Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: Crescent DAO Protocol
Platform: Moonbeam Network
Language: Solidity
Date: June 24th, 2022

Table of contents

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO THE PUBLIC AFTER ISSUES ARE RESOLVED.

Email: audit@EtherAuthority.io

Introduction

EtherAuthority was contracted by Crescent DAO to perform the Security audit of the Crescent DAO Protocol smart contracts code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on June 24th, 2022.

The purpose of this audit was to address the following:

- Ensure that all claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in the smart contract.

Project Background

- Crescent DAO is a DeFi project which has functions like mint, swap, OpenTrade, burn, twap, spot, update, info, transfer, set pool, claimable, zap, addLiquidity, cleanDust, etc.
- The Crescent DAO contract inherits the IERC721, ERC20, SafeERC20, Ownable, ReentrancyGuard, Address, IUniswapV2Router02, IUniswapV2Pair, IERC20, Math, SafeMath, Initializable, ERC20Burnable, TransparentUpgradeableProxy standard smart contracts from the OpenZeppelin library.
- These OpenZeppelin contracts are considered community-audited and time-tested, and hence are not part of the audit scope.

Audit scope

Name	**Code Review and Security Analysis Report for Crescent DAO Protocol Smart Contracts**
Platform	**Moonbeam / Solidity**
File 1	Pool.sol
File 1 MD5 Hash	014DC90C6AD4B3867DE93EDC865BACE2
File 2	SwapStrategyPOL.sol
File 2 MD5 Hash	53A53AF07B8469F6A83F375EA5FC80D3

File 3	Timelock.sol
File 3 MD5 Hash	7C1C21559F192FD0CBD71441481DE67B
File 4	CrescentDaoChef.sol
File 4 MD5 Hash	A8155b377b448bbd9a34ce912fb33d29
File 5	CrescentDaoStaking.sol
File 5 MD5 Hash	Db40ef9fad8b87542bbe189f264d6041
File 6	CrescentDaoZapMMSwap.sol
File 6 MD5 Hash	EF23876741700F7EC37BBAD9E7E07716
File 7	Fund.sol
File 7 MD5 Hash	97C4322C4361F5F9EE499C7A03D87CE4
File 8	CRSTDaoFund.sol
File 8 MD5 Hash	4C479B01CFD58077EA3085A95B3ED4AA
File 9	CRSTDevFund.sol
File 9 MD5 Hash	1ADD50486B590AD8954EDA23880F5F25
File 10	CRSTReserve.sol
File 10 MD5 Hash	317BB0E3A23F40418F03B0C8EAC9ACFD
File 11	CRSTTreasuryFund.sol
File 11 MD5 Hash	918CEE8384F94CB3A70221DB4103B333
File 12	MasterOracle.sol
File 12 MD5 Hash	907F87B061B83D4F0E09A1603F222BD0
File 13	UniswapPairOracle.sol
File 13 MD5 Hash	2F3769D4BA17C7B87A8818F20686D8EA
File 14	XToken.sol
File 14 MD5 Hash	5A75362ECD721A9E57E871DE10108AB5
File 15	YToken.sol
File 15 MD5 Hash	4A892A825DCE95C5E92682A2B31F455B
File 16	CRST.sol

File 16 MD5 Hash	239809621DF2ECEC8033B37B0863B2BF
File 17	GLMX.sol
File 17 MD5 Hash	13274608429D3F449D96A9379A197F82
File 18	CrescentDaoTreasury.sol
File 18 MD5 Hash	E16E77A69C630849E616117484D282D3
File 19	StratRecollateralize.sol
File 19 MD5 Hash	589B4C17597ECBABF3B8E4844FFE196D
File 20	StratReduceReserveLP.sol
File 20 MD5 Hash	91D7A6202E1BCB9434FFC08CFE6498A2
Audit Date	June 24th,2022

Claimed Smart Contract Features

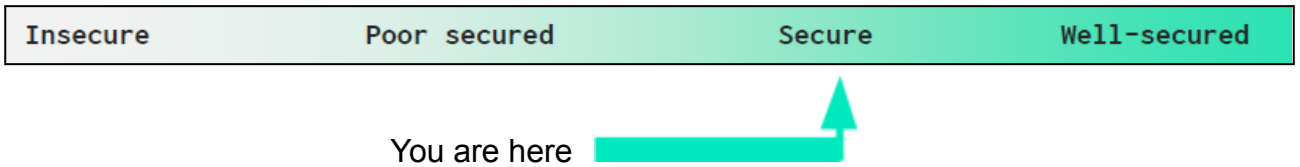
Claimed Feature Detail	Our Observation
File 1 Pool.sol • Refresh Cooldown: 1 hour • Ratio StepUp: 0.2% • Ratio StepDown: 0.2% • Price Target: 1 GLMR • Price Band: 0.004 GLMR • Minimum Collateral Ratio: 9,00,000 • YToken Slippage: 20% • Redemption Fee: 0.5% • Redemption Fee Maximum: 0.9% • Minting Fee: 0.3% • Minting Fee Maximum: 0.5%	**YES, This is valid.**
File 2 SwapStrategyPOL.sol • Swap Slippage: 20%	**YES, This is valid.**
File 3 Timelock.sol • Grace Period: 14 Days • Minimum Delay: 12 Hours • Maximum Delay: 30 Days	**YES, This is valid.**
File 4 CrescentDaoChef.sol • CrescentDaoChef has functions like: pendingReward, updatePool, etc.	**YES, This is valid.**
File 5 CrescentDaoStaking.sol • Rewards Duration: 1 week • Lock Duration: 8 weeks • Team Reward Percent: 20%	**YES, This is valid.**
File 6 CrescentDaoZapMMSwap.sol CrescentDaoZap is a ZapperFi's simplified version	**YES, This is valid.**

of zapper contract which will: 1. use ETH to swap to target token 2. make LP between ETH and target token 3. add into CrescentDaoChef farm	
File 7 Fund.sol • Fund has functions like: allocation, claimable, etc.	**YES, This is valid.**
File 8 CRSTDaoFund.sol • Allocation: 10% • Vesting Duration: 3 Years	**YES, This is valid.**
File 9 CRSTDevFund.sol • Allocation: 10% • Vesting Duration: 2 Years	**YES, This is valid.**
File 10 CRSTReserve.sol • CRSTReserve has functions like: initialize, setRewarder, etc.	**YES, This is valid.**
File 11 CRSTTreasuryFund.sol • Allocation: 10% • Vesting Duration: 3 Years	**YES, This is valid.**
File 12 MasterOracle.sol • MasterOracle has functions like: getYTokenPrice, getYTokenTWAP, etc.	**YES, This is valid.**
File 13 UniswapPairOracle.sol • Period: 60-minute Twap (Time-weighted Average Price) • Maximum Period: 48 Hours • Minimum Period: 10 Minutes • Leniency: 12 Hours	**YES, This is valid.**
File 14 XToken.sol	**YES, This is valid.**

• XToken has functions like: mint, etc.	
File 15 YToken.sol • YToken has functions like: burn, etc.	**YES, This is valid.**
File 16 CRST.sol • Total Supply: 30 Million ether • CRST has functions like: OpenTrade, etc.	**YES, This is valid.**
File 17 GLMX.sol • Genesis Supply = 100 ether will be minted at genesis for liq pool seeding.	**YES, This is valid.**
File 18 CrescentDaoTreasury.sol • The CrescentDaoTreasury owner can add a new strategy. • CrescentDaoTreasury owner can remove current strategy	**YES, This is valid.**
File 19 StratRecollateralize.sol • StratRecollateralize can recollateralize the minting pool.	**YES, This is valid.**
File 20 StratReduceReserveLP.sol • StratReduceReserveLP can remove liquidity, buy back YToken and burn.	**YES, This is valid.**

Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are **"Secured"**. Also, these contracts do contain owner control, which does not make them fully decentralized.



We used various tools like Slither, Solhint and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.
All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

We found 0 critical, 0 high, 0 medium and 2 low and some very low level issues.

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Technical Quick Stats

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Moderated
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Moderated
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	N/A
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Features claimed	Passed
	Other programming issues	Moderated
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Unused code	Passed
Gas Optimization	“Out of Gas” Issue	Passed
	High consumption ‘for/while’ loop	Moderated
	High consumption ‘storage’ storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Moderated
	“Short Address” Attack	Passed
	“Double Spend” Attack	Passed

Overall Audit Result: **PASSED**

Code Quality

This audit scope has 20 smart contract files. Smart contracts contain Libraries, Smart contracts, inherits and Interfaces. This is a compact and well written smart contract.

The libraries in the Crescent DAO Protocol are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the Crescent DAO Protocol.

The Crescent DAO team has not provided unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Some code parts are not well commented on smart contracts. We suggest using Ethereum's NatSpec style for the commenting.

Documentation

We were given a Crescent DAO Protocol smart contract code in the form of a file. The hash of that code is mentioned above in the table.

As mentioned above, code parts are not well commented. But the logic is straightforward. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Use of Dependencies

As per our observation, the libraries are used in this smart contracts infrastructure that are based on well known industry standard open source projects.

Apart from libraries, its functions are used in external smart contract calls.

AS-IS overview

Pool.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	nonReentrant	modifier	Passed	No Issue
8	info	external	Passed	No Issue
9	usableCollateralBalance	read	Passed	No Issue
10	calcMint	read	Passed	No Issue
11	calcRedeem	read	Passed	No Issue
12	calcExcessCollateralBalance	read	Passed	No Issue
13	refreshCollateralRatio	write	Passed	No Issue
14	mint	external	Other Programming issue	Refer Audit Findings
15	redeem	external	Passed	No Issue
16	collect	external	Passed	No Issue
17	recollateralize	external	Passed	No Issue
18	checkPriceFluctuation	internal	Passed	No Issue
19	toggle	write	access only Owner	No Issue
20	setCollateralRatioOptions	write	access only Owner	No Issue
21	toggleCollateralRatio	write	access only Owner	No Issue
22	setFees	write	access only Owner	No Issue
23	setMinCollateralRatio	external	access only Owner	No Issue
24	reduceExcessCollateral	external	access only Owner	No Issue
25	setSwapStrategy	external	access only Owner	No Issue
26	setOracle	external	access only Owner	No Issue
27	setYTokenSlippage	external	access only Owner	No Issue
28	setTreasury	external	Ambiguous Error Message	Refer Audit Findings
29	transferToTreasury	internal	Passed	No Issue

SwapStrategyPOL.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue

3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	lpBalance	read	Passed	No Issue
8	execute	external	Passed	No Issue
9	calculateSwapInAmount	internal	Passed	No Issue
10	swap	internal	Passed	No Issue
11	addLiquidity	internal	Passed	No Issue
12	cleanDust	external	access only Owner	No Issue
13	changeSlippage	external	access only Owner	No Issue

Timelock.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	setDelay	write	Passed	No Issue
3	acceptAdmin	write	Passed	No Issue
4	setPendingAdmin	write	Passed	No Issue
5	queueTransaction	write	Passed	No Issue
6	cancelTransaction	write	Passed	No Issue
7	executeTransaction	write	Passed	No Issue
8	getBlockTimestamp	internal	Passed	No Issue

CrescentDaoChef.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	poolLength	read	Passed	No Issue
8	pendingReward	external	Passed	No Issue
9	updatePool	write	Passed	No Issue
10	massUpdatePools	write	Infinite loop	Refer Audit Findings
11	deposit	write	Passed	No Issue
12	withdraw	write	Passed	No Issue
13	harvest	write	Passed	No Issue
14	withdrawAndHarvest	write	Passed	No Issue
15	emergencyWithdraw	write	Passed	No Issue

16	harvestAllRewards	external	Infinite loop	Refer Audit Findings
17	checkPoolDuplicate	internal	Infinite loop	Refer Audit Findings
18	add	write	access only Owner	No Issue
19	set	write	access only Owner	No Issue
20	setRewardPerSecond	write	access only Owner	No Issue
21	setRewardMinter	external	Passed	No Issue

CrescentDaoStaking.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	nonReentrant	modifier	Passed	No Issue
8	addReward	write	Function input parameters lack of check	Refer Audit Findings
9	approveRewardDistributor	external	Function input parameters lack of check	Refer Audit Findings
10	_rewardPerToken	internal	Passed	No Issue
11	_earned	internal	Passed	No Issue
12	lastTimeRewardApplicable	read	Passed	No Issue
13	getRewardForDuration	external	Passed	No Issue
14	claimableRewards	external	Passed	No Issue
15	totalBalance	external	Passed	No Issue
16	unlockedBalance	external	Passed	No Issue
17	earnedBalances	external	Passed	No Issue
18	withdrawableBalance	read	Passed	No Issue
19	stake	external	Passed	No Issue
20	mint	external	Function input parameters lack of check, Division before multiplication	Refer Audit Findings
21	withdraw	write	Passed	No Issue
22	getReward	write	Passed	No Issue
23	emergencyWithdraw	external	Critical operation lacks event log	Refer Audit Findings
24	_notifyReward	internal	Passed	No Issue

25	notifyRewardAmount	external	Function input parameters lack of check	Refer Audit Findings
26	recoverERC20	external	Owner can drain all ERC20 tokens	Refer Audit Findings
27	setTeamWalletAddress	external	Passed	No Issue
28	setTeamRewardPercent	external	Passed	No Issue
29	updateReward	modifier	Passed	No Issue
30	rewardPerToken	external	Passed	No Issue
31	lockedBalances	external	Passed	No Issue
32	withdrawExpiredLocks	external	Critical operation lacks event log	Refer Audit Findings

CrescentDaoZapMMSwap.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	nonReentrant	modifier	Passed	No Issue
8	zap	external	Passed	No Issue
9	swap	internal	Passed	No Issue
10	doSwapETH	internal	Passed	No Issue
11	approveToken	internal	Passed	No Issue
12	calculateSwapInAmount	internal	Passed	No Issue
13	addZap	external	access only Owner	No Issue
14	removeZap	external	access only Owner	No Issue

Fund.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	initializer	modifier	Passed	No Issue
8	reinitializer	modifier	Passed	No Issue
9	onlyInitializing	modifier	Passed	No Issue
10	_disableInitializers	internal	Passed	No Issue

11	_setInitializedVersion	write	Passed	No Issue
12	initialize	external	Passed	No Issue
13	allocation	read	Passed	No Issue
14	vestingStart	read	Passed	No Issue
15	vestingDuration	read	Passed	No Issue
16	currentBalance	read	Passed	No Issue
17	vestedBalance	read	Passed	No Issue
18	claimable	read	Passed	No Issue
19	transfer	external	access only Owner	No Issue

CRSTDaoFund.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initialize	external	Passed	No Issue
3	allocation	read	Passed	No Issue
4	vestingStart	read	Passed	No Issue
5	vestingDuration	read	Passed	No Issue
6	currentBalance	read	Passed	No Issue
7	vestedBalance	read	Passed	No Issue
8	claimable	read	Passed	No Issue
9	transfer	external	access only Owner	No Issue
10	allocation	write	Passed	No Issue
11	vestingStart	write	Passed	No Issue
12	vestingDuration	write	Passed	No Issue

CRSTDevFund.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initialize	external	Passed	No Issue
3	allocation	read	Passed	No Issue
4	vestingStart	read	Passed	No Issue
5	vestingDuration	read	Passed	No Issue
6	currentBalance	read	Passed	No Issue
7	vestedBalance	read	Passed	No Issue
8	claimable	read	Passed	No Issue
9	transfer	external	access only Owner	No Issue
10	allocation	write	Passed	No Issue
11	vestingStart	write	Passed	No Issue
12	vestingDuration	write	Passed	No Issue

CRSTReserve.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initializer	modifier	Passed	No Issue
3	reinitializer	modifier	Passed	No Issue
4	onlyInitializing	modifier	Passed	No Issue
5	_disableInitializers	internal	Passed	No Issue
6	_setInitializedVersion	write	Passed	No Issue
7	initialize	external	Passed	No Issue
8	setRewarder	external	Passed	No Issue
9	setPool	external	Passed	No Issue
10	transfer	external	Passed	No Issue

CRSTTreasuryFund.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initialize	external	Passed	No Issue
3	allocation	read	Passed	No Issue
4	vestingStart	read	Passed	No Issue
5	vestingDuration	read	Passed	No Issue
6	currentBalance	read	Passed	No Issue
7	vestedBalance	read	Passed	No Issue
8	claimable	read	Passed	No Issue
9	transfer	external	access only Owner	No Issue
10	allocation	write	Passed	No Issue
11	vestingStart	write	Passed	No Issue
12	vestingDuration	write	Passed	No Issue

MasterOracle.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	getXTokenPrice	write	Passed	No Issue
8	getYTokenPrice	write	Passed	No Issue
9	getXTokenTWAP	write	Passed	No Issue

10	getYTokenTWAP	write	Passed	No Issue

UniswapPairOracle.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	setPeriod	external	access only Owner	No Issue
8	update	external	Passed	No Issue
9	twap	external	Passed	No Issue
10	spot	external	Passed	No Issue
11	currentBlockTimestamp	internal	Passed	No Issue
12	currentCumulativePrices	internal	Passed	No Issue

XToken.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	burn	write	Passed	No Issue
3	burnFrom	write	Passed	No Issue
4	onlyMinter	modifier	Passed	No Issue
5	setMinter	external	Passed	No Issue
6	mint	external	Unlimited Minting	Refer Audit Findings

YToken.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	burn	write	Passed	No Issue
3	burnFrom	write	Passed	No Issue

CRST.sol

Functions

Sl.	Functions	Type	Observation	Conclusion

1	constructor	write	Passed	No Issue
2	onlyMinter	modifier	Passed	No Issue
3	setMinter	external	Passed	No Issue
4	mint	external	access only Minter	No Issue
5	OpenTrade	external	Passed	No Issue
6	includeToWhitelist	write	Passed	No Issue
7	excludeFromWhitlist	write	Passed	No Issue
8	_transfer	internal	Passed	No Issue

GLMX.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	onlyMinter	modifier	Passed	No Issue
3	setMinter	external	Passed	No Issue
4	mint	external	access only Minter	No Issue
5	OpenTrade	external	Passed	No Issue
6	includeToWhitelist	write	Passed	No Issue
7	excludeFromWhitlist	write	Passed	No Issue
8	_transfer	internal	Passed	No Issue

CrescentDaoTreasury.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	balanceOf	read	Passed	No Issue
8	requestFund	external	Function input parameters lack of check	Refer Audit Findings
9	addStrategy	external	access only Owner	No Issue
10	removeStrategy	external	access only Owner	No Issue
11	allocateFee	external	Other Programming issue	Refer Audit Findings

StratRecollateralize.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	recollateralize	external	Other Programming issue	Refer Audit Findings
3	owner	read	Passed	No Issue
4	onlyOwner	modifier	Passed	No Issue
5	renounceOwnership	write	access only Owner	No Issue
6	transferOwnership	write	access only Owner	No Issue
7	_transferOwnership	internal	Passed	No Issue

StratReduceReserveLP.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	renounceOwnership	write	access only Owner	No Issue
5	transferOwnership	write	access only Owner	No Issue
6	_transferOwnership	internal	Passed	No Issue
7	reduceReserve	external	access only Owner	No Issue
8	swap	internal	Other Programming issue	Refer Audit Findings

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial
Medium	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens lose
Low	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

Email: audit@EtherAuthority.io

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No Medium severity vulnerabilities were found.

