Risk Assessment - **aCVX** Collateral Asset on FiRM

Useful Links

Documentation and Contract Addresses

- Aladdin DAO
- Concentrator
- Documentation
- aCVX Contracts

GitHub Repositories

- AladdinDAO Github

Community and Social Media

- Discord: https://t.co/0WqyLl23u3
- Telegram: https://t.me/aladdin_dao
- Twitter: https://twitter.com/aladdindao

Governance and Proposals

- Forum
- Aladdin DAO Governance
- Concentrator Governance

Audits

- AlladinDAO v3 Contracts
- aCVX Audit

Bug Bounty

- Security Bounty

Additional Information

- aCVX Documentation
- Aladdin DAO Medium

TL;DR

Overview:

- **Protocol**: Aladdin DAO is a decentralized builder and incubator of cutting edge DeFi protocols.To date Aladdin has built three products: Concentrator, Clever, and f(x) Protocol. Their current focus is in building new approaches to yield farming optimization and automation within the Curve ecosystem and with their latest product, f(x) Protocol, they are expanding to scalable decentralized stablecoins.
- **Proposal**: The use of aCVX, an autocompounding staked CVX vault token from the Concentrator Protocol, as collateral on FiRM, following the collaboration between Inverse Finance and Aladdin DAO.
- **Utility**: aCVX currently serves as a vault receipt, with the potential for expanded utility as collateral in lending markets such as FiRM, enhancing yield over simple CVX staking.

Key Points:

- **Governance**: AladdinDAO utilizes a decentralized governance model with multisig contracts, improvement proposals, community discussions, and snapshot voting, indicating a community-driven decision-making process.
- **Security**: AladdinDAO does not have an in-house security team but frequently collaborates with SecBit for audits and security consulting. A structured bug bounty program is also in place to incentivize vulnerability reporting.
- **Regulatory Risks:** While this assessment doesn't explicitly mention regulatory risks, it's important to consider the broader regulatory environment in which AladdinDAO operates.
- **Collateral & Liquidity**: aCVX represents the amount of CVX in the Concentrator vault, and thus while assessing the collateral for on-chain liquidity and manageable slippage, naked CVX is studied. The vault, given it's recent launch, has a limited number of users.
- **Competitive Edge**: Inverse faces no competition with integrating aCVX into FiRM as the market would be first of it's kind, giving us a first-mover's advantage.

Conclusion & Recommendations:

- **Asset Score**: The Total Asset Score for aCVX is 6.22/10, which appropriately is slightly lower than the TAS for CVX, recently scored at 6.96. This is because AlladinDAO carries more of a risk profile compared to Convex Finance.
- **Parameter Recommendations**: We strongly advise AlladinDAO commision a supplementary audit prior to Inverse bringing aCVX to FiRM. The AladdinDAO team has expressed intent to conduct a second on the aCVX vault and turn the contract immutable soon after, thus fulfilling this request.

Background

Inverse Finance and Aladdin DAO have been exploring collaborative opportunities centered around Aladdin DAO's Concentrator and the new f(x) Protocols. The Concentrator Protocol features aCVX, an autocompounding staked CVX vault considered for collateral on FiRM. The updated aCVX (released October 23, 2023) is fully liquid, with no withdrawal delay or withdrawal fee. The f(x) Protocol introduces fETH and xETH, with fETH acting as a fractional ETH having 10% of ETH's price movements, and xETH offering 2-4x leverage without a funding cost, ideal for long-term positions with no liquidation risk. The idea here includes an allocation from Inverse's Treasury to fETH and the creation of a DOLA/fETH pool on Curve. The f(x) protocol is set to move out of beta (launched in August 2023) post its upcoming fourth audit, indicating readiness for broader engagements.

