



SOLIDITY FINANCE

Crypto Volatility Index

Smart Contract Audit Report

AUDIT SUMMARY



Crypto Volatility Index (CVI) is an innovative cryptocurrency volatility tracker that aggregates pricing data from multiple sources.

For this audit, we reviewed the project team's contracts folder at commit [9af98b54cf9dd61e7c5ef27fb2e5921eae98f0e4](#) on the team's private GitHub repository.

AUDIT FINDINGS

Please ensure trust in the team prior to investing as they have substantial control in the ecosystem.

Date: June 8th, 2022.

Updated: August 3rd, 2022 with updates from commit

5dcda64ec501e5014b2fa5afb889c8f05158b18b to commit

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

Finding #1 - Platform - Low (Acknowledged)

Description: The last deposit timestamp is reset whenever liquidity is added.

Risk/Impact: As liquidity is added through the Theta Vault, the last deposit timestamp will be updated when any user adds liquidity. This will prevent other users from withdrawing until the LP lock up period passes.

Recommendation: The last deposit timestamp should not prevent withdrawal for all users.

Resolution: The team has acknowledged this and plan to set the LP lock up period to 0.

Finding #2 - VolatilityToken - Low (Resolved)

Description: The `rebase()` function is public.

Risk/Impact: The rebaser address could trigger a positive rebase without syncing the LP pools. This would allow a theft of liquidity attack.

Recommendation: The `rebase()` function should be internal.

Resolution: The team has made the `rebase()` function internal so that a positive rebase is not possible.

CONTRACTS OVERVIEW

- The contracts utilize `ReentrancyGuard` to protect against reentrancy attacks in applicable functions.

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

- *The team should avoid using ERC-777 and fee-on-transfer tokens. If using fee on transfer tokens, ensure the contract is excluded from fees.*

GOVI contract

- *This contract defines the GOVI token.*
- *The total supply of 32 million tokens is minted to the owner upon deployment.*
- *No mint or burn functions exist, though the circulating supply can be decreased by sending tokens to the 0x..dead address if desired.*
- *The contract is ERC20 compliant, all standard functionality is present.*

GOVIAirdrop Contract

- *This contract is used to distribute a specified token to various addresses.*
- *The owner may distribute any number of tokens to any number of addresses at any time.*
- *The contract must be provided the tokens or the distribution will fail.*

FeesCalculator Contract

- *This contract is used to calculate and return fees for various other contracts.*
- *The "State Updater" address may trigger an update of the "turbulence indicator percent", indicating the size of change between the last two CVI measurements, at any time.*
- *The State Updater address may trigger an update of the "adjusted volume timestamp" and the "close adjusted volume timestamp", used*

- *The owner may update the CVI Oracle and State Updater address at any time.*
- *The owner may set the Deposit, Withdraw, Open Position, Close Position, Open Position LP, and Close Position LP fees at any time.*
- *The owner may set the Close Max, Buying Premium Max, and Closing Premium Max fee values at any time.*

RequestFeesCalculator Contract

- *This contract is used to calculate and return fees associated with Volatility Token mint and burn requests.*
- *A time penalty fee is calculated from a request's target fulfillment time. Time penalty fees are split into three tiers.*
- *If the current time is after the minimum wait time and before the target timestamp, the time penalty fee will start at the "before target time max percentage" decreasing as time approaches the target timestamp.*
- *If the current time is after the target timestamp and the "middle wait time" from the target, the penalty will start at 0 and increase to the "after target mid time" fee percentage.*
- *If the current time is after the middle wait time from the target, the penalty will increase up to the "after target max time" percentage.*
- *Once the after target max time from the target timestamp has passed, users' requests are considered liquidable and may be liquidated by any user or will be liquidated when the request is fulfilled.*
- *The time delay on a Request must be between the minimum and maximum time windows. A time delay fee is then calculated from the time delay where the larger the time delay the smaller the fee.*
- *The finders and keepers fee are calculated as a flat percentage of the*

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

keepers fee amount.