Low

(1) Critical operation lacks event log:**- CrescentDaoStaking.sol**

Missing event log for: emergencyWithdraw, withdrawExpiredLocks.

Resolution: Write an event log for listed events.

(2) Function input parameters lack of check:

Variable validation is not performed in below functions:

CrescentDaoStaking.sol

- addReward =_rewardsToken
- approveRewardDistributor = _rewardsToken ,_distributor
- mint = user
- notifyRewardAmount = _rewardsToken

CrescentDaoTreasury.sol

- requestFund = _token

Resolution: We advise to put validation like integer type variables should be greater than 0 and address type variables should not be address(0).

Very Low / Informational / Best practices:

(1) Unlimited Minting: **- XToken.sol**

Minter can mint unlimited tokens.

Resolution: We suggest putting a minting limit.

(2) Division before multiplication: **CrescentDaoStaking.sol**

```
// Mint new tokens
// Minted tokens receive rewards normally but incur a 50% penalty when
// withdrawn before lockDuration has passed.
function mint(address user, uint256 amount) external updateReward(user) {
    require(minters[msg.sender], "MultiFeeDistribution::mint: Only minters allowed");
    totalSupply = totalSupply.add(amount);
    Balances storage bal = balances[user];
    bal.total = bal.total.add(amount);
    bal.earned = bal.earned.add(amount);
    uint256 unlockTime = block.timestamp.div(rewardsDuration).mul(rewardsDuration).add(lockDuration);
    LockedBalance[] storage earnings = userEarnings[user];
    uint256 idx = earnings.length;

    if (idx == 0 || earnings[idx - 1].unlockTime < unlockTime) {
        earnings.push(LockedBalance({amount: amount, unlockTime: unlockTime}));
    } else {
        earnings[idx - 1].amount = earnings[idx - 1].amount.add(amount);
    }
    stakingTokenReserve.transfer(address(this), amount);
    emit Staked(user, amount);
}
```

Solidity being resource constrained language, dividing any amount and then multiplying will cause discrepancies in the outcome. Therefore, always multiply the amount first and then divide it.

Resolution: Consider ordering multiplication before division.

(3) Ambiguous Error Message: **- Pool.sol**

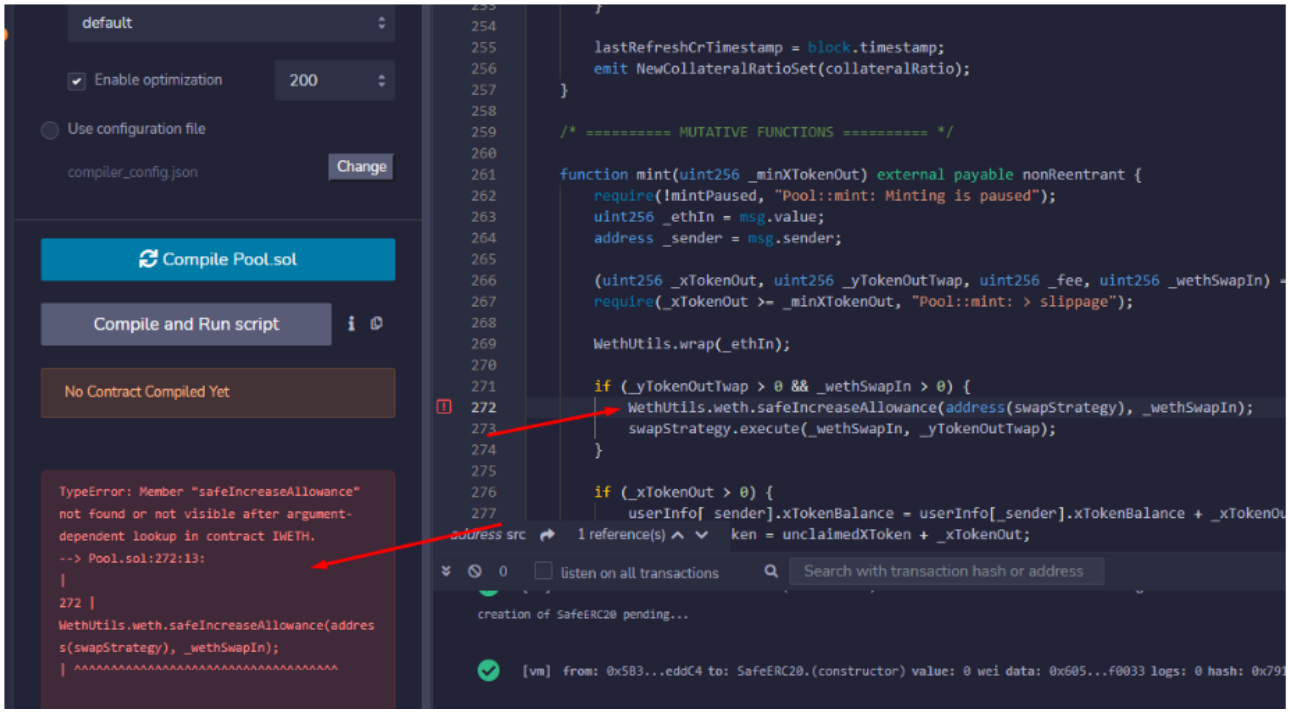
```
    /// @notice Set the address of Treasury
    /// @param _treasury address of Treasury contract
    function setTreasury(address _treasury) external {
        require(treasury == address(0), "Pool::setTreasury: not allowed");
        treasury = _treasury;
        emit TreasurySet(_treasury);
    }
```

The mentioned error message does not explain exactly the error of the operation.

Resolution: As error messages are intended to notify users about failing conditions, they should provide enough information so that appropriate corrections can be made to interact with the system.

(4) Other Programming issue:

Pool.sol



A "safeIncreaseAllowance" not found or not visible after argument-dependent lookup in contract IWETH.

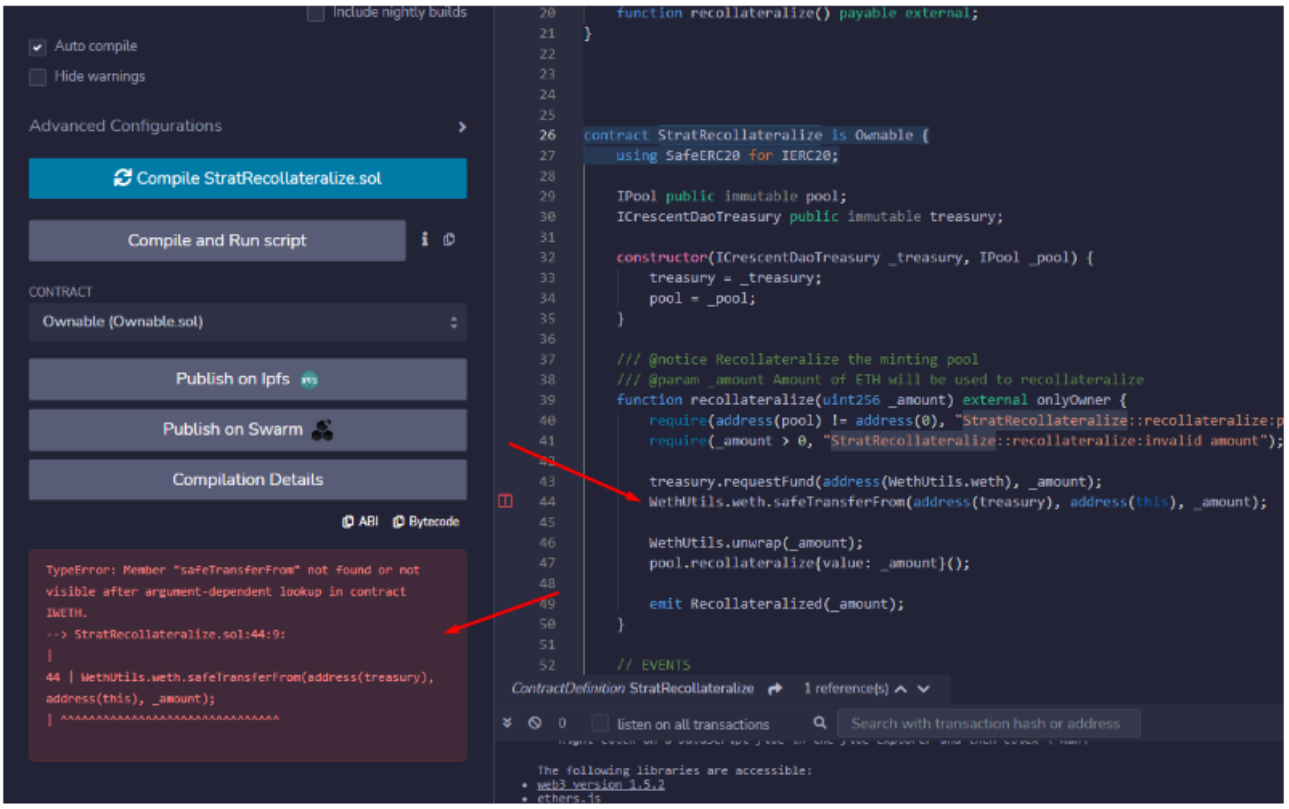
Resolution: We suggest, In pool contract use add this line "using SafeERC20 for IWETH;

CrescentDaoTreasury.sol

The “allocateFee” function is accessible to onlyOwner ,It uses notifyRewardAmount from staking contract which is accessible to only distributors. In this case if daotreasury owner & staking distributor are not identical then this function will not execute.

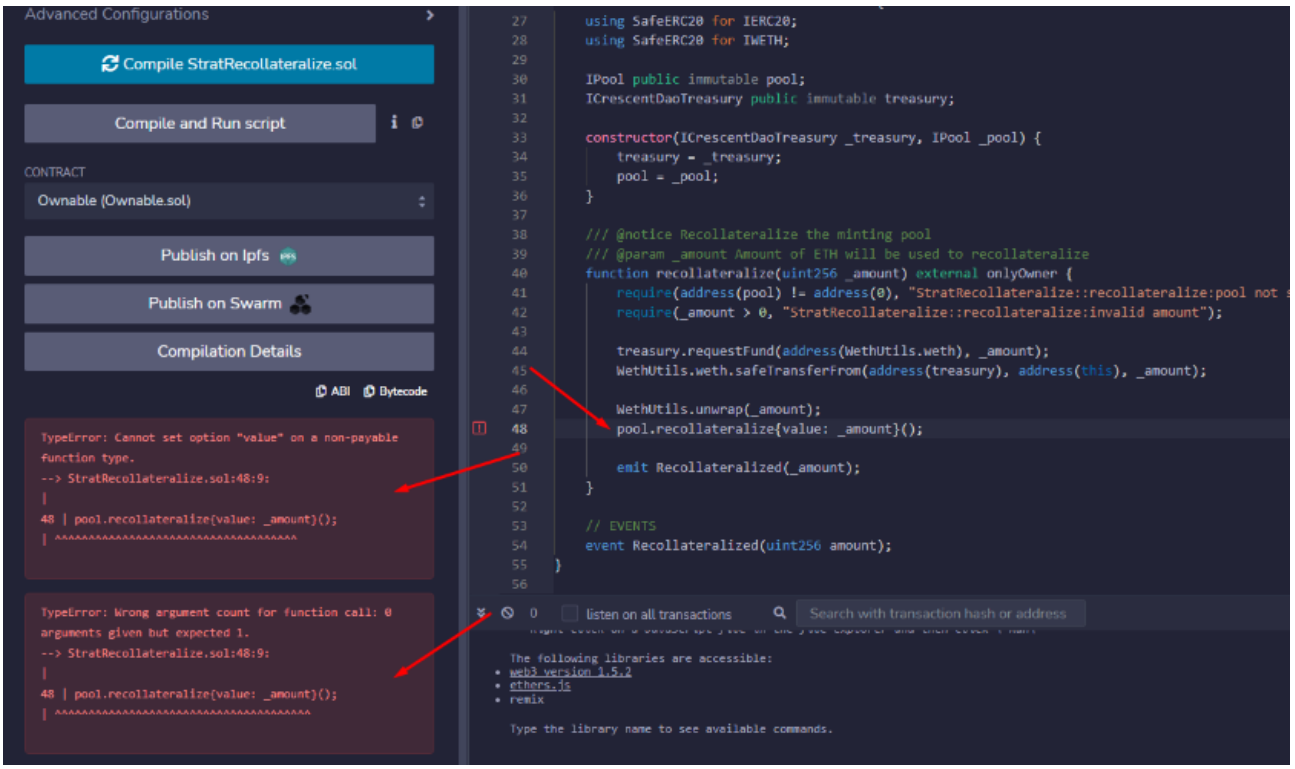
Resolution: We suggest making sure you have identical addresses for both the listed contract functions.

StratRecollateralize.sol



Member "safeTransferFrom" not found or not visible after argument-dependent lookup in contract IWETH.

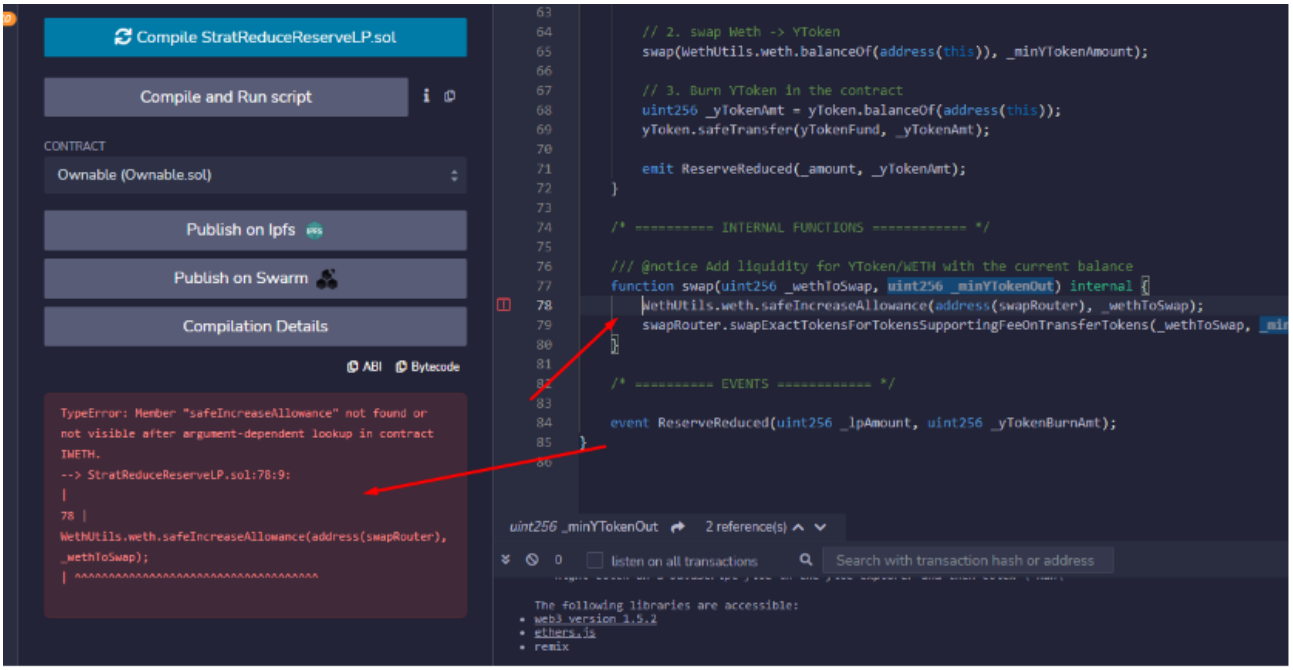
Resolution: We suggest adding this line "using SafeERC20 for IWETH; " in contract.



Cannot set option "value" on a non-payable function type. Wrong argument count for function call: 0 arguments given but expected 1.

Resolution: We suggest making changes in the Ipool interface , removing the amount parameter and making the recollateralize function payable.

StratReduceReserveLP.sol



Member "safeIncreaseAllowance" not found or not visible after argument-dependent lookup in contract IWETH.

Resolution: We suggest to add this line "using SafeERC20 for IWETH; " in contract.

(5) Owner can drain all ERC20 tokens: **- CrescentDaoStaking.sol.sol**

The function recoverERC20() will allow the owner to withdraw all the ERC20 tokens. This would create trust issues in the users.

Resolution: If these are desired features, then please ignore this point.

(6) Infinite loop: **- CrescentDaoChef.sol**

In below functions ,for loops do not have upper length limit , which costs more gas : checkPoolDuplicate , harvestAllRewards , massUpdatePools.

Resolution: Upper bound poolInfo.length should have a certain limit in for loops.

Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble. Following are Admin functions:

- toggle: Pool owner can Turn on / off minting and redemption.
- setCollateralRatioOptions: Pool owner can configure variables related to Collateral Ratio.
- toggleCollateralRatio: Pool Owner can pause or unpause collateral ratio updates.
- setFees: Pool owners can set the protocol fees.
- setMinCollateralRatio: Pool owner can set the minimum Collateral Ratio.
- reduceExcessCollateral: Pool owner can transfer the excess balance of WETH to FeeReserve.
- setSwapStrategy: Pool owner can set the address of Swapper utils.
- setOracle: Pool owner can set new oracle address.
- setYTokenSlippage: Pool owner can set yTokenSlipage.
- setTreasury: Pool owner can set the address of the Treasury.
- cleanDust: SwapStrategyPOL owner can clean dust.
- changeSlippage: SwapStrategyPOL owner can change slippage value.
- add: CrescentDaoChef owner can add a new LP to the pool.
- set: CrescentDaoChef owner can update the given pool's reward allocation point and `IRewarder` contract.
- setRewardPerSecond: CrescentDaoChef owner can set the reward per second to be distributed.
- setRewardMinter: CrescentDaoChef owner can set the address of rewardMinter.
- setNftController: CrescentDaoChef owner can set NFT controller address.
- setNftBoostRate: CrescentDaoChef owner can set NFT Boost Rate value.
- addReward: CrescentDaoStaking owner can add a new reward token to be distributed to stakers.
- approveRewardDistributor: CrescentDaoStaking owner can modify approval for an address to call notifyRewardAmount.
- recoverERC20:CrescentDaoStaking owner can be added to support recovering LP Rewards from other systems such as BAL to be distributed to holders.

- setTeamWalletAddress:CrescentDaoStaking owner can set the address of the team wallet.
- setTeamRewardPercent:CrescentDaoStaking owner can set percent of team reward.
- addZap: CrescentDaoZapMMSwap owner can add new zap configuration.
- removeZap: CrescentDaoZapMMSwap owner can deactivate a Zap configuration.
- transfer: Fund owners can transfer tokens.
- transfer: CRSTReserve::transfer owner can only allow funds to withdraw.
- setPeriod: UniswapPairOracle owner can set maximum and minimum period.
- setMinter: XToken minter can set minter for XToken.
- mint: XToken minter can mint new XToken.
- OpenTrade: GLMX owners can trade openly.
- includeToWhitelist: GLMX owner can include address to whitelist.
- excludeFromWhitlist: GLMX owner can exclude address to whitelist.
- OpenTrade: CRST owners can trade openly.
- includeToWhitelist: CRST owner can include address to whitelist.
- excludeFromWhitlist: CRST owner can exclude address to whitelist.
- addStrategy: CrescentDaoTreasury owner can add new strategy.
- removeStrategy: CrescentDaoTreasury owner can remove current strategy.
- allocateFee:CrescentDaoTreasury owner can allocate protocol's fee to stakers.
- recollateralize: StratRecollateralize owner can recollateralize the minting pool.
- reduceReserve: StratReduceReserveLP owner can remove liquidity, buy back YToken and burn.

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

Conclusion

We were given a contract code in the form of files. And we have used all possible tests based on given objects as files. We have not observed any major issues in the smart contracts. **So, the smart contracts are ready for the mainnet deployment**.

Since possible test cases can be unlimited for such smart contracts protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high-level description of functionality was presented in the As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract, based on standard audit procedure scope, is **"Secured"**.

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

Manual Code Review:

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

Vulnerability Analysis:

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

Suggested Solutions:

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

Disclaimers

EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

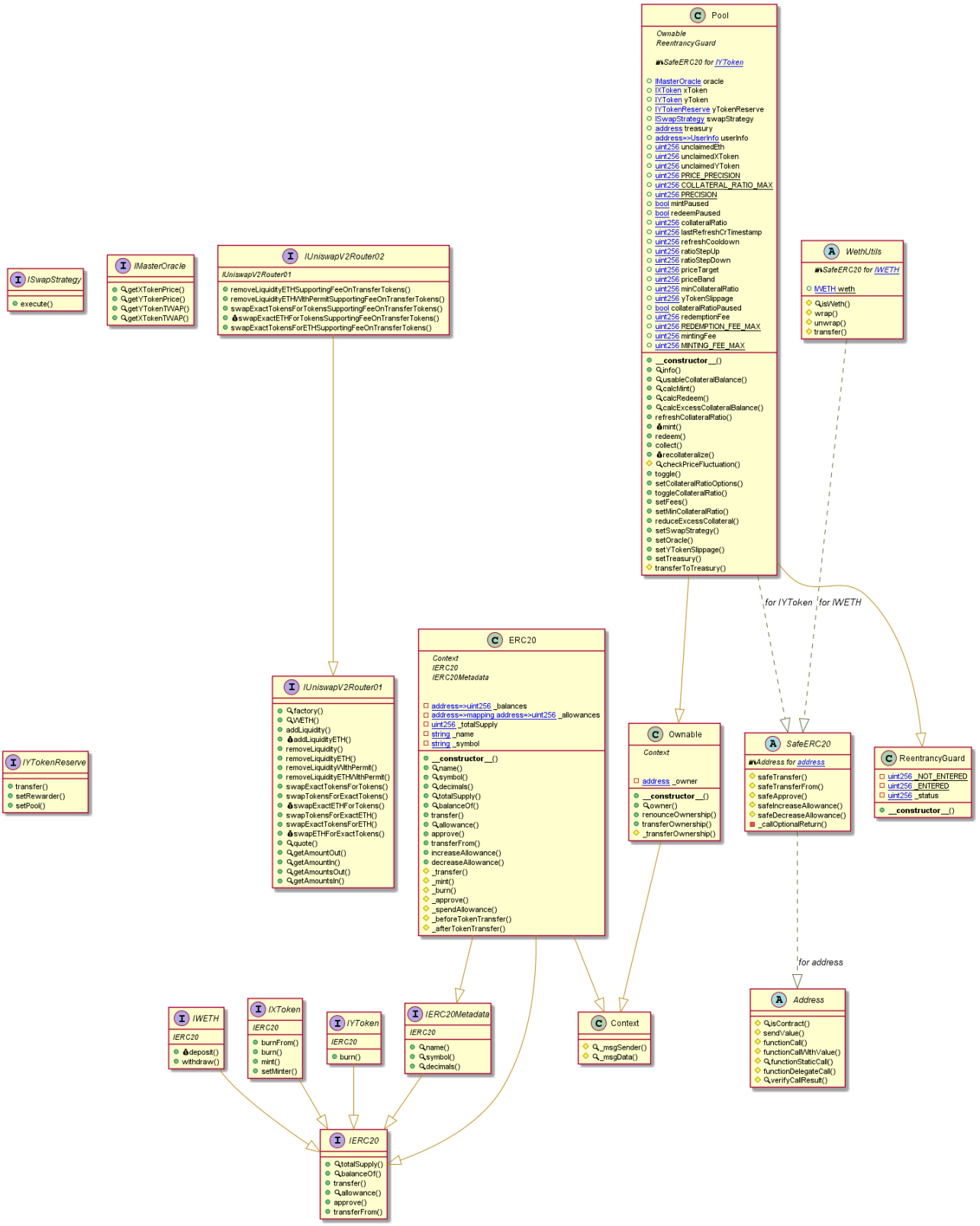
Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can’t guarantee explicit security of the audited smart contracts.

