

www.EtherAuthority.io audit@etherauthority.io

# SMART CONTRACT

# Security Audit Report

Project: Website: Platform: Language: Date:

Decentralized Foundation <u>https://defo.app</u> Avalanche Network Solidity May 12th, 2022

# **Table of contents**

Introduction	
Project Background	4
Audit Scope	5
Claimed Smart Contract Features	6
Audit Summary	8
Technical Quick Stats	
Code Quality	10
Documentation	
Use of Dependencies	
AS-IS overview	11
Severity Definitions	
Audit Findings	19
Conclusion	
Our Methodology	
Disclaimers	
Appendix	
Code Flow Diagram	
Slither Results Log	
Solidity static analysis	
Solhint Linter	

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.

> This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

steers warming a strengthered and

# Introduction

EtherAuthority was contracted by the Defo Contracts team to perform the Security audit of the Defo Contracts 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 May 12th, 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**

- Decentralized Foundation (DEFO) is a DeFi-As-A-Service protocol on the AVAX network that aims to leverage the world of DeFi to generate funds while also helping the most in need through the charity donations.
- The Defo Contracts have functions like burn, mint, initialize, fallback, receive, isPair, RedeemMint, MintGem, BoostGem, RedeemMint, transferLog, Compound, unstakeTokens, etc.
- The Defo Contracts inherit the Ownable, ERC20, ERC20Burnable, AccessControlUpgradeable, OwnableUpgradeable, Initializable, IERC20, SafeERC20, IERC721Enumerable, SafeMath, Address, Context, Strings, console 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 Defo Contracts Protocol Smart Contracts
Platform	Avalanche / Solidity
File 1	DefoErc20.sol
File 1 MD5 Hash	B8FEE41D9A557EFC48B3AEC65503F64A
File 2	DefoLimiter.sol
File 2 MD5 Hash	0ABD9395AB9D4294244AFB56652571FC
File 3	Diamond.sol
File 3 MD5 Hash	C5C1B4ECBF45A50FEF6F03467D06CC0D
File 4	DiamondInit.sol
File 4 MD5 Hash	A526ABD7D1B125AD8A768B1C0BDB9F43
File 5	LpManager.sol
File 5 MD5 Hash	32336CBEFBCC63799C439768750364EB
File 6	Redeem.sol
File 6 MD5 Hash	652B270D7F0A3833F190AEAD9E5DE5CE
File 7	DiamondCutFacet.sol
File 7 MD5 Hash	FB675C8189FD9D6CD4CAF93BB200A98F
File 8	DiamondLoupeFacet.sol
File 8 MD5 Hash	84553C4947D9917B1C73F83BFCF62B68
File 9	ERC721Enumerable.sol
File 9 MD5 Hash	30EA4861F52D9AD443509CB25D101CAD
File 10	ERC721Facet.sol
File 10 MD5 Hash	F7636C5D8C29AE0C59BD5D7EF9DE4847
File 11	GemFacet.sol
File 11 MD5 Hash	198FD8793B0BCC22198CF2223828B723

File 12	GemGettersFacet.sol
File 12 MD5 Hash	6AE044E55A2E950003F4C8C2ABD1122E
File 13	NodeLimiterFacet.sol
File 13 MD5 Hash	608D61E7914E26EB76546F82EC9FC450
File 14	OwnerFacet.sol
File 14 MD5 Hash	EA1DC6EABD981C327EF21C348B17D616
File 15	OwnershipFacet.sol
File 15 MD5 Hash	D392728362597E7666A0FCFF960A8CB9
File 16	VaultStakingFacet.sol
File 16 MD5 Hash	5A29BA843AB1E10EE747D70FF6E3F658
Audit Date	May 12th,2022

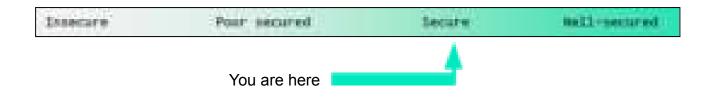
# **Claimed Smart Contract Features**

Claimed Feature Detail	Our Observation
File 1 DefoErc20.sol	YES, This is valid.
Name: Defo Token	
Symbol: DEFO	
Decimal: 18	
Total Supply: 0.2 Million	
File 2 DefoLimiter.sol	YES, This is valid.
Total Supply a wallet can sell: 10	
Time Frame Expiration: 1 days	
File 3 Diamond.sol	YES, This is valid.
<ul> <li>Find facet for function that is called and</li> </ul>	
execute the function if a facet is found	
File 4 DiamondInit.sol	YES, This is valid.
It initializes the diamond	
File 5 LpManager.sol	YES, This is valid.
It manages LP Tokens which includes, adding	
liquidity, create pair, buffer system, etc.	
File 6 Redeem.sol	YES, This is valid.
Redeem contract allows to redeem from	
presale and second presale.l	
<ul> <li>It has functions like: setNodeAddress,</li> </ul>	
flipActive, etc.	
File 7 DiamondCutFacet.sol	YES, This is valid.
<ul> <li>DiamondCutFacet has functions like:</li> </ul>	
diamondCut.	
File 8 DiamondLoupeFacet.sol	YES, This is valid.
<ul> <li>DiamondLoupeFacet has functions like:</li> </ul>	

facets, facetFunctionSelectors, facetAddress, etc.	
<ul> <li>File 9 ERC721Enumerable.sol</li> <li>ERC721Enumerable has functions like: tokenOfOwnerByIndex, tokenByIndex, etc.</li> </ul>	YES, This is valid.
<ul> <li>File 10 ERC721Facet.sol</li> <li>ERC721Facet has functions like: balanceOf, tokenURI, ownerOf, getApproved, etc.</li> </ul>	YES, This is valid.
File 11 GemFacet.sol <ul> <li>GemFacet has functions like:</li> <li>_distributePayment, _sendRewardTokens.</li> </ul>	YES, This is valid.
<ul> <li>File 12 GemGettersFacet.sol</li> <li>GemGettersFacet has functions like: GemOf, GetGemTypeMetadata, etc.</li> </ul>	YES, This is valid.
<ul> <li>File 13 NodeLimiterFacet.sol</li> <li>NodeLimiterFacet has functions like: transferLimit, addToWhitelist, etc.</li> </ul>	YES, This is valid.
<ul> <li>File 14 OwnerFacet.sol</li> <li>OwnerFacet has functions like: setTaperRate, ChangePaymentToken, etc.</li> </ul>	YES, This is valid.
<ul> <li>File 15 OwnershipFacet.sol</li> <li>OwnershipFacet has functions like: transferOwnership, etc.</li> </ul>	YES, This is valid.
<ul> <li>File 16 VaultStakingFacet.sol</li> <li>VaultStakingFacet has functions like: showStakedAmount, unstakeTokens,etc.</li> </ul>	YES, This is valid.

# **Audit Summary**

According to the standard audit assessment, Customer's solidity smart contracts are **"Secured"**. 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, 2 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 too old	Passed
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Moderate
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Moderate
	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	Moderate
Code	Function visibility not explicitly declared	Passed
Specification	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	Passed
	High consumption 'storage' storage	Passed
	Assert() misuse	Passed
Business Risk	The maximum limit for mintage not set	Passed
	"Short Address" Attack	Passed
	"Double Spend" Attack	Passed

**Overall Audit Result: PASSED** 

# **Code Quality**

This audit scope has 16 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 Defo Contracts 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 Defo Contracts Protocol.

The Defo Contracts Protocol team has provided unit test scripts, which have helped to determine the integrity of the code in an automated way.

Code parts are **not** well commented on smart contracts.

# Documentation

We were given a Defo Contracts Protocol smart contract code in the form of a Github weblink. The hash of that code is mentioned above in the table.

As mentioned above, code parts are **not well** commented. So it is not 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.

Another source of information was its official website <u>https://defo.app</u> which provided rich information about the project architecture and tokenomics.

# **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

## DefoErc20.sol

### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	name	read	Passed	No Issue
3	symbol	read	Passed	No Issue
4	decimals	read	Passed	No Issue
5	totalSupply	read	Passed	No Issue
6	balanceOf	read	Passed	No Issue
7	transfer	write	Passed	No Issue
8	allowance	read	Passed	No Issue
9	approve	write	Passed	No Issue
10	transferFrom	write	Passed	No Issue
11	increaseAllowance	write	Passed	No Issue
12	decreaseAllowance	write	Passed	No Issue
13	_transfer	internal	Passed	No Issue
14	_mint	internal	Passed	No Issue
15	_burn	internal	Passed	No Issue
16	_approve	internal	Passed	No Issue
17	spendAllowance	internal	Passed	No Issue
18	_beforeTokenTransfer	internal	Passed	No Issue
19	_afterTokenTransfer	internal	Passed	No Issue
20	burn	write	Passed	No Issue
21	burnFrom	write	Passed	No Issue
22	owner	read	Passed	No Issue
23	onlyOwner	modifier	Passed	No Issue
24	renounceOwnership	write	access only Owner	No Issue
25	transferOwnership	write	access only Owner	No Issue
26	_transferOwnership	internal	Passed	No Issue
27	onlyLiquidityPoolManager	modifier	Passed	No Issue
28	getLiquidityPoolManager	read	Passed	No Issue
29	setLiquidityPoolManager	write	access only Owner	No Issue
30	recoverLostTokens	external	access only Owner	No Issue

## DefoLimiter.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	Ownable_init	internal	access only Initializing	No Issue
3	Ownable_init_unchaine d	internal	access only Initializing	No Issue

4	owner	read	Passed	No Issue
5	onlyOwner	modifier	Passed	No Issue
6	renounceOwnership	write	access only Owner	No Issue
7	transferOwnership	write	access only Owner	No Issue
8	transferOwnership	internal	Passed	No Issue
9	AccessControl_init	internal	access only	No Issue
		internal	Initializing	140 15500
10	AccessControl_init_unc hained	internal	Passed	No Issue
11	onlyRole	modifier	Passed	No Issue
12	supportsInterface	read	Passed	No Issue
13	hasRole	read	Passed	No Issue
14	checkRole	internal	Passed	No Issue
15	getRoleAdmin	read	Passed	No Issue
16	grantRole	write	access only Role	No Issue
17	revokeRole	write	access only Role	No Issue
18	renounceRole	write	Passed	No Issue
19	_setupRole	internal	Passed	No Issue
20	setRoleAdmin	internal	Passed	No Issue
21	_grantRole	internal	Passed	No Issue
22	_revokeRole	internal	Passed	No Issue
23	initialize	write	Passed	No Issue
24	onlyDefoToken	modifier	Passed	No Issue
25	checkTimeframe	modifier	Passed	No Issue
26	notDenied	modifier	Passed	No Issue
27	isPair	read	Passed	No Issue
28	transferLog	external	access only Defo Token	No Issue
29	setMaxPercentage	external	Owner can stop the sell	Refer audit findings
30	setTokenAddress	external	access only Role	No Issue
31	setLPAddress	external	access only Role	No Issue
32	setLPManager	external	access only Role	No Issue
33	setDiamond	write	access only Role	No Issue
34	setTimeframeExpiration	external	access only Role	No Issue
35	editWhitelist	external	access only Role	No Issue
36	editBlocklist	external	access only Role	No Issue
50	GUILDIUGNIIBL	CALCITIAI		110 13506

## Diamond.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	fallback	external	Passed	No Issue
3	receive	external	Passed	No Issue

## DiamondInit.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	init	external	Passed	No Issue

## LpManager.sol

#### Functions

SI.	Functions	Туре	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	recoverLostTokens	external	access only Owner	No Issue
8	validAddress	modifier	Passed	No Issue
9	buffer	external	access only Owner	No Issue
10	addLiquidityToken	write	Passed	No Issue
11	bufferDefo	internal	Passed	No Issue
12	createPairWith	write	Passed	No Issue
13	setAllowance	write	access only Owner	No Issue
14	shouldLiquify	write	access only Owner	No Issue
15	setBufferThreshHold	write	access only Owner	No Issue
16	getRouter	external	Passed	No Issue
17	getPair	external	Passed	No Issue
18	getLeftSide	external	Passed	No Issue
19	getRightSide	external	Passed	No Issue
20	isPair	read	Passed	No Issue
21	getLeftBalance	read	Passed	No Issue
22	getRightBalance	read	Passed	No Issue
23	isLiquidityAdded	external	Passed	No Issue
24	isRouter	read	Passed	No Issue
25	getSupply	external	Passed	No Issue
26	setPairAllowance	write	Passed	No Issue
27	getReserver0	external	Passed	No Issue
28	getReserver1	external	Passed	No Issue
29	checkBalance	external	Passed	No Issue
30	token0	external	Passed	No Issue
31	token1	external	Passed	No Issue

