TechRate
September, 2022

TECH
RATE

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

Metavault Trade

Deployer address

0xf9d6d1bff8a32e908768afd1489e9546debdbb35

Client contacts:

Metavault Trade team

Blockchain

Polygon

Project website:

https://metavault.trade

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn’t say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and TechRate hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

Background

TechRate was commissioned by Metavault Trade to perform an audit of smart contracts:

- https://polygonscan.com/address/0x2760e46d9bb43dafcbecaad1f64b93207f9f0ed7
- https://polygonscan.com/address/0x39bdDc22D9B75727244CcC8F39b67d5A546937eC
- https://polygonscan.com/address/0x32848e2d3aecfa7364595609fb050a301050a6b4
- https://polygonscan.com/address/0xca9c89410025f2bc3befb07ce57529f26ad69093
- https://polygonscan.com/address/0x25f3434ce5873d169f3E73Ffc422C200dE22Be09

The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

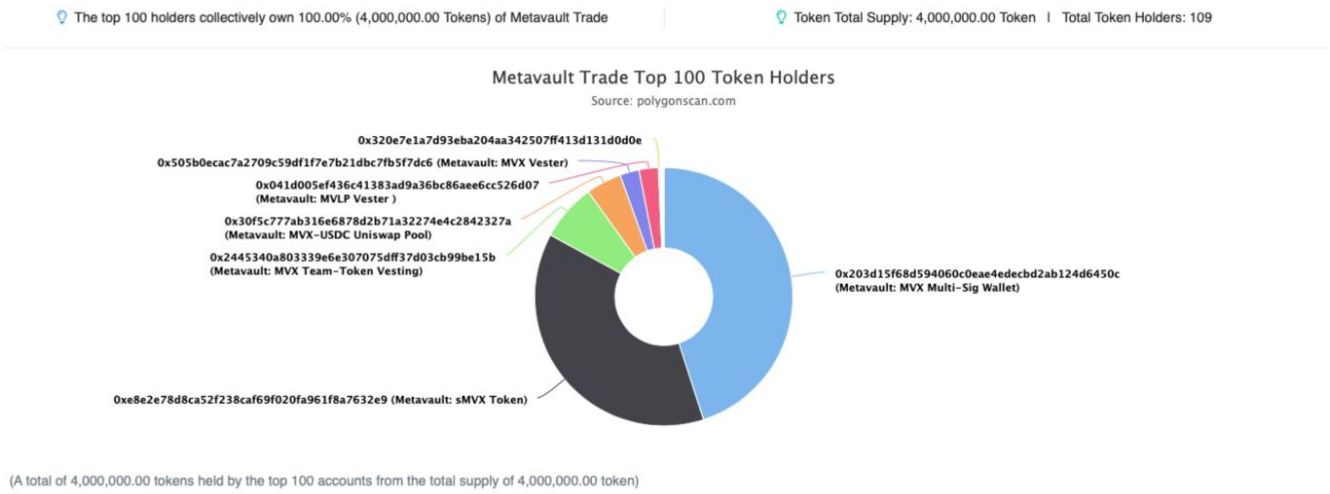
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 23.09.2022

Contract name	Metavault Trade
Contract address	0x2760E46d9BB43dafCbEcaad1F64b93207f9f0eD7
Total supply	4,000,000
Token ticker	MVX
Decimals	18
Token holders	109
Transactions count	20,984
Top 100 holders dominance	100.00%
Contract deployer address	0xf9d6d1bff8a32e908768afd1489e9546debdbb35
GOV address	0x39bddc22d9b75727244ccc8f39b67d5a546937ec

Metavault Trade Token Distribution



The top 100 holders collectively own 100.00% (4,000,000.00 Tokens) of Metavault Trade

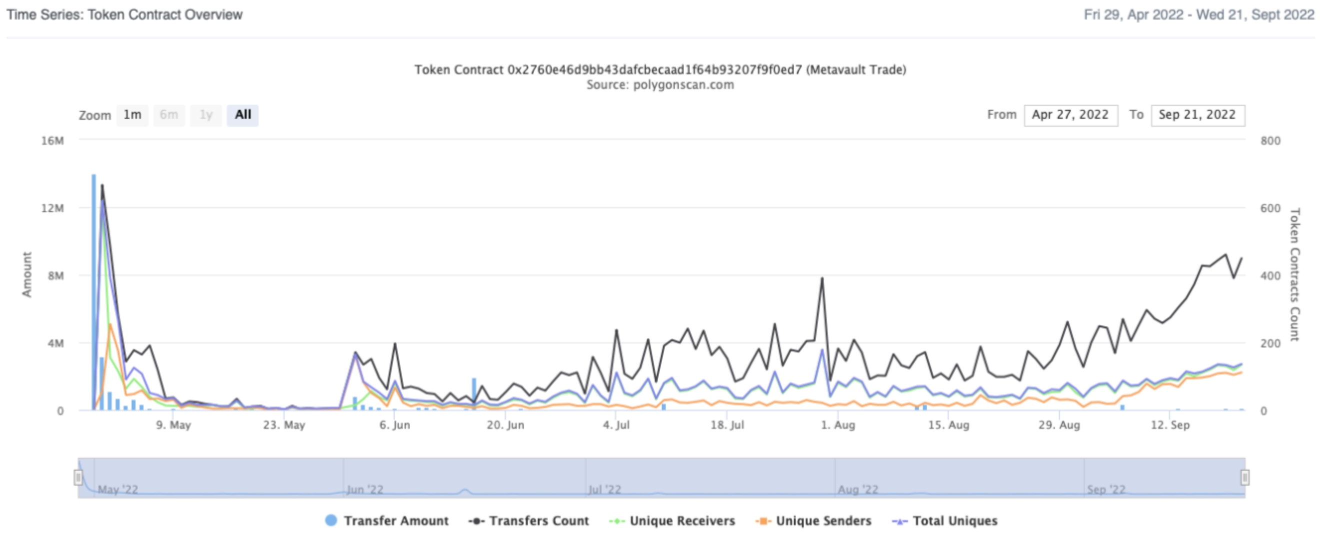
Token Total Supply: 4,000,000.00 Token | Total Token Holders: 109

Metavault Trade Top 100 Token Holders

Source: polygonscan.com

(A total of 4,000,000.00 tokens held by the top 100 accounts from the total supply of 4,000,000.00 token)