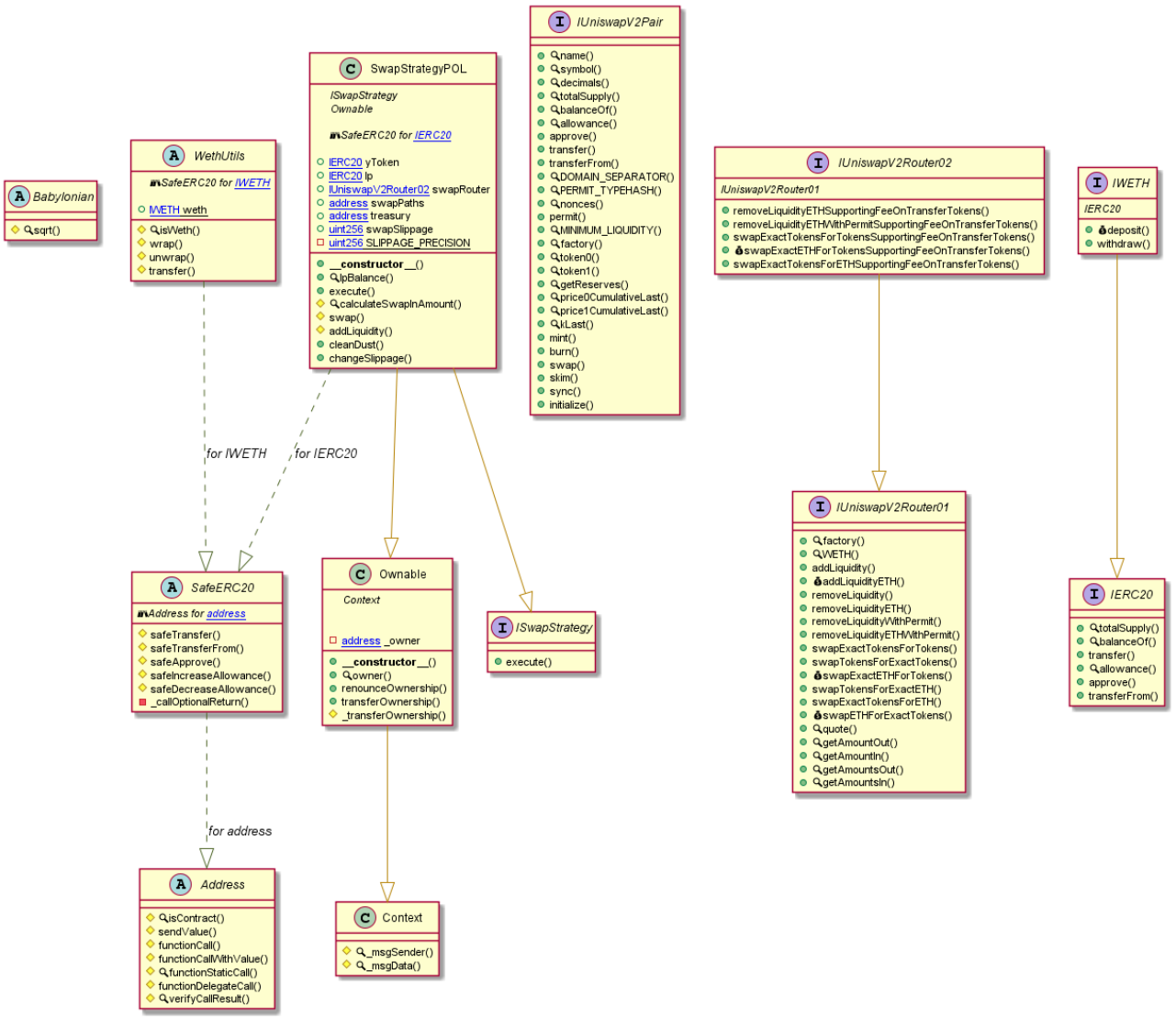
Appendix

Code Flow Diagram - Crescent DAO Protocol

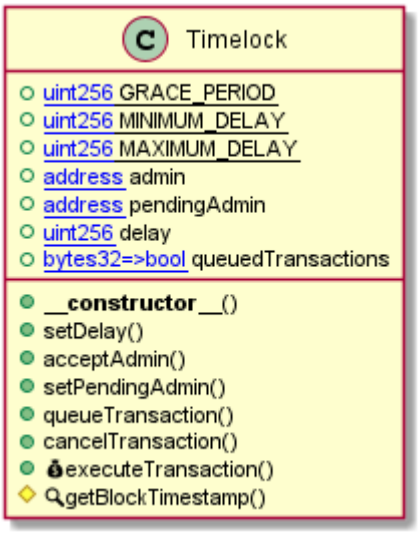
Pool Diagram



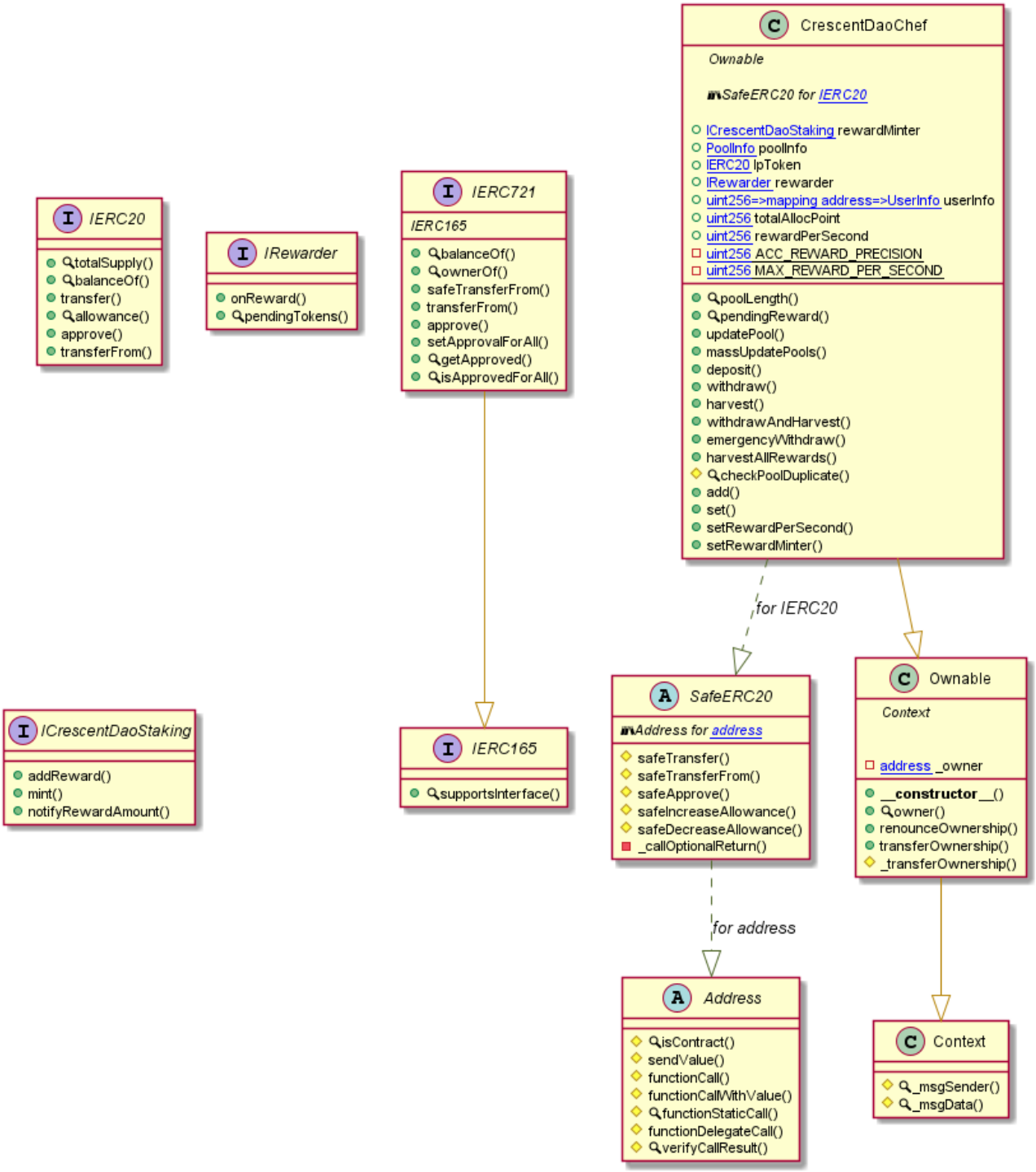
SwapStrategyPOL Diagram



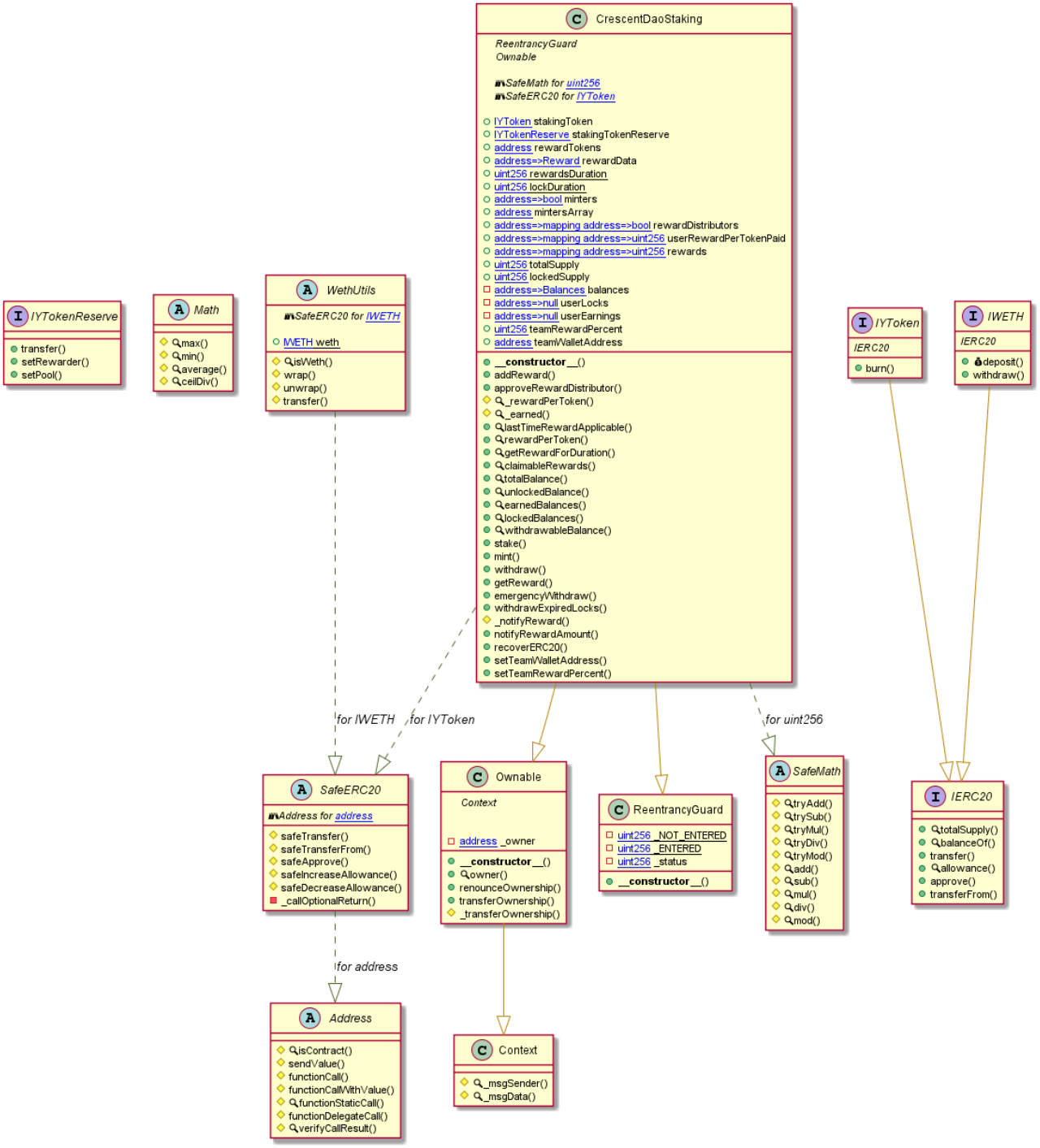
Timelock Diagram



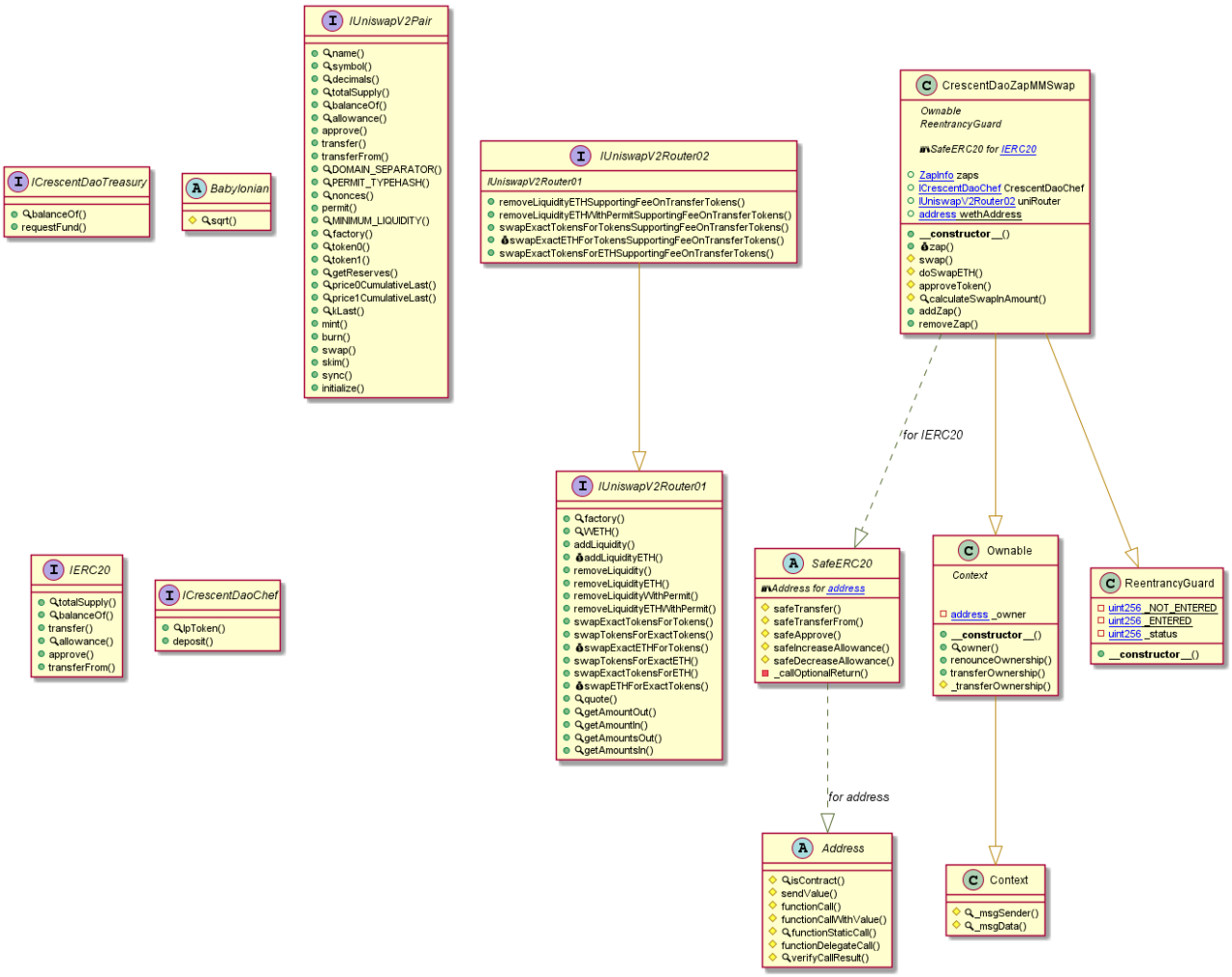
CrescentDaoChef Diagram



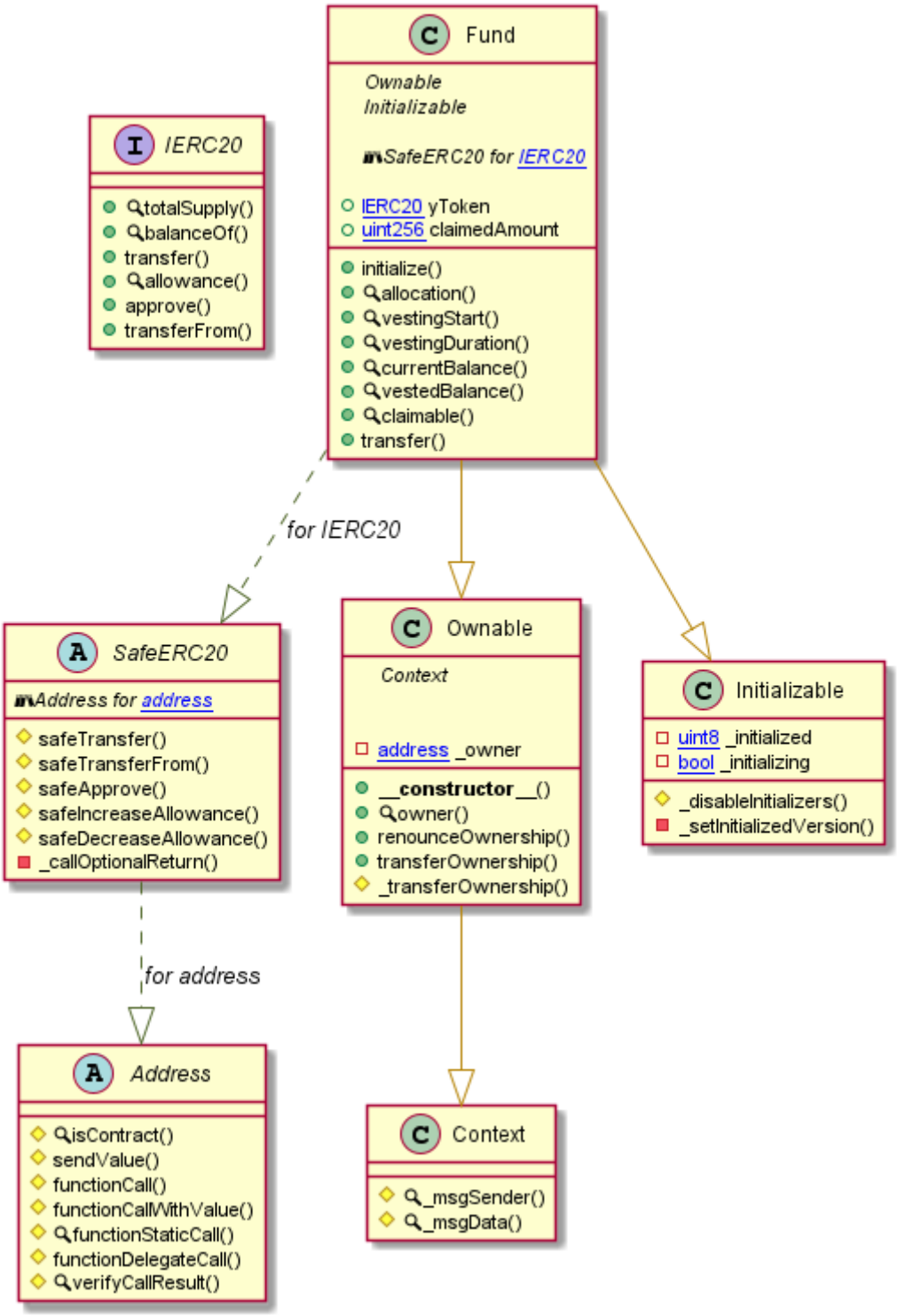
CrescentDaoStaking Diagram



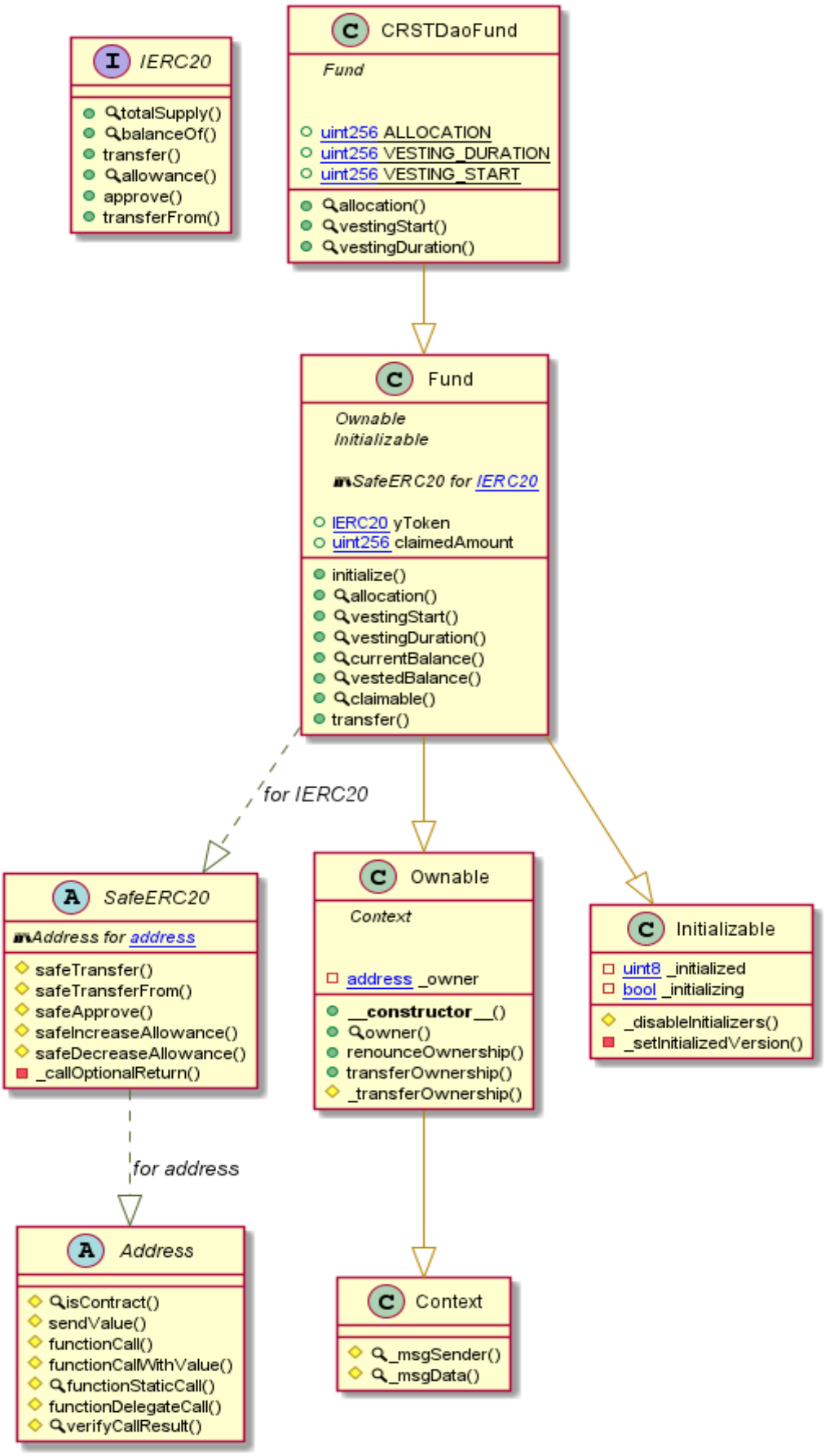
CrescentDaoZapMMSwap Diagram



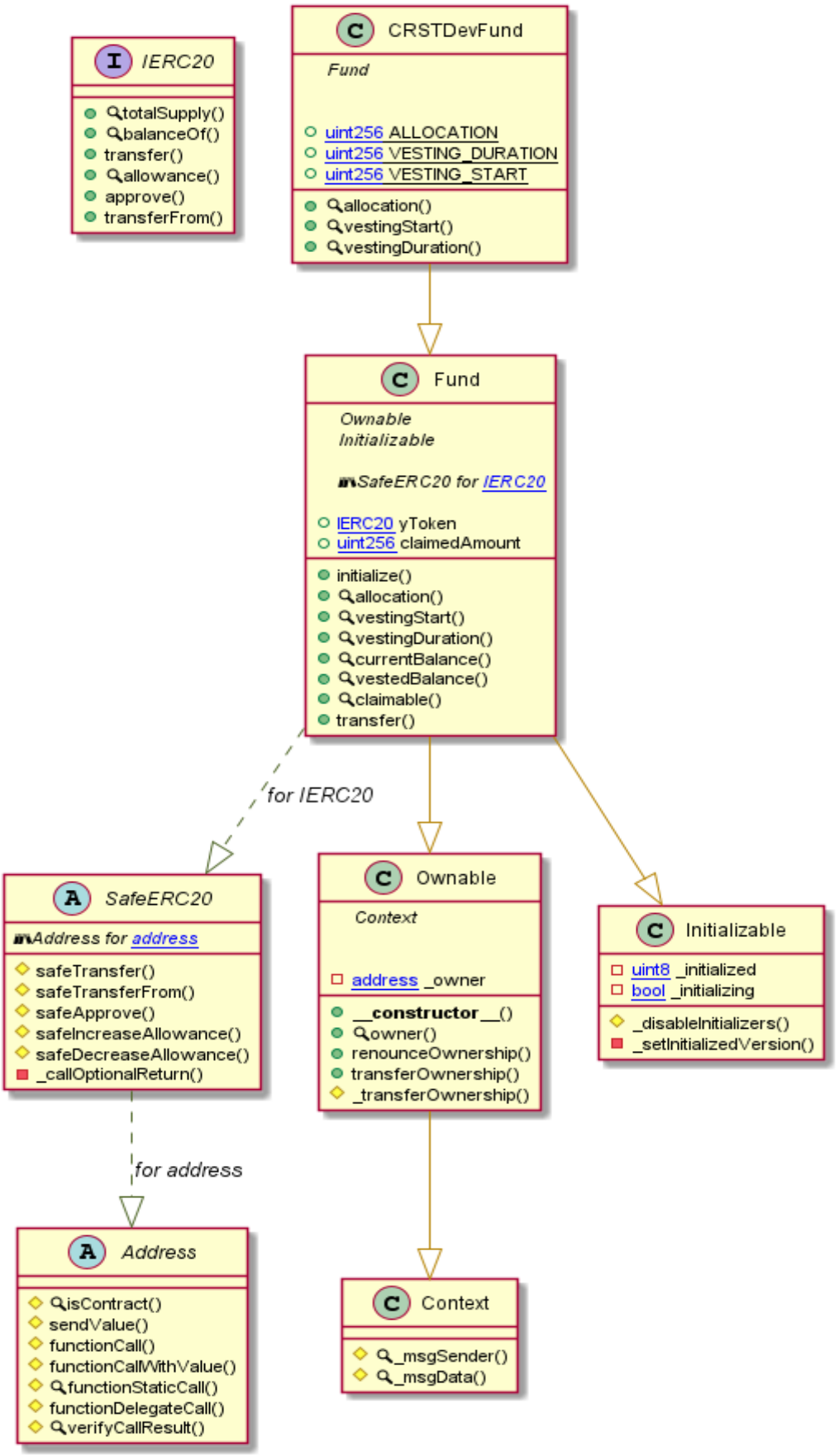
Fund Diagram



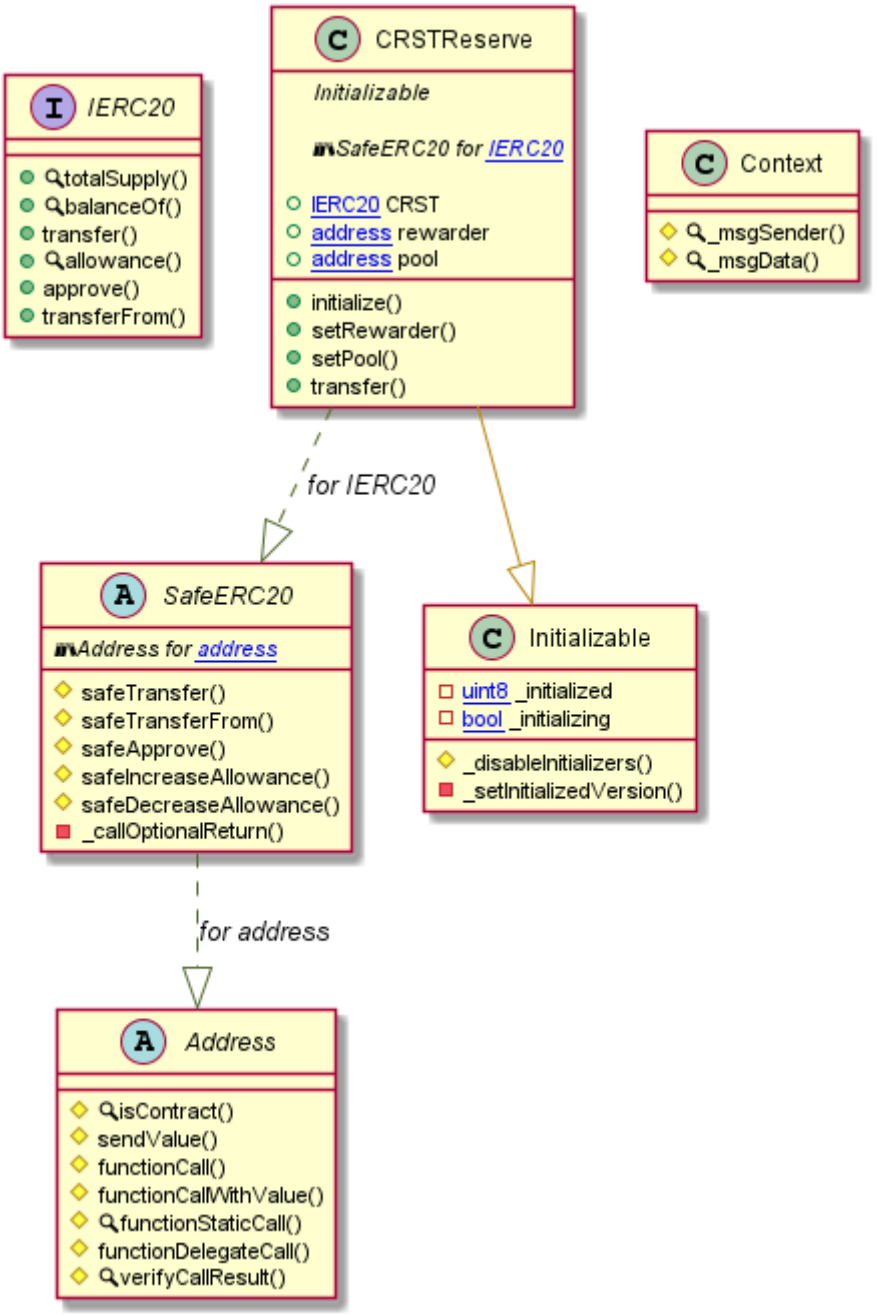
CRSTDaoFund Diagram



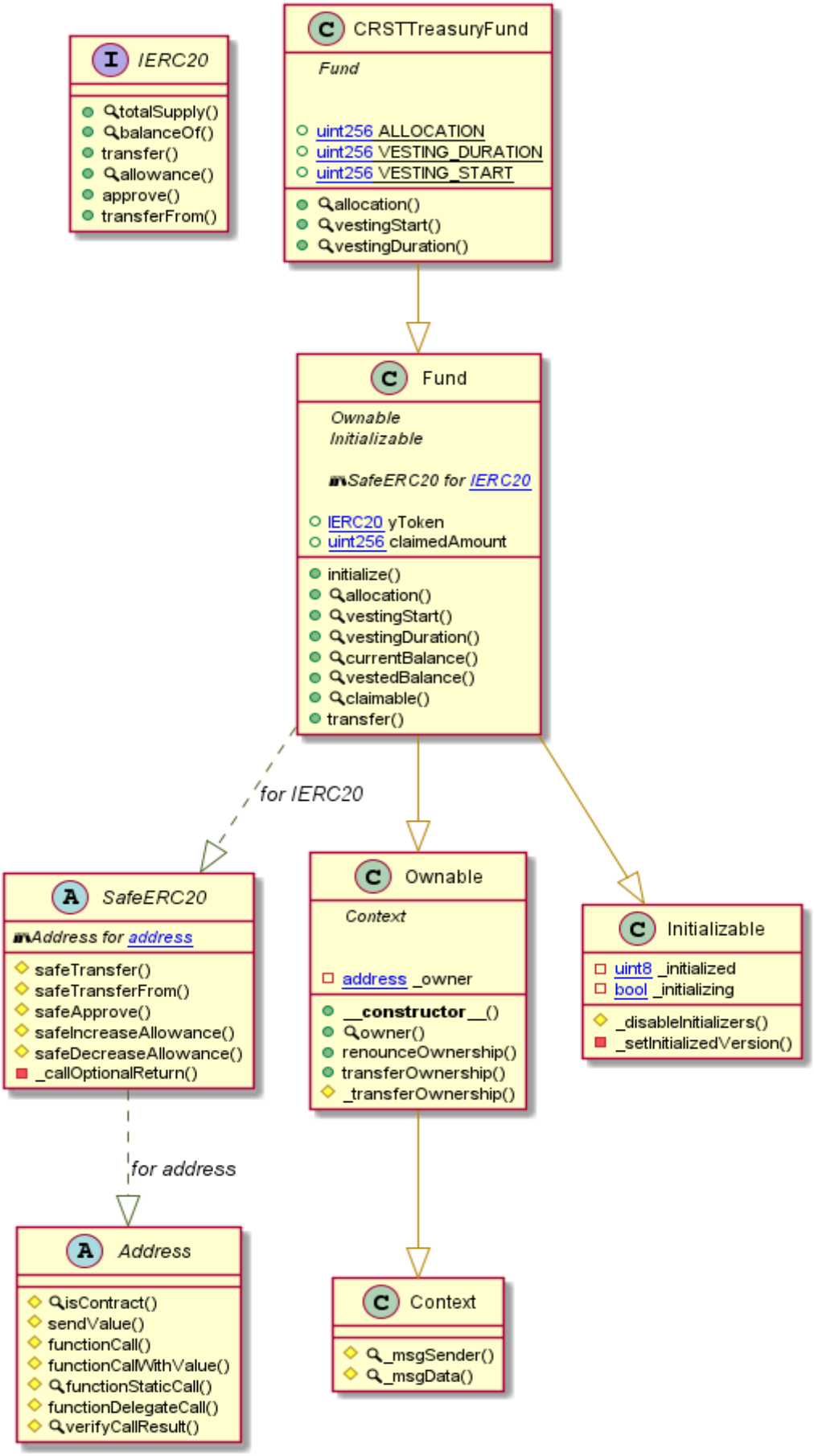
CRSTDevFund Diagram



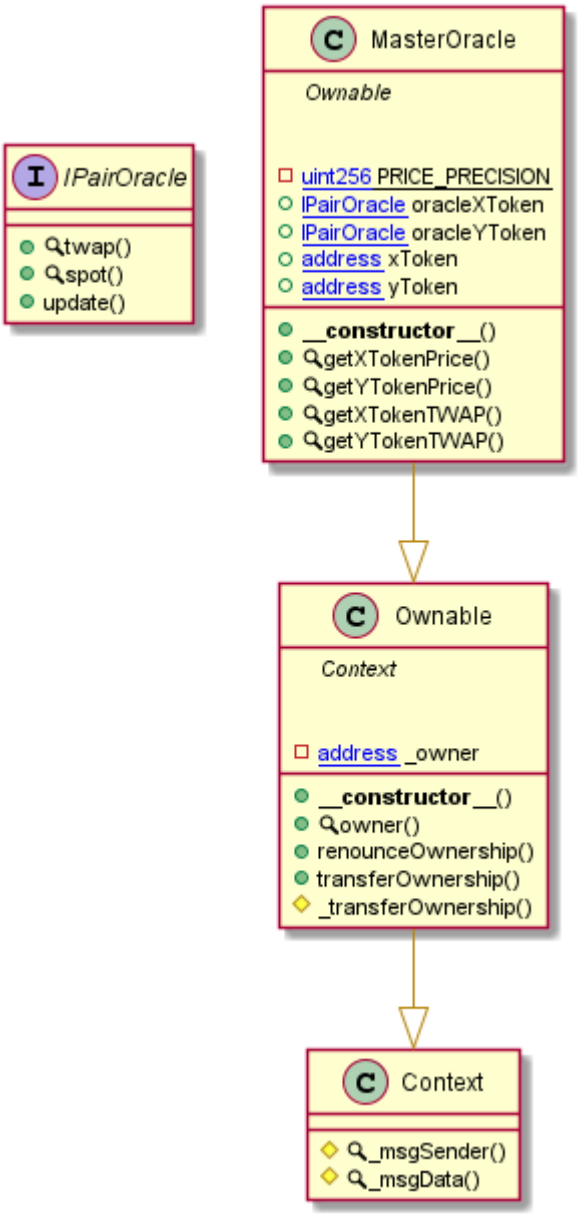
CRSTReserve Diagram



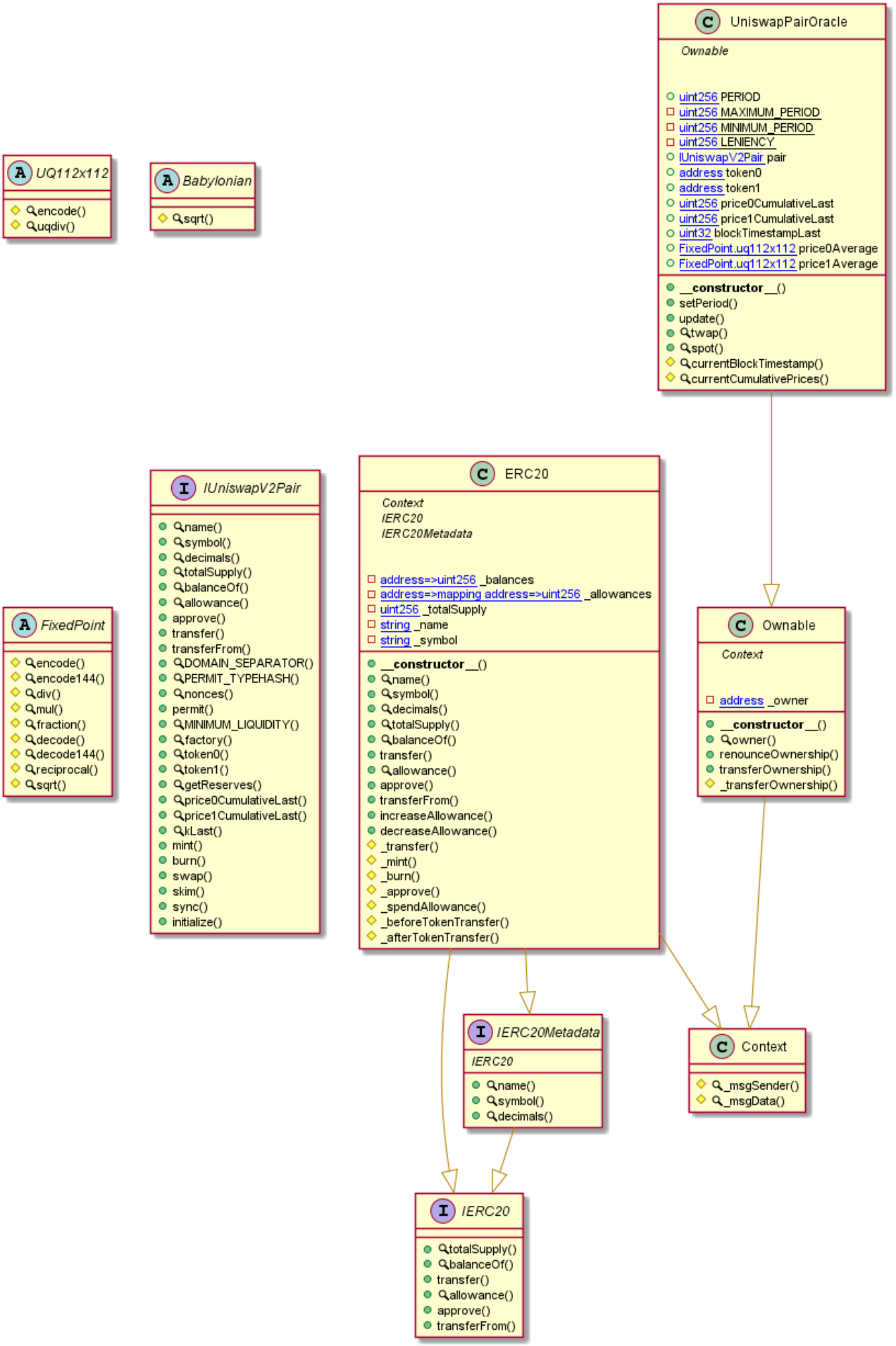
CRSTTreasuryFund Diagram



masterOracle Diagram



UniswapPairOracle Diagram



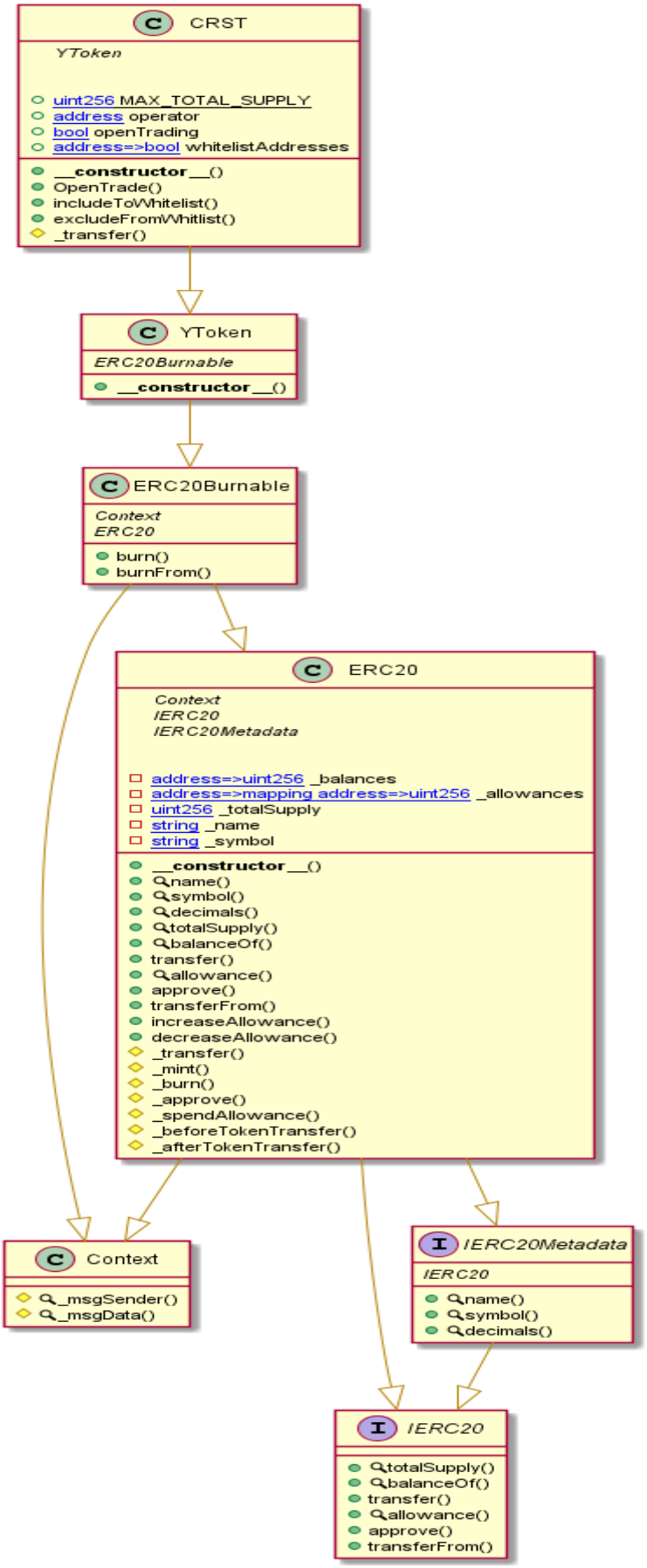
XToken Diagram

Email: audit@EtherAuthority.io

YToken Diagram

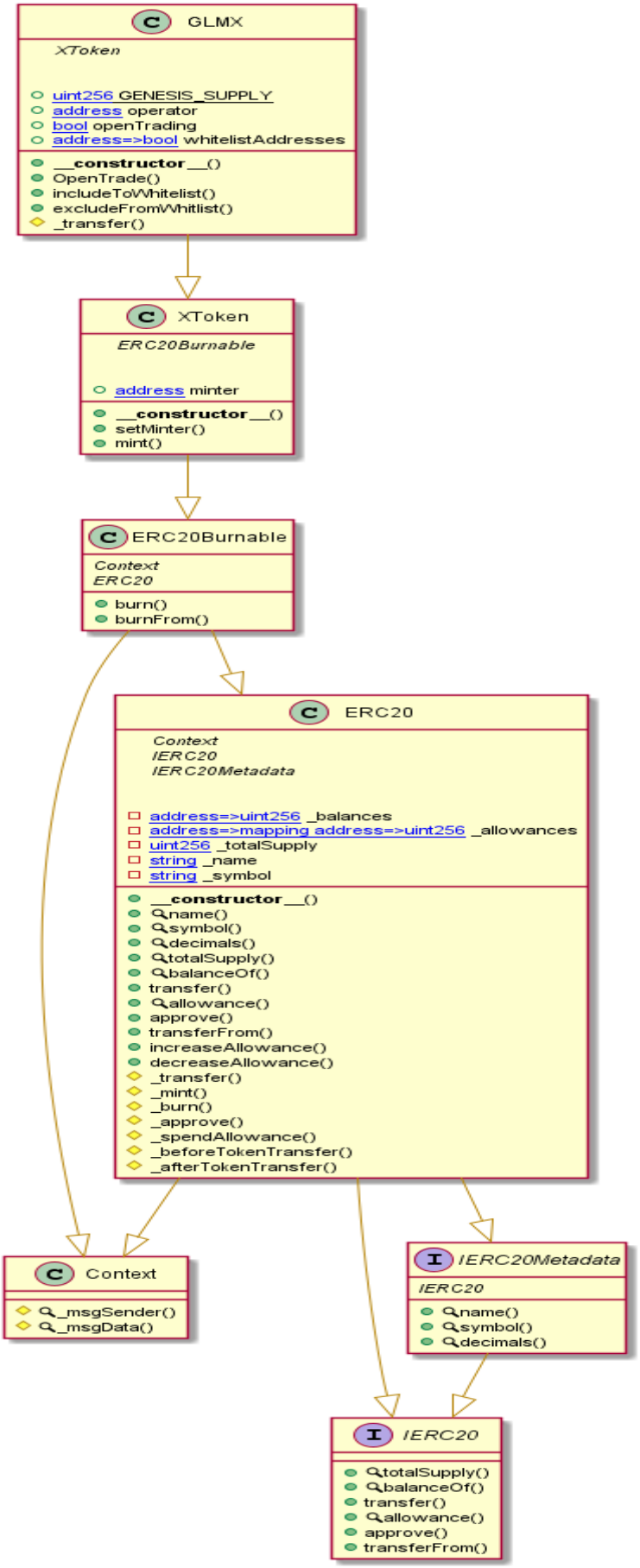
Email: audit@EtherAuthority.io

CRST Diagram



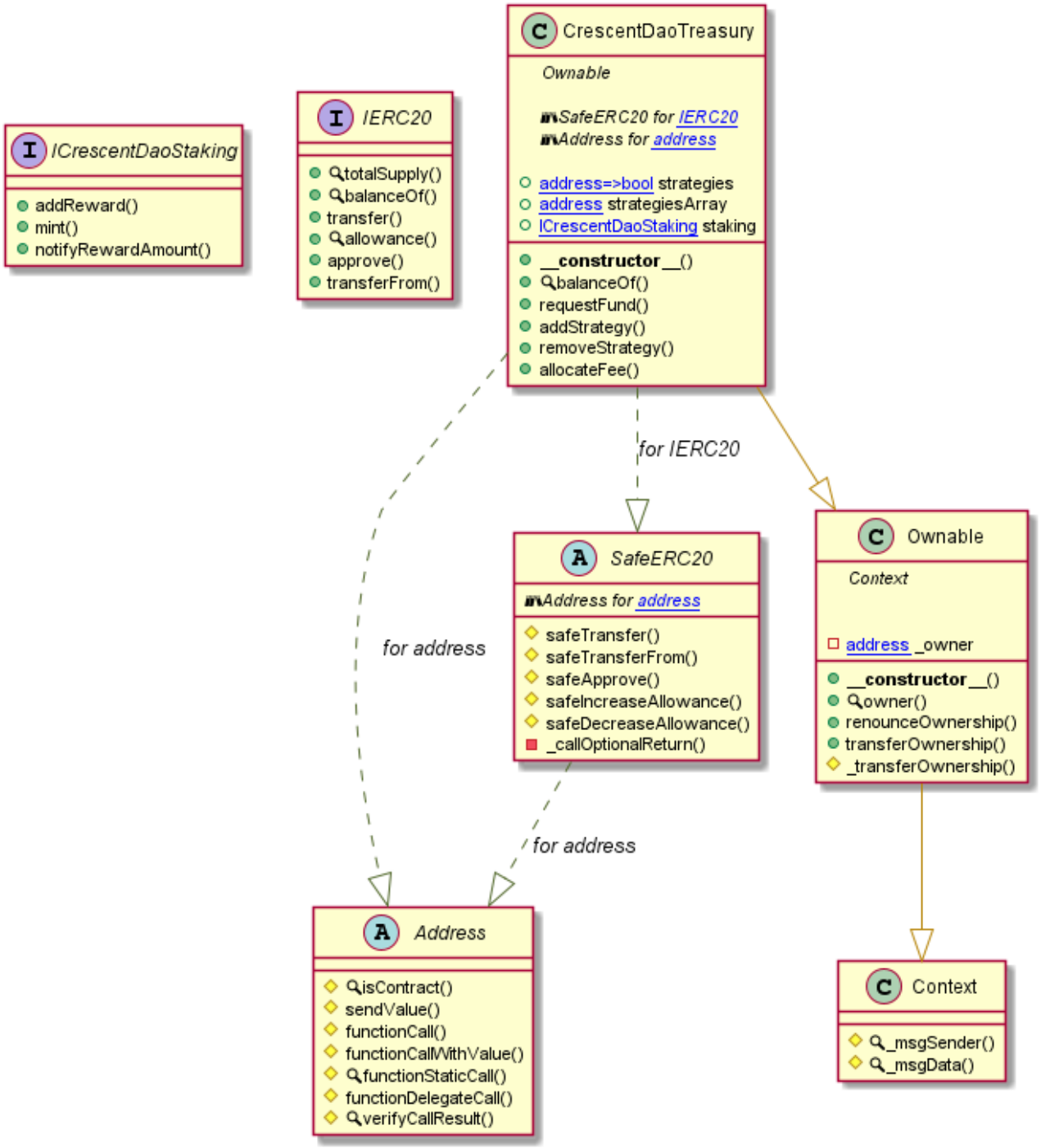
Email: audit@EtherAuthority.io

GLMX Diagram

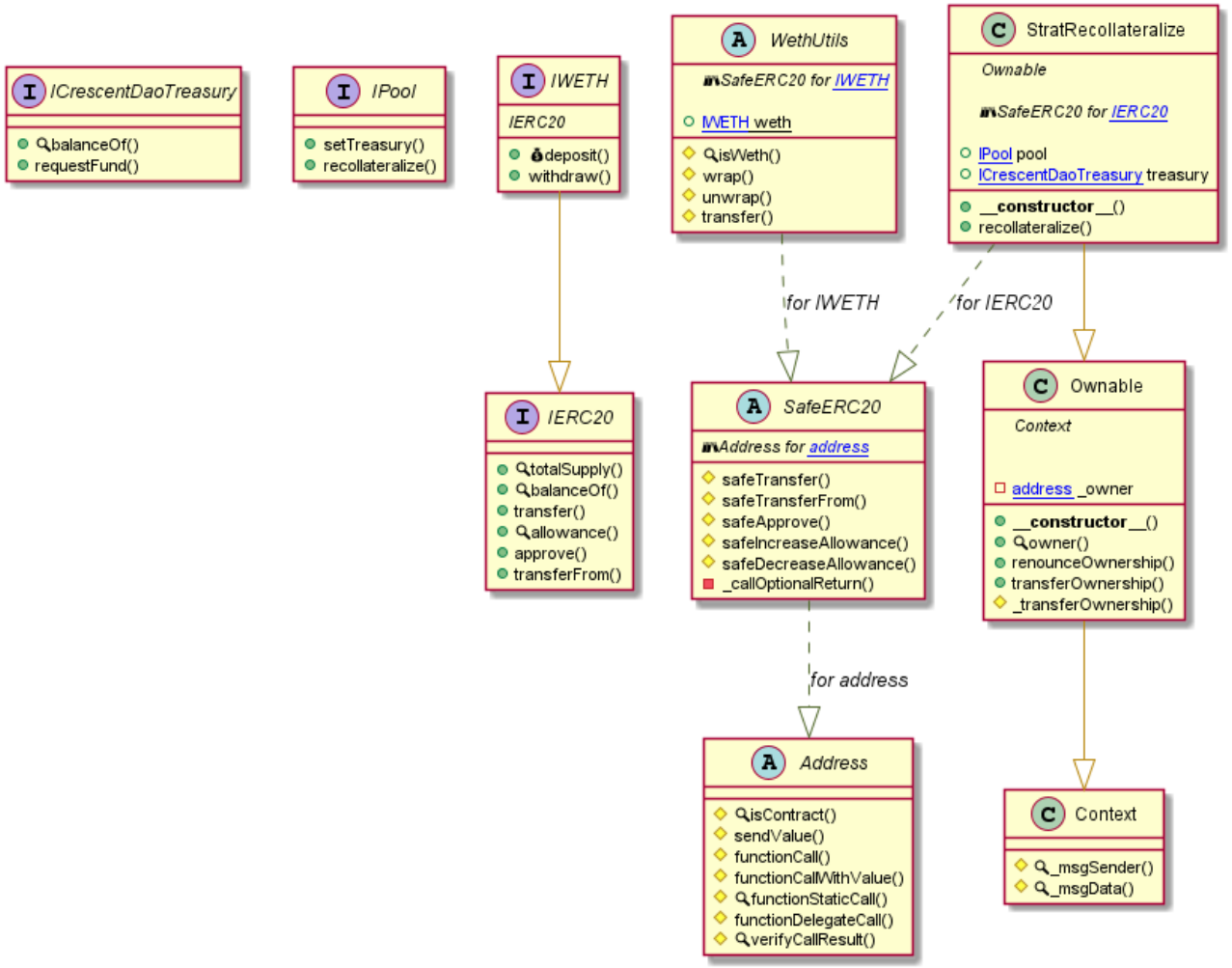


Email: audit@EtherAuthority.io

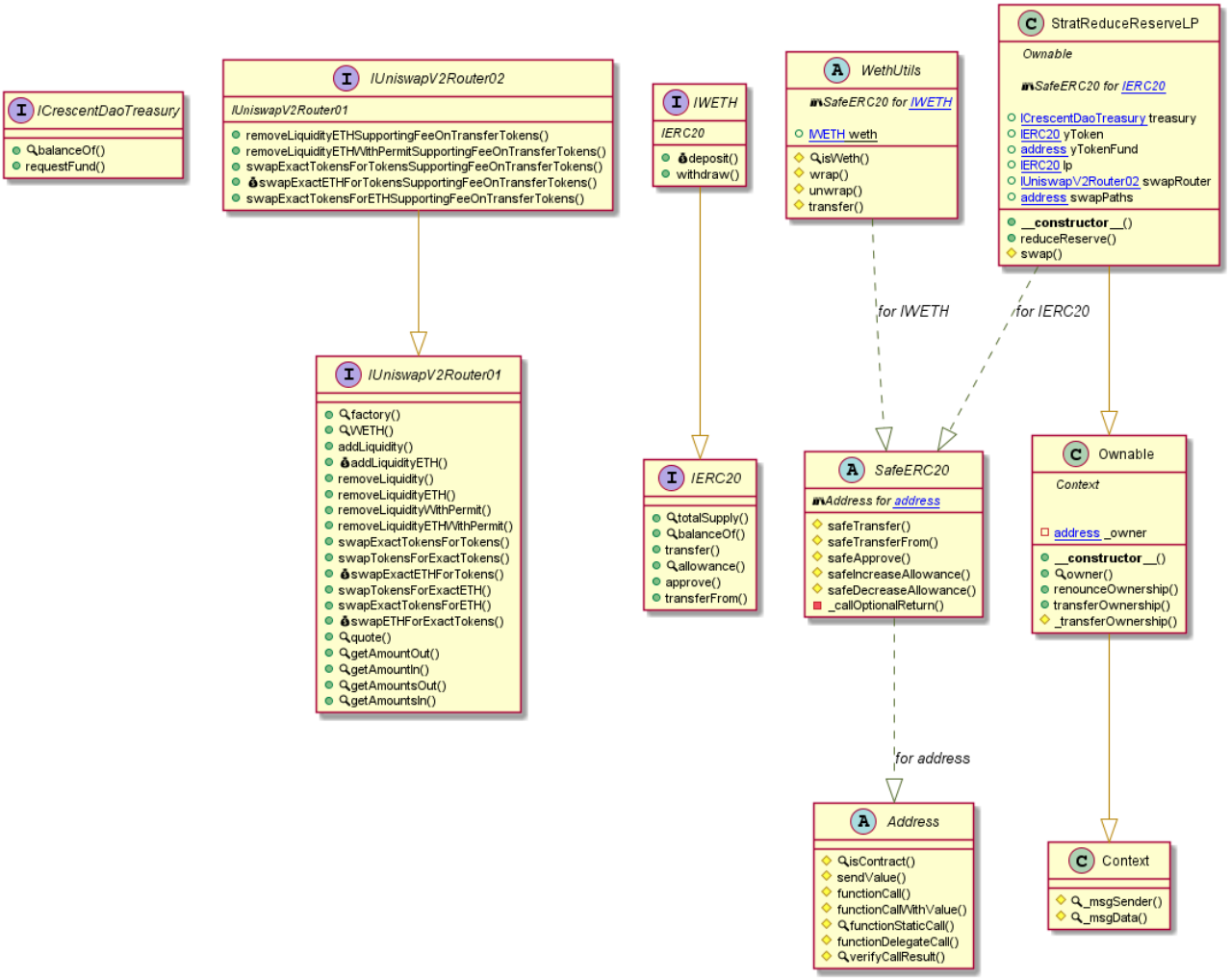
CrescentDaoTreasury Diagram



StratRecollateralize Diagram



StratReduceReserveLP Diagram



Slither Results Log

Slither log >> Pool.sol

```
INFO:Detectors:
Pool.setTreasury(address)._treasury (Pool.sol#1488) lacks a zero-check on :
                - treasury = _treasury (Pool.sol#1490)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Reentrancy in Pool.constructor(address,address,address) (Pool.sol#1111-1124):
        External calls:
        - xToken.setMinter(address(this)) (Pool.sol#1120)
        State variables written after the call(s):
        - yToken = IYToken(_yToken) (Pool.sol#1121)
        - yTokenReserve = IYTokenReserve(_yTokenReserve) (Pool.sol#1122)
Reentrancy in Pool.mint(uint256) (Pool.sol#1260-1284):
        External calls:
        - WethUtils.wrap(_ethIn) (Pool.sol#1268)
        - swapStrategy.execute(_wethSwapIn,_yTokenOutTwap) (Pool.sol#1272)
        State variables written after the call(s):
        - unclaimedXToken = unclaimedXToken + _xTokenOut (Pool.sol#1277)
        - userInfo[_sender].xTokenBalance = userInfo[_sender].xTokenBalance + _xTokenOut (Pool.sol#1276)