## Redeem.sol

Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	owner	read	Passed	No Issue
3	onlyOwner	modifier	Passed	No Issue
4	transferOwnership	write	access only Owner	No Issue
5	_transferOwnership	internal	Passed	No Issue
6	renounceOwnership	write	access only Owner	No Issue
7	isActive	modifier	Passed	No Issue
8	nonReentrant	modifier	Passed	No Issue
9	presaleCompliance	modifier	Passed	No Issue
10	secondPresaleCompliance	modifier	Passed	No Issue
11	timeCompliance	modifier	Passed	No Issue
12	setNodeAddress	write	access only Owner	No Issue
13	startTimer	write	access only Owner	No Issue
14	flipActive	write	access only Owner	No Issue
15	redeem	write	For loops can be	Refer audit
			merged	findings
16	secondPresaleRedeem	write	access is Active	No Issue

## DiamondCutFacet.sol

### Functions

S	SI.	Functions	Туре	Observation	Conclusion
	1	constructor	write	Passed	No Issue
	2	diamondCut	external	Passed	No Issue

## DiamondLoupeFacet.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	facets	external	Passed	No Issue
3	facetFunctionSelectors	external	Passed	No Issue
4	facetAddresses	external	Passed	No Issue
5	facetAddress	external	Passed	No Issue
6	supportsInterface	external	Passed	No Issue

## ERC721Enumerable.sol

#### **Functions**

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initializeERC721Enumerable	write	Passed	No Issue
3	tokenOfOwnerByIndex	read	Passed	No Issue
4	totalSupply	read	Passed	No Issue
5	tokenByIndex	read	Passed	No Issue

## ERC721Facet.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initialize	write	Passed	No Issue
3	balanceOf	read	Passed	No Issue
4	name	read	Passed	No Issue
5	symbol	read	Passed	No Issue
6	tokenURI	read	Passed	No Issue
7	_baseURI	internal	Passed	No Issue
8	ownerOf	read	Passed	No Issue
9	getApproved	read	Passed	No Issue
10	isApprovedForAll	read	Passed	No Issue
11	approve	write	Passed	No Issue
12	setApprovalForAll	write	Passed	No Issue
13	transferFrom	write	Passed	No Issue
14	safeTransferFrom	write	Passed	No Issue
15	safeTransferFrom	write	Passed	No Issue

## GemFacet.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	SaleLock	modifier	Passed	No Issue
3	onlyGemOwner	modifier	Passed	No Issue
4	onlyActive	modifier	Passed	No Issue
5	mintTimeLimit	modifier	Passed	No Issue
6	_mintGem	internal	Passed	No Issue
7	_compound	internal	Passed	No Issue
8	_maintenance	internal	Passed	No Issue
9	_maintenanceDiscount	internal	Passed	No Issue
10	RedeemMint	write	Function input	Refer audit
			parameters lack of	findings
			check	
11	RedeemMintBooster	write	Function input	Refer audit
			parameters lack of	findings
			check	
12	BoostGem	write	access only Gem	No Issue
			Owner	
13	MintGem	external	Passed	No Issue
14	Maintenance	external	access only Gem	No Issue
			Owner	
15	BatchMaintenance	external	Passed	No Issue
16	Compound	external	access only Gem	No Issue
			Owner	

17	isActive	read	Passed	No Issue
18	checkRawReward	read	Passed	No Issue
19	checkTaperedReward	read	Passed	No Issue
20	checkTaxedReward	read	Passed	No Issue
21	checkPendingMaintenanc	read	Passed	No Issue
	е			
22	getGemIdsOf	read	Passed	No Issue
23	getGemIdsOfWithType	read	Passed	No Issue
24	_distributePayment	internal	Passed	No Issue
25	_sendRewardTokens	internal	Passed	No Issue
26	ClaimRewards	external	access only Gem	No Issue
			Owner	
27	BatchClaimRewards	external	Passed	No Issue

## GemGettersFacet.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	GemOf	external	Passed	No Issue
3	GetGemTypeMetadata	external	Passed	No Issue
4	getTotalCharity	external	Passed	No Issue
5	getMeta	external	Passed	No Issue

## NodeLimiterFacet.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	onlyOwner	write	Passed	No Issue
3	addToWhitelist	external	access only Owner	No Issue
4	transferLimit	write	Passed	No Issue

## **OwnerFacet.sol**

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	onlyOwner	modifier	Passed	No Issue
3	initialize	external	access only Owner	No Issue
4	setGemSettings	external	access only Owner	No Issue
5	setAddressAndDistTreasu	external	access only Owner	No Issue
	ry			
6	setAddressAndDistRewar	external	access only Owner	No Issue
	dPool			
7	setAddressDonation	external	access only Owner	No Issue

8	setAddressAndDistTeam	external	access only Owner	No Issue
9	setAddressAndDistLiquidi	external	access only Owner	No Issue
	ty			
10	setAddressVault	external	access only Owner	No Issue
11	setBaseURI	external	access only Owner	No Issue
12	setMinterAddress	external	access only Owner	No Issue
13	setLimiterAddress	external	access only Owner	No Issue
14	setMinReward	external	access only Owner	No Issue
15	setMinRewardTime	external	access only Owner	No Issue
16	setMintLimitHours	external	access only Owner	No Issue
17	setTaperRate	external	access only Owner	No Issue
18	setRewardTax	external	access only Owner	No Issue
19	ToggleSaleLock	external	access only Owner	No Issue
20	ToggleTransferLock	external	access only Owner	No Issue

## **OwnershipFacet.sol**

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	transferOwnership	external	Function input parameters lack of check	Refer audit findings
3	owner	external	Passed	No Issue

## VaultStakingFacet.sol

#### Functions

SI.	Functions	Туре	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	onlyGemOwner	modifier	Passed	No Issue
3	onlyActive	modifier	Passed	No Issue
4	batchAddTovault	external	Deploy error	Refer audit
				findings
5	addToVault	write	access only Gem	No Issue
			Owner	
6	showStakedAmount	read	Passed	No Issue
7	unstakeTokens	write	access only Gem	No Issue
			Owner	

# **Severity Definitions**

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
Hìgh	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.

# **Audit Findings**

## **Critical Severity**

No Critical severity vulnerabilities were found.

## **High Severity**

No High severity vulnerabilities were found.

## Medium

#### (1) Deploy error: VaultStakingFacet.sol

```
function batchAddTovault(
   wint256[] calldate _tokenIds,
   uivt256[] calldata _amounts
) external (
   LibGem.DiamondStorage storage digem = LibGem.diamondStorage();
   LibHets.DiscondStorage storage metads = LibHets.discondStorage[];
   LibUser.DiscondStorage storage userds = LibUser.discondStorage{};
   LibUser.UserData storage user = userds.GetUserData[LibNets.msgSender()]:
   LibVaultStaking.DiamondStorage storage ds = LibVaultStaking
        .dismondStorage();
    far (uint156 index = 0; index < _tokenIds.length; index++) {</pre>
        require(
            LibERC721. ownerOf(_tokenEds[index]) == LibERC721.msgSender(),
            "You don't own this gem"
        2.8
        require(LibGem._isActive(_tokenEds[index]), "Gem is deactivated");
        uint256 _pendingRewards = LibBem_taperCalculate(_tokenEds[index]);
        regulare()
            _anouvts[index] >= _pendingRewards,
            "Not enough pending rewards"
        100
        LibGen.Gen storage gen - dagen.GenOf[_tokenIds[index]];
        uint156 charityRecurt = (metads.CharityRate * _amounts[index]) /
            10001
        _amounts[index] = _amounts[index] - charityAmount;
```

Calldata arrays are read-only. So \_amounts variable cannot be updated.

**Resolution:** We suggest correcting the code by changing calldata to memory for the \_amounts.

This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity. Ernail: audit@EtherAuthority.io

their sound. Frue second of the

(2) Owner can stop the sell: DefoLimiter.sol

```
function setMaxPercentage(uinti% _newPercentage) external onlyRole(DEFALLT_ADMIN_ROLE) {
    sellLimitVsTotalSupply = _newPercentage;
}
```

The owner can set sellLimitVsTotalSupply to 0 using setMaxPercentage. Hence users cannot sell their tokens.

Resolution: We suggest using some minimum limit to set sellLimitVsTotalSupply.

## Low

(1) For loops can be merged: Redeem.sol



This is a private and confidential document. No part of this document should be disclosed to third party without price written permission of Etherlathenity. Email: audit@EtherAuthority.io

Contraction and a second second second second second





In the Redeem function, these loops can be merged and use conditions to check for the last element and avoid transferFrom for that.

**Resolution:** We suggest using only 1 loop for each balance and use conditions to check for the last element and avoid transferFrom for that.

This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity. Ernail: audit@EtherAuthority.io

state and the street of street.

(2) Function input parameters lack of check:

Variable validation is not performed in below functions :

### GemFacet.sol

- RedeemMint
- RedeemMintBooster

#### OwnershipFacet.sol

• transferOwnership

**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) Unused variable: DefoErc20.sol

The MAXSELLLIMIT is defined but not used anywhere.

Resolution: We suggest removing unused variables.

(2) Critical operation lacks event log: GemFacet.sol

Missing event log for:

- Compound
- BatchClaimRewards
- BatchMaintenance
- RedeemMint
- RedeemMintBooster
- BoostGem
- MintGem
- Maintenance
- BatchMaintenance
- BatchClaimRewards

**Resolution:** We suggest adding logs for the listed events.

# 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:

- transferLog: DefoLimiter DefoToken owner can call before any token transfer.
- setMaxPercentage: DefoLimiter role owner can set maximum percentage.
- setTokenAddress: DefoLimiter role owner can set token address.
- setLPAddress: DefoLimiter role owner can set LP address.
- setLPManager: DefoLimiter role owner can set token manager address.
- setDiamond: DefoLimiter role owner can set diamond address.
- setTimeframeExpiration: DefoLimiter role owner can set time frame expiration.
- editWhitelist: DefoLimiter role owner can update whitelist addresses and status.
- editBlocklist: DefoLimiter role owner can update blocklist addresses and status.
- setAllowance: LpManager owner can set allowance status.
- shouldLiquify: LpManager owner should set liquify status.
- setBufferThreshHold: LpManager owner can set buffer threshold value.
- setNodeAddress: Redeem owner can set node address.
- startTimer: Redeem owner can set start timer.
- flipActive: Redeem owner can flip active redeem.
- addToWhitelist: NodeLimiterFacet owner can add new address in whitelist.
- initialize: OwnerFacet owner can initialize address.
- setGemSettings: OwnerFacet owner can create a new gem type or change a gem type settings.
- setAddressAndDistTreasury: OwnerFacet owner can set distribution treasury addresses.
- setAddressAndDistRewardPool: OwnerFacet owner can set distribution reward addresses.
- setAddressDonation: OwnerFacet owner can set donation addresses.
- setAddressAndDistTeam: OwnerFacet owner can set address and dist team.
- setAddressAndDistLiquidity: OwnerFacet owner can set address and dist liquidity address.

This is a private and confidential document. We part of this document should be disclosed to third party without price written permission of Etherlasherity. Email: audit@EtherAuthority.io

nam annamentantativa

- setAddressVault: OwnerFacet owner can set new vault address.
- setBaseURI: OwnerFacet owner can set base uri.
- setMinterAddress: OwnerFacet owner can set new minter address.
- setLimiterAddress: OwnerFacet owner can set new limiter address.
- setMinReward: OwnerFacet owner can set minimum reward value.
- setMinRewardTime: OwnerFacet owner can set minimum reward time value.
- setMintLimitHours: OwnerFacet owner can set minimum limit hours time value.
- ChangePaymentToken: OwnerFacet owner can change payment token address.
- setTaperRate: OwnerFacet owner can set taper rate value.
- setRewardTax: OwnerFacet owner can set reward tax value.
- ToggleSaleLock: OwnerFacet owner can toggle sale lock.
- ToggleTransferLock: OwnerFacet owner can toggle transfer lock.
- batchAddTovault: VaultStakingFacet owner can set batch address to vault address.
- addToVault: VaultStakingFacet owner can add new vault address.
- unstakeTokens: VaultStakingFacet owner can unstake tokens.