- The owner may set the minimum and maximum time window for time delays to any value at any time.*
- The owner may set the minimum time delay fee and maximum time delay fee up to the max fee percentage at any time.*
- The owner may set the minimum wait time at any time.*
- The owner may set the before target time, after target mid time, and after target max time fee percentages up to the max fee percentage at any time.*
- The owner may set the finders and keepers fee to any value up to the max fee percentage at any time.*
- The owner may set the maximum keepers fee to any value at any time.*

FeesCollector Contract

- This contract is used to collect and distribute fees from throughout the platform.*
- Any user may transfer USDC to the contract at any time. Contracts should use the provided functionality for collecting profit rather than sending tokens directly to prevent a transfer at an unwanted time.*
- The Funds Sender address may trigger the distribution of collected funds at any time.*
- If conversion to USDC is enabled and the accumulated funds in the contract are past the threshold, the contract's USDC will be converted to ETH or WETH depending on an owner-determined toggle.*
- The transaction may optionally be submitted to the Arbitrum Inbox to be recorded.*
- In addition to the Funds Sender address "allowed" senders on a*

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

the whitelist is not enabled, any user may trigger the upkeep.

- If the transaction is not being recorded using the Arbitrum Inbox and conversion to USDC is not enabled, the contract's ETH or WETH balance will be distributed in various ways.*
- If a Treasury Address has been set, a percentage of the contract's accumulated funds will be sent to the Treasury Address.*
- If enabled, the remaining funds will be used to buyback GOVI tokens from a Uniswap Liquidity Pool; the calling address will provide a current ETH/WETH to GOVI price to prevent excessive slippage.*
- Otherwise, the remaining funds will be transferred to the Staking address.*
- The owner may update the Price Aggregator, Uniswap Router, Staking, and Arbitrum addresses at any time.*
- The owner may update the Treasury Address and the percentage of ETH transferred to the Treasury Address at any time.*
- The owner may update the percentage of the contract's total ETH distributed at once, the maximum slippage allowed during swaps, the minimum amount of ETH to be converted, and the minimum amount of ETH to be transferred at any time.*
- The owner may toggle whether the contract will record to the Arbitrum address, whether the contract will perform a buyback, and if the contract will convert its ETH to USDC at any time.*
- The owner may set a new Funds Sender address and toggle any address as an allowed sender at any time.*
- The owner may set the wrapped token address and toggle whether the contract will use native ETH or the wrapped token at any time.*

- Any address may stake GOVI tokens at any time; in return, the user will receive xGOVI tokens representing shares proportional to the total value they are contributing to the pool.
- Users will earn rewards in various rewards tokens per block based on the current rewards rate and the amount of tokens staked; rewards tokens must be supplied to the contract from a Staking Vault or rewards claims will fail.
- Users may unstake out of the contract once the "stake lockup time" has passed since the last time the user has staked; the specified amount of the user's xGOVI tokens will be burned for the proportional ratio of GOVI tokens.
- Staking and unstaking tokens will store the user's due rewards for all claimable tokens, but the rewards must be claimed separately; users may claim their rewards for all rewards tokens or any specific rewards token at any time.
- If the contract has a non-zero total supply, any address may transfer an approved non-GOVI token to the contract to be distributed as rewards.
- If the contract has no total supply, the tokens will be transferred to a "fallback recipient" address.
- The owner may add and remove tokens as a reward token at any time.
- The owner may set the stake lockup time and the reward rate at any time.

StakingRewards Contract

- When not paused, any address may transfer the specified staking token to the contract; users will receive a reward amount per block during the rewards duration based on the amount of tokens staked and the

- *Users may withdraw any amount of deposited staking tokens at any time.*
- *The Rewards Distribution address may "notify rewards" to the contract at any time.*
- *Notifying rewards will update the reward rate for the current rewards period; rewards tokens must be supplied to the contract or rewards distribution will fail.*
- *The owner may withdraw any token that is not the staking token, rewards token, or Sythentix (\$SNX) token at any time.*
- *The owner may update the rewards duration to any value if the end of the current rewards duration has not been set or the current rewards duration has ended.*
- *The owner may set the Rewards Duration address at any time.*

StakingVault & KeepersFeeVault Contracts

- *These contracts are used to allow a specified contract to store and withdraw a specified token.*
- *The specified contract may withdraw any amount of the specified token at any time.*
- *The owner may update the specified address to any address at any time.*
- *The owner may withdraw any amount of the specified token from the StakingVault contract at any time.*

Treasury Contract

- *This contract is used to allow the owner to store and withdraw ETH.*
- *The owner may withdraw all ETH from the contract at any time.*