Metavault Trade Contract Interaction Details



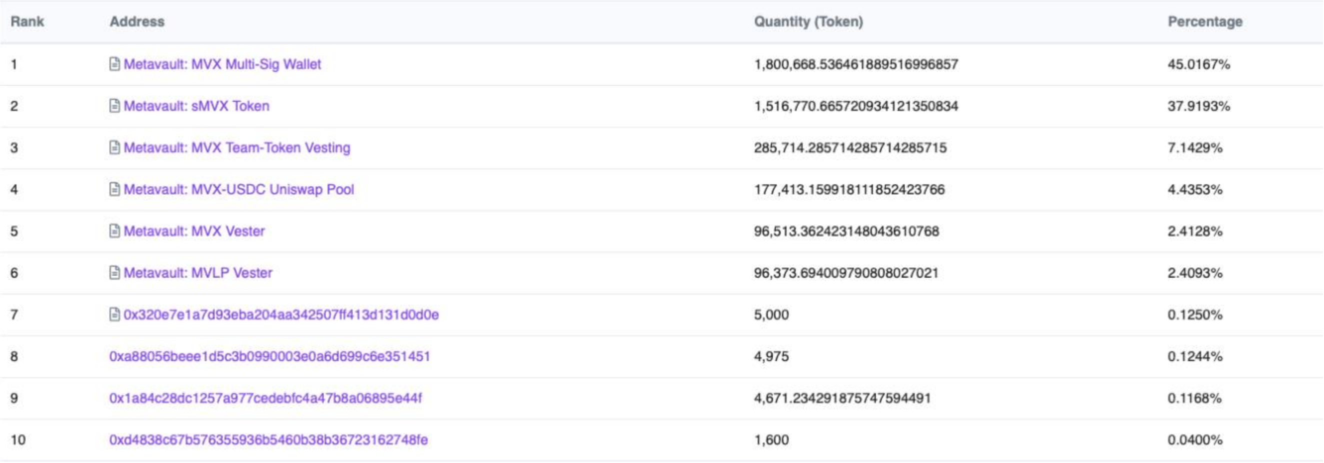
Time Series: Token Contract Overview

Fri 29, Apr 2022 - Wed 21, Sept 2022

Token Contract 0x2760e46d9bb43dafcbecaad1f64b93207f9f0ed7 (Metavault Trade)

Source: polygonscan.com

Metavault Trade Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	Metavault: MVX Multi-Sig Wallet	1,800,668.536461889516996857	45.0167%
2	Metavault: sMVX Token	1,516,770.665720934121350834	37.9193%
3	Metavault: MVX Team-Token Vesting	285,714.285714285714285715	7.1429%
4	Metavault: MVX-USDC Uniswap Pool	177,413.159918111852423766	4.4353%
5	Metavault: MVX Vester	96,513.362423148043610768	2.4128%
6	Metavault: MVLP Vester	96,373.694009790808027021	2.4093%
7	0x320e7e1a7d93eba204aa342507ff413d131d0d0e	5,000	0.1250%
8	0xa88056beee1d5c3b0990003e0a6d699c6e351451	4,975	0.1244%
9	0x1a84c28dc1257a977cedebfc4a47b8a06895e44f	4,671.234291875747594491	0.1168%
10	0xd4838c67b576355936b5460b38b36723162748fe	1,600	0.0400%

Contract functions details

```
+ [Lib] Address
   - [Int] isContract
   - [Int] sendValue #
   - [Int] functionCall #
   - [Int] functionCall #
   - [Int] functionCallWithValue #
   - [Int] functionCallWithValue #
   - [Int] functionStaticCall
   - [Int] functionStaticCall
   - [Int] functionDelegateCall #
   - [Int] functionDelegateCall #
   - [Prv] _verifyCallResult

 + [Int] IBaseToken
   - [Ext] totalStaked
   - [Ext] stakedBalance
   - [Ext] removeAdmin #
   - [Ext] setInPrivateTransferMode #
   - [Ext] withdrawToken #

 + [Int] IYieldTracker
   - [Ext] claim #
   - [Ext] updateRewards #
   - [Ext] getTokensPerInterval
   - [Ext] claimable

 + [Lib] SafeERC20
   - [Int] safeTransfer #
   - [Int] safeTransferFrom #
   - [Int] safeApprove #
   - [Int] safeIncreaseAllowance #
   - [Int] safeDecreaseAllowance #
   - [Prv] _callOptionalReturn #

 + [Int] IERC20
   - [Ext] totalSupply
   - [Ext] balanceOf
   - [Ext] transfer #
   - [Ext] allowance
   - [Ext] approve #
   - [Ext] transferFrom #
```

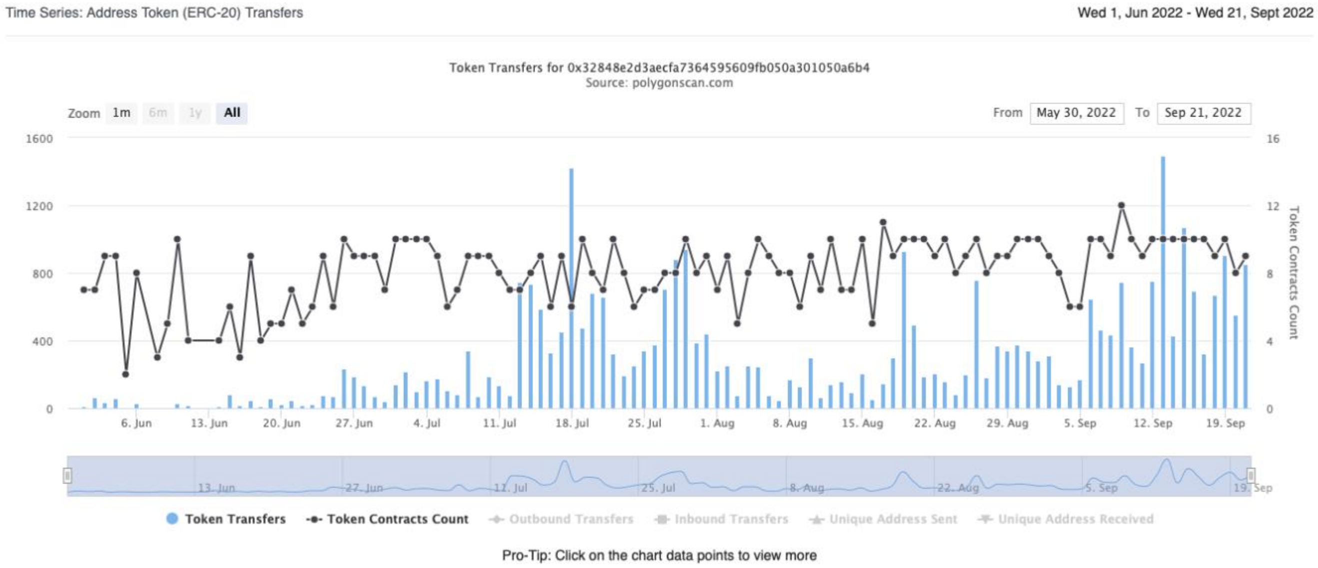
```
+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ [Int] IMintable
  - [Ext] isMinter #
  - [Ext] setMinter #
  - [Ext] mint #
  - [Ext] burn #

+  BaseToken (IERC20, IBaseToken)
  - [Pub] <Constructor> #
  - [Ext] setGov #
    - modifiers: onlyGov
  - [Ext] setInfo #
    - modifiers: onlyGov
  - [Ext] setYieldTrackers #
    - modifiers: onlyGov
  - [Ext] addAdmin #
    - modifiers: onlyGov
  - [Ext] removeAdmin #
    - modifiers: onlyGov
  - [Ext] withdrawToken #
    - modifiers: onlyGov
  - [Ext] setInPrivateTransferMode #
    - modifiers: onlyGov
  - [Ext] setHandler #
    - modifiers: onlyGov
  - [Ext] addNonStakingAccount #
    - modifiers: onlyAdmin
  - [Ext] removeNonStakingAccount #
    - modifiers: onlyAdmin
  - [Ext] recoverClaim #
    - modifiers: onlyAdmin
  - [Ext] claim #
  - [Ext] totalStaked
  - [Ext] balanceOf
  - [Ext] stakedBalance
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #
  - [Int] _mint #
  - [Int] _burn #
  - [Prv] _transfer #
  - [Prv] _approve #
  - [Prv] _updateRewards #

+  MintableBaseToken (BaseToken, IMintable)
  - [Pub] <Constructor> #
    - modifiers: BaseToken
  - [Ext] setMinter #
    - modifiers: onlyGov
  - [Ext] mint #
    - modifiers: onlyMinter
  - [Ext] burn #
    - modifiers: onlyMinter

+  MVX (MintableBaseToken)
  - [Pub] <Constructor> #
    - modifiers: MintableBaseToken
  - [Ext] id


($) = payable function
# = non-constant function
```