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

This is a private and confidential document, its part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

tioner wanning Protection and the

# Conclusion

We were given a contract code in the form of github links. And we have used all possible tests based on given objects as files. We have observed some issues in the smart contracts. So, **it's good to go to production by fixing those issues**.

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".

This is a private and confidential document. No part of this document should be disclosed to third party without price written permission of Etherlatherity. Ereal: audit@EtherAuthority.io

Constant and the and the state of the state

# **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.

This is a private and confidential document. No part of this document should be disclosed to third party without price written permission of Etherlatherity. Ereal: audit@EtherAuthority.io

Contraction and an and a second contraction of the

#### **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.

This is a private and confidential document, its part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

Trease and the state of the second set and

# 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).

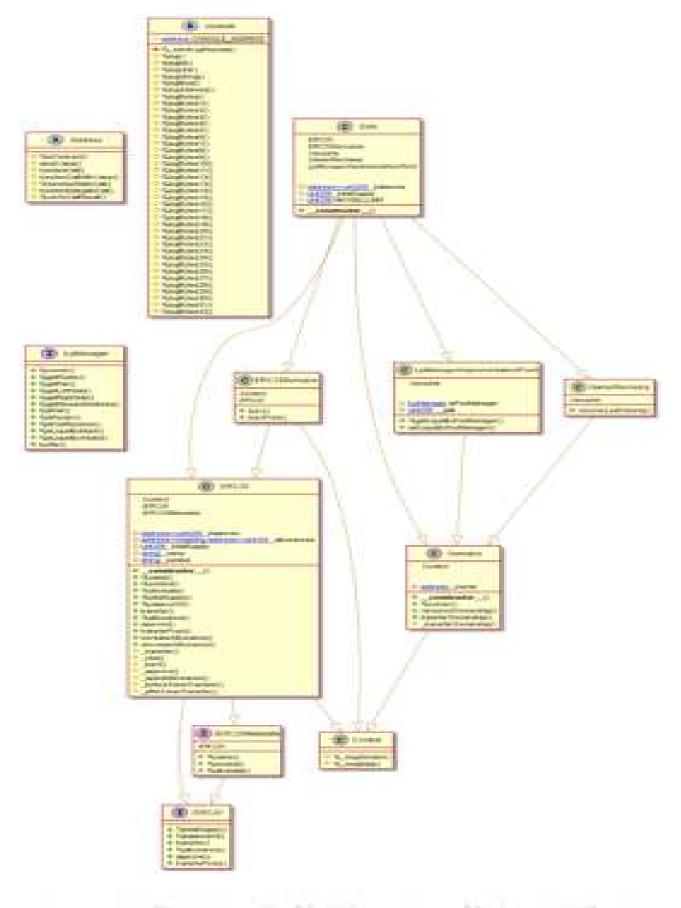
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we 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.

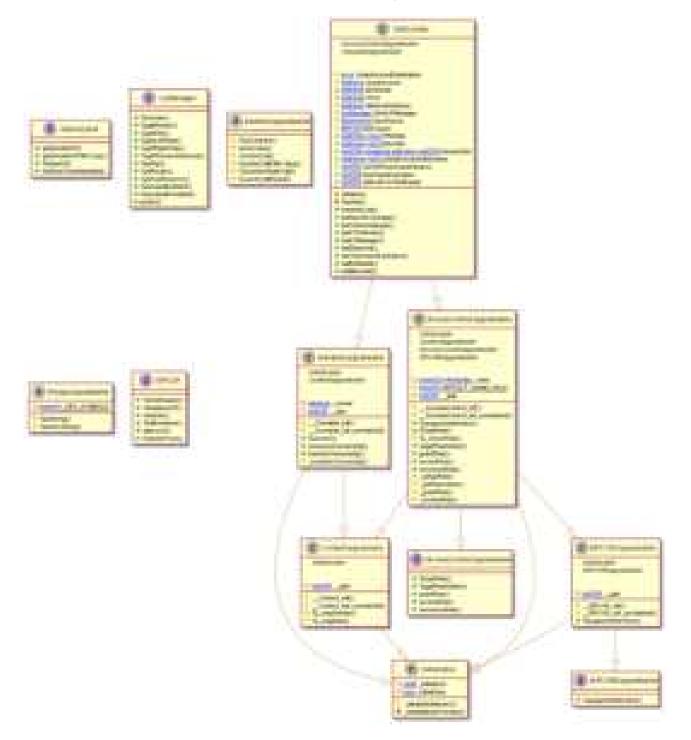
# Appendix

## Code Flow Diagram - Defo Contracts Protocol



## DefoErc20 Diagram

## DefoLimiter Diagram



## **Diamond Diagram**

	LECiemond
	Interaction Storage Position
(DiamondCat     damondCat)	QuitemondStorage()     setCantractOwner()     QuantractOwner()     QuantractOwner()     QuantractOwner()     demondCut()     addFunctions()     neplaceFunctions()     nemoveFunctions()     removeFunction()     retial2eDiamondCut()     QuantraceHasCuntractCude()



## **DiamondInit Diagram**

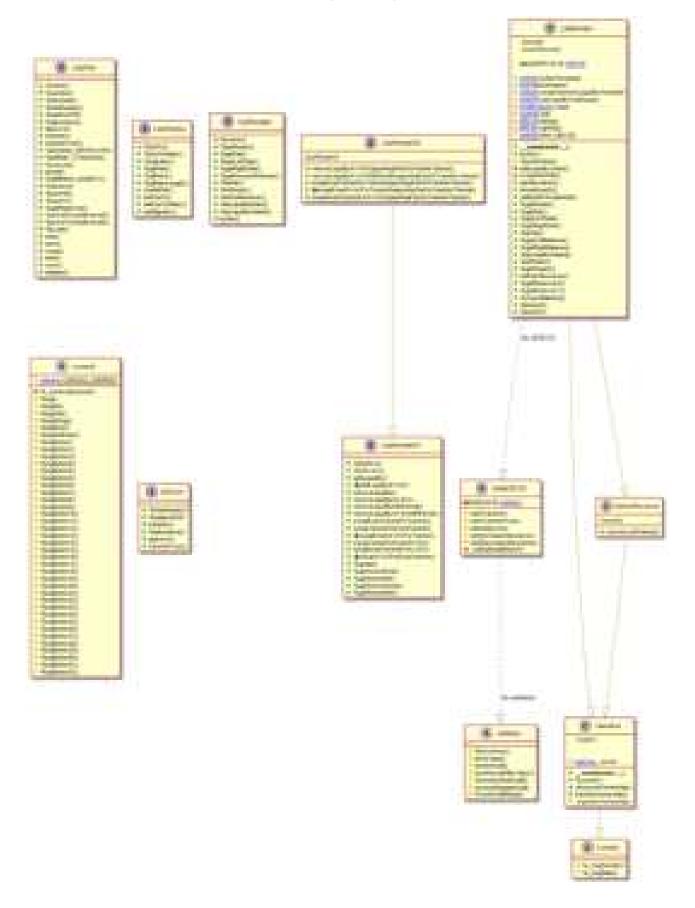




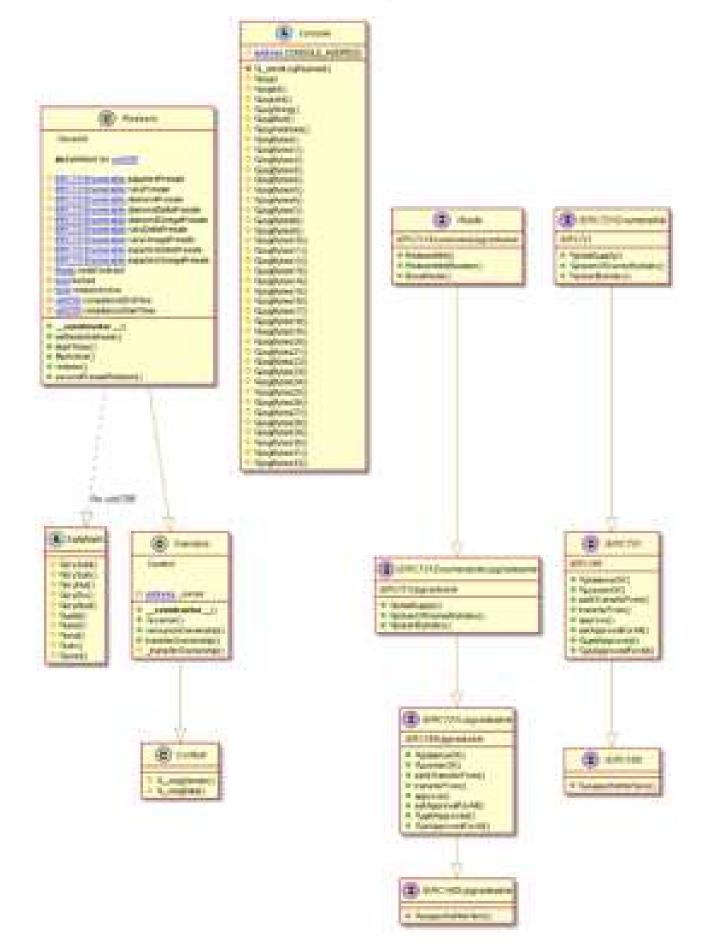
This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Otherlatherity. Ernail: audit@EtherAuthority.io

Control and the second s

## LpManager Diagram



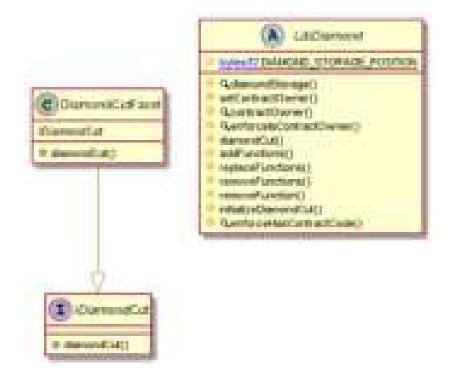
#### **Redeem Diagram**



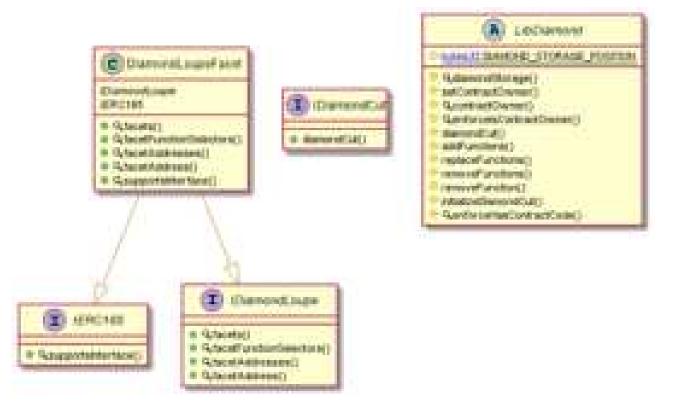
Two, is a private and confidential document, he part of the document should be disclosed to third party without prior written permission of Ethenhaltenity, Email: audit@EtherAuthority.io