        - userInfo[_sender].lastAction = block.number (Pool.sol#1280)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2
```

```
INFO:Detectors:
Pool.priceTarget (Pool.sol#1097) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (Pool.sol#632-634)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (Pool.sol#640-643)
name() should be declared external:
        - ERC20.name() (Pool.sol#683-685)
symbol() should be declared external:
        - ERC20.symbol() (Pool.sol#691-693)
decimals() should be declared external:
        - ERC20.decimals() (Pool.sol#708-710)
totalSupply() should be declared external:
        - ERC20.totalSupply() (Pool.sol#715-717)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (Pool.sol#722-724)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (Pool.sol#734-738)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (Pool.sol#757-761)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (Pool.sol#779-788)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (Pool.sol#802-806)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (Pool.sol#822-831)
refreshCollateralRatio() should be declared external:
        - Pool.refreshCollateralRatio() (Pool.sol#1230-1256)
toggle(bool,bool) should be declared external:
        - Pool.toggle(bool,bool) (Pool.sol#1401-1405)
setCollateralRatioOptions(uint256,uint256,uint256,uint256) should be declared external:
        - Pool.setCollateralRatioOptions(uint256,uint256,uint256,uint256) (Pool.sol#1412-1423)
```

```
setCollateralRatioOptions(uint256,uint256,uint256,uint256) should be declared external:
        - Pool.setCollateralRatioOptions(uint256,uint256,uint256,uint256) (Pool.sol#1412-1423)
toggleCollateralRatio(bool) should be declared external:
        - Pool.toggleCollateralRatio(bool) (Pool.sol#1427-1432)
setFees(uint256,uint256) should be declared external:
        - Pool.setFees(uint256,uint256) (Pool.sol#1437-1443)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:Pool.sol analyzed (18 contracts with 75 detectors), 95 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> SwapStrategyPOL.sol

```
INFO:Detectors:
SwapStrategyPOL.addLiquidity(uint256,uint256,uint256) (SwapStrategyPOL.sol#763-786) uses timestamp for comparisons
        Dangerous comparisons:
        - yTokenAmt > 0 && wethAmt > 0 (SwapStrategyPOL.sol#769)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (SwapStrategyPOL.sol#489-509) uses assembly