CVIOracle Contract

- *This contract is used to fetch and maintain an active CVI value from a specified CVI Aggregator.*
- *The CVI Aggregator was outside of the scope of this audit so we cannot give an assessment with regard to security.*
- *Any address may trigger a request for the "round data" from the CVI Aggregator at any time; round data consists of the CVI timestamp and CVI value.*
- *Any address may trigger a request for the latest round data from the CVI Aggregator at any time; if enabled, the request will check that the change between the returned CVI value does not exceed the "deviation threshold".*
- *The owner may toggle whether the deviation is checked at any time.*
- *The owner may set the max deviation allowed to any value at any time.*

Liquidation Contract

- *This contract is used to determine whether a Position in the Platform contract is a candidate to be liquidated*
- *A Position is a liquidation candidate if the Position's current balance is less than the liquidation threshold for the Position's leverage.*
- *If a Position is a liquidation candidate it is eligible for one of 3 tiers of liquidation rewards for the user liquidating.*
- *If the Position balance is less than the minimum liquidation reward, based on the original position balance, the liquidation reward is the minimum liquidation reward.*
- *If greater than the minimum liquidation reward, users will receive the current position balance up to the maximum liquidation reward*

- *The owner may set the threshold for liquidation for each leverage tier to any value at any time.*
- *The owner may set the minimum and maximum liquidation rewards percent for each tier to any value at any time.*

PositionRewards Contract

- *This contract is used to distribute additional rewards in the form of a specified token for users who have opened a Position on the Platform.*
- *Users may claim rewards from the time their Position is created through the max claim period.*
- *A maximum daily reward amount will be distributed across all claims. Once the daily reward is reached, users will be unable to claim rewards until the next day.*
- *Users will earn a reward amount per block until the max reward time has passed.*
- *Rewards tokens must be supplied to the contract or rewards claim will fail.*
- *The owner may set the max daily reward and reward factor to any value at any time.*
- *The owner may set the max claim period, max reward time, and max reward time percentage gain to any value at any time.*
- *The owner may update the Platform address at any time.*
- *The owner may withdraw all rewards tokens out of the contract at any time.*

Platform Contract

- *This is the main contract for interacting with the C4 platform users*

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

- *Addresses on the Liquidity Providers whitelist may deposit tokens to serve as collateral given that the last time the CVI snapshot was updated is not longer than the "max time allowed after latest round".*
- *The Liquidity Provider will receive LP tokens representing shares proportional to the amount they are contributing to the total unleveraged collateral; the amount of LP tokens being minted must be greater than the "minimum LP token" amount.*
- *If there are no tokens in the Platform, the Liquidity Provider will receive the "initial token to LP token rate" of tokens.*
- *If a deposit fee value has been set in the FeesCalculator contract, a deposit fee is taken and transferred to the Fee Collector address.*
- *Liquidity Providers may burn their LP tokens for the underlying tokens, given that the "LP lockup period" has passed since their last deposit.*
- *If a withdraw fee value has been set in the FeesCalculator contract, a withdraw fee is taken and transferred to the Fee Collector address.*
- *Users who have been added to the Shared Pool Allowed Addresses list may directly deposit tokens to the contract for collateral.*
- *Addresses on the "No Fee" list may open and close Positions without any of the various associated fees.*
- *Any address may open a Position within the allowed leverage and CVI values; the last time the CVI snapshot was updated must not be longer than the max time allowed after the latest round.*
- *If a user has an existing position, they may update their position within the same leverage but may not open positions across leverages.*
- *If applicable, an Open Position fee and Buying Premium fee are taken from the Position's token amount and transferred to the Fee Collector address.*

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

- *If applicable, a Close Position Fee and Closing Premium Fee are taken from the tokens being received and transferred to the Fee Collector address.*
- *If a Position's balance is negative, the Position will be liquidated when it is closed.*
- *Users may provide a list of addresses and liquidate their Positions if they are eligible.*
- *Users will receive a "finders fee" determined by the Liquidation Contract for each Position being liquidated.*
- *The owner may set the Fees Collector, CVI Oracle, Rewards, Liquidation, Staking, and Fees Calculator address at any time.*
- *The owner may update the latest Oracle Round ID, the max time allowed after a CVI update, and the LP and buyers lock up periods at any time.*
- *The owner may add and remove an address from any of the various whitelists at any time.*
- *The owner may toggle emergency withdraws and the deletion of old CVI snapshots at any time.*
- *The owner may set the maximum allowed leverage at any time.*