treater water the protocol sector and the

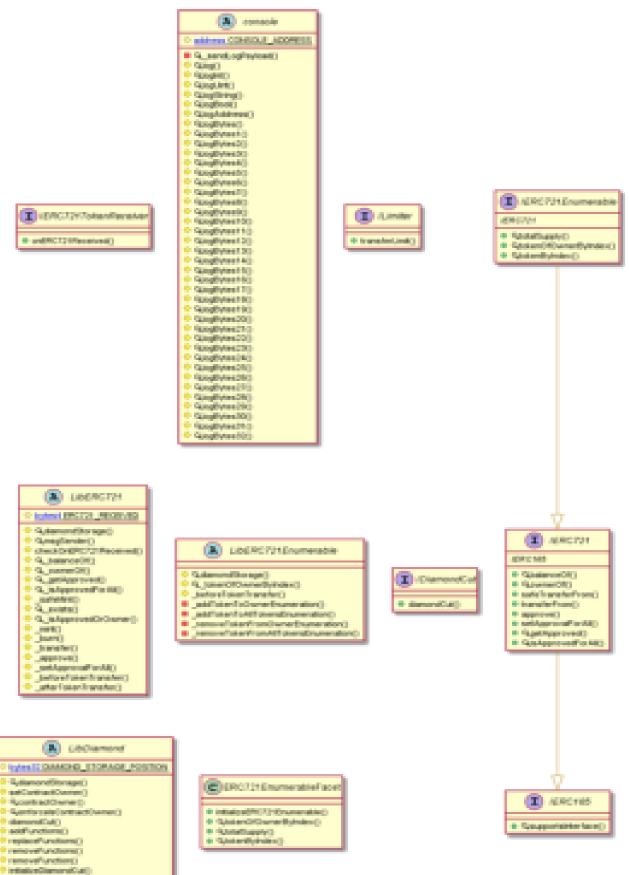
## DiamondCutFacet Diagram



## DiamondLoupeFacet Diagram

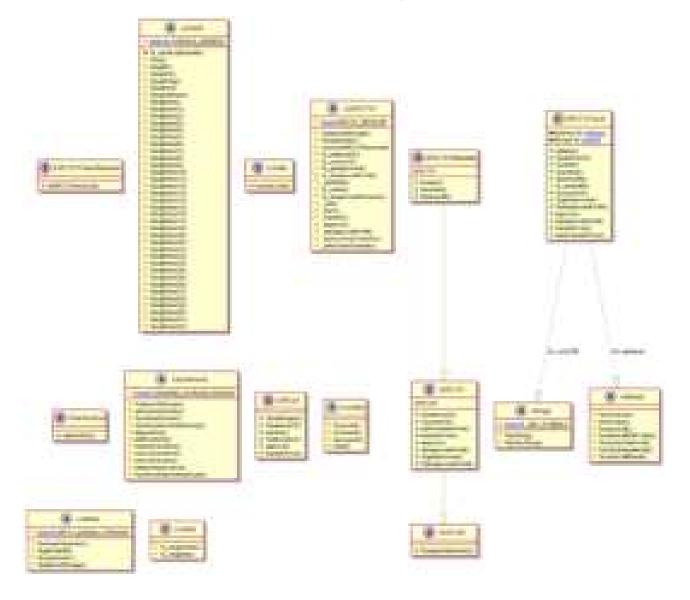


## ERC721Enumerable Diagram



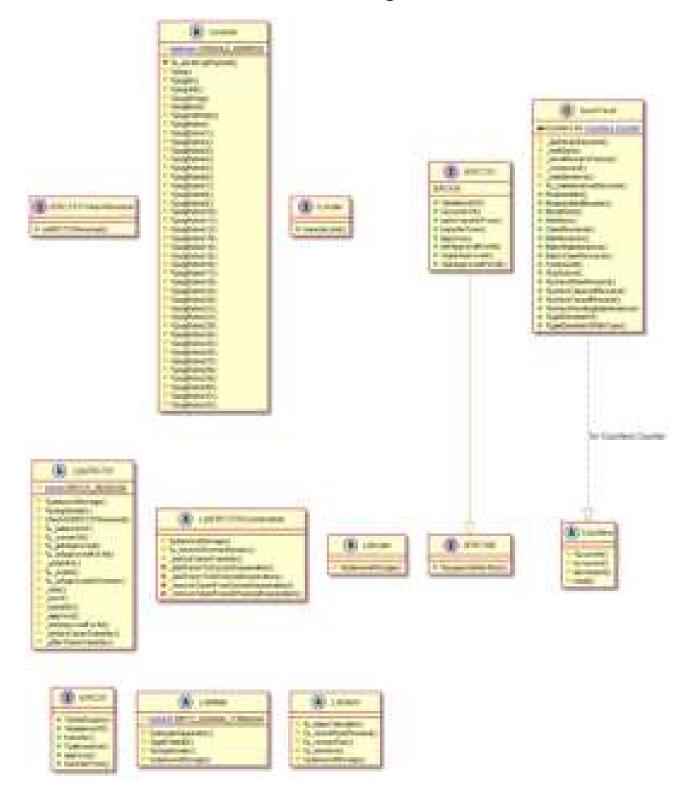
· Rently setting Corts and Code()

# ERC721Facet Diagram



This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity, Email: audit@EtherAuthority.io

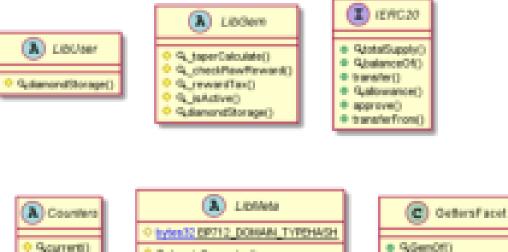
# **GemFacet Diagram**



This is a private and confidential document. We part of this document should be disclosed to third party without prior written permission of Etherlistheity. Email: audit@EtherAuthority.io

train addition and the second second second

# GemGettersFacet Diagram





- QGetGenTypeMetadata()
- GgetTeteChartsCi
- Gjethelarji

# NodeLimiterFacet Diagram

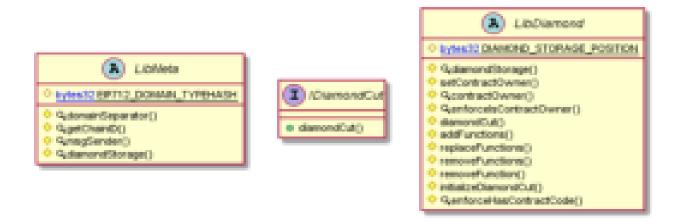


QuismainSeparator()

Q\_damond(lionage())

9,getCharlDO

Questionaler()





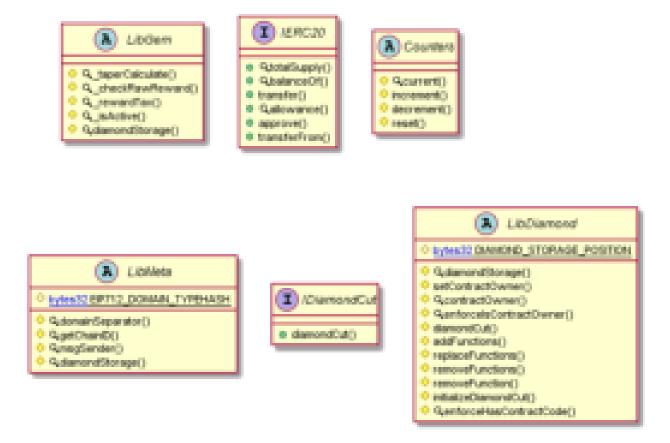
increment()

decrement()

reset():

This is a private and confidential document. He part of this document should its flucinised to third party without price written permission of Etherladiumity. Email: audit@EtherAuthority.io

# **OwnerFacet Diagram**





This is a private and confidential document, the part of this document should be disclosed to third party without price written permission of Etherlathenity. Ernail: audit@EtherAuthority.io

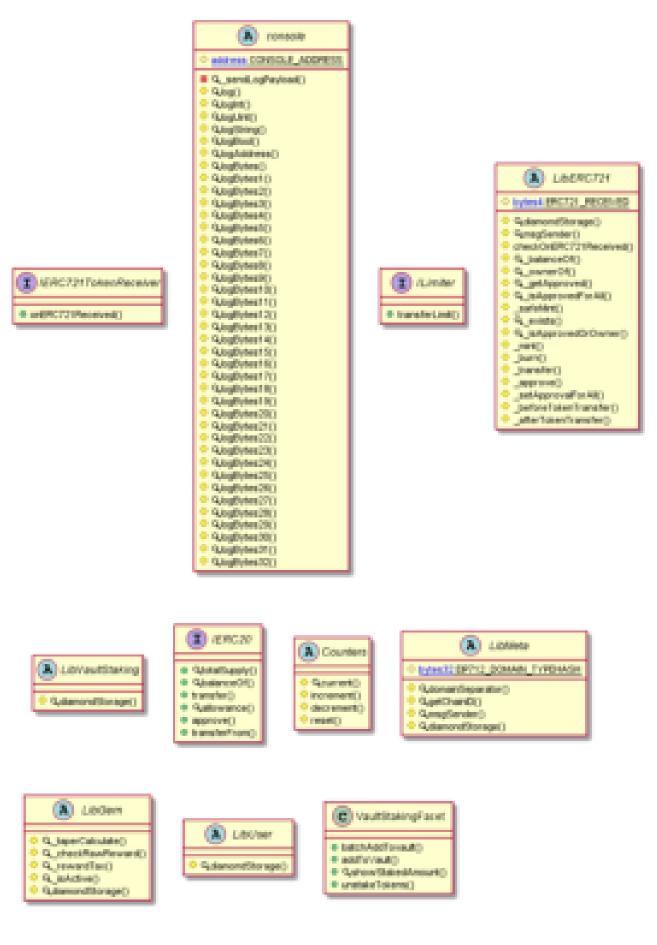
contraction and a second s

# OwnershipFacet Diagram

OwtenshipFacet      Afficiat      A transferConventing()      Theorem ()	LINCOMPAGE POINT() Submit DAMOD VIDMAGE POINT() Submit DAMOD VIDMAGE POINT() Submit Dame() Submit Dame() S
Constant) * SalateConstant)	

This is a private and confidential document, he part of this document should be disclosed to third party without prior written permission of Etherlatherity. Email: audit@EtherAuthority.io

# VaultStakingFacet Diagram

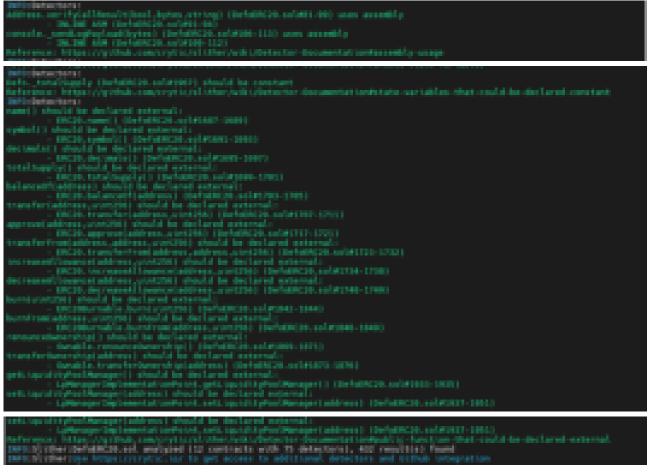


This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

user some benersterningen

# **Slither Results Log**

# Slither log >> DefoErc20.sol



# Slither log >> Diamond.sol

Particular and a Langer (Constant) (Efficiency Conference and Article (Constant)) (Constant) (Const
<pre>Mail Sector 1. If a University is an any regression to research to be transfer; domainer deploying with toth Sym. 5.4 Figure and the sector recommends for deployment And the sector recommends for deployment is and the sector recommend for deployment is an and the sector recommend for deployment is an</pre>

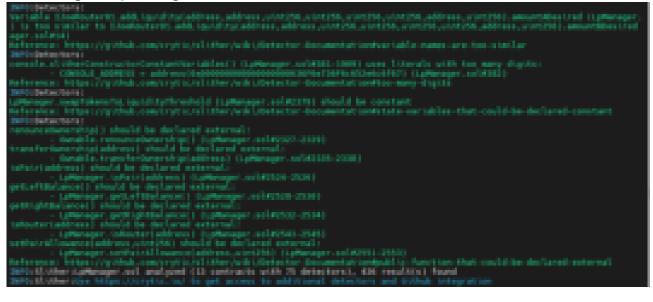
This, is a private and confidential document, he part of this document stands be disclosed to third party without prior written permission of Etherlatherity.