This risk assessment will focus on the use of aCVX as collateral on FiRM, with Aladdin DAO keen on making necessary adjustments to meet FiRM's requirements, including the removal of the withdrawal delay in aCVX. As such, it will look into AladdinDAO broadly, and the Concentrator protocol more specifically.

aCVX is the Concentrator protocol's latest compounder, launched on October 19th, 2023, which utilizes staked CVX as its base asset, earning its rewards from Curve & Convex fees and swapping these for more CVX and staked on Convex. As of October 31st, aCVX balance is 389,126.71, and the index is 1.0037, hence there is 390566.47 CVX deposited in the vault. At a price per CVX of $2.81, that equates to $1,097,491 deposited in the vault. Concentrator takes a 10% treasury fee and a 2% harvest fee on yields. The fees are collected during the harvest process and distributed to the Treasury and Keeper respectively.

Protocol Analysis

Org. Structure

- ☐ **Is the Protocol a DAO? How is it governed eg. delegates , snapshot (10)**

The Aladdin DAO employs a decentralized governance structure, with various components indicating a community-driven decision-making process.

- **Contracts and Multisigs**: Aladdin DAO has a set of smart contracts governing different aspects of the protocol. These contracts are governed by multisigs, requiring approval from multiple parties for certain actions. The contracts cover areas like the Treasury, Concentrator, and Vaults among others.
- **Improvement Proposals**: The community can discuss proposals in the Aladdin DAO forum before they are moved to the Snapshot voting stage. The forum has designated sections for different types of proposals, including Concentrator Improvement Proposals and CLever Improvement Proposals. The Aladdin DAO has a structure for proposing improvements to the protocol, known as Aladdin Improvement Proposals (AIPs). These

proposals provide a transparent process for evolving the protocol as per the community's needs and circumstances.
- **Snapshot Voting**: Proposals that have been discussed in the community Discord and moved to the forum can be put to a Snapshot Vote based on community feedback. Snapshot voting is a gasless voting mechanism used by many decentralized organizations to gauge community sentiment without on-chain transactions.

The above is a familiar structure for DAOs and one that leverages both on-chain contracts and off-chain community discussions to manage and evolve the protocol. Through the combination of multisig contracts, improvement proposals, community discussions, and snapshot voting, Aladdin DAO engages its community in the governance process. However, detailed specifics on the delegation process or the involvement of delegates weren't provided in the shared links.

☐ **Does Protocol publish analytics / transparency via Dune or similar (6)**

Aladdin DAO appears to have some level of analytics or transparency via Dune as evidenced by a dashboard (for their Clever and Concentrator protocols) created by a user diligentdeer 8 months ago, according to a listing on Dune's site. Dilligentdeer is on various AlladinDAO-affiliated Multisigs, as well as a member of the LlamaRisk Team. However, the details of the analytics or the breadth of transparency provided are not elaborated upon.

☐ **working group structure (3)**

The working group and team structures within AladdinDAO are not explicitly detailed on their website or documentation. While their documentation mentions various contracts and roles such as governance multisigs, it doesn't provide a clear delineation of working groups or teams like treasury, community, growth, risk, product, analytics, etc.

The search results indicate that there's a "core team" and "community managers" within the DAO, suggesting some level of organizational structure. However, the specifics regarding the working group structure or clear team structures are not provided in the available resources.

☐ **are core contributors compensated / Doxed (5)**

AladdinDAO was launched in 2021 by a consortium of 14 founding contributors and investors, including notable and infamous entities such as Polychain, Digital Currency Group, 1kx, Multicoin, CMS, Nascent, Alameda, DeFi Alliance, Robert Leshner, Kain Warwick, Hart Lambur, Alex Pack, Ashwin Ramachandran, and Sharlyn Wu. Compensation structure isn't immediately clear, but day-to-day operations are managed by members using pseudonyms.

☐ **Any known controversies in crypto space (e.g. Sifu) (3)**

None according to preliminary research. Unclear what role, if any, disgraced entities such as Alameda and Multicoin (lead by Kyle Samani) play as original founders/contributors in the DAO. The AlladinDAO core team "does not know" either.

- ☐ **do they have a security or risk management team (7)**

AlladinDAO does not have a dedicated in-house security or risk management team. In the words of a contributor, they are a very small team. However they have engaged the services of an external auditor, SecBit, who also performs security consulting work for them. Given the frequency of audit reports produced by SecBit (see *Audits & Bug Bounties* section), one can speculate that AlladinDAO has them on retainer.