        - INLINE ASM (SwapStrategyPOL.sol#501-504)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (Swap
StrategyPOL.sol#89) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,
uint256).amountBDesired (SwapStrategyPOL.sol#90)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar
INFO:Detectors:
SwapStrategyPOL.slitherConstructorVariables() (SwapStrategyPOL.sol#685-803) uses literals with too many digits:
        - swapSlippage = 200000 (SwapStrategyPOL.sol#693)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (SwapStrategyPOL.sol#660-662)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (SwapStrategyPOL.sol#668-671)
lpBalance() should be declared external:
        - SwapStrategyPOL.lpBalance() (SwapStrategyPOL.sol#712-714)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:SwapStrategyPOL.sol analyzed (13 contracts with 75 detectors), 43 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> Timelock.sol

```
INFO:Detectors:
Pragma version0.8.4 (Timelock.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Timelock.executeTransaction(address,uint256,string,bytes,uint256) (Timelock.sol#86-117):
        - (success,returnData) = target.call{value: value}(callData) (Timelock.sol#111)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
setDelay(uint256) should be declared external:
        - Timelock.setDelay(uint256) (Timelock.sol#31-38)
acceptAdmin() should be declared external:
        - Timelock.acceptAdmin() (Timelock.sol#40-45)
setPendingAdmin(address) should be declared external:
        - Timelock.setPendingAdmin(address) (Timelock.sol#47-52)
queueTransaction(address,uint256,string,bytes,uint256) should be declared external:
        - Timelock.queueTransaction(address,uint256,string,bytes,uint256) (Timelock.sol#54-69)
cancelTransaction(address,uint256,string,bytes,uint256) should be declared external:
        - Timelock.cancelTransaction(address,uint256,string,bytes,uint256) (Timelock.sol#71-84)
executeTransaction(address,uint256,string,bytes,uint256) should be declared external:
        - Timelock.executeTransaction(address,uint256,string,bytes,uint256) (Timelock.sol#86-117)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:Timelock.sol analyzed (1 contracts with 75 detectors), 15 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CrescentDaoChef.sol