Email: audit@EtherAuthority.io

Slither log >> DiamondInit.sol

INFORMATION (Construction of the subsection of t
The second se
Proper version 0.4.4 (biamondinit.ed)() recentives a version too recent to be transed, donaider deploying with 0.4.52/0.7.0. adv0.4.4 to not recentered for deployment Autorover. Attor (.e) that contry(cyth)/department contents to the recent to one target of and dity (
Low Sevel 1435, St. 1005ammet, 161114/3240 (amongCuttabless), bytes 1.001ammet/2011-0116003-02011
- Internet actively a local defendance [1] collidered [1] collidered [1]
<ul> <li>Lauriness verses) =iest.delagatecult; sid/bitata( lliumieslost, as/ACM); Asferences: Mitge: Digitibul: concerption/of other well-colling between at another - beest - colling</li> </ul>
terreter a terreter de la seconda de la s
the second of th
and the second
<pre>Perimeter Lidrimend.settemptertedneriedners), enderer (finnendinit,self); is not in elsediese Perimeter Lidrimend.dimendint Dismendint terbitet( Perimeter Lidrimendint,dimendint Dismendint terbitet), address dyter), dimendinit selficit, selfitti is not in elsediese Perimeter Lidrimend.dimendint Dismendint Section(), address dyter), ord (Limendinit self); is not in elsediese Perimeter Lidrimend.eddiese(); is not in elsediese dyter), address dyter), ord (Limendinit self); is not in elsediese Perimeter Lidrimend.eddiese(); is dismendint destine(); address dyter(); is not in elsediese Perimeter Lidrimend.eddiese; is dismendint(); is not in elsediese Perimeter Lidrimend.eddiese; is dismendiese; dyter();</pre>
Parameter i Shirament, addjuestionel address (system) (), Santanderes (Diameter) (Diameter), sportibly) is not in minediase
Personnels Colorament, restance and the statements of the line of the statement of the annexity of the statement and
Per amonto is destanded, che al anciente a seconda a
Parameter U.M. amond, replaceture (international difference) (I. Direct parts bettern international context to rest to reserve and the second seco
An amount is appropriate to the approximation of the second s
Recomptor ()driamond, removationstandstand, bitand()). Tentrionstelletters (stamondbrot, soletter) in not in minediase Recomptor ()driamond, removationstandstand, bytess)toleteddross (stamondbrot, soletter) is not in mixediase
Persenter ( ) de amond, removerant tant address (dytess) ( ) altertar (d) amondarit, silvent) is not in mised and
Terranetar i der sebere over sen ten sebere der see arres i over interesentre de strett of the off of tradition
Parameter Constantiation Constantiation and an end of the constant and and the second
reserver consider the second and the second s
Persenter Coloraneed, to training and tamentarianty and the contract of the second of the second and the exact and the second
An an and a second se
the contract of the second book and a second to be the second sec
the state of the state of the second state of the second state of the second state of the state of the second state of the sec

# Slither log >> LpManager.sol



# Slither log >> Redeem.sol

<pre>Instructions approximation ( ) (Andreen and 2001 2011) as an assembly - Soc Def With (Andreen and 2009 2011) to for second to Equily (Andreen and 2009 2011) to for second to Equily (Andreen and 2009 2014) (Decryock (Detector - Constantial Second and 2019 2019) Social Constant and 2019 2019 (Instrumentation of the Second and 2019 2019) (Instrumentation of the Second and 2019 2019) - Andreen and 2019 2019 (Instrumentation of the Second and Andreen and 2019 2019) - Andreen and 2019 2019 (Instrumentation of the Second and Andreen and 2019 2019) - Andreen and 2019 2019 2019 2019 2019 2019 2019 2019</pre>	
<pre>Definitions: remound advances/spip() shawled be declineed subscraft; . Benable, remound advances/spip() (Rembers.collegic</pre>	

This, is a private and confidential document, he part of this document stands be disclosed to third party without prior written permission of Etherlatherity.

Email: audit@EtherAuthority.io

# Slither log >> DiamondCutFacet.sol

5
<pre>Introduction to the second introduction of a second introduction o</pre>
<ul> <li>THE THE AREA DISCHMENT AND ADDRESS AND ADDRESS ADDRE ADDRESS ADDR</li></ul>
An Foreinen i Del type (201) Blade, com/coryt (2010) Blade (1913) 2/Better for class annertial Contracted (1910) ange The Foreine Land
CONTINUES INTERPOLIE (I) (I) LANSAUGUET AND
repairs were interested. I. A (Diamondoptingst, soluti) necessitates a verying too recent to be trusted. Enseider deploying with 0.0.1275
add/-d.d.4 is not recommended for deplement and arrange ( https://github.com/orytic/sl/chercede/decommentationarraet-eers ions-of-eel/dity individual area
uner Tenert (na 1.) en 1. dettemment der Ertel Generaliset anbeiten "Beten"). (Ertemmethertferent, anbeiten 1840) 1. Bezeitenen (na 2. dette 1.) er Bruck angelen af 11. jun Materia). Detemmethertferent, anbeiten) Referensen (1840) genezige Basis, angelen yf Grytherten (dettemmetherten demonstelle Basis) and Basis (and Basis)
<pre>Introductions for sectors for sectors</pre>
An american L SUCramenel Ferminenture L Les andress Lupiterel L Carleston (OriginandCulture). La VerSUED: La VerS in antendicare for american L SUCramenel Leviture Landonautoritation and the construction of the second structure of the second str
Parameter (Converticities), diametilatificametilatificametilatificameticities), addites, bytes), addites, bitametilatificamet Infinitiviticametilatificametilatificametilatificametilatificametilatificametilatificametilatificametilatificamet

# Slither log >> DiamondLoupeFacet.sol

# Slither log >> ERC721Enumerable.sol

This is a private and confidential document. He part of this document stands be disclosed to third party without prior written permission of Otherlationity. Email: audit@EtherAuthority.io



# Slither log >> ERC721Facet.sol

Denvision and Review (
consistssend.cgPepiedChytes) (DECT[FaceL.orDF17-D4) uses assembly - DALTHE ADM (DECT[FaceL.orDF17-D4)
Libbl(1)1.dissocitorape().0000201playet.so(00000-1575) uses essentily
<ul> <li>DALMALASM LOD(1111Acom_colletSiz_2014)</li> <li>(d00(1211-maplassier()) LOD(1211Acom_colletSiz_2010) seens assembly</li> </ul>
<ul> <li>IN ME ANY CONTINUES AND ADDRESS</li> </ul>
L MERCELL, And MARCELLARD MARCELLARD AND AND AND AND AND AND AND AND AND AN
Libb Landred, disanded its inget 1 1080203040040, and 000021 uses an anticity
<ul> <li>DALDHI ADM (DECIDING) and ADD - DEDI</li> <li>Librian and an annual and a second decide a</li></ul>
<ul> <li>DCDM_ASH_CONCEPTION AND ADDRESS</li> </ul>
( dewise performance) ( DECTYTICATE and Argent And Argent And Argent Arg
(definition of the second s
<ul> <li>Da. Dal. ASM (DBC1010 and -college) and a constrainty and a constrainty.</li> </ul>
<ul> <li>DEDM_ADM_TERCED_001401027_20101</li> </ul>
iddress.com/stycalliterational.instances/com/control/contro
Reference: https://wythds.com/cryticzelither/wikit/betecter-documentation/hencedily-usage
DATE (MONOTO THE THE OWNER OF THE OWNER
consile of the time to the time termine to the time
Haffarence : https://githdo.com/crytic/sithdocrealizedecrealize
instituti instanta energi utendati instituti anterendi.
<ul> <li>INCIDE/acres. Init for the second strength of the second se</li></ul>
telanostitedheesi should be declared Esternali - UNCTITINOT belanostitedheesi IUNCTITINOT, silette 2001
name: a should be declared esternal (
<ul> <li>- EMCTRIPHONE (Annual ) IEEECTIFACET, and at an internal control of the second of the s</li></ul>
- 0011012010001 (100011010000) (00110000) (00110000)
talamidil(virti550) sharid()an declarad anternal; (0077957acm).talamid()(virti550) 10073155acm).ar/002520.25001
perentificate(200) should be destarted entertails
<ul> <li>INCTODENT Jone Winder (2010) 1180 CED (2010) 2010(1) 2010(1) petagenerged (2010) 2011 (should be declared external);</li> </ul>
<ul> <li>International contraction of the second contract of the</li></ul>
<pre>tampproved():111address.pddress) stop11 be declared external:</pre>
approver, appress, and the second be delivered asterner.
<ul> <li>Obl VST access aggregated addition a control (1) 0000 VST access and 00000 -00000) antigger scaling addition a check at the decision accessed a</li> </ul>
<ul> <li>INCIDE/Secret-setApproval/EntAll(address Janel) (INCIDESacpt setERED); 2001)</li> </ul>
Example Print address under statistic statistic statistics and statistics - SPETER and Example Statistics - SPETER and Example Statistics - SPETER STATISTICS - SPECE - SPE
autoreauto
<ul> <li>INCTED/NOTLasfetYon/Activity address (address (addres</li></ul>
March Syntherromotophic analysed its contracts with its detectors), 475 resulting found
infinition and signal system in the second to additional detectors and signal integration

# Slither log >> GemFacet.sol

1971 (Berlet Kerst
Control & Marchant for Constant for Solidary (1) (Conformation 2010) Solidary States (2010) Solidary (2010) CONTROL (2020) 33 - address (Control Control Control Control Control Control (2010) 2010)
COMULE_ACOMESE = address 1 Interested/docomenocodecomenocodecoment/Content (Content and Content (Content (Co
terforment: https://opithub.com/crytil/v/crbstretk//briefer-decumentation/ter-depite
<pre>tedeostictlocit.address) should be declared external;</pre>
regentry tion (or
<ul> <li>bandwardt Andrandturdises tart storti () (blam Honester, address) (bandwardt osf249808-2411) Innertiani) (blam Honester, stortiki) (blands ha das Lared arternal);</li> </ul>
boordead; doan her tar, concret, that's be deligred arts anternal.
<ul> <li>Gendlauert Josep Hand), Bolen, Booster (2010) (Gendlauert, 2010) (1000)</li> </ul>
talicities(stor)2001 should be declared esteroid)
<ul> <li>Gendrativi, Indu Grand (and 1981) [Bendrativit, and 60110-18120]</li> </ul>
checkbasheserdis intitlet checks de declared esteriol:
<ul> <li>destruct.cheiktautean(juut201) (destruct.a)(200-200)</li> <li>cheiktaperedtean(duut201) (heidel be declared esternal)</li> </ul>
Construction of the second sec
Jean Francy Construction and a second s
Contract of the second se
characterization and a second a second a second second and a second se
<ul> <li>SamParet Charlement replaced inservation 2001 (SamParet, self40441, 2001)</li> </ul>
antipation (i address) should be declared artered.
<ul> <li>Construct - predombile (Assidences) (Construct-carbitete) 26(2) (</li> </ul>
antipeditor/watching address a with shadd be declared esterial.
<ul> <li>Construction and the statement address and the statement and statement an</li></ul>
Reference: Mitge Unit Bab, concervinity) the relativistic to decomparizations with the transition - and the termination -
Description resolution and produced the contracts with Th detectory), 462 (soughting found
INFERING EDuction intercoverse is not present to additional delegtors and dithab integration

This, is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of Etherladianity.

Email: audit@EtherAuthority.io

# Slither log >> GemGettersFacet.sol



# Slither log >> NodeLimiterFacet.sol

INTERPORTATION CONTRACTOR OF C
frages service to be tracked, and the service to the recent to be tracked. Consider deglaying with 0.5.52
DATA AND A REAL PROPERTY AND A
andar itali da wata yana manakali itan digilagan yi Kafarandari iti kana Appilikala angeriyi kafala Abai peli tafatan bar dan ameriati kasti san yanta wata sala alahiyi
The basis of the second s
contenent call, or calificanced, writial conframendout address Joynes' reside, active Paper, solwers-ettl:
<ul> <li>destinent.acces) =witLikiegetycali()_sidLikta() diedet.witecttacyt.aple()()</li> </ul>
terforgenze i littgen zvig ritedu snijvznyt isznifistherselik szterbezten iteratuentat sentise-benet -iailta
THE REPORT OF THE PARTY OF THE
<pre>/srumster ( 00/unund.setContractOurs ( address), reademer (mode, briteriscet, so(d1)4) is not in elsedians /srumster ( 00/unund.diamondist())) is not in elsedia.</pre>
Personation 1, Obtained diamond attained at Acceleration [
the sector is followered strategies described (as strategies) and the sector faces and the sector faces and the strategies of the sector faces and the secto
harameter L 001ament additions address Apres (2). Jacribblings (Medic Interfacet, 1918273) is rest in misediana
For another 1. GBC annest Lability of Camerical Break, Append (1). Parent Labolatorian (Bandel Griter Camerican) (Annest Labolatorian) (An
An another & G2 Langerd - Spillar Planci and and server Apple of 1. See Cardon Sectors ( Model, and an Papel and S201) or not to manuface
the matter is different construction of information for the first state of the stat
Har sector's DDD amond -resoverance intel address digites (1). "And Canterbacters I Made, interfaced address to the Mined Cane Farameter & DD amond -resoverance intel address digites (, "agetAddress (Mode, Interfaced, address) is not in mixed Cane
Termitter L (Disaming removery) on address (Artest), "Articless (Mode LatterTace), address 1 a rol (a standism
Haramater ( 001amond resovations) includings, (Start), Tarbetter (Made, Bitterfacet, Schwedt) in not in misediage Haramater ( 001amond, Initial/petiamondist/address_bytes), shit (Made, Bitterfacet, Schwedt) in not in misediage
termeter & Detamined initial continential address between Continue Content action for the second and the second second and the second
Parameter 1, Deltament and an anter electron tractional address (attrict), producer (Redel Sectoritan to address). In our in attaching a
the units i defended and extended and each of the set o
Heremeter Houle Griterians, adding to be address . readdings ( hous interface) and the result of missing as
An Personal Children //gittlab.com/crytic/st/station/witic/bitan/sir documentation/surfacements for ball of thy maning conventuums 1970 Decisions
transfert beit Laderes attrans. sint 200 shardd be deitared esteratio
<ul> <li>Rode: Sector/acet. transfert.ta(tradiness.eddress.eddress.etc1204) (Rode: LetterPacet.es/P011-024)</li> </ul>
References in the constraint and constraint. One was constrained and added to share the constraint entering.
Invests):therinade.initerinate.nel analyzed of contracts with TS detectorib. We resulting found
INFOLDIBUILDING AND A

# Slither log >> OwnerFacet.sol

<pre>Definitions() Prophetics() Prophetics().0.4 (Demonstration).0.6(0) necessifiation a veryion too recent to be trusted. Consider deploying with 0.6.1270.7.0 Index.4.12.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.0.</pre>
Development and the set Less Development and the Link Landership ()
Persenter : Softwaren interverieren (editeren (editeren (
<pre>Partments: Derectors:</pre>

This is a private and confidential document. He part of this document should be disclosed to third party without price onitian permission of Etherlatherity.