Multisig Structure

- ☐ **Is protocol transparent of multisigs and signers, List/links of multisigs, purpose, and setup x of x (6)**

All relevant AlladinDAO multisigs are viewable here. These include:

- Management
- CLever Treasury
- Concentrator Treasury
- f(x) Treasury

On top of that, the team let us know there is an additional multisig that runs “some daily expenses”. We confirm these are all the multisigs on mainnet.

9 signers are listed on the AlladinDAO docs but multisig setups are not clearly labeled.

More information on deployed contracts can be found here.

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

No

Influence, Reputation, and Partnerships

- ☐ **How long has the protocol been around , have they endured long bear markets (10)**

AlladinDAO has been around since at least April 2021, per this CoinMarketCap article. This is their first bear market.

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

Per the research conducted, there have been no exploits to AlladinDAO or its subprotocols CLever, Concentrator, and f(x) protocol.

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

In their own words, AladdinDAO is a decentralized platform focused on shifting crypto investments from venture capitalists to collective value discovery by the community, while building and incubating innovative DeFi protocols for yield farming optimization and automation.

Based on the research conducted, one can conclude they are a net positive in the DeFi space. Their Concentrator protocol, a yield enhancer that boosts yields on Convex vaults by auto-compounding rewards, has set the stage for partnerships with Convex (via aCRV), Frax Finance (via aFXS), and Stake DAO (via asdCRV) to name a few. Now, with the recently launched f(x) protocol, which is built on top of Convex, these partnerships have been solidified, with both Convex and StakeDAO locking sizeable amounts of the FXN token.

AladdinDAO are keen to work with Inverse and build a multi-layered partnership with us.

Audits & Bug Bounties

Previous and Ongoing

- ☐ **Previous and Ongoing audits & bounties with links (10)**

Aladdin DAO has a structured approach towards ensuring the security and robustness of its protocols. All past audits can be accessed on the AlladinDAO Github page. There is a clear recurring relationship with SecBit, one can speculate AlladinDAO, in absence of an in-house security team, has SecBit on retainer. emphasis on maintaining a high level of trust and assurance within the community. The below table presents an up-to-date list of audits, sorted by date:

Auditor	Date	Topic	Report
SecBit	3-Feb-2022	abcCVX	Link
SecBit	4-Mar-2022	Concentrator	Link
SecBit	8-Mar-2022	Concentrator Harvester	Link
SecBit	31-Mar-2022	Concentrator	Link
PeckShield	2-Apr-2022	Concentrator	Link
SecBit	21-Apr-2022	CLever	Link
SecBit	1-Jul-2022	Concentrator IFO	Link
SecBit	1-Jul-2022	Generic Version of CLever	Link
PeckShield	4-Jul-2022	Concentrator	Link
SecBit	17-Aug-2022	aFXS	Link

SecBit	28-Sep-2022	ClevUSD Strategy	Link
SecBit	28-Sep-2022	TokenSale Contract	Link
SecBit	11-Nov-2022	Furnace Update of CLever	Link
SecBit	9-Dec-2022	abcCVX	Link
SecBit	22-Dec-2022	aETH	Link
SecBit	2-Feb-2023	Concentrator sdCRV Strategy	Link
SecBit	3-Feb-2023	aCRV V2	Link
SecBit	14-Jun-2023	f(x) Protocol	Link
SecBit	16-Jun-2023	Concentrator sdCRV Strategy	Link
SecBit	25-Jul-2023	Rebalance Pool of f(x) Protocol	Link
SecBit	15-Aug-2023	aFXS v2	Link
SecBit	17-Sep-2023	f(x) Protocol update	Link
SecBit	18-Oct-2023	Concentrator aCVX update	Link

The proposed new collateral, aCVX, was audited as recently as October 18th, 2023. Furthermore, the AladdinDAO team has expressed intent to conduct a second on it and turn the contract immutable soon after, if aCVX is to be onboarded to FiRM.