Contracts Details

Token contract details for 23.09.2022

Contract name	Vault
Contract address	0x2760E46d9BB43dafCbEcaad1F64b93207f9f0eD7
Tax/swap basis points	50/30
priceFeed	0xb022b0353fe4c4af6fb3f5b1243a8da8a12e7c42
Max gas price	0
Error controller	0xe25fa5ffd1f3302b49117ba2f60a475c9a932fdc
Router	0xca9c89410025f2bc3befb07ce57529f26ad69093
USDM	0x533403a3346ca31d67c380917ffaf185c24e7333
Contract deployer address	0xf9d6d1bff8a32e908768afd1489e9546debdbb35
GOV address	0x25f3434ce5873d169f3e73ffc422c200de22be09

Vault Contract Interaction Details



Time Series: Address Token (ERC-20) Transfers

Wed 1, Jun 2022 - Wed 21, Sept 2022

Token Transfers for 0x32848e2d3aecfa7364595609fb050a301050a6b4
Source: polygonscan.com

Pro-Tip: Click on the chart data points to view more

Contract functions details

```
+ [Lib] Address
   - [Int] isContract
   - [Int] sendValue #
   - [Int] functionCall #
   - [Int] functionCall #
   - [Int] functionCallWithValue #
   - [Int] functionCallWithValue #
   - [Int] functionStaticCall
   - [Int] functionStaticCall
   - [Int] functionDelegateCall #
   - [Int] functionDelegateCall #
   - [Prv] _verifyCallResult

 + [Int] IVaultPriceFeed
   - [Ext] adjustmentBasisPoints
   - [Ext] isAdjustmentAdditive
   - [Ext] setAdjustment #
   - [Ext] setUseV2Pricing #
   - [Ext] setIsAmmEnabled #
   - [Ext] setIsSecondaryPriceEnabled #
   - [Ext] setSpreadBasisPoints #
   - [Ext] setSpreadThresholdBasisPoints #
   - [Ext] setFavorPrimaryPrice #
   - [Ext] setPriceSampleSpace #
   - [Ext] setMaxStrictPriceDeviation #
   - [Ext] getPrice
   - [Ext] getAmmPrice
   - [Ext] getPrimaryPrice
   - [Ext] setTokenConfig #

 + [Int] IVaultUtils
   - [Ext] updateCumulativeFundingRate #
   - [Ext] validateIncreasePosition
   - [Ext] validateDecreasePosition
   - [Ext] validateLiquidation
   - [Ext] getEntryFundingRate
   - [Ext] getPositionFee
   - [Ext] getFundingFee
   - [Ext] getBuyUsdmFeeBasisPoints
   - [Ext] getSellUsdmFeeBasisPoints
   - [Ext] getSwapFeeBasisPoints
```

```
  - [Ext] getFeeBasisPoints

+ [Int] IVault
  - [Ext] isInitialized
  - [Ext] isSwapEnabled
  - [Ext] isLeverageEnabled
  - [Ext] setVaultUtils #
  - [Ext] setError #
  - [Ext] router
  - [Ext] usdm
  - [Ext] gov
  - [Ext] whitelistedTokenCount
  - [Ext] maxLeverage
  - [Ext] minProfitTime
  - [Ext] hasDynamicFees
  - [Ext] fundingInterval
  - [Ext] totalTokenWeights
  - [Ext] getTargetUsdmAmount
  - [Ext] inManagerMode
  - [Ext] inPrivateLiquidationMode
  - [Ext] maxGasPrice
  - [Ext] approvedRouters
  - [Ext] isLiquidator
  - [Ext] isManager
  - [Ext] minProfitBasisPoints
  - [Ext] tokenBalances
  - [Ext] lastFundingTimes
  - [Ext] setMaxLeverage #
  - [Ext] setInManagerMode #
  - [Ext] setManager #
  - [Ext] setIsSwapEnabled #
  - [Ext] setIsLeverageEnabled #
  - [Ext] setMaxGasPrice #
  - [Ext] setUsdmAmount #
  - [Ext] setBufferAmount #
  - [Ext] setMaxGlobalShortSize #
  - [Ext] setInPrivateLiquidationMode #
  - [Ext] setLiquidator #
  - [Ext] setFundingRate #
  - [Ext] setFees #
  - [Ext] setTokenConfig #
  - [Ext] setPriceFeed #
  - [Ext] withdrawFees #
  - [Ext] directPoolDeposit #
  - [Ext] buyUSDM #
```

  - [Ext] sellUSDM #
  - [Ext] swap #
  - [Ext] increasePosition #
  - [Ext] decreasePosition #
  - [Ext] liquidatePosition #
  - [Ext] tokenToUsdMin
  - [Ext] priceFeed
  - [Ext] fundingRateFactor
  - [Ext] stableFundingRateFactor
  - [Ext] cumulativeFundingRates
  - [Ext] getNextFundingRate
  - [Ext] getFeeBasisPoints
  - [Ext] liquidationFeeUsd
  - [Ext] taxBasisPoints
  - [Ext] stableTaxBasisPoints
  - [Ext] mintBurnFeeBasisPoints
  - [Ext] swapFeeBasisPoints
  - [Ext] stableSwapFeeBasisPoints
  - [Ext] marginFeeBasisPoints
  - [Ext] allWhitelistedTokensLength
  - [Ext] allWhitelistedTokens
  - [Ext] whitelistedTokens
  - [Ext] stableTokens
  - [Ext] shortableTokens
  - [Ext] feeReserves
  - [Ext] globalShortSizes
  - [Ext] globalShortAveragePrices
  - [Ext] maxGlobalShortSizes
  - [Ext] tokenDecimals
  - [Ext] tokenWeights
  - [Ext] guaranteedUsd
  - [Ext] poolAmounts
  - [Ext] bufferAmounts
  - [Ext] reservedAmounts
  - [Ext] usdmAmounts
  - [Ext] maxUsdmAmounts
  - [Ext] getRedemptionAmount
  - [Ext] getMaxPrice
  - [Ext] getMinPrice
  - [Ext] getDelta
  - [Ext] getPosition