PlatformMigrator Contract

- *This contract is used to migrate LP tokens between two iterations of the Platform.*
- *Users specify a minimum amount of the new tokens they would like to receive for the transaction to succeed.*
- *The old tokens are transferred from the user to the contract where they are withdrawn from the old Platform*

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

- *The old tokens are then swapped for the new tokens; the swap will fail if the user will not receive the minimum amount of tokens specified.*
- *The received new tokens are then deposited into the new Platform and transferred to the user.*
- *The user will additionally receive a "reward amount" of the rewards token; the rewards tokens must be supplied to the contract or the transaction will fail.*
- *The owner may set the old Platform, new Platform, and Uniswap Router addresses at any time.*
- *The owner may update the reward amount to any value at any time.*
- *The owner may withdraw all of the rewards tokens from the contract at any time.*

Rebaser Contract

- *This contract is used to manually rebase a specified Volatility Token address and sync the associated LP pools.*
- *Any valid Rebaser address, or any address if the whitelist is not enabled, may trigger a rebase within this contract within the first 15 minutes of each day.*
- *This will first trigger a rebase of the Volatility token serving as a frictionless reduction of the total supply of the token.*
- *Once the Volatility token is rebased, all of the LP Pairs set within the contract will be synced to reflect an accurate balance within the pools.*
- *The owner may set the Volatility token and Uniswap pairs to any address at any time.*
- *The owner may set the upkeep interval and upkeep time window to any value at any time*

- *The owner may toggle the whitelist and toggle a user as a valid rebaser at any time.*

VolatilityToken Contract

- *The Rebase address may trigger a CVI rebase of the token serving as a frictionless reduction of the total supply of the token and each user's balance.*
- *The Rebase address may manually trigger a rebase serving as a frictionless increase or decrease of the total supply of the token and each user's balance.*
- *If capped rebases are enabled, the rebase amount must be between the minimum and maximum deviation percentage.*
- *Users may submit a mint request at any time with the option to use a keeper; if the user opts to use a keeper, the amount of tokens being deposited must be greater than the minimum keeper mint amount.*
- *If enabled, the current total tokens across all mint requests must remain under the max total requests amount.*
- *If users are not using a keeper, they must only supply the time delay fee and max fees amount of underlying tokens when submitting a mint request.*
- *If users are using a keeper, they must supply the entire underlying token amount.*
- *After a mint request has been submitted and the time delay has passed, the fulfiller address may fulfill the mint request.*
- *If the request was not created using keepers, the user who submitted the request may fulfill the mint request.*
- *Users may elect to fulfill their mint request before the target*

timestamp must have passed for the request to be fulfilled.

- *Users who did not mint using keepers will need to pay a fulfill fee calculated in the RequestFeesCalculator contract based on when the request is fulfilled relative to the target timestamp.*
- *Users who minted using keepers will have to pay a keepers fee.*
- *All users must pay a time delay fee.*
- *Users who did not use a keeper must provide the remaining tokens after fees at this point.*
- *The deposited tokens will be used to open a Position in the Platform Contract. The user is subsequently minted volatility tokens corresponding to the size of the Position they have opened relative to the total Platform position units created through this contract.*
- *The time delay and fulfill fees are sent to the Fees Collector whereas the keepers fee is sent to the Keepers Fee Vault.*
- *Users have the option to fulfill their mint request as a collateralized mint.*
- *This functions in the same way as a regular mint except that a portion of the tokens will be used to add liquidity to the Platform contract.*
- *If the collateralized mint is not possible users will receive a percentage of tokens deposited in addition to the time delay fee.*
- *Users may submit a burn request at any time with the option to use a keeper; if the user opts to use a keeper, the amount of tokens being burned must be greater than the minimum keeper burn amount.*
- *If users are not using a keeper, they must only supply the time delay fee and max fees amount of volatility tokens when submitting a burn request.*
- *If users are using a keeper, they must supply the entire token amount.*