AladdinDAO has a self-hosted bug bounty program inviting security researchers to identify vulnerabilities in their system. The scope of the program covers all contracts in the AladdinDAO V2Contracts, Concentrator, CLever, and f(x). Rewards for identifying bugs range from up to $2,000 for low-severity bugs to up to $500,000 for critical severity bugs based on the CVSS Risk Rating scale.

- ☐ Reputation, Qualifications and Industry Experience of Audit Firm

SecBit Labs is a China-based blockchain security company that focuses on building high-confidence and trustworthy protocols, applications, and facilities on the blockchain. While they are relatively unknown, they have been operating in the space since at least 2018. Their areas of expertise include formal verification, practices of zero-knowledge proofs, and blockchain security. SecBit has ventured into full formal verification for token smart contracts and decentralized exchanges. They have also designed and implemented zkPoD, a decentralized protocol for data exchange, and reported many buggy smart contracts on Ethereum, including well-known issues in Fomo3D. Their portfolio includes a Security Audit Report for Loopring Protocol 3.0 after a thorough three-month code review and analysis.

SecBit Labs also contributes to the community by providing tools like the SecBit Solidity Static Analysis Extension for Visual Studio Code, which extends the Solidity compiler to provide additional diagnostics on known issues and violations of best practices. They also maintain active repositories and projects on GitHub where they share articles, codes, and tools related to

zero-knowledge proofs, showcasing their commitment to knowledge sharing and community engagement[4].

Contracts in Scope

- [ ] **Is the scope a comprehensive list of contracts including collateral and wrappers**

The scope of AladdinDAO's bug bounty program encompasses all contracts within AladdinDAO's V2Contracts, Concentrator, CLever, and f(x). These are linked here.

Reward Payouts

- [ ] **Rewards paid, vulnerabilities found with severity**

Research did not yield relevant information regarding past rewards paid to security researchers or white hat hackers for AladdinDAO's bug bounty program, or the vulnerabilities found and their severities.

Collateral Analysis

Oracles

- [ ] **Available Chainlink Oracles**

CVX can count on two Chainlink price feeds, one for the CVX/USD pair and one for CVX/ETH. CVX chainlink feed updates every 24 hours or when there's a 2% price deviation.

- [ ] **Any advanced oracle or market implementation required**

No advanced oracle required. For market implementation, aCVX issues a receipt token. As such, the rewards implementation shouldn't differ compared to other reward-generating collaterals with markets on FiRM.

- [ ] **Peg Risk if any**

No impermanent loss or peg risk.

Token Statistics

- [ ] **Contracts**

CvxCompounder: 0xb0903Ab70a7467eE5756074b31ac88aEBb8fB777
CvxStakingStrategy: 0x837592b44EE5447074b80Cb21bF37a8c5E4c08f8

- [ ] **Price / Market Cap / Circulating Supply / Locked Supply / True Circulating / Total / Max**

The total amount of CVX contained in the Concentrator vault is equal to the total aCVX balance multiplied by the current index. As of October 31st, aCVX balance is 389,126.71, and the index is 1.0037, hence there is 390566.47 CVX deposited in the vault. At a price per CVX of $2.81, that equates to $1,097,491 deposited in the vault.

Liquidity

The on-chain liquidity figures presented below are all pertaining to CVX.

- [ ] **Mainnet Dex Liquidity**

On-chain liquidity for CVX currently stands at $23.94M per DeFiLlama, with a yearly high of $70.8M and an all-time high of ~$241M.