+ [Int] IUSDM
  - [Ext] addVault #
  - [Ext] removeVault #

  - [Ext] mint #
  - [Ext] burn #

+ ReentrancyGuard
  - [Int] <Constructor> #

+ [Lib] SafeERC20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ Vault (ReentrancyGuard, IVault)
  - [Pub] <Constructor> #
  - [Ext] initialize #
  - [Ext] setVaultUtils #
  - [Ext] setErrorController #
  - [Ext] setError #
  - [Ext] allWhitelistedTokensLength
  - [Ext] setInManagerMode #
  - [Ext] setManager #
  - [Ext] setInPrivateLiquidationMode #
  - [Ext] setLiquidator #
  - [Ext] setIsSwapEnabled #
  - [Ext] setIsLeverageEnabled #

- [Ext] setMaxGasPrice #
- [Ext] setGov #
- [Ext] setPriceFeed #
- [Ext] setMaxLeverage #
- [Ext] setBufferAmount #
- [Ext] setMaxGlobalShortSize #
- [Ext] setFees #
- [Ext] setFundingRate #
- [Ext] setTokenConfig #
- [Ext] clearTokenConfig #
- [Ext] withdrawFees #
- [Ext] addRouter #
- [Ext] removeRouter #
- [Ext] setUsdmAmount #
- [Ext] upgradeVault #
- [Ext] directPoolDeposit #
  - modifiers: nonReentrant
- [Ext] buyUSDM #
  - modifiers: nonReentrant
- [Ext] sellUSDM #
  - modifiers: nonReentrant
- [Ext] swap #
  - modifiers: nonReentrant
- [Ext] increasePosition #
  - modifiers: nonReentrant
- [Ext] decreasePosition #
  - modifiers: nonReentrant
- [Prv] _decreasePosition #
- [Ext] liquidatePosition #
  - modifiers: nonReentrant
- [Pub] validateLiquidation
- [Pub] getMaxPrice
- [Pub] getMinPrice
- [Pub] getRedemptionAmount
- [Pub] getRedemptionCollateral
- [Pub] getRedemptionCollateralUsd
- [Pub] adjustForDecimals
- [Pub] tokenToUsdMin
- [Pub] usdToTokenMax
- [Pub] usdToTokenMin
- [Pub] usdToToken
- [Pub] getPosition
- [Pub] getPositionKey
- [Pub] updateCumulativeFundingRate #
- [Pub] getNextFundingRate

- [Pub] getUtilisation
- [Pub] getPositionLeverage
- [Pub] getNextAveragePrice
- [Pub] getNextGlobalShortAveragePrice
- [Pub] getGlobalShortDelta
- [Pub] getPositionDelta
- [Pub] getDelta
- [Pub] getEntryFundingRate
- [Pub] getFundingFee
- [Pub] getPositionFee
- [Pub] getFeeBasisPoints
- [Pub] getTargetUsdmAmount
- [Prv] _reduceCollateral #
- [Prv] _validatePosition
- [Prv] _validateRouter
- [Prv] _validateTokens
- [Prv] _collectSwapFees #
- [Prv] _collectMarginFees #
- [Prv] _transferIn #
- [Prv] _transferOut #
- [Prv] _updateTokenBalance #
- [Prv] _increasePoolAmount #
- [Prv] _decreasePoolAmount #
- [Prv] _validateBufferAmount
- [Prv] _increaseUsdmAmount #
- [Prv] _decreaseUsdmAmount #
- [Prv] _increaseReservedAmount #
- [Prv] _decreaseReservedAmount #
- [Prv] _increaseGuaranteedUsd #
- [Prv] _decreaseGuaranteedUsd #
- [Prv] _increaseGlobalShortSize #
- [Prv] _decreaseGlobalShortSize #
- [Prv] _onlyGov
- [Prv] _validateManager
- [Prv] _validateGasPrice
- [Prv] _validate

($) = payable function
# = non-constant function

Contracts Details

Token contract details for 23.09.2022

Contract name	MvxTimelock
Contract address	0x39bdDc22D9B75727244CcC8F39b67d5A546937eC
Admin address	0xc1048db8e91e68b468b1d7b513fbb666c6e1622d
Max token supply	10000000000000000000000000
Max buffer	604800
Token manager	0x93415c0b0f59ff7c8f5b763ed1fcc617d1418df9
Long buffer	604800
Buffer	86400
Contract deployer address	0xc1048db8e91e68b468b1d7b513fbb666c6e1622d

Contract functions details

```
+ [Int] IERC20
   - [Ext] totalSupply
   - [Ext] balanceOf
   - [Ext] transfer #
   - [Ext] allowance
   - [Ext] approve #
   - [Ext] transferFrom #
+ [Lib] SafeMath
   - [Int] add
   - [Int] sub
   - [Int] sub
   - [Int] mul
   - [Int] div
   - [Int] div
   - [Int] mod
   - [Int] mod
+ [Int] IMintable
   - [Ext] isMinter #
   - [Ext] setMinter #
   - [Ext] mint #
   - [Ext] burn #
+ [Int] IBaseToken
   - [Ext] totalStaked
   - [Ext] stakedBalance
   - [Ext] removeAdmin #
   - [Ext] setInPrivateTransferMode #
   - [Ext] withdrawToken #

 + [Int] IYieldToken
   - [Ext] totalStaked
   - [Ext] stakedBalance
   - [Ext] removeAdmin #

 + [Int] IAdmin
   - [Ext] setAdmin #
+ [Int] IMvxTimelock
   - [Ext] setAdmin #
   - [Ext] signalSetGov #

 + [Int] ITimelockTarget
   - [Ext] setGov #
```