```
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (CrescentDaoChef.sol#441-461) uses assembly
        - INLINE ASM (CrescentDaoChef.sol#453-456)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (CrescentDaoChef.sol#590-592)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (CrescentDaoChef.sol#598-601)
poolLength() should be declared external:
        - CrescentDaoChef.poolLength() (CrescentDaoChef.sol#650-652)
deposit(uint256,uint256,address) should be declared external:
        - CrescentDaoChef.deposit(uint256,uint256,address) (CrescentDaoChef.sol#701-722)
withdraw(uint256,uint256,address) should be declared external:
        - CrescentDaoChef.withdraw(uint256,uint256,address) (CrescentDaoChef.sol#728-749)
withdrawAndHarvest(uint256,uint256,address) should be declared external:
        - CrescentDaoChef.withdrawAndHarvest(uint256,uint256,address) (CrescentDaoChef.sol#780-808)
emergencyWithdraw(uint256,address) should be declared external:
        - CrescentDaoChef.emergencyWithdraw(uint256,address) (CrescentDaoChef.sol#813-827)
add(uint256,IERC20,IRewarder) should be declared external:
        - CrescentDaoChef.add(uint256,IERC20,IRewarder) (CrescentDaoChef.sol#852-865)
set(uint256,uint256,IRewarder,bool) should be declared external:
        - CrescentDaoChef.set(uint256,uint256,IRewarder,bool) (CrescentDaoChef.sol#872-885)
setRewardPerSecond(uint256) should be declared external:
        - CrescentDaoChef.setRewardPerSecond(uint256) (CrescentDaoChef.sol#889-894)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:CrescentDaoChef.sol analyzed (10 contracts with 75 detectors), 50 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CrescentDaoStaking.sol

```
INFO:Detectors:
CrescentDaoStaking.constructor(address,address,address[],address)._teamWalletAddress (CrescentDaoStaking.sol#845) lacks a zero
-check on :
                - teamWalletAddress = _teamWalletAddress (CrescentDaoStaking.sol#859)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
```

```
INFO:Detectors:
CrescentDaoStaking.userLocks (CrescentDaoStaking.sol#832) is never used in CrescentDaoStaking (CrescentDaoStaking.sol#777-1266
)
CrescentDaoStaking.userEarnings (CrescentDaoStaking.sol#833) is never used in CrescentDaoStaking (CrescentDaoStaking.sol#777-1
266)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unused-state-variables
INFO:Detectors:
CrescentDaoStaking.lockedSupply (CrescentDaoStaking.sol#828) should be constant
CrescentDaoStaking.teamRewardPercent (CrescentDaoStaking.sol#836) should be constant
CrescentDaoStaking.totalSupply (CrescentDaoStaking.sol#827) should be constant
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (CrescentDaoStaking.sol#709-711)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (CrescentDaoStaking.sol#717-720)
addReward(address,address) should be declared external:
        - CrescentDaoStaking.addReward(address,address) (CrescentDaoStaking.sol#865-873)
withdrawableBalance(address) should be declared external:
        - CrescentDaoStaking.withdrawableBalance(address) (CrescentDaoStaking.sol#998-1016)
withdraw(uint256) should be declared external:
        - CrescentDaoStaking.withdraw(uint256) (CrescentDaoStaking.sol#1069-1112)
getReward() should be declared external:
        - CrescentDaoStaking.getReward() (CrescentDaoStaking.sol#1115-1131)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:CrescentDaoStaking.sol analyzed (13 contracts with 75 detectors), 76 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CrescentDaoZapMMSwap.sol

```
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (CrescentDaoZapMMSwap.sol#489-509) uses assembly
        - INLINE ASM (CrescentDaoZapMMSwap.sol#501-504)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (Cres
centDaoZapMMSwap.sol#85) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,add
ress,uint256).amountBDesired (CrescentDaoZapMMSwap.sol#86)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (CrescentDaoZapMMSwap.sol#638-640)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (CrescentDaoZapMMSwap.sol#646-649)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:CrescentDaoZapMMSwap.sol analyzed (13 contracts with 75 detectors), 45 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> Fund.sol

```
INFO:Detectors:
Fund.vestedBalance() (Fund.sol#564-575) uses timestamp for comparisons
        Dangerous comparisons:
        - block.timestamp <= _start (Fund.sol#568)
        - block.timestamp > _start + _duration (Fund.sol#571)
Fund.transfer(address,uint256) (Fund.sol#582-589) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(amount <= claimable(),Fund::transfer: > vestedAmount) (Fund.sol#585)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (Fund.sol#272-292) uses assembly
        - INLINE ASM (Fund.sol#284-287)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Parameter Fund.initialize(address)._yToken (Fund.sol#547) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
Fund (Fund.sol#540-591) does not implement functions:
        - Fund.allocation() (Fund.sol#554)
        - Fund.vestingDuration() (Fund.sol#558)
        - Fund.vestingStart() (Fund.sol#556)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#unimplemented-functions
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (Fund.sol#421-423)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (Fund.sol#429-432)
currentBalance() should be declared external:
        - Fund.currentBalance() (Fund.sol#560-562)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:Fund.sol analyzed (7 contracts with 75 detectors), 28 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CRSTDaoFund.sol

```
INFO:Detectors:
Fund.vestedBalance() (CRSTDaoFund.sol#566-577) uses timestamp for comparisons
        Dangerous comparisons:
        - block.timestamp <= _start (CRSTDaoFund.sol#570)
        - block.timestamp > _start + _duration (CRSTDaoFund.sol#573)
Fund.transfer(address,uint256) (CRSTDaoFund.sol#584-591) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(amount <= claimable(),Fund::transfer: > vestedAmount) (CRSTDaoFund.sol#587)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (CRSTDaoFund.sol#273-293) uses assembly
        - INLINE ASM (CRSTDaoFund.sol#285-288)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Pragma version0.8.4 (CRSTDaoFund.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (CRSTDaoFund.sol#132-137):
        - (success) = recipient.call{value: amount}() (CRSTDaoFund.sol#135)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (CRSTDaoFund.sol#200-211):
        - (success,returndata) = target.call{value: value}(data) (CRSTDaoFund.sol#209)
Low level call in Address.functionStaticCall(address,bytes,string) (CRSTDaoFund.sol#229-238):
        - (success,returndata) = target.staticcall(data) (CRSTDaoFund.sol#236)
Low level call in Address.functionDelegateCall(address,bytes,string) (CRSTDaoFund.sol#256-265):
        - (success,returndata) = target.delegatecall(data) (CRSTDaoFund.sol#263)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Parameter Fund.initialize(address)._yToken (CRSTDaoFund.sol#549) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (CRSTDaoFund.sol#422-424)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (CRSTDaoFund.sol#430-433)
currentBalance() should be declared external:
        - Fund.currentBalance() (CRSTDaoFund.sol#562-564)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:CRSTDaoFund.sol analyzed (8 contracts with 75 detectors), 27 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CRSTDevFund.sol

```
INFO:Detectors:
Pragma version0.8.4 (CRSTDevFund.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (CRSTDevFund.sol#131-136):
        - (success) = recipient.call{value: amount}() (CRSTDevFund.sol#134)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (CRSTDevFund.sol#199-210):
        - (success,returndata) = target.call{value: value}(data) (CRSTDevFund.sol#208)
Low level call in Address.functionStaticCall(address,bytes,string) (CRSTDevFund.sol#228-237):
        - (success,returndata) = target.staticcall(data) (CRSTDevFund.sol#235)
Low level call in Address.functionDelegateCall(address,bytes,string) (CRSTDevFund.sol#255-264):
        - (success,returndata) = target.delegatecall(data) (CRSTDevFund.sol#262)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Parameter Fund.initialize(address)._yToken (CRSTDevFund.sol#546) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (CRSTDevFund.sol#421-423)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (CRSTDevFund.sol#429-432)
currentBalance() should be declared external:
        - Fund.currentBalance() (CRSTDevFund.sol#559-561)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:CRSTDevFund.sol analyzed (8 contracts with 75 detectors), 27 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CRSTReserve.sol

```
INFO:Detectors:
Pragma version0.8.4 (CRSTReserve.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Low level call in Address.sendValue(address,uint256) (CRSTReserve.sol#131-136):
        - (success) = recipient.call{value: amount}() (CRSTReserve.sol#134)
Low level call in Address.functionCallWithValue(address,bytes,uint256,string) (CRSTReserve.sol#199-210):
        - (success,returndata) = target.call{value: value}(data) (CRSTReserve.sol#208)
Low level call in Address.functionStaticCall(address,bytes,string) (CRSTReserve.sol#228-237):
        - (success,returndata) = target.staticcall(data) (CRSTReserve.sol#235)
Low level call in Address.functionDelegateCall(address,bytes,string) (CRSTReserve.sol#255-264):
        - (success,returndata) = target.delegatecall(data) (CRSTReserve.sol#262)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
INFO:Detectors:
Parameter CRSTReserve.initialize(address)._crst (CRSTReserve.sol#491) is not in mixedCase
Parameter CRSTReserve.setRewarder(address)._rewarder (CRSTReserve.sol#498) is not in mixedCase
Parameter CRSTReserve.setPool(address)._pool (CRSTReserve.sol#504) is not in mixedCase
Parameter CRSTReserve.transfer(address,uint256)._to (CRSTReserve.sol#510) is not in mixedCase
Parameter CRSTReserve.transfer(address,uint256)._amount (CRSTReserve.sol#510) is not in mixedCase
Variable CRSTReserve.CRST (CRSTReserve.sol#484) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Slither:CRSTReserve.sol analyzed (6 contracts with 75 detectors), 30 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CRSTTreasuryFund.sol

```
INFO:Detectors:
Fund.vestedBalance() (CRSTTreasuryFund.sol#564-575) uses timestamp for comparisons
        Dangerous comparisons:
        - block.timestamp <= _start (CRSTTreasuryFund.sol#568)
        - block.timestamp > _start + _duration (CRSTTreasuryFund.sol#571)
Fund.transfer(address,uint256) (CRSTTreasuryFund.sol#582-589) uses timestamp for comparisons
        Dangerous comparisons:
        - require(bool,string)(amount <= claimable(),Fund::transfer: > vestedAmount) (CRSTTreasuryFund.sol#585)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (CRSTTreasuryFund.sol#272-292) uses assembly
        - INLINE ASM (CRSTTreasuryFund.sol#284-287)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Parameter Fund.initialize(address)._yToken (CRSTTreasuryFund.sol#547) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (CRSTTreasuryFund.sol#421-423)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (CRSTTreasuryFund.sol#429-432)
currentBalance() should be declared external:
        - Fund.currentBalance() (CRSTTreasuryFund.sol#560-562)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:CRSTTreasuryFund.sol analyzed (8 contracts with 75 detectors), 27 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> masterOracle.sol

```
INFO:Detectors:
Context._msgData() (masterOracle.sol#16-18) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
INFO:Detectors:
Pragma version0.8.4 (masterOracle.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Variable MasterOracle.constructor(address,address,address,address)._oracleXToken (masterOracle.sol#91) is too similar to Maste
rOracle.constructor(address,address,address,address)._oracleYToken (masterOracle.sol#92)
Variable MasterOracle.oracleXToken (masterOracle.sol#82) is too similar to MasterOracle.oracleYToken (masterOracle.sol#83)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar
```

```
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (masterOracle.sol#55-57)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (masterOracle.sol#63-66)
getXTokenPrice() should be declared external:
        - MasterOracle.getXTokenPrice() (masterOracle.sol#104-106)
getYTokenPrice() should be declared external:
        - MasterOracle.getYTokenPrice() (masterOracle.sol#108-110)
getXTokenTWAP() should be declared external:
        - MasterOracle.getXTokenTWAP() (masterOracle.sol#112-114)
getYTokenTWAP() should be declared external:
        - MasterOracle.getYTokenTWAP() (masterOracle.sol#116-118)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:masterOracle.sol analyzed (4 contracts with 75 detectors), 11 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> UniswapPairOracle.sol

```
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (UniswapPairOracle.sol#291-293)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (UniswapPairOracle.sol#299-302)
name() should be declared external:
        - ERC20.name() (UniswapPairOracle.sol#342-344)
symbol() should be declared external:
        - ERC20.symbol() (UniswapPairOracle.sol#350-352)
decimals() should be declared external:
        - ERC20.decimals() (UniswapPairOracle.sol#367-369)
totalSupply() should be declared external:
        - ERC20.totalSupply() (UniswapPairOracle.sol#374-376)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (UniswapPairOracle.sol#381-383)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (UniswapPairOracle.sol#393-397)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (UniswapPairOracle.sol#416-420)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (UniswapPairOracle.sol#438-447)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (UniswapPairOracle.sol#461-465)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (UniswapPairOracle.sol#481-490)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:UniswapPairOracle.sol analyzed (10 contracts with 75 detectors), 48 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> XToken.sol

```
INFO:Detectors:
XToken.constructor(string,string)._name (XToken.sol#496) shadows:
        - ERC20._name (XToken.sol#113) (state variable)
XToken.constructor(string,string)._symbol (XToken.sol#496) shadows:
        - ERC20._symbol (XToken.sol#114) (state variable)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
XToken.setMinter(address)._minter (XToken.sol#502) lacks a zero-check on :
                - minter = _minter (XToken.sol#504)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
INFO:Detectors:
Context._msgData() (XToken.sol#101-103) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
```

```
INFO:Detectors:
name() should be declared external:
        - ERC20.name() (XToken.sol#133-135)
symbol() should be declared external:
        - ERC20.symbol() (XToken.sol#141-143)
decimals() should be declared external:
        - ERC20.decimals() (XToken.sol#158-160)
totalSupply() should be declared external:
        - ERC20.totalSupply() (XToken.sol#165-167)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (XToken.sol#172-174)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (XToken.sol#184-188)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (XToken.sol#207-211)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (XToken.sol#229-238)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (XToken.sol#252-256)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (XToken.sol#272-281)
burn(uint256) should be declared external:
        - ERC20Burnable.burn(uint256) (XToken.sol#462-464)
burnFrom(address,uint256) should be declared external:
        - ERC20Burnable.burnFrom(address,uint256) (XToken.sol#477-480)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:XToken.sol analyzed (6 contracts with 75 detectors), 21 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> YToken.sol

```
INFO:Detectors:
YToken.constructor(string,string)._name (YToken.sol#484) shadows:
        - ERC20._name (YToken.sol#113) (state variable)
YToken.constructor(string,string)._symbol (YToken.sol#484) shadows:
        - ERC20._symbol (YToken.sol#114) (state variable)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
```

```
INFO:Detectors:
name() should be declared external:
        - ERC20.name() (YToken.sol#133-135)
symbol() should be declared external:
        - ERC20.symbol() (YToken.sol#141-143)
decimals() should be declared external:
        - ERC20.decimals() (YToken.sol#158-160)
totalSupply() should be declared external:
        - ERC20.totalSupply() (YToken.sol#165-167)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (YToken.sol#172-174)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (YToken.sol#184-188)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (YToken.sol#207-211)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (YToken.sol#229-238)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (YToken.sol#252-256)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (YToken.sol#272-281)
burn(uint256) should be declared external:
        - ERC20Burnable.burn(uint256) (YToken.sol#462-464)
burnFrom(address,uint256) should be declared external:
        - ERC20Burnable.burnFrom(address,uint256) (YToken.sol#477-480)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:YToken.sol analyzed (6 contracts with 75 detectors), 18 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CRST.sol

```
INFO:Detectors:
YToken.constructor(string,string)._name (CRST.sol#484) shadows:
        - ERC20._name (CRST.sol#113) (state variable)
YToken.constructor(string,string)._symbol (CRST.sol#484) shadows:
        - ERC20._symbol (CRST.sol#114) (state variable)
CRST.constructor(string,string,address,address,address,address)._name (CRST.sol#495) shadows:
        - ERC20._name (CRST.sol#113) (state variable)
CRST.constructor(string,string,address,address,address,address)._symbol (CRST.sol#496) shadows:
        - ERC20._symbol (CRST.sol#114) (state variable)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
Context._msgData() (CRST.sol#101-103) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
```

```
INFO:Detectors:
name() should be declared external:
        - ERC20.name() (CRST.sol#133-135)
symbol() should be declared external:
        - ERC20.symbol() (CRST.sol#141-143)
decimals() should be declared external:
        - ERC20.decimals() (CRST.sol#158-160)
totalSupply() should be declared external:
        - ERC20.totalSupply() (CRST.sol#165-167)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (CRST.sol#172-174)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (CRST.sol#184-188)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (CRST.sol#207-211)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (CRST.sol#229-238)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (CRST.sol#252-256)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (CRST.sol#272-281)
burn(uint256) should be declared external:
        - ERC20Burnable.burn(uint256) (CRST.sol#462-464)
burnFrom(address,uint256) should be declared external:
        - ERC20Burnable.burnFrom(address,uint256) (CRST.sol#477-480)
includeToWhitelist(address) should be declared external:
        - CRST.includeToWhitelist(address) (CRST.sol#516-521)
excludeFromWhitlist(address) should be declared external:
        - CRST.excludeFromWhitlist(address) (CRST.sol#523-528)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:CRST.sol analyzed (7 contracts with 75 detectors), 24 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> GLMX.sol

```
INFO:Detectors:
XToken.constructor(string,string)._name (GLMX.sol#496) shadows:
        - ERC20._name (GLMX.sol#113) (state variable)
XToken.constructor(string,string)._symbol (GLMX.sol#496) shadows:
        - ERC20._symbol (GLMX.sol#114) (state variable)
GLMX.constructor(string,string)._name (GLMX.sol#522) shadows:
        - ERC20._name (GLMX.sol#113) (state variable)
GLMX.constructor(string,string)._symbol (GLMX.sol#522) shadows:
        - ERC20._symbol (GLMX.sol#114) (state variable)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing
INFO:Detectors:
XToken.setMinter(address)._minter (GLMX.sol#502) lacks a zero-check on :
                - minter = _minter (GLMX.sol#504)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#missing-zero-address-validation
```

```
INFO:Detectors:
Pragma version0.8.4 (GLMX.sol#3) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6
solc-0.8.4 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
```

```
INFO:Detectors:
name() should be declared external:
        - ERC20.name() (GLMX.sol#133-135)
symbol() should be declared external:
        - ERC20.symbol() (GLMX.sol#141-143)
decimals() should be declared external:
        - ERC20.decimals() (GLMX.sol#158-160)
totalSupply() should be declared external:
        - ERC20.totalSupply() (GLMX.sol#165-167)
balanceOf(address) should be declared external:
        - ERC20.balanceOf(address) (GLMX.sol#172-174)
transfer(address,uint256) should be declared external:
        - ERC20.transfer(address,uint256) (GLMX.sol#184-188)
approve(address,uint256) should be declared external:
        - ERC20.approve(address,uint256) (GLMX.sol#207-211)
transferFrom(address,address,uint256) should be declared external:
        - ERC20.transferFrom(address,address,uint256) (GLMX.sol#229-238)
increaseAllowance(address,uint256) should be declared external:
        - ERC20.increaseAllowance(address,uint256) (GLMX.sol#252-256)
decreaseAllowance(address,uint256) should be declared external:
        - ERC20.decreaseAllowance(address,uint256) (GLMX.sol#272-281)
burn(uint256) should be declared external:
        - ERC20Burnable.burn(uint256) (GLMX.sol#462-464)
burnFrom(address,uint256) should be declared external:
        - ERC20Burnable.burnFrom(address,uint256) (GLMX.sol#477-480)
includeToWhitelist(address) should be declared external:
        - GLMX.includeToWhitelist(address) (GLMX.sol#533-538)
excludeFromWhitlist(address) should be declared external:
        - GLMX.excludeFromWhitlist(address) (GLMX.sol#540-545)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:GLMX.sol analyzed (7 contracts with 75 detectors), 28 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> CrescentDaoTreasury.sol