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

- *If the request was not created using keepers, the user who submitted the request may fulfill the burn request.*
- *Users may elect to fulfill their burn request before the target timestamp. If the request was made using keepers, the target timestamp must have passed for the request to be fulfilled.*
- *Users who did not burn using keepers will need to pay a fulfill fee calculated in the RequestFeesCalculator contract based on when the request is fulfilled relative to the target timestamp.*
- *All users must pay a time delay fee.*
- *Users who did not use a keeper must provide the remaining tokens at this point.*
- *The specified number of tokens will be burned and the corresponding number of Position units will be closed in the Platform contract.*
- *A volume, time delay, and fulfill fees will be taken and transferred to the Fees Collector address.*
- *If a keeper was used, a keepers fee will be taken and transferred to the Keepers Vault address.*
- *The remaining tokens after fees are transferred back to the user.*
- *When fulfilling a request, if the "after target max time" has passed from a request's target timestamp the request will instead be liquidated.*
- *Any address may provide a request ID and liquidate the request if the after target max time from the request's target timestamp has passed.*
- *If the request was made using keepers, the request owner will receive their remaining tokens, after the finders fee and applicable burns are calculated.*
- *If the request was not made using keepers, the remaining tokens after fees and burns will be transferred to the Fees Collector address.*

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

- *The Minter address may mint and burn any amount of tokens at any time.*
- *The owner may update the Vault, Fulfiller, Minter, Platform, Fees Calculator, Fees Collector, Request Fees Calculator, and CVI Oracle addresses at any time.*
- *The owner may update the Rebaser address at any time.*
- *The owner may update the minimum and maximum deviation percentages at any time.*
- *The owner may toggle capped rebases and verifying max total token request amounts at any time.*
- *The owner may update the max total token request amount at any time.*

ThetaVault Contract

- *This contract is used to add liquidity to the Platform contract while mitigating token loss over time.*
- *The contract attempts to maintain a "minimum skew percentage" between the volatility token balance and a specified token balance in a corresponding liquidity pool; the minimum skew percentage defaults to 3%.*
- *If the pool is skewed during any transaction, the contract will attempt to rebalance the pool.*
- *A rebalance will use tokens being deposited, in a deposit transaction, or withdraw tokens from the Platform contract in other transactions.*
- *The tokens will be used to perform a swap equal to half of the skew in the pool. If the skew does not return to below the minimum skew percentage the transaction will fail*

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

- Any address may submit a deposit request while the total tokens controlled by the Vault and the tokens requested to be deposited remain under the deposit cap.
- The underlying tokens are transferred to the contract when submitting the deposit request.
- Once the request delay has passed, the Fulfiller address or the user who submitted the request may fulfill the deposit request.
- The user will receive theta tokens representing shares proportional to the total value they are contributing to the pool.
- On the first deposit, the user will receive the "initial token to theta token rate" of tokens.
- The deposited tokens will be split between adding liquidity to a Uniswap Liquidity Pool and adding liquidity to the Platform Contract.
- Any user may submit a withdrawal request once the lockup period has passed since their last deposit.
- The theta tokens are transferred to the contract when submitting the withdrawal request.
- Once the request delay has passed, the Fulfiller address or the user who submitted the request may fulfill the deposit request.
- The specified number of theta tokens will be burned and the following actions will occur:
 - The proportional amount of tokens will be removed from the Uniswap liquidity pool where the received volatility tokens are subsequently burned for the underlying token.
 - The proportional amount of LP tokens will be removed from the Platform contract.
 - The total amount of underlying tokens received are transferred to

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

- Any address may provide a request ID and liquidate the corresponding request if the liquidation time from the request's target timestamp has passed.
- The user who submitted their request will be returned their corresponding theta tokens or underlying tokens.
- The owner may trigger a rebalance at any time. This will withdraw some liquidity from the Platform and redeposit the received tokens between both the Platform and the Liquidity Pool.
- The owner may update the Fulfiller address at any time.
- The owner may set the minimum skew percentage to any value at any time.
- The owner may set the extra liquidity percentage, request delay, deposit cap, lockup period, and liquidation period at any time.

VolTokenRequestFulfiller & ThetaVaultRequestFulfiller Contracts

- These contracts are used to fulfill requests for the VolatilityToken and ThetaVault Contracts.
- If the whitelist is not enabled, any user may trigger "upkeep"; if the whitelist is enabled only a valid Fulfiller address may trigger upkeep.
- When upkeep is triggered, the contract will fetch all of the current VolatilityToken and ThetaVault requests from the corresponding contract, iterate over them, and fulfill all possible requests.
- The owner may set the RequestManager address at any time.
- The owner may toggle the whitelist at any time.
- The owner may toggle any address as a Fulfiller at any time.