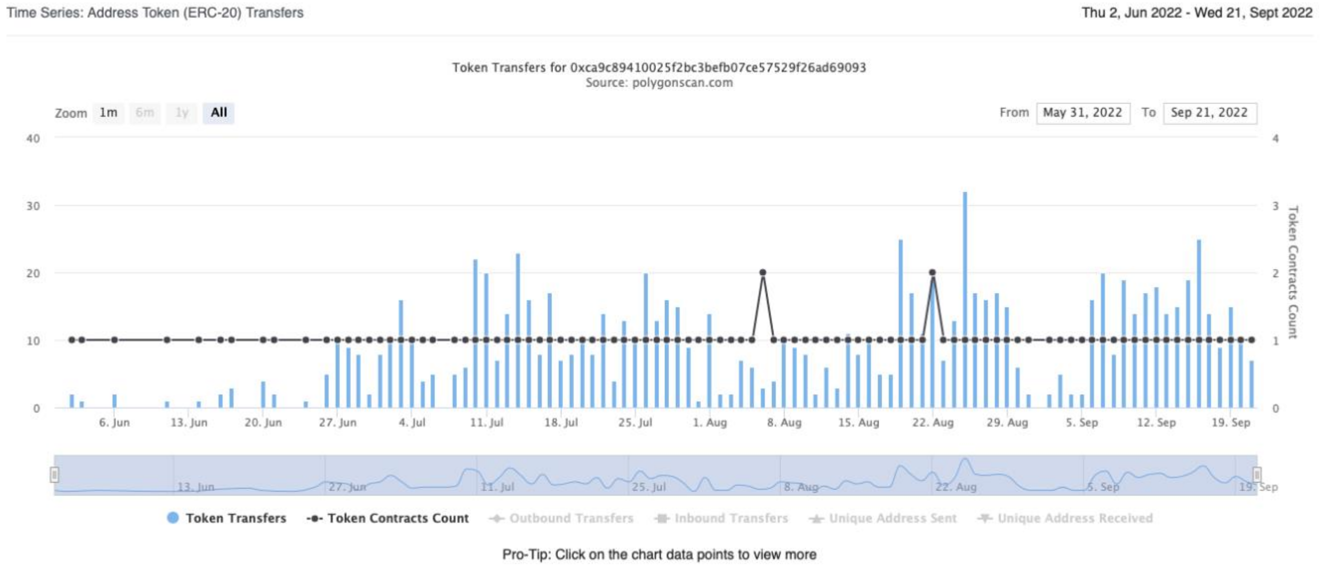
```
  - [Ext] withdrawToken #

+  MvxTimelock (IMvxTimelock)
  - [Pub] <Constructor> #
  - [Ext] setAdmin #
    - modifiers: onlyTokenManager
  - [Ext] setExternalAdmin #
    - modifiers: onlyAdmin
  - [Ext] setContractHandler #
    - modifiers: onlyAdmin
  - [Ext] setBuffer #
    - modifiers: onlyAdmin
  - [Ext] removeAdmin #
    - modifiers: onlyAdmin
  - [Ext] setInPrivateTransferMode #
    - modifiers: onlyAdmin
  - [Ext] transferIn #
    - modifiers: onlyAdmin
  - [Ext] signalApprove #
    - modifiers: onlyAdmin
  - [Ext] approve #
    - modifiers: onlyAdmin
  - [Ext] signalWithdrawToken #
    - modifiers: onlyAdmin
  - [Ext] withdrawToken #
    - modifiers: onlyAdmin
  - [Ext] signalMint #
    - modifiers: onlyAdmin
  - [Ext] processMint #
    - modifiers: onlyAdmin
  - [Ext] signalSetGov #
    - modifiers: onlyTokenManager
  - [Ext] setGov #
    - modifiers: onlyAdmin
  - [Ext] cancelAction #
    - modifiers: onlyAdmin
  - [Prv] _mint #
  - [Prv] _setPendingAction #
  - [Prv] _setLongPendingAction #
  - [Prv] _validateAction
  - [Prv] _clearAction #

($) = payable function
# = non-constant function
```

Contracts Details

Token contract details for 23.09.2022

Contract name	Router
Contract address	0xCA9c89410025F2bc3BeFb07CE57529F26ad69093
Weth	0x0d500b1d8e8ef31e21c99d1db9a6444d3adf1270
Vault	0x32848e2d3aecfa7364595609fb050a301050a6b4
USDM	0x533403a3346ca31d67c380917ffaf185c24e7333
Contract deployer address	0xf9d6d1bff8a32e908768afd1489e9546debdbb35
GOV address	0x25f3434ce5873d169f3e73ffc422c200de22be09

Router Contract Interaction Details



Time Series: Address Token (ERC-20) Transfers

Thu 2, Jun 2022 - Wed 21, Sept 2022

Token Transfers for 0xca9c89410025f2bc3befb07ce57529f26ad69093
Source: polygonscan.com

Pro-Tip: Click on the chart data points to view more

Contract functions details

```
+ [Int] IVaultUtils
   - [Ext] updateCumulativeFundingRate #
   - [Ext] validateIncreasePosition
   - [Ext] validateDecreasePosition
   - [Ext] validateLiquidation
   - [Ext] getEntryFundingRate
   - [Ext] getPositionFee
   - [Ext] getFundingFee
   - [Ext] getBuyUsdmFeeBasisPoints
   - [Ext] getSellUsdmFeeBasisPoints
   - [Ext] getSwapFeeBasisPoints
   - [Ext] getFeeBasisPoints

 + [Int] IRouter
   - [Ext] addPlugin #
   - [Ext] pluginTransfer #
   - [Ext] pluginIncreasePosition #
   - [Ext] pluginDecreasePosition #
   - [Ext] swap #

 + [Int] IVault
   - [Ext] isInitialized
   - [Ext] isSwapEnabled
   - [Ext] isLeverageEnabled
   - [Ext] setVaultUtils #
   - [Ext] setError #
   - [Ext] router
   - [Ext] usdm
   - [Ext] gov
   - [Ext] whitelistedTokenCount
   - [Ext] maxLeverage
   - [Ext] minProfitTime
   - [Ext] hasDynamicFees
   - [Ext] fundingInterval
   - [Ext] totalTokenWeights
   - [Ext] getTargetUsdmAmount
   - [Ext] inManagerMode
   - [Ext] inPrivateLiquidationMode
   - [Ext] maxGasPrice
   - [Ext] approvedRouters
   - [Ext] isLiquidator
```

- [Ext] isManager
- [Ext] minProfitBasisPoints
- [Ext] tokenBalances
- [Ext] lastFundingTimes
- [Ext] setMaxLeverage #
- [Ext] setInManagerMode #
- [Ext] setManager #
- [Ext] setIsSwapEnabled #
- [Ext] setIsLeverageEnabled #
- [Ext] setMaxGasPrice #
- [Ext] setUsdmAmount #
- [Ext] setBufferAmount #
- [Ext] setMaxGlobalShortSize #
- [Ext] setInPrivateLiquidationMode #
- [Ext] setLiquidator #
- [Ext] setFundingRate #
- [Ext] setFees #
- [Ext] setTokenConfig #
- [Ext] setPriceFeed #
- [Ext] withdrawFees #
- [Ext] directPoolDeposit #
- [Ext] buyUSDM #
- [Ext] sellUSDM #
- [Ext] swap #
- [Ext] increasePosition #
- [Ext] decreasePosition #
- [Ext] liquidatePosition #
- [Ext] tokenToUsdMin
- [Ext] priceFeed
- [Ext] fundingRateFactor
- [Ext] stableFundingRateFactor
- [Ext] cumulativeFundingRates
- [Ext] getNextFundingRate
- [Ext] getFeeBasisPoints
- [Ext] liquidationFeeUsd
- [Ext] taxBasisPoints
- [Ext] stableTaxBasisPoints
- [Ext] mintBurnFeeBasisPoints
- [Ext] swapFeeBasisPoints
- [Ext] stableSwapFeeBasisPoints
- [Ext] marginFeeBasisPoints
- [Ext] allWhitelistedTokensLength
- [Ext] allWhitelistedTokens
- [Ext] whitelistedTokens
- [Ext] stableTokens

```
  - [Ext] shortableTokens
  - [Ext] feeReserves
  - [Ext] globalShortSizes
  - [Ext] globalShortAveragePrices
  - [Ext] maxGlobalShortSizes
  - [Ext] tokenDecimals
  - [Ext] tokenWeights
  - [Ext] guaranteedUsd
  - [Ext] poolAmounts
  - [Ext] bufferAmounts
  - [Ext] reservedAmounts
  - [Ext] usdmAmounts
  - [Ext] maxUsdmAmounts
  - [Ext] getRedemptionAmount
  - [Ext] getMaxPrice
  - [Ext] getMinPrice
  - [Ext] getDelta
  - [Ext] getPosition

+ [Int] IWETH
  - [Ext] deposit ($)
  - [Ext] transfer #
  - [Ext] withdraw #

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Prv] _verifyCallResult

+ [Lib] SafeERC20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #
```

```
+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+  Router (IRouter)
  - [Pub] <Constructor> #
  - [Ext] <Fallback> ($)
  - [Ext] setGov #
    - modifiers: onlyGov
  - [Ext] addPlugin #
    - modifiers: onlyGov
  - [Ext] removePlugin #
    - modifiers: onlyGov
  - [Ext] approvePlugin #
  - [Ext] denyPlugin #
  - [Ext] pluginTransfer #
  - [Ext] pluginIncreasePosition #
  - [Ext] pluginDecreasePosition #
  - [Ext] directPoolDeposit #
  - [Pub] swap #
  - [Ext] swapETHToTokens ($)
  - [Ext] swapTokensToETH #
  - [Ext] increasePosition #
  - [Ext] increasePositionETH ($)
  - [Ext] decreasePosition #
  - [Ext] decreasePositionETH #
  - [Ext] decreasePositionAndSwap #
  - [Ext] decreasePositionAndSwapETH #
  - [Prv] _increasePosition #
  - [Prv] _decreasePosition #
  - [Prv] _transferETHToVault #
```