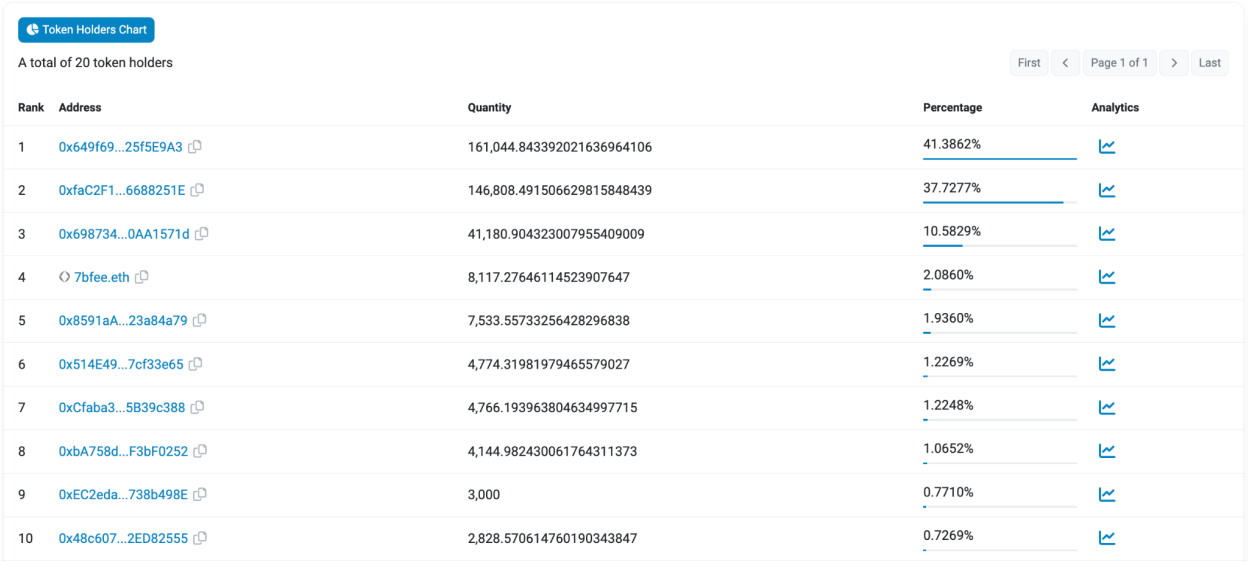
LP	Protocol	Liquidity ($)	24 Hour Volume ($)
CVX/ETH	Curve	16.23M	835k
CVX/frxETH	Curve	4.13M	60k
CVX/FraxBP	Curve	707k	16k
CVX/wETH	Sushiswap	557k	48k
CVX/wETH	Uniswap v2	445k	16k

☐ On-Chain Slippage

Trade	CVX	ETH	USDC	DOLA	Slippage (%)
$50,000	17182	27.111	49235	49331	-1.34%
$100,000	34482	54.321	98645	98844	-1.16%
$250,000	86206	135.278	245533	245983	-1.61%
$500,000	172413	266.033	482658	483486	-3.30%
$1,000,000	344827	505.518	917110	918494	-8.15%
$2,000,000	689655	910.795	1651572	1653578	-17.32%
$4,000,000	1379310	1519.610	2758197	2760328	-30.99%
$6,000,000	2068965	1959.467	3557230	3558876	-40.69%

☐ **Token Holders**

aCVX: 20 Holders may seem like a small amount, but the vault was deployed 8 days before this risk assessment was produced. The expectation is that holders will increase due to higher yields offered compared to simple CVX staking and due to new utility if aCVX is onboarded to FiRM. For top 10 holders, see screenshot below.



Token Holders Chart

A total of 20 token holders

First | Page 1 of 1 | Last

Rank	Address	Quantity	Percentage	Analytics
1	0x649f69...25f5E9A3	161,044.843392021636964106	41.3862%	
2	0xfaC2F1...6688251E	146,808.491506629815848439	37.7277%	
3	0x698734...0AA1571d	41,180.904323007955409009	10.5829%	
4	7bfee.eth	8,117.276461145239076 47	2.0860%	
5	0x8591aA...23a84a79	7,533.55733256428296838	1.9360%	
6	0x514E49...7cf33e65	4,774.31981979465579027	1.2269%	
7	0xCfaba3...5B39c388	4,766.193963804634997715	1.2248%	
8	0xbA758d...F3bF0252	4,144.982430061764311373	1.0652%	
9	0xEC2eda...738b498E	3,000	0.7710%	
10	0x48c607...2ED82555	2,828.570614760190343847	0.7269%	

Utility & Use Case

- ☐ **Does the Token have utility (5)**

At the moment, aCVX has no utility beyond being a vault receipt. However, its potential for integration in compatible lending markets such as FiRM can lead it to have utility as a collateral option.