```
INFO:Detectors:
Parameter CrescentDaoTreasury.balanceOf(address)._token (CrescentDaoTreasury.sol#468) is not in mixedCase
Parameter CrescentDaoTreasury.requestFund(address,uint256)._token (CrescentDaoTreasury.sol#477) is not in mixedCase
Parameter CrescentDaoTreasury.requestFund(address,uint256)._amount (CrescentDaoTreasury.sol#477) is not in mixedCase
Parameter CrescentDaoTreasury.addStrategy(address)._strategy (CrescentDaoTreasury.sol#486) is not in mixedCase
Parameter CrescentDaoTreasury.removeStrategy(address)._strategy (CrescentDaoTreasury.sol#496) is not in mixedCase
Parameter CrescentDaoTreasury.allocateFee(address,uint256)._token (CrescentDaoTreasury.sol#513) is not in mixedCase
Parameter CrescentDaoTreasury.allocateFee(address,uint256)._amount (CrescentDaoTreasury.sol#513) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (CrescentDaoTreasury.sol#427-429)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (CrescentDaoTreasury.sol#435-438)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:CrescentDaoTreasury.sol analyzed (7 contracts with 75 detectors), 30 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> StratRecollateralize.sol

```
INFO:Detectors:
Reentrancy in StratRecollateralize.recollateralize(uint256) (StratRecollateralize.sol#500-511):
        External calls:
        - treasury.requestFund(address(WethUtils.weth),_amount) (StratRecollateralize.sol#504)
        - WethUtils.unwrap(_amount) (StratRecollateralize.sol#507)
        Event emitted after the call(s):
        - Recollateralized(_amount) (StratRecollateralize.sol#510)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
```

```
INFO:Detectors:
Constant WethUtils.weth (StratRecollateralize.sol#399) is not in UPPER_CASE_WITH_UNDERSCORES
Parameter StratRecollateralize.recollateralize(uint256)._amount (StratRecollateralize.sol#500) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (StratRecollateralize.sol#462-464)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (StratRecollateralize.sol#470-473)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:StratRecollateralize.sol analyzed (10 contracts with 75 detectors), 33 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Slither log >> StratReduceReserveLP.sol

```
INFO:Detectors:
Address.verifyCallResult(bool,bytes,string) (StratReduceReserveLP.sol#415-435) uses assembly
        - INLINE ASM (StratReduceReserveLP.sol#427-430)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
INFO:Detectors:
Variable IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (Stra
tReduceReserveLP.sol#16) is too similar to IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,add
ress,uint256).amountBDesired (StratReduceReserveLP.sol#17)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar
INFO:Detectors:
renounceOwnership() should be declared external:
        - Ownable.renounceOwnership() (StratReduceReserveLP.sol#586-588)
transferOwnership(address) should be declared external:
        - Ownable.transferOwnership(address) (StratReduceReserveLP.sol#594-597)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external
INFO:Slither:StratReduceReserveLP.sol analyzed (11 contracts with 75 detectors), 33 result(s) found
INFO:Slither:Use https://crytic.io/ to get access to additional detectors and Github integration
```

Solidity Static Analysis

Pool.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in Pool.redeem(uint256,uint256,uint256): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 1286:4:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 1254:33:

Gas & Economy

Gas costs:

Gas requirement of function Pool.setYTokenSlippage is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 1480:4:

Miscellaneous

Constant/View/Pure functions:

Pool.transferToTreasury(uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 1495:4:

Similar variable names:

Pool.collect() : Variables have very similar names "_xTokenAmount" and "_yTokenAmount". Note: Modifiers are currently not considered by this static analysis.
Pos: 1364:44:

Email: audit@EtherAuthority.io

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1496:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 1393:26:

SwapStrategyPOL.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in SwapStrategyPOL.addLiquidity(uint256,uint256,uint256): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 763:4:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 782:16:

Gas & Economy

Gas costs:

Gas requirement of function SwapStrategyPOL.yToken is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 688:4:

ERC

ERC20:

ERC20 contract's "decimals" function should have "uint8" as return type
more
Pos: 37:4:

Miscellaneous

Constant/View/Pure functions:

SwapStrategyPOL.cleanDust() : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 788:4:

Similar variable names:

SwapStrategyPOL.addLiquidity(uint256,uint256,uint256) : Variables have very similar names "_amountA" and "_amountB". Note: Modifiers are currently not considered by this static analysis.
Pos: 774:13:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 794:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 771:34:

Timelock.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in Timelock.executeTransaction(address,uint256,string,bytes,uint256): Could potentially lead to re-entrancy vulnerability.

more

Pos: 86:4:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.

more

Pos: 120:15:

Gas & Economy

Gas costs:

Gas requirement of function Timelock.executeTransaction is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 86:4:

Miscellaneous

Similar variable names:

Timelock.(address,uint256) : Variables have very similar names "MINIMUM_DELAY" and "MAXIMUM_DELAY".

Pos: 24:26:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 112:8:

CrescentDaoChef.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in CrescentDaoChef.emergencyWithdraw(uint256,address): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.

more

Pos: 813:4:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.

more

Pos: 863:72:

Gas & Economy

Gas costs:

Gas requirement of function CrescentDaoChef.setRewardPerSecond is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 889:4:

Miscellaneous

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 899:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 791:53:

CrescentDaoStaking.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in CrescentDaoStaking.getReward(): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 1115:4:

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 1185:49:

Gas & Economy

Gas costs:

Gas requirement of function CrescentDaoStaking.setTeamRewardPercent is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 1218:4:

Delete dynamic array:

The "delete" operation when applied to a dynamically sized array in Solidity generates code to delete each of the elements contained. If the array is large, this operation can surpass the block gas limit and raise an OOG exception. Also nested dynamically sized objects can produce the same results.
more
Pos: 1089:24:

For loop over dynamic array:

Loops that do not have a fixed number of iterations, for example, loops that depend on storage values, have to be used carefully. Due to the block gas limit, transactions can only consume a certain amount of gas. The number of iterations in a loop can grow beyond the block gas limit which can cause the complete contract to be stalled at a certain point. Additionally, using unbounded loops incurs in a lot of avoidable gas costs. Carefully test how many items at maximum you can pass to such functions to make it successful.
more
Pos: 1242:8:

Miscellaneous

Constant/View/Pure functions:

CrescentDaoStaking.lockedBalances(address) : Is constant but potentially should not be. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 970:4:

Similar variable names:

CrescentDaoStaking.notifyRewardAmount(address,uint256) : Variables have very similar names "reward" and "rewards". Note: Modifiers are currently not considered by this static analysis.
Pos: 1194:30:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1220:8:

Delete from dynamic array:

Using "delete" on an array leaves a gap. The length of the array remains the same. If you want to remove the empty position you need to shift items manually and update the "length" property.
more
Pos: 1089:24:

CrescentDaoZapMMSwap.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in CrescentDaoZapMMSwap.zap(uint256,uint256,bool): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.

more

Pos: 741:4:

Gas & Economy

Gas costs:

Gas requirement of function CrescentDaoZapMMSwap.zap is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 741:4:

Miscellaneous

Constant/View/Pure functions:

CrescentDaoZapMMSwap.approveToken(address,address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.

more

Pos: 833:4:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 871:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.

Pos: 852:15:

Fund.sol

Security

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 574:31:

Miscellaneous

Constant/View/Pure functions:

SafeERC20._callOptionalReturn(contract IERC20,bytes) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 364:4:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 585:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 574:15:

CRSTDaoFund.sol

Security

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 576:31:

Gas & Economy

Gas costs:

Gas requirement of function CRSTDaoFund.currentBalance is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 562:4:

Miscellaneous

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 587:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 576:15:

CRSTDevFund.sol

Security

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 573:31:

Gas & Economy

Gas costs:

Gas requirement of function CRSTDevFund.transfer is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 581:4:

Miscellaneous

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 584:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 573:15:

CRSTReserve.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in SafeERC20.safeDecreaseAllowance(contract IERC20,address,uint256): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 345:4:

Gas & Economy

Gas costs:

Gas requirement of function CRSTReserve.transfer is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 510:4:

Miscellaneous

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 512:8:

CRSTTreasuryFund.sol

Security

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 574:31:

Gas & Economy

Gas costs:

Gas requirement of function CRSTTreasuryFund.transfer is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 582:4:

Miscellaneous

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 585:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 574:15:

masterOracle.sol

Gas & Economy

Gas costs:

Gas requirement of function MasterOracle.getYTokenTWAP is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 116:4:

Miscellaneous

Similar variable names:

MasterOracle.getYTokenTWAP() : Variables have very similar names "xToken" and "yToken". Note: Modifiers are currently not considered by this static analysis.
Pos: 117:33:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 97:8:

UniswapPairOracle.sol

Security

Block timestamp:

Use of "block.timestamp": "block.timestamp" can be influenced by miners to a certain degree. That means that a miner can "choose" the block.timestamp, to a certain degree, to change the outcome of a transaction in the mined block.
more
Pos: 767:22:

Gas & Economy

Gas costs:

Gas requirement of function UniswapPairOracle.spot is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 748:4:

Miscellaneous

Constant/View/Pure functions:

UniswapPairOracle.currentCumulativePrices(address) : Is constant but potentially should not be. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 771:4:

Similar variable names:

UniswapPairOracle.twap(address,uint256) : Variables have very similar names "token" and "token0". Note: Modifiers are currently not considered by this static analysis.
Pos: 736:21:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 754:8:

Data truncated:

Division of integer values yields an integer value again. That means e.g. 10 / 100 = 0 instead of 0.1 since the result is an integer again. This does not hold for division of (only) literal values since those yield rational constants.
Pos: 759:21:

XToken.sol

Gas & Economy

Gas costs:

Gas requirement of function ERC20.decreaseAllowance is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 272:4:

Miscellaneous

Constant/View/Pure functions:

ERC20._afterTokenTransfer(address,address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 449:4:

Similar variable names:

ERC20Burnable.burnFrom(address,uint256) : Variables have very similar names "account" and "amount". Note: Modifiers are currently not considered by this static analysis.
Pos: 479:23:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 503:8:

YToken.sol

Gas & Economy

Gas costs:

Gas requirement of function ERC20.decreaseAllowance is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 272:4:

Miscellaneous

Constant/View/Pure functions:

ERC20._afterTokenTransfer(address,address,uint256) : Potentially should be constant/view/pure but is not.
more
Pos: 449:4:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 408:12:

CRST.sol

Gas & Economy

Gas costs:

Gas requirement of function CRST.burnFrom is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 477:4:

Miscellaneous

Constant/View/Pure functions:

CRST._transfer(address,address,uint256) : Potentially should be constant/view/pure but is not.

more

Pos: 530:4:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 535:8:

GLMX.sol

Gas & Economy

Gas costs:

Gas requirement of function GLMX.mint is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 510:4:

Miscellaneous

Constant/View/Pure functions:

GLMX._transfer(address,address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.

more

Pos: 547:4:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 548:8:

CrescentDaoTreasury.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in StratReduceReserveLP.reduceReserve(uint256,uint256): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.

more

Pos: 641:4:

Gas & Economy

Gas costs:

Gas requirement of function CrescentDaoTreasury.balanceOf is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)

Pos: 468:4:

Miscellaneous

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.

more

Pos: 515:8:

Delete from dynamic array:

Using "delete" on an array leaves a gap. The length of the array remains the same. If you want to remove the empty position you need to shift items manually and update the "length" property.

more

Pos: 498:8:

StratRecollateralize.sol

Security

Low level calls:

Use of "delegatecall": should be avoided whenever possible. External code, that is called can change the state of the calling contract and send ether from the caller's balance. If this is wanted behaviour, use the Solidity library feature if possible.
more
Pos: 280:50:

Gas & Economy

Gas costs:

Gas requirement of function StratRecollateralize.recollateralize is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 500:4:

Miscellaneous

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 502:8:

StratReduceReserveLP.sol

Security

Check-effects-interaction:

Potential violation of Checks-Effects-Interaction pattern in StratReduceReserveLP.reduceReserve(uint256,uint256): Could potentially lead to re-entrancy vulnerability. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 641:4:

Gas & Economy

Gas costs:

Gas requirement of function StratReduceReserveLP.reduceReserve is infinite: If the gas requirement of a function is higher than the block gas limit, it cannot be executed. Please avoid loops in your functions or actions that modify large areas of storage (this includes clearing or copying arrays in storage)
Pos: 641:4:

Miscellaneous

No return:

IERC20.transferFrom(address,address,uint256): Defines a return type but never explicitly returns a value.
Pos: 211:4:

Constant/View/Pure functions:

WethUtils.transfer(address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 537:4:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 642:8:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 643:8:

Solhint Linter

Pool.sol

```
Pool.sol:522:18: Error: Parse error: missing ';' at '{'
Pool.sol:826:18: Error: Parse error: missing ';' at '{'
Pool.sol:859:18: Error: Parse error: missing ';' at '{'
Pool.sol:908:18: Error: Parse error: missing ';' at '{'
Pool.sol:959:22: Error: Parse error: missing ';' at '{'
```

SwapStrategyPOL.sol

```
SwapStrategyPOL.sol:567:18: Error: Parse error: missing ';' at '{'
```

Timelock.sol

```
Timelock.sol:3:1: Error: Compiler version 0.8.4 does not satisfy the
r semver requirement
Timelock.sol:23:5: Error: Explicitly mark visibility in function (Set
ignoreConstructors to true if using solidity >=0.7.0)
Timelock.sol:111:51: Error: Avoid using low level calls.
Timelock.sol:120:16: Error: Avoid to make time-based decisions in
your business logic
```

CrescentDaoChef.sol

```
CrescentDaoChef.sol:519:18: Error: Parse error: missing ';' at '{'
```

CrescentDaoStaking.sol

```
CrescentDaoStaking.sol:56:18: Error: Parse error: missing ';' at '{'
CrescentDaoStaking.sol:69:18: Error: Parse error: missing ';' at '{'
CrescentDaoStaking.sol:81:18: Error: Parse error: missing ';' at '{'
CrescentDaoStaking.sol:98:18: Error: Parse error: missing ';' at '{'
CrescentDaoStaking.sol:110:18: Error: Parse error: missing ';' at '{'
CrescentDaoStaking.sol:206:18: Error: Parse error: missing ';' at '{'
CrescentDaoStaking.sol:229:18: Error: Parse error: missing ';' at '{'
CrescentDaoStaking.sol:255:18: Error: Parse error: missing ';' at '{'
CrescentDaoStaking.sol:616:18: Error: Parse error: missing ';' at '{'
```

CrescentDaoZapMMSwap.sol

```
CrescentDaoZapMMSwap.sol:567:18: Error: Parse error: missing ';' at
'{'
```

Fund.sol

```
Fund.sol:350:18: Error: Parse error: missing ';' at '{'
```

CRSTDaoFund.sol

```
CRSTDaoFund.sol:351:18: Error: Parse error: missing ';' at '{'
```

CRSTDevFund.sol

```
CRSTDevFund.sol:350:18: Error: Parse error: missing ';' at '{'
```

CRSTReserve.sol

```
CRSTReserve.sol:350:18: Error: Parse error: missing ';' at '{'
```

CRSTTreasuryFund.sol

```
CRSTTreasuryFund.sol:350:18: Error: Parse error: missing ';' at '{'
```

MasterOracle.sol

```
masterOracle.sol:3:1: Error: Compiler version 0.8.4 does not satisfy
the r semver requirement
masterOracle.sol:29:5: Error: Explicitly mark visibility in function
(Set ignoreConstructors to true if using solidity >=0.7.0)
masterOracle.sol:88:5: Error: Explicitly mark visibility in function
(Set ignoreConstructors to true if using solidity >=0.7.0)
```

UniswapPairOracle.sol

```
UniswapPairOracle.sol:485:18: Error: Parse error: missing ';' at '{'
UniswapPairOracle.sol:518:18: Error: Parse error: missing ';' at '{'
UniswapPairOracle.sol:567:18: Error: Parse error: missing ';' at '{'
UniswapPairOracle.sol:618:22: Error: Parse error: missing ';' at '{'
UniswapPairOracle.sol:709:18: Error: Parse error: missing ';' at '{'
UniswapPairOracle.sol:788:18: Error: Parse error: missing ';' at '{'
```

XToken.sol

```
XToken.sol:276:18: Error: Parse error: missing ';' at '{'
XToken.sol:309:18: Error: Parse error: missing ';' at '{'
XToken.sol:358:18: Error: Parse error: missing ';' at '{'
XToken.sol:409:22: Error: Parse error: missing ';' at '{'
```

YToken.sol

```
YToken.sol:276:18: Error: Parse error: missing ';' at '{'
YToken.sol:309:18: Error: Parse error: missing ';' at '{'
YToken.sol:358:18: Error: Parse error: missing ';' at '{'
YToken.sol:409:22: Error: Parse error: missing ';' at '{'
```

CRST.sol

```
CRST.sol:276:18: Error: Parse error: missing ';' at '{'
CRST.sol:309:18: Error: Parse error: missing ';' at '{'
CRST.sol:358:18: Error: Parse error: missing ';' at '{'
CRST.sol:409:22: Error: Parse error: missing ';' at '{'
```

GLMX.sol

```
GLMX.sol:276:18: Error: Parse error: missing ';' at '{'
GLMX.sol:309:18: Error: Parse error: missing ';' at '{'
GLMX.sol:358:18: Error: Parse error: missing ';' at '{'
GLMX.sol:409:22: Error: Parse error: missing ';' at '{'
```

CrescentDaoTreasury.sol

```
CrescentDaoTreasury.sol:356:18: Error: Parse error: missing ';' at
'{'
```

StratRecollateralize.sol

```
StratRecollateralize.sol:368:18: Error: Parse error: missing ';' at
'{'
```

StratReduceReserveLP.sol

```
StratReduceReserveLP.sol:493:18: Error: Parse error: missing ';' at
'{'
```

Software analysis result:

These software reported many false positive results and some are informational issues. So, those issues can be safely ignored.

Email: audit@EtherAuthority.io