- [Prv] _transferOutETH #
- [Prv] _swap #
- [Prv] _vaultSwap #
- [Prv] _sender
- [Prv] _validatePlugin

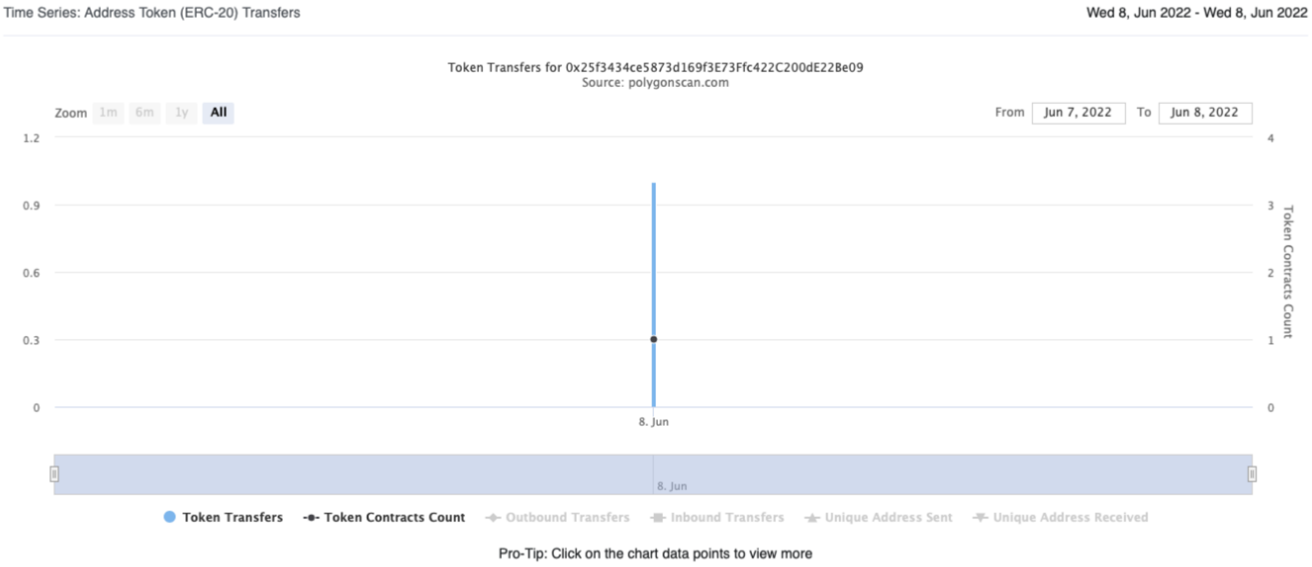
($) = payable function
# = non-constant function

Contracts Details

Token contract details for 23.09.2022

Contract name	Timelock
Contract address	0x25f3434ce5873d169f3E73Ffc422C200dE22Be09
Mint receiver	0x93415c0b0f59ff7c8f5b763ed1fcc617d1418df9
Reward manager	0x37a259cf77ff5f9ab61c4e8e83490f371b34a1ea
Token manager	0x93415c0b0f59ff7c8f5b763ed1fcc617d1418df9
Contract deployer address	0xf9d6d1bff8a32e908768afd1489e9546debdbb35
Admin address	0xc1048db8e91e68b468b1d7b513fbb666c6e1622d

Timelock Contract Interaction Details



Time Series: Address Token (ERC-20) Transfers

Wed 8, Jun 2022 - Wed 8, Jun 2022

Token Transfers for 0x25f3434ce5873d169f3E73Ffc422C200dE22Be09
Source: polygonscan.com

From Jun 7, 2022 To Jun 8, 2022

Pro-Tip: Click on the chart data points to view more

Contract functions details

```
+ [Int] IERC20
   - [Ext] totalSupply
   - [Ext] balanceOf
   - [Ext] transfer #
   - [Ext] allowance
   - [Ext] approve #
   - [Ext] transferFrom #

 + [Lib] SafeMath
   - [Int] add
   - [Int] sub
   - [Int] sub
   - [Int] mul
   - [Int] div
   - [Int] div
   - [Int] mod
   - [Int] mod

 + [Int] IVester
   - [Ext] rewardTracker
   - [Ext] claimForAccount #
   - [Ext] claimable
   - [Ext] cumulativeClaimAmounts
   - [Ext] claimedAmounts
   - [Ext] pairAmounts
   - [Ext] getVestedAmount
   - [Ext] transferredAverageStakedAmounts
   - [Ext] transferredCumulativeRewards
   - [Ext] cumulativeRewardDeductions
   - [Ext] bonusRewards
   - [Ext] transferStakeValues #
   - [Ext] setTransferredAverageStakedAmounts #
   - [Ext] setTransferredCumulativeRewards #
   - [Ext] setCumulativeRewardDeductions #
   - [Ext] setBonusRewards #
   - [Ext] getMaxVestableAmount
   - [Ext] getCombinedAverageStakedAmount

 + [Int] IUSDM
   - [Ext] addVault #
   - [Ext] removeVault #
```

  - [Ext] mint #
  - [Ext] burn #

+ [Int] IMintable
  - [Ext] isMinter #
  - [Ext] setMinter #
  - [Ext] mint #
  - [Ext] burn #

+ [Int] IBaseToken
  - [Ext] totalStaked
  - [Ext] stakedBalance
  - [Ext] removeAdmin #
  - [Ext] setInPrivateTransferMode #
  - [Ext] withdrawToken #

+ [Int] IYieldToken
  - [Ext] totalStaked
  - [Ext] stakedBalance
  - [Ext] removeAdmin #

+ [Int] IReferralStorage
  - [Ext] codeOwners
  - [Ext] getTraderReferralInfo
  - [Ext] setTraderReferralCode #
  - [Ext] setTier #
  - [Ext] setReferrerTier #
  - [Ext] govSetCodeOwner #