Vulnerability Category	Notes	Result
Arbitrary Jump/Storage Write	N/A	PASS
Centralization of Control	- There are instances where fees may reach 100%. - The team may change where user's funds are sent in the VolatilityToken contract. - The team may withdraw all rewards tokens from the PositionRewards contract.	WARNING
Compiler Issues	N/A	PASS
Delegate Call to Untrusted Contract	N/A	PASS
Dependence on Predictable Variables	N/A	PASS
Ether/Token Theft	N/A	PASS
Flash Loans	N/A	PASS

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

Vulnerability Category	Notes	Result
Front Running	N/A	PASS
Improper Events	N/A	PASS
Improper Authorization Scheme	N/A	PASS
Integer Over/Underflow	N/A	PASS
Logical Issues	N/A	PASS
Oracle Issues	N/A	PASS
Outdated Compiler Version	N/A	PASS
Race Conditions	N/A	PASS
Reentrancy	N/A	PASS
Signature Issues	N/A	PASS
Unbounded Loops	N/A	PASS

Vulnerability Category	Notes	Result
Overall Contract Safety		PASS

CONTRACT SOURCE SUMMARY AND VISUALIZATIONS

Name	Address/Source Code	Visualized (Hover-Zoom Recommended)
GOVI	GitHub (Not yet deployed on mainnet)	Inheritance Chart. Function Graph.
GOVIAirdrop	GitHub (Not yet deployed on mainnet)	Inheritance Chart. Function Graph.
FeesCalculator	GitHub (Not yet deployed on mainnet)	Inheritance Chart.

RequestFeesCalculator	GitHub (Not yet deployed on mainnet)	Inheritance Chart. Function Graph.
FeesCollector	GitHub (Not yet deployed on mainnet)	Inheritance Chart. Function Graph.
Staking	GitHub (Not yet deployed on mainnet)	Inheritance Chart. Function Graph.
StakingRewards	GitHub (Not yet deployed on mainnet)	Inheritance Chart. Function Graph.
StakingVault	GitHub (Not yet deployed on mainnet)	Inheritance Chart. Function Graph.

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

[mainnet\)](#)

Treasury

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

CVIOracle

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

Liquidation

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

PositionRewards

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

Platform

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

PlatformMigrator

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

Rebaser

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

VolatilityToken

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

ThetaVault

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

VolTokenRequestFulfiller

[GitHub \(Not yet
deployed on
mainnet\)](#)

[Inheritance Chart.](#)
[Function Graph.](#)

ThetaVaultRequestFulfiller

[GitHub \(Not yet
deployed on](#)

[Inheritance Chart.](#)
[Function Graph](#)

Please review our [Terms & Conditions and Privacy Policy](#). By using this site, you agree to these terms.

ABOUT SOLIDITY FINANCE

Solidity Finance was founded in 2020 and quickly grew to have one of the most experienced and well-equipped smart contract auditing teams in the industry. Our team has conducted 1000+ solidity smart contract audits covering all major project types and protocols, securing a total of over \$50 billion U.S. dollars in on-chain value across 1500 projects!.

Our firm is well-reputed in the community and is trusted as a top smart contract auditing company for the review of solidity code, no matter how complex. Our team of experienced solidity smart contract auditors performs audits for tokens, NFTs, crowdsales, marketplaces, gambling games, financial protocols, and more!

Contact us today to get a free quote for a smart contract audit of your project!

WHAT IS A SOLIDITY AUDIT?

Typically, a smart contract audit is a comprehensive review process designed to discover logical errors, security vulnerabilities, and optimization opportunities within code. A *Solidity Audit* takes this a step further by verifying economic logic to ensure the stability of smart contracts and highlighting privileged functionality to create a report that is easy to understand for developers and community members alike.

HOW DO I INTERPRET THE FINDINGS?

Each of our Findings will be labeled with a Severity level. We always recommend the team resolve High, Medium, and Low severity findings prior to deploying the code to the mainnet. Here is a breakdown on what each Severity level means for the project:

- **High** severity indicates that the issue puts a large number of users' funds at risk and has a high probability of exploitation, or the smart contract contains serious logical issues which can prevent the code from operating as intended.
- **Medium** severity issues are those which place at least some users' funds at risk and has a

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.

- **Low** severity issues have a relatively minor risk association; these issues have a low probability of occurring or may have a minimal impact.
- **Informational** issues pose no immediate risk, but inform the project team of opportunities for gas optimizations and following smart contract security best practices.

G O H O M E

© Solidity Finance LLC. | All rights reserved.

Please note we are not associated with the Solidity programming language or the core team which develops the language.

Please review our Terms & Conditions and Privacy Policy. By using this site, you agree to these terms.