Email: audit@EtherAuthority.io

# Slither log >> OwnershipFacet.sol

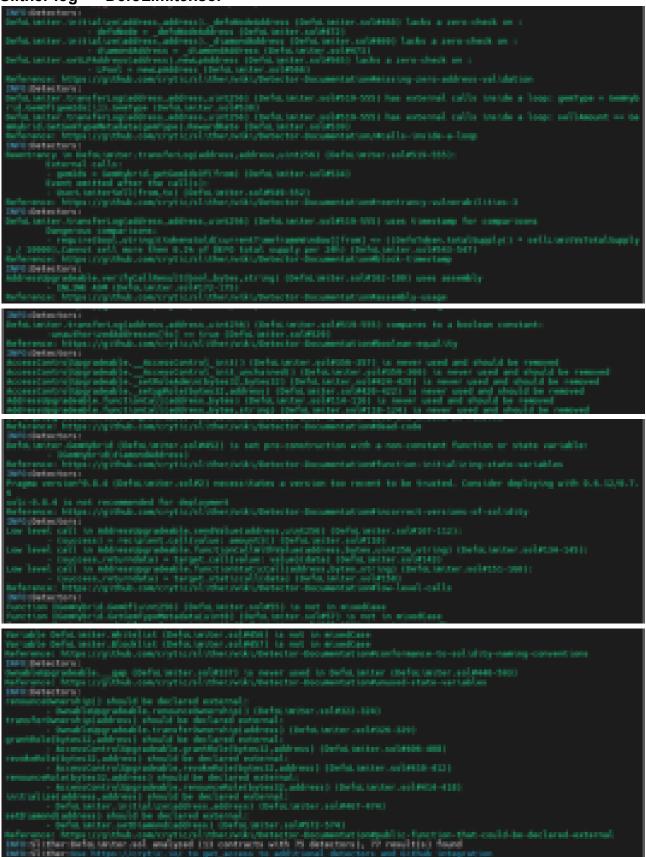
(add statement of Lanced Statement () ( Descende by Facet, ser (MS2-75)) uses assembly ( 300 Facet ( 100 ASN ( Statement of Asia) 201)	
<ul> <li>L BD Lawred on Forcesta Contract Code (address, string) (Devery high set, sch 500 (DB)) uses assessing - 20, 201 ADM (Devery high set address) (DD)</li> <li>Reference: https://withdo.com/continues/high sets/bir/bir/bir/bir/bir/bir/bir/bir/bir/bir</li></ul>	
The fore secure is the property of the second secon	
nalls (k. K. A. (n. 1994), recommended for deployment forfaces of https://www.internet.com/orgenics/file/internet/com/orgenics/file/internet/com/org/file/internet/com/orgenics/file/in	
Note that an analysis is a second of the	

# Slither log >> VaultStakingFacet.sol

1870 Sector Sector Sector Sector State (Splanet, Sector Sector) and a sector (Splanet, Sector
<ul> <li>Des Def wird straid implie en and De-200</li> <li>Sidder XII - Filmenditie regel ( ) The Difference ( and Filmen - 2004) unen annendity</li> </ul>
<ul> <li>THE THE WHAT CONSTRUCTED AND ADDRESS AND ADDRESS ADDR ADDRESS ADDRESS ADD</li></ul>
<ul> <li>- Statistical Control of the second control of the se</li></ul>
- De Del acte (veu) total ingitie et columnia ingitie et al.
In the sector sector sector and the sector sec
COMMENTAL SPECIFICATION (C) (C) and EXCAR INSTITUTES, and EXCARDED LARGES AND
The same show the second state of the second s
COMPACE_INTERPOLITION applies [ ] [ March 2010 Gale (Compact Compact Compac
Closes Algenorith to report (CrossContraction Contraction Contraction Contraction)
<ul> <li>Bit Die Wild (Stack Stack September, Self-1997)</li> <li>Stander Standersbergerigt (Stack September, Self-1997)</li> <li>Bit Die Wild (Stack September, Sent) (Stack S</li></ul>
the foreverse a life type of a principal sector of the sector decommental transmission and a sector of the sector
TRADE Detectors: Frages version/0.0.4 (raultituking/scot.self() reconstitutes a version too recent to be trusted, consider deploying with 0.0.22
20, 7.8 solg-4.4.4 is not recommended for dealparent
deference: Ditge://githds.com/crytic/sl/the/wiki/detector/decommentstices/sect/vers/arm-of/sel/thig Infiniteset Contract constants (Saultitation/sectorsl/thigt) is not in Capitoria
An environ - Cold 2011 - And Andrew Cold Andrews, address, a bet 2011, bytes (
The number 1 (BARTEL And ANDER DECEMBED (Address, address, address, address, address, address), from (Nav2011addreptacet.address) is not to addred/and
Parameter 1 (0000721.checkbed000000000000000000000000000000000000
<pre>isinfarts(bit()): chark(shin()): thereised(address,address,sint): (chark(s), chark(s): (chark(s)): (chark(s))</pre>
Parameter Yestillation/acet.hebbaad/organics.iet104[].cort104[]set104[]set204.10a/00144/opfacet.es145123] is not to minedCase Parameter YestIllation/acet.hebbaad/organics.iet104[].cort104[]megets[]Baa/00144/opfacet.es145123] is not to minedCase
An employ tradition options, balanded transformed the set 200 (1set 200 (1
Constall of Enterthemeters to the state of the Advanced State of State and State and State 1997 (1997) and the state of
1 N - 1 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2 2
<pre>choittakedhooyxt11 doolad be declared enternal:</pre>
Individual Venezia and a second of the second of the second
This is a private and confidential document. He part of this document should

ise disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

# Slither log >> DefoLimiter.sol



This is a private and confidential document. He part of this document should its fluctuated to third party without prior oritize permission of Ethaniatherity. Email: audit@EtherAuthority.io

# **Solidity Static Analysis**

# DefoErc20.sol

Security

# Check-effects-interaction

Personal Weldone of Cheeks (Places American pattern in)

Anthena the entroined at Mithal and the rest of the set of the set

100.024.4

# Gas & Economy

### Gan costan

East respectment of function Detainment Los Detains in infester this gas respectment of a function in higher that the block ges innit, it cannot be executed. These event locate in ever functions an advaluation that modify large ensus of storage this includes clearing or copying amers at storage. Here, 2303-4.

# Modellameours

# Constant/View/Pure functions:

Epithenegettedier(): Potentially should be constant. An exclusion but is not. None Meditiens are iterative test considered by the static products.

100

Not 21099-4

### Similar variable names:

Elympic Die Berner ander berner der Berner ander State in Verstabilitet besone einer primitiget besonen, "anzenend" and in "Samergent" Martinak Mathema and roomentige met consistentiet big their at state versals of the second state of the second

# Guard conditions:

Upon Passion (2) (2) (1) prior responses according to the factory rest intrarry Architecture to prove the target of a provided length of a factory personnel.

Non 334418

# Data truncated:

Desiring of integer volume and its an integer value again. That means e.g. 10.7 100 + 0 integer agains the relation of control literal volume theory literal volume theory and relation of control literal volume theory and the second s

This is a private and confidential document, the part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

user some sector sound in the

# DefoLimiter.sol

Security

### Check-effects-interaction:

Personal values of Cherge Units Americation patient of 1 Debit extention considering address and 2500 Court extentially loss to be entrance extendability flate Muddless are consetty our considered by this status analysis.

Phil 272.4

## Gas & Economy

### Gan costs:

Use requirement of Quectors Detrict molect add/Ambrand to to here if the gast requirement of a function to higher their the black gast limit, it commut be precised. Please award to point user functions or actions that modify large areas of storage (this functions clearing to contribute an increase) - Storage

# For loop over dynamic array:

Lisspe that do not have a fixed solution of detailors, for example, losses that paperal in the lange values, have to be used confide. Due to the back gas level, the second to be block yes list arrange errors of a gas. The reaction of the short on a loss can grow beyond the block yes list which can cause the transfer to contract to be stabled at a birtary sales, Additionally, using and on the second to be brocked at a week date gas methy. Cambaby test have many denies at tractman who are paint to use a freedom for make it successful.

Abar Malain

# Mitchillamonus

### Constant/View/Pure functions:

IT HERE Distances in Proceeding and the second state of the state strategies.

Pes 875 4

# Similar variable names:

According to the second description of the second distribution of the second se

### No return:

III PR. 20 Argument your participant, adult associed 2500; Defining a return type that have a separatly returns a second 2500.

Twis is a private and confidential document, the part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

their sound characteristics

Uper Canonettra P. (Construction over weath a to be failure, not in any construction of instart from a page or while control. Under Versionship: of sizers the failure, close to do instantial result for a failing instartion and any page of

Pos. STTAL

#### Data truncated:

Description of remight estimate yields an interpret solice again. That research is go 10.1 1000 - U restand of 0.1. Second the result is an orthogen again. This from not beret for Homory of hereigt liberal balance show places provid patternel correlates.

Pbs 399(21)

# Diamond.sol

### Security

#### Inline assembly:

The Contrast as an initial assembly, this is unly allothed in risk insure. Additionally about analytic insultant to early advance of the Automobile this can be at to early an example best to a

North Date in

#### Gan & Economy

#### Gas costs:

Fallback Deschars of contract Dearbord requires his inside gas definited. If the fallback function requires more they 2000 gas, the contract connect receive Difest. Post 401 m.

### For loop over dynamic array:

Longers that the next have a franch reactions of Renations, Bar examples, Income that there is considered on managers replaces have to be used contribute. Does to the beings gas locat, thereas there between extremes a certain arrented of gas, The mantpart of remaining is a locat can grow beyond the brack past lenk which can consider the complete contract to be statistically a certain poors. Additionally, using antenanded locate the complete contract to be statistically a certain poors. Additionally, using whether are point to were in a loc of available in statistical.

2010 2020 10

#### Modellaneous

## Constant/View/Pure functions

LEConverte and an and the Converte statistic device an important to a constant but an interfacts about that the

- Plan 1970 1

This is a private and confidential document, its part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

user some strengthered and the

User Taxonerstal füll jong menne anne wordt is to the failer, put in later constraints to passet from a bag in a net control, biter "amouteen fait a can be taking their to stig, immittel legest or a failing external startsponent.

Aug 4303.00

# Delete from dynamic array:

Uning "stelets" on an array basis a gen. The weigh of the array toward the parts. If you want to a strong the sength matter of a state with the strong to an array basis of the strong to a strong to

Post Light

# DiamondInit.sol

#### Security

### Low level calls:

Use of "changeter alth the deltary contract and set of efforts the caller's balleron. If this is exertical induced in the calleron of the call

Anna 100 Mill

# Gar & Economy

# For loop over dynamic array;

Length that during have a fixed mention of iterations, for an excepted tone that departs on attracts a voluent toke to be eased coordinate to the book up to the providence of a top of the book gas tend instant, annound to paul. The transform of foundations is a long cart provided the block gas tend which can course the correspond contours to be shalled at a contain provid Additional (a using unboarded to transform is a lat of providence to part them. Constant, provided the block of many provided to say any second to a lat of providence and contain the base heavy Additional of many provided to such flashing to track a source to be the second by too have heavy Additional of many provided to such flashing to track a source to be the second by too the second by the second tender of the second by the second tenders of the second by provided to such flashing to track a source to be the second by the second by the second second by the second by the second by the second second by the second by the second second second by the second by the second second second second second second by the second secon

Personal

# Mecallanobus

# Constant/View/Pure functions:

LabOlamord and and an annial College & sound reading a la constant but assertiatly about include the second second reading and the second second reading and the second seco

No.4CH

This is a private and confidential document, its part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

their solution crusters and the

User "annumited" if you response seems sound a far the ballon, and he may termenutarity (appart front a barg or when childed, Units "remain whet if a case has have to only meaned input or a failing external sirtaninett.