+ [Int] IRouter
  - [Ext] addPlugin #
  - [Ext] pluginTransfer #
  - [Ext] pluginIncreasePosition #
  - [Ext] pluginDecreasePosition #
  - [Ext] swap #

+ [Int] IFastPriceFeed
  - [Ext] lastUpdatedAt
  - [Ext] lastUpdatedBlock
  - [Ext] setIsSpreadEnabled #
  - [Ext] setSigner #

+ [Int] IVaultPriceFeed
  - [Ext] adjustmentBasisPoints
  - [Ext] isAdjustmentAdditive

  - [Ext] setAdjustment #
  - [Ext] setUseV2Pricing #
  - [Ext] setIsAmmEnabled #
  - [Ext] setIsSecondaryPriceEnabled #
  - [Ext] setSpreadBasisPoints #
  - [Ext] setSpreadThresholdBasisPoints #
  - [Ext] setFavorPrimaryPrice #
  - [Ext] setPriceSampleSpace #
  - [Ext] setMaxStrictPriceDeviation #
  - [Ext] getPrice
  - [Ext] getAmmPrice
  - [Ext] getPrimaryPrice
  - [Ext] setTokenConfig #

+ [Int] IVaultUtils
  - [Ext] updateCumulativeFundingRate #
  - [Ext] validateIncreasePosition
  - [Ext] validateDecreasePosition
  - [Ext] validateLiquidation
  - [Ext] getEntryFundingRate
  - [Ext] getPositionFee
  - [Ext] getFundingFee
  - [Ext] getBuyUsdmFeeBasisPoints
  - [Ext] getSellUsdmFeeBasisPoints
  - [Ext] getSwapFeeBasisPoints
  - [Ext] getFeeBasisPoints

+ [Int] IVault
  - [Ext] isInitialized
  - [Ext] isSwapEnabled
  - [Ext] isLeverageEnabled
  - [Ext] setVaultUtils #
  - [Ext] setError #
  - [Ext] router
  - [Ext] usdm
  - [Ext] gov
  - [Ext] whitelistedTokenCount
  - [Ext] maxLeverage
  - [Ext] minProfitTime
  - [Ext] hasDynamicFees
  - [Ext] fundingInterval
  - [Ext] totalTokenWeights
  - [Ext] getTargetUsdmAmount
  - [Ext] inManagerMode
  - [Ext] inPrivateLiquidationMode

- [Ext] maxGasPrice
- [Ext] approvedRouters
- [Ext] isLiquidator
- [Ext] isManager
- [Ext] minProfitBasisPoints
- [Ext] tokenBalances
- [Ext] lastFundingTimes
- [Ext] setMaxLeverage #
- [Ext] setInManagerMode #
- [Ext] setManager #
- [Ext] setIsSwapEnabled #
- [Ext] setIsLeverageEnabled #
- [Ext] setMaxGasPrice #
- [Ext] setUsdmAmount #
- [Ext] setBufferAmount #
- [Ext] setMaxGlobalShortSize #
- [Ext] setInPrivateLiquidationMode #
- [Ext] setLiquidator #
- [Ext] setFundingRate #
- [Ext] setFees #
- [Ext] setTokenConfig #
- [Ext] setPriceFeed #
- [Ext] withdrawFees #
- [Ext] directPoolDeposit #
- [Ext] buyUSDM #
- [Ext] sellUSDM #
- [Ext] swap #
- [Ext] increasePosition #
- [Ext] decreasePosition #
- [Ext] liquidatePosition #
- [Ext] tokenToUsdMin
- [Ext] priceFeed
- [Ext] fundingRateFactor
- [Ext] stableFundingRateFactor
- [Ext] cumulativeFundingRates
- [Ext] getNextFundingRate
- [Ext] getFeeBasisPoints
- [Ext] liquidationFeeUsd
- [Ext] taxBasisPoints
- [Ext] stableTaxBasisPoints
- [Ext] mintBurnFeeBasisPoints
- [Ext] swapFeeBasisPoints
- [Ext] stableSwapFeeBasisPoints
- [Ext] marginFeeBasisPoints
- [Ext] allWhitelistedTokensLength

  - [Ext] allWhitelistedTokens
  - [Ext] whitelistedTokens
  - [Ext] stableTokens
  - [Ext] shortableTokens
  - [Ext] feeReserves
  - [Ext] globalShortSizes
  - [Ext] globalShortAveragePrices
  - [Ext] maxGlobalShortSizes
  - [Ext] tokenDecimals
  - [Ext] tokenWeights
  - [Ext] guaranteedUsd
  - [Ext] poolAmounts
  - [Ext] bufferAmounts
  - [Ext] reservedAmounts
  - [Ext] usdmAmounts
  - [Ext] maxUsdmAmounts
  - [Ext] getRedemptionAmount
  - [Ext] getMaxPrice
  - [Ext] getMinPrice
  - [Ext] getDelta
  - [Ext] getPosition

+ [Int] IAdmin
  - [Ext] setAdmin #

+ [Int] IHandlerTarget
  - [Ext] isHandler #
  - [Ext] setHandler #

+ [Int] ITimelock
  - [Ext] setAdmin #
  - [Ext] enableLeverage #
  - [Ext] disableLeverage #
  - [Ext] setIsLeverageEnabled #
  - [Ext] signalSetGov #
  - [Ext] managedSetHandler #
  - [Ext] managedSetMinter #

+ [Int] ITimelockTarget
  - [Ext] setGov #
  - [Ext] withdrawToken #

+ Timelock (ITimelock)
  - [Prv] _onlyAdminOrHandler
  - [Pub] <Constructor> #

- [Ext] setAdmin #
  - modifiers: onlyTokenManager
- [Ext] setExternalAdmin #
  - modifiers: onlyAdmin
- [Ext] setContractHandler #
  - modifiers: onlyAdmin
- [Ext] setBuffer #
  - modifiers: onlyAdmin
- [Ext] mint #
  - modifiers: onlyAdmin
- [Ext] setMaxLeverage #
  - modifiers: onlyAdmin
- [Ext] setFundingRate #
- [Ext] setShouldToggleIsLeverageEnabled #
- [Ext] setMarginFeeBasisPoints #
- [Ext] setSwapFees #
- [Ext] setFees #
- [Ext] enableLeverage #
- [Ext] disableLeverage #
- [Ext] setIsLeverageEnabled #
- [Ext] setTokenConfig #
- [Ext] setMaxGlobalShortSize #
  - modifiers: onlyAdmin
- [Ext] removeAdmin #
  - modifiers: onlyAdmin
- [Ext] setIsAmmEnabled #
  - modifiers: onlyAdmin
- [Ext] setIsSecondaryPriceEnabled #
- [Ext] setMaxStrictPriceDeviation #
- [Ext] setUseV2Pricing #
- [Ext] setAdjustment #
- [Ext] setSpreadBasisPoints #
- [Ext] setSpreadThresholdBasisPoints #
- [Ext] setFavorPrimaryPrice #
- [Ext] setPriceSampleSpace #
- [Ext] setIsSwapEnabled #
- [Ext] setIsSpreadEnabled #
- [Ext] setTier #
- [Ext] setReferrerTier #
- [Ext] govSetCodeOwner #
- [Ext] setVaultUtils #
  - modifiers: onlyAdmin
- [Ext] setMaxGasPrice #
  - modifiers: onlyAdmin
- [Ext] withdrawFees #