- ☐ **Goal of the token, where is value derived from (8)**

aCVX simply represents the compounding CVX in the Concentrator vault. As such, the goal and value of the aCVX token are closely tied to those of CVX, with some distinctions, notably enhancing yield. The value of aCVX is derived from its underlying earnings potential (via the strategy deployed) and how it compares to competitor strategies.

In assessing the value of a token, some considerations to keep in mind include platform performance (how any action to Concentrator and/or AlladinDAO and unrelated to aCVX might affect aCVX), and the broader regulatory environment.

Competitive Analysis

Competitive Markets & Implementation

- ☐ **Competitor Markets with supply & borrow capacity**

As of October 31st, 2023, no competitor protocol has integrated aCVX into their lending market.

- ☐ **Competitor Oracle Solutions**

N/A

- ☐ **Notable competitor failures**

AlphaHomora, Tranchess

Conclusion

Asset Score

October 30th, 2023: The RWG evaluated aCVX making use of our in-house comprehensive asset scoring model. This framework evaluates the relative “risk” of CVX as an asset, using wETH as a benchmark, by considering six essential factors, four of which (market capitalization, trading volume, price volatility, token distribution) were measured by studying CVX, and two

(project fundamentals, and token utility) by studying aCVX and AlladinDAO. A breakdown of the Total Asset Score (TAS) follows:

Component	Link/Rationale	Score
Market Capitalization	MCS=min(10, (CVX Supply * CVX Price * 200) /(wETH Supply * wETH price)	9.74
DEX Trading Volume	TVS =min(10, (30 Day Avg Token Trading Volume * 200 / 30 Day Avg wETH Trading Volume)	2.65
Price Volatility	PVS =min(10, 10 - (Token Log Price Volatility / wETH Log Price Volatility) * 9)	4.43
Token Distribution	Token Distribution Score = min((1- Token Gini Index) * 10 / (1 - wETH Gini Index);10)	4.47
Project Fundamentals	Risk Assessment aCVX Collateral on FiRM - See Protocol Analysis, and Audits & Bug Bounties Sections	7.32
Token Utility	Risk Assessment aCVX Collateral on FiRM - See Collateral Analysis Section	6.50

Total Asset Score

$$TAS = 9.74 * 0.2 + 2.65 * 0.15 + 4.43 * 0.15 + 4.47 * 0.1 + 7.32 * 0.2 + 6.50 * 0.2$$

$$TAS = 6.22/10$$

Comparatively, CVX, which was last assessed September 12th, 2023, scored a 6.96.

Parameter Recommendations

When recommending parameters for the proposed aCVX market on FiRM, the key factor is evaluating the aCVX vault smart contract. The additional smart contract (aCVX Convex Compounder) makes aCVX inherently riskier than CVX simply because two custody contracts is

more dangerous than one (aCVX = both Convex Compounder by AlladinDAO and Convex's staked contract). Without this, considerations for aCVX would be identical to those made for the currently deployed CVX market, as liquidity profiles between CVX and aCVX are expected to be identical.

As mentioned in the *Audits & Bug Bounties section*, the aCVX vault smart contract has been audited by SecBit as recently as October, 2023. SecBit's relatively unknown reputation in the realm of smart contract auditing introduces an element of risk when compared to a scenario where this audit be conducted by a reputable tier-1 firm.

Therefore, along with the recommended parameter settings detailed in the table below, we strongly advise AlladinDAO commision a supplementary audit prior to Inverse bringing aCVX to FiRM. The AladdinDAO team has expressed intent to conduct a second on the aCVX vault and turn the contract immutable soon after, thus fulfilling this request.

Supply Ceiling	1,000,000 DOLA
Initial Fed Supply	500,000 DOLA
Daily Borrow Limit	200,000 DOLA
Collateral Factor	70%
Liquidation Factor	36.5%
Liquidation Incentive	10%
Minimum Debt Amount	3,000 DOLA