No. ASSAULT

### Delete from dynamic array:

Using "cheers" on an array tenners a gas. The largest of the array remains the same. If you can't toterrorys. The singly possible, year seatt to phill merci manually and spdate the "langth" property

Res 1000 001

# LpManager.sol

### Security.

#### Block timestamp

"This of "block from the we's "black dynamical and " have be nethernized by menors to a contact degree. That means that a reveal care arrange the black investance is a carlast degree. To change the meters a transaction is the mined block.

Per 246812

# Gas & Economy

#### Gau costa:

The improvement of transform ( phases per period all labora is instantial if the part requirement of a forements may set than the block gas invel, it convert he executed. Plasse avoid larger in your furthers or accore that muddly large areas of storage drive instation cleaning or converg areas at PERSONAL PROPERTY.

Fee 25284

### RC.

```
ERC20
```

ERC20 contract a "decimals" foregan analyticase "seatt" as retaris was

Press 222 4

### Mooillaneoux

# Similar variable names:

LaManager suffer() : Venallies have been semilar surnes "beendlat" and "cleard?", fone Monthers and charpenetty into increasing the time starm, analysis, Per 241912

> This is a private and confidential document. He part of this document should its flucinsed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

Use "emertips" if your board over water a follow fides, not its any containstained legart from a long in your studet. Use "Versainsing" if a can be false, the to ap, its old legart or a falling external. complete it.

Des 24388

# Data truncated:

Characteristic strategies and any problem are antisper walker again. These measures way, 107/100 - Concerned of 0.1 precise the measure is an integer again. This characteristic for advances of particle biancel values, are an Oncor Websi concerns is precised.

Ples 281322

### Redeem.sol

#### Security

#### Block timestang:

Use of "block treestares" "block treestares" can be ediamized by movers to a certain degree. That is instant that a treestare we between the block treestares, to a certain degree, to block the second secon

Post 2345-346

# Gas & Ecohorwy

## Gas costs:

Get requirement of function fields in a United Address is infrated if the gat requirement of a function is bigher than the MACK gas limits of correct its constant. Plants avoid langes in an enfunction actions that readily large areas of starage (this included classing to converg adays of staraget flars 2247.4

Miscellaneous

#### Constant/View/Pure functions:

ICPICATES metApproval in All address benet: Platermailer should be constant, we when is had to not. Note: Modifiers are consetly not competened by this static analysis.

Non 10484

### Guard conditions:

User Passertipe Fill enterenter soner warette be be fadere, best in any conservations in passet from a large en whet compt, the Passateria, " if a cars he fatere from the sole in a game addition and a failing enterest. companies.

Dog 211944

Twis is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity, Email: audit d/EtherAuthority.io

their sound structure and the

### DiamondCutFacet.sol

#### Security

#### Low level calls:

Use of Passageterall's mould be availed whenever providing Constant case, that is defed cart change the state of the calling contract and send other time the caller's behavior. If the is worked Inclusional tase the Schulte Used a feature if preside

Pres 222,439

### Gas & Exphony

#### Gas costs:

Casi remainstrated of Nations Discourses that facing discours Cast is indices. If the gas remainstrated of a Reactant is higher than the library gas ideal, it cannot be incruded. Please event longs in your Advertising including that residely large attack of stations this includes clearing or conjung where in dat most

For this is

#### For loop over dynamic array.

Loopis that divisit have a fived exercise of detailors, for example, loops that depend to statupe values. Nave to be used sampled p. Due to the block gas limit, transactions can use formulate a instant arrestet of gas. The riseber of detabory is a long cart grow beyond the black gas bird which can cause the consciete constant to be statled at a seriar pairs. Additionally, using artimumbed longs involus in a lot of autoblatic gas costs. Cambridge last how many darps all mu NEW CONTRACT TO MARK REACTIONS IN MARKE & STATESTICS.

Plan Street

#### Miscellamenus

#### Constant/View/Pure functions:

Lationensie foreities and and and alter and a strong of a constant but passettially should not be and the second

#### Guard conditions

Dies "Antestick?" Hyper means wear ward a to be false, but in any incompletes parent from a burg in proof country. Units "responsespon" of a class bas balance other to may recepted insect on a factoring accounted and the party of the local division of the l

Boord 200

#### Delete from dynamic array:

Using "deleter" on an array laster as pay. The langth of the array measure the series if you word to series we the senarty predice you must be shall been invested by and tabilite the "toroght" proceeds.

Post III I

This is a private and confidential document. He part of this document should its flucinsed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

### DiamondLoupeFacet.sol

## Security

#### Inline assembly:

The Contract sums when assumpting this provident in our parent Additionally manifester and the Permittee on the last as we were Assumpting the care being to write generate the results.

Pass 42018

### Gan & Economy

### Gas costs:

Ges requirements of futures of Discontinuous data and the state of the second second second of a function of the part theory from the block and invested to second and the second second begins to provide the function of actions that muchly large areas of storage title second second provides are storying arrays in storage).

Res Cittain

### For loop over dynamic array:

Linger: that do not have a fixed reaction of testations. As weareds, fixed that the stating where, have to be say it and to be the fixed to be block and joint. The exception field depend on stating to fact an array of the part of the terminant of the block and joint. The exception that depend on stating which can prove the constants of the terminant to be station over prove theory of the block pas limit. A schedule the part of the constants of a second date gas point. Constants have they were been block to be the terminant articles of the terminants of a lost of available gas points. Constantly lead have many there at the terminant terminants in a lost of available gas points. Constantly lead have many there at the terminant terminants to week flatentiates to the terminants.

Page 3333 mil

#### Missellaneeds

# Constant/View/Pure functions:

Discound mapsificant suggestioners (by teach) its constant that potentially should not be

No. ett. -

#### Guard conditions:

Uses "according of these second ever would a to be follow, not be any estimated according to be a failed in which cannot a black because to the follow the follow should reput for a failing determal strategement.

Post of This

ACCURATE AND

#### Delete from dynamic array:

Lising "delets" en an error leven a gas. The length of the arrive measure the same if you want to remove the scorety produce you need to staff more metally and applets the "length" anamets Res 350 ft

> This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity, Email: audit d/EtherAuthority.io

their sound structure structure.

### ERC721Enumerable.sol

Security

#### intine assembly:

The Contract asian allow appendix, this is only advised to non-tables. Ackingments states analysis recolution its rest partic filling Assembly line call land to wrong analyze results.

Des: 2003-0

PROFESSION .

# Low level calls:

Dat of "delegaterall" stant the eventset element providing Talental code that is salled two sharings the state of the sallary consider and send other from the salar's belance. If this is worthat Interesting the through langer through the

Port 2045-89

#### Gas & Economy

#### Gan costs

Uas regulationed of function ERC/210 nomeration workloker/POwnerHybers is articles if the year requirement of a function is higher than the block gas time, it cannot be executed. Please avoid locars in your functions, or activity that modify large prose, of storage this induction couring or Engrand deliary in Manager

Pin Dilling

### For loop over dynamic array:

Loops that do not have a fired particul of Astalians, he examples light flat depart on storage ordaes, there to be used carefully. Due to the total gas level, three-activity that only consistents a centate amount of gas. The member of Residums in a long can provide second the Most gas Lourd which can cause the complete contract to be piplied at a contact point. Additionally using undekended loops incars in a lot of evoluble gas tosts. Carefully test new many kerns at teaciment and the president of the state Sec.

No. 1549

#### Minnellartebur.

# Constant/View/Pure functions:

THEFT I I manual distribution of the transformed by the terminant of the partner that partner that partner that the standard part loss

Rep. 27104

#### Similar variable names:

LIGERCHI 1. It ansherladdmin.arkitems.ares/5411. Variables have very service tranes. "Do" and "ha" Press and a state of the

> This is a private and confidential document. He part of this document should its flucinsed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

Was "paparticle" if you reave must want a to be false, not as any circlantifance (papart from a bog in which controls to be required as the final on the state of a standard report on a factory conternor. distances of the

No. Intellig

# Delete from dynamic array:

Change "denoted on any array Assess in pain. The Langth of the entary memory the party. If pice exact ha metable the ampty product you must to shall have a marked a well applyin the "langin" despects. Per 2001.0

# ERC721Facet.sol

# internet to

#### Check-effects-interaction:

Principal sedators of Overlag USects Attention pattern re-

Address Information and With Waterlandsheets Barters and 2000 attended to the wettancy APPRILATE AND

FOR SEVILA

# intine assembly:

The Contract uses index amongship this is only advance in tare taxed. Address ally static stations mucholain the next marine infiner Alternamy two cars liked to accord undersity to be attain

Des 1960.10

### Low level calls:

the of "delegatorial") month the elected whereave provides. Laterial code, that is called care whange die state of the calling contract and antil efter from the maler's talares. If the is waited bettervistati une the Schillty Useara feature il provible.

Inc. 19350-541

### Gas & Economy

# Gas costs:

Gas parameters of function EHCR21P scattering in whethis II the gas report work of a function in higher that the low's gas lines, it served he executed. These event hears in your functions or actions that weathy large even of charges (In-sections in copying enough it stanget) Place Street, A.

> This is a private and confidential document. No part of this document should its flucinsed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

# Constant/View/Pure functions:

ERC721Facet.symbol() : is constant but potentially should not be more Pos: 3016:4:

#### Guard conditions:

Live Passentijs (\* it provinces avvertigent of to include, not bit any conservation of (assert front) a bag in privat couter, take Democratication a constant state, short to explore and input on a failing insternal constant particular.

STREET, STREET, STREET, ST

Post HIRDS

### GemFacet.sol

Security

#### Block timestamp:

Uper of "Devick (presentancy)" "Devick (presentancy)" can be exhibited by measuring a context degree. Then measure that a measure uper "strokes" the black (presentancy), to a contain degree, he change the batterne is a transaction in the measure block.

Apr anal 20.

2020

#### Gan & Economy

# Gas costs:

Care requirements of Automatic General acts: Planmann Made to infrares: If the gast requirements of a hospital ininglest than the black gast local, is correct for executed. Denote proof local in providents or in turns that readily large arount of abbraught (the installes closeling on topologi arrays, in the upper Place 2001, Au

# For loop over dynamic array:

Langes that do not have a fixed mention of Bandoms, for asserting, forms that depend on changes where, have no be exect constanting. Due to the topic lique term, topicarters cart and compositions a ention is any contract of gat. The mention of Bandom by a lique cart grow topicart the black gas term which care contract the standards compared to be trained at a contract point. Additionalist units arbounded broom from the standards of exceeded parts from Constants from these many there is a provided broom from the standards of exceeded parts from Constants from these many there is a standard process of the standards to reach the standard parts of the standard from these many there is a standard part cart parts to much functions to reach it contains the standard from the standard barry is to react the standard form

Page 22215-00

10.000

Hocetta records

This is a private and confidential document, its part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

# Constant/View/Pure functions:

General and provide the second development of the second s

FOR HER I H

# Similar variable names:

Community of Committee Converting and Committee Converting by the static seation.

#### Guard conditions:

Line "accerting" if you have ever want a to be faine, out to any victor starts in part from a tag in War states, the "responsing" if a core we faine must be approvaled report or a failing external continues.

Pos 2011.0

### Data truncated:

Unclaimented being arresolated preside and being arrested against their investiging and / 5000 = 0 interview of 0.1. presentive treasts in an interpret agains. There does not being the interview of investiging the interview of the set of the

Proc. 30107 (20)

### GemGettersFacet.sol

# Security

#### Infine assembly:

The Contract case intro-assembly, the totely extrined in being analysis insuffy shalls into any site of the case into a second to writing analysis insuffy.

Pour Different

#### Gas & Economy

#### Gas costs:

Gas requirements of function Cetteral acet. Level is informed in the perimutation of a function in higher than the block per level, it cornel be concluded. Plance devid longer is pass functions or withing that mostly large areas of stanger this includes classing or cooring strays is storaged Free 372-4.

## Mitcillamonus

# Constant/View/Pure functions:

1800er sharreneffiturageij i is immitare but setterthelig efseldt not ten

Berthe

Twis is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity, Email: audit d/EtherAuthority.io

terr some far the second second second

Constant/View/Pure functions-

Gatteria and goldenia - Is intestant but generative deaded out her

2723 Post 1981 4

# Guard conditions:

Une "annalitiet" of your burdet and t ward a top be fieldet, and in any presentational parall front a burg or preservations that the parameter of a carrier fallow man for a jumph of a part of a family estimated - TANKAR

Pbg 264.8

# NodeLimiterFacet.sol

#### Security

# inline assembly:

The Contract issue inline advertise this is into advised in ture cause. Another alle each constraint insides its not pares inten According this part and to wrong analysis results.

Here 500 H

#### Gas & Economy

#### Gan coets:

Care remainsment of takenum Readed and and and add Taket address is independent of the gas responses of a function to higher their the black per limit. It cannot be wentered. Prove sound imposite your functions or actions that modify large amail of shinkept this includes inserting or coanting amain inabbraget.

Res 605

#### For loop over dynamic array:

Licens that do not have a fixed rounder of Penaltons, for examples, incom that depend on charage values, have to be used constally. Due to the black gas treat, to reactions out only compare a contract or exactly of gals. The regardler of iterations is a long can grow beyond the block per limit which can be used the complete contract to be statised at a collars point. Additionally, teams ardyounded inside invariant of a last of avoidably gas conto. Carofully heat force many know or many your the place to much functions to make a marmeral.

Per saute

#### Miscellanetes

#### Similar variable names:

Name in the Fact manufact in all and we wild manufact 2013 (Varialities have very module names "do" and "to", None Modifiers are currently het considered by the state assigns. Per 616.8

> This is a private and confidential document. He part of this document should its fluctuated to third party without price written permission of Ethanialization by Email: audit@EtherAuthority.io

Use "asserting" if you have send want want is to be false, out in any circulations based from a long in your corps. Use "respecteds" if a can be false, the to also movid rank of a falling enternal warpathe.

Pes Siniz

# Delate from dynamic array:

Using "density" are not array known in gain. The langth of the array contacts the series of you count to move the array is produced and read to shall dones manually and update the "array of descents."

Fby 523.0

# OwnerFacet.sol

# Security

### Intine assembly:

The Contract source where accountly, this is only advised receive taxant Additionedly matic analysis moderns do not same where Accountly, this tax lead to wrong analysis meets.

R 200

# Gas & Economy

### Gas costs:

Hist requirement of Astrono OwnerParet, Milatian is informed the gas requirement of a function in Softer that the block gas liver, it correct for excluded. Flowers avoid longs is prior functions as in turns that include large serves of storage (the instantic closeng or controls) and is not aga; For 222-1

### Miscellaneous

# Constant/View/Pure functions:

Deman Farmer, meta produce Arthresson and dresson in Protocollarity schedule in a construction or approximation in the Construction of the International Society and the International Society and Soc

And the state of t

### Guant conditions:

Use Passertport Plans enverance marries have be failed, not in several constance passet from a long or some scores. Use frequenties of a contine failer through mound report on a failing enternal correspondent.

Post 7141

This is a private and confidential document. He part of this document should be disclosed to third party without price written permission of Ethenlatherity. Email: audit@EtherAuthority.io

# Delete from dynamic array:

Upping "defects" and all entrop becomes in page. The brength of the barrier incontant the Service II provident to an entropy of the shart iteration and leaders the "foreignt" provems

### OwnershipFacet.sol

### Security

#### Inline assembly:

The Contract uses intre-momentally, this is into extrined in ours taxes. Additionally make and you make and you make an analysis.

File SEA

# Gas & Economy

### Ges costs

Car requirement of Ariston Ownerstated and Developments Concepting to advance if the gas requirement of

- Interchant is higher than the block gas limit it period be executed. Please and begin in your.
   Interchant is without that mustify large amount of atomical block includes clausing or copying ensure at atomical
- For 2014

#### Miscellaneous

# Constant/View/Pure functions:

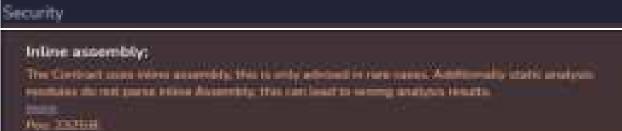
Converting Count Inverset # . Is constant hat preservingly glowed net be-

Fibs. #00.4

#### Guard conditions:

Uses "another the fit of a multiple of the same best when the best failure, not in a multiple of the failure in the same of the failure of of th

### VaultStakingFacet.sol



This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

under weden die Freesenderen und seine

# Ges & Economy

## Gas costs:

Ges remains and the second Vasibilitating factor betchvill finness is a dense. If the gas requests of a function is been and the book gas level, it there exercised. Places second being on poor benchmen an action that readily large areas of stations this instacted clearing or conving arises in more gas.

Res. 23464

#### For loop over dynamic array:

Lations that the text have a first manifest of iterations. An exemption forms that there due attaining values, have to be used coordially. Then to the tatest gas limit, transactions can only contains a contain errorated of gals. The number of iterations is a local can grow beyond the tooks gas limit which can could the complete constants to be coulded at a contain prove. Additionally, thing arthourselve have been by a local of available gas costs, Cambala test have many items at stacement yes can point to each functions to make it southered.

Phil.2356(B)

### Micoellaneoge

# Constant/View/Pure functions:

Vaultiliating/acet showStatedArsnurt(): Is constant to A polandadly visual ration. How Holdhars and connectly rule screakers: by this status analytics.

STREET, .....

PERSONAL AU

# Similar variable names:

Month Sale and Area to a second and the second of the second second

### Guard conditions:

Une Concerting of it was rever ever locarity to be follow, not be any addated around from a begin was control. Che Pressent of all a care be follow that to age revelating of a solaring determal mangament.

Non-Jackson

A COLUMN TWO IS NOT

#### Data truncated:

Environ of relarger values yields an integer value agains. Fruit means a.g. 10.4 100 - Dividual of 0.1 serves the install is set integer again. This lines not heat the illication of good (therei adaes sizes these yield related constants.

Postalascal

This is a private and confidential document, its part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

were working a running and still and

# **Solhint Linter**

# DefoErc20.sol

DefoErc20.sol:2:1: Error: Compiler version ^0.8.0 does not satisfy the r semver requirement DefoErc20.sol:59:28: Error: Avoid using low level calls. DefoErc20.sol:133:51: Error: Avoid using low level calls. DefoErc20.sol:209:17: Error: Avoid using inline assembly. It is acceptable only in rare cases DefoErc20.sol:221:1: Error: Contract name must be in CamelCase DefoErc20.sol:222:2: Error: Explicitly mark visibility of state DefoErc20.sol:227:3: Error: Avoid using inline assembly. It is acceptable only in rare cases DefoErc20.sol:227:3: Error: Avoid using inline assembly. It is acceptable only in rare cases DefoErc20.sol:229:8: Error: Variable "r" is unused DefoErc20.sol:2179:24: Error: Code contains empty blocks DefoErc20.sol:2236:5: Error: Explicitly mark visibility in function (Set ignoreConstructors to true if using solidity >=0.7.0) DefoErc20.sol:2374:5: Error: Variable name must be in mixedCase DefoErc20.sol:2377:5: Error: Explicitly mark visibility in function (Set ignoreConstructors to true if using solidity >=0.7.0)

# DefoLimiter.sol

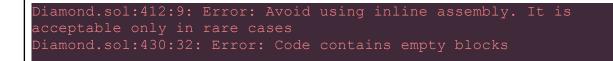
DefoLimiter.sol:889:33: Error: Parse error: mismatched input '('
expecting {';', '='}
DefoLimiter.sol:889:54: Error: Parse error: extraneous input ')'
expecting {';', '='}
DefoLimiter.sol:984:46: Error: Parse error: mismatched input '('
expecting {';', '='}

# Diamond.sol

```
Diamond.sol:2:1: Error: Compiler version ^0.8.0 does not satisfy the
r semver requirement
Diamond.sol:42:5: Error: Explicitly mark visibility of state
Diamond.sol:76:9: Error: Avoid using inline assembly. It is
acceptable only in rare cases
Diamond.sol:358:50: Error: Avoid using low level calls.
Diamond.sol:375:9: Error: Avoid using inline assembly. It is
acceptable only in rare cases
Diamond.sol:384:5: Error: Explicitly mark visibility in function (Set
ignoreConstructors to true if using solidity >=0.7.0)
Diamond.sol:401:5: Error: Fallback function must be simple
Diamond.sol:405:9: Error: Avoid using inline assembly. It is
```

This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Etherlatherity. Email: audit@EtherAuthority.io

Date water the consideration of the



# DiamondInit.sol

DiamondInit.sol:2:1: Error: Compiler version ^0.8.4 does not satisfy the r semver requirement DiamondInit.sol:114:5: Error: Explicitly mark visibility of state DiamondInit.sol:148:9: Error: Avoid using inline assembly. It is acceptable only in rare cases DiamondInit.sol:430:50: Error: Avoid using low level calls. DiamondInit.sol:447:9: Error: Avoid using inline assembly. It is acceptable only in rare cases

### LpManager.sol

LpManager.sol:2418:18: Error: Parse error: missing ';' at '{' LpManager.sol:2425:18: Error: Parse error: missing ';' at '{' LpManager.sol:2447:18: Error: Parse error: missing ';' at '{'

### Redeem.sol

```
Redeem.sol:12:18: Error: Parse error: missing ';' at '{'
Redeem.sol:25:18: Error: Parse error: missing ';' at '{'
Redeem.sol:37:18: Error: Parse error: missing ';' at '{'
Redeem.sol:54:18: Error: Parse error: missing ';' at '{'
Redeem.sol:66:18: Error: Parse error: missing ';' at '{'
Redeem.sol:162:18: Error: Parse error: missing ';' at '{'
Redeem.sol:185:18: Error: Parse error: missing ';' at '{'
Redeem.sol:185:18: Error: Parse error: missing ';' at '{'
```

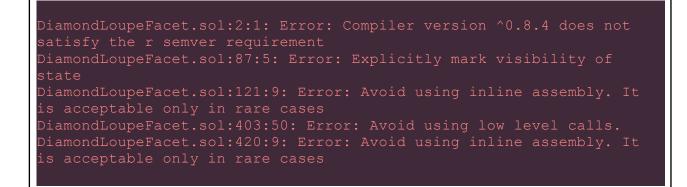
# DiamondCutFacet.sol

DiamondCutFacet.sol:2:1: Error: Compiler version ^0.8.4 does not satisfy the r semver requirement DiamondCutFacet.sol:39:5: Error: Explicitly mark visibility of state DiamondCutFacet.sol:73:9: Error: Avoid using inline assembly. It is acceptable only in rare cases DiamondCutFacet.sol:355:50: Error: Avoid using low level calls. DiamondCutFacet.sol:372:9: Error: Avoid using inline assembly. It is acceptable only in rare cases

# DiamondLoupeFacet.sol

Two, is a private and confidential document, he part of this document should be disclosed to third party without prior written permission of Ethenlatherity, Email: audit@EtherAuthority.io

CHELE ROLLING CONTRACTOR CONTRACTOR



## ERC721Enumerable.sol

ERC721Enumerable.sol:3:1: Error: Compiler version ^0.8.4 does not satisfy the r semver requirement ERC721Enumerable.sol:191:1: Error: Contract name must be in CamelCase ERC721Enumerable.sol:192:2: Error: Explicitly mark visibility of state ERC721Enumerable.sol:197:3: Error: Avoid using inline assembly. It is ERC721Enumerable.sol:199:8: Error: Variable "r" is unused ERC721Enumerable.sol:1745:9: Error: Variable name must be in mixedCase ERC721Enumerable.sol:1762:9: Error: Avoid using inline assembly. It ERC721Enumerable.sol:1802:13: Error: Avoid using inline assembly. It is acceptable only in rare cases ERC721Enumerable.sol:1822:9: Error: Avoid using inline assembly. It ERC721Enumerable.sol:2106:16: Error: Code contains empty blocks ERC721Enumerable.sol:2139:9: Error: Avoid using inline assembly. It is