  - modifiers: onlyAdmin
- [Ext] setInPrivateLiquidationMode #
  - modifiers: onlyAdmin
- [Ext] setLiquidator #
  - modifiers: onlyAdmin
- [Ext] addExcludedToken #
  - modifiers: onlyAdmin
- [Ext] setInPrivateTransferMode #
  - modifiers: onlyAdmin
- [Ext] managedSetHandler #
  - modifiers: onlyRewardManager
- [Ext] managedSetMinter #
  - modifiers: onlyRewardManager
- [Ext] batchSetBonusRewards #
  - modifiers: onlyAdmin
- [Ext] transferIn #
  - modifiers: onlyAdmin
- [Ext] signalApprove #
  - modifiers: onlyAdmin
- [Ext] approve #
  - modifiers: onlyAdmin
- [Ext] signalWithdrawToken #
  - modifiers: onlyAdmin
- [Ext] withdrawToken #
  - modifiers: onlyAdmin
- [Ext] signalMint #
  - modifiers: onlyAdmin
- [Ext] processMint #
  - modifiers: onlyAdmin
- [Ext] signalSetGov #
  - modifiers: onlyAdmin
- [Ext] setGov #
  - modifiers: onlyAdmin
- [Ext] signalSetHandler #
  - modifiers: onlyAdmin
- [Ext] setHandler #
  - modifiers: onlyAdmin
- [Ext] signalSetPriceFeed #
  - modifiers: onlyAdmin
- [Ext] setPriceFeed #
  - modifiers: onlyAdmin
- [Ext] signalAddPlugin #
  - modifiers: onlyAdmin
- [Ext] addPlugin #
  - modifiers: onlyAdmin

- [Ext] signalSetPriceFeedWatcher #
    - modifiers: onlyAdmin
- [Ext] setPriceFeedWatcher #
    - modifiers: onlyAdmin
- [Ext] signalRedeemUsdm #
    - modifiers: onlyAdmin
- [Ext] redeemUsdm #
    - modifiers: onlyAdmin
- [Ext] signalVaultSetTokenConfig #
    - modifiers: onlyAdmin
- [Ext] vaultSetTokenConfig #
    - modifiers: onlyAdmin
- [Ext] signalPriceFeedSetTokenConfig #
    - modifiers: onlyAdmin
- [Ext] priceFeedSetTokenConfig #
    - modifiers: onlyAdmin
- [Ext] cancelAction #
    - modifiers: onlyAdmin
- [Prv] _mint #
- [Prv] _setPendingAction #
- [Prv] _validateAction
- [Prv] _clearAction #

($) = payable function
# = non-constant function

Issues Checking Status

	Issue description	Checking status
1.	**Compiler errors.**	Passed
2.	**Race conditions and Reentrancy. Cross-function race conditions.**	Passed
3.	**Possible delays in data delivery.**	Passed
4.	**Oracle calls.**	Passed
5.	**Front running.**	Passed
6.	**Timestamp dependence.**	Passed
7.	**Integer Overflow and Underflow.**	Passed
8.	**DoS with Revert.**	Passed
9.	**DoS with block gas limit.**	Low issues
10.	**Methods execution permissions.**	Passed
11.	**Economy model of the contract.**	Passed
12.	**The impact of the exchange rate on the logic.**	Passed
13.	**Private user data leaks.**	Passed
14.	**Malicious Event log.**	Passed
15.	**Scoping and Declarations.**	Passed
16.	**Uninitialized storage pointers.**	Passed
17.	**Arithmetic accuracy.**	Low issues
18.	**Design Logic.**	Low issues
19.	**Cross-function race conditions.**	Passed
20.	**Safe Open Zeppelin contracts implementation and usage.**	Passed
21.	**Fallback function security.**	Passed

Security Issues

✓ High Severity Issues

No high severity issues found.

✓ Medium Severity Issues

No medium severity issues found.

✓ Low Severity Issues

1. Out of gas

Issue (Metavault Trade):

- The function recoverClaim(), claim() and _updateRewards() uses the loop to iterate through the yieldTrackers list. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.

Recommendation:
Check that the array length is not too big.

Issue (Timelock):

- The function batchSetBonusRewards() uses the loop to iterate through the _accounts list. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.

Recommendation:
Check that the array length is not too big.

2. Clearing token issue

Issue (Vault):

- clearTokenConfig() function doesn't clear allWhitelistedTokens.

Recommendation:
Remove deleted tokens from allWhitelistedTokens array.

3. Rounding error

Issue (Vault):

- updateCumulativeFundingRate() function divides block.timestamp with fundingInterval before multiplication. In Solidity we don’t have floating points, but instead we get rounding errors.

Recommendation:

Do division after multiplication.

Notes:

- Handler address can transfer tokens without allowance (not an issue when handler address is the contract).
- setUsdmAmount() function could not decrease USDM amount higher than current USDM amount for token (SafeMath).

Owner privileges (In the period when the owner is not renounced)

- Metavault Trade:
  - Minter address can mint and burn tokens.
  - Admin address can add/remove NonStakingAccounts.
  - Admin address can manually claim for addresses.
  - Gov address can change name and symbol.
  - Gov address can change yieldTrackers.
  - Gov address can add/remove admins.
  - Gov address can withdraw ERC20 tokens.
  - Gov address can enable/disable inPrivateTransferModel.
  - Gov address can change handler addresses.
  - Gov address can add minters.

- Timelock:
  - Token manager can change admin address.
  - Reward manager can change handler to targets.
  - Admin can call any other public functions.

- Router:
  - Gov address can change gov address.
  - Gov address can add/remove plugins.

- Vault:
  - Gov address can initialize the contract.
  - Gov address can add/remove managers.
  - Gov address can change vaultUtils.
  - Gov address can change errorController address.
  - Gov address can change error codes.
  - Gov address can change inManagerMode value.
  - Gov address can change inPrivateLiquidationMode value.
  - Gov address can change Liquidator addresses.
  - Gov address can change isSwapEnabled, isLeverageEnabled values.
  - Gov address can change gov address.
  - Gov address can change maxGasPrice and maxLeverage values.
  - Gov address can change priceFeed address.
  - Gov address can change bufferAmounts and maxGlobalShortSizes for address.
  - Gov address can change fees.
  - Gov address can change token configs.
  - Gov address can withdraw fees.
  - Gov address can increase/decrease USDM amounts for tokens.

    - Gov address can transfer tokens to new vault.
    - Manager address can buy/sell USDM.

- MvxTimelock:
    - Token manager can change admin address.
    - Admin can set external admins for targets.
    - Admin can set handler.
    - Admin can change buffer.
    - Admin can change _inPrivateTransferMode of target token.
    - Admin can call transferrin(), signalApprove, approve(), signalWithdrawToken(), withdrawToken(), signalMint() and processMint() functions .
    - Token manager can set *setGov* action.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract’s security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details are provided by the team:
https://polygonscan.com/address/0x203D15f68d594060C0EaE4edecBD2aB124d6450C#code

Security score: 73.

TechRate note:
Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.