRM.
- TAS < 5 should seldom be considered worthy of a FiRM market.

Token Contract Address: 0xd1b5651e55d4ceed36251c61c50c889b36f6abb5
Assessment date: May 10th, 2023

Component	Link/Rationale	Score
Market Capitalization	MCS=min(10, (sdCRV Supply * sdCRV Price * 200) /(wETH Supply * wETH price)	0.74
DEX Trading Volume	TVS =min(10, (30 Day Avg Token Trading Volume * 200 / 30 Day Avg wETH Trading Volume)	0.19
Price Volatility	PVS =min(10, 10 - (Token Log Price Volatility / wETH Log Price Volatility) * 9)	3.37
Token Distribution	Token Distribution Score = min((1- Token Gini Index) * 10 / (1 - wETH Gini Index);10)	1.48
Project Fundamentals	Risk Assessment sdCRV Collateral on FiRM - See Protocol Analysis, and Audits & Bug Bounties Sections	7.77
Token Utility	Risk Assessment sdCRV Collateral on FiRM - See Collateral Analysis Section	10

Total Asset Score

$$TAS = 0.74 * 0.2 + 0.19 * 0.15 + 3.37 * 0.15 + 1.48 * 0.1 + 7.77 * 0.2 + 10 * 0.2$$

$$TAS = 4.38 / 10$$

Parameter Recommendations

Supply Ceiling	$1,000,000
Initial Fed Supply	$500,000
Daily Borrow Limit	$100,000
Liquidation Factor	50%
Firm Global Supply Ceiling	$23,000,000

Collateral Factor	50%

- ☐ **Supply Ceiling** - Setting the supply ceiling for an asset, though influenced by such factors as market demand, collateral volatility, correlation with other assets, and overall risk appetite, should ultimately be determined by considering the overall liquidity picture and slippage figures for said asset. Put simply, If the collateral has high liquidity, then the supply ceiling can be set higher because it is easier to sell the collateral in case of liquidations. In the case of sdCRV, liquidity is slim. Furthermore, Stake DAO has yet to migrate sdCRV liquidity from the old Curve LP to the new more reliable sdCRV/CRV pool. After this migration we can expect at least 1.9M CRV “backing” sdCRV. Slippage figures are somewhat encouraging, with a $100k sdCRV trade incurring only 0.32% slippage, and $500k sdCRV incurring 1.67% (see table above). Simulations were also ran on a 1M sdCRV sell order, which resulted in a 9.09% price drop. Based on the above, we recommend the initial supply ceiling for sdCRV be set to $1,000,000. The data suggests this amount is on the higher end of what we can consider safe, that is until liquidity for sdCRV deepens.

- ☐ **Initial Fed Supply** - the amount the Fed injects to the market up to supply ceiling. The RWG recommends this amount be $500,000.

- ☐ **Daily Borrow Limit** - Like all factors here, daily borrow limit is set to strike a balance between meeting market demand and managing risk. sdCRV scored poorly in our asset scoring model framework, particularly in volume, distribution, and price volatility. Based on this, the RWG recommends the daily borrow limit amount be set to $100,000 per day. This figure matches the deployment parameter for the cvxCRV market on FiRM. While one might consider this figure to be somewhat aggressive given the present-day total asset score and liquidity picture, we believe the potential for a sdCRV market on FiRM will incentivize StakeDAO to deepen sdCRV liquidity. Assuming this occurs, and the asset scoring model returns more favorable scores, daily borrow limit can be readjusted at a future date.

- ☐ **Liquidation Factor** - It is important to set the liquidation factor carefully to ensure that the platform can manage its risk exposure effectively. If the collateral has a history of high price volatility, if the collateral has low liquidity, and if the platform has a low risk appetite, these are all true in our case and are grounds to set a higher liquidation factor. At the same time, it’s likely our TWG will have to carry out liquidations for this market initially as we can’t assume automated liquidations will take place by MEV liquidators (until we can prove sdCRV is being searched). As such, we recommend the liquidation factor be set to 50%, so that the liquidation incentive matches with CF.

- ☐ **Firm Global Supply Ceiling** - Global Supply ceiling (currently set at $22,000,000) will increase to $23,000,000 to account for the supply ceiling for the sdCRV market.

- [ ] **Collateral Factor** - Setting the collateral factor requires balancing the risks associated with the asset being used as collateral with the demand for loans. Assets with lower risks may have higher collateral factors, while assets with higher risks may have lower collateral factors. Ultimately, the collateral factor is closely related to, and influenced by many of the factors pertaining to the parameters presented above. While parameters above act as a backstop, the collateral factor determines whether an attack on the protocol can be profitable for the potential exploiter capable of manipulating our price oracle implementation. Given all the above and taking into account the results of our Asset Scoring Model, the RWG recommends we launch the sdCRV market with collateral factor set at 50%. At 50% CF, the protocol starts to take on bad debt if the sdCRV oracle price allows for an account's collateral to become less than 10% the value of the loan position. For this to happen, a price drop of 45% or more is needed for the collateral asset before a full liquidation is able to take place (full liquidation meaning the position is brought back to health, not the entire loan being repaid). A 45% price drop would occur if ~$1.5M sdCRV was dumped on the market, which far exceeds the daily borrow limit, as well as the supply ceiling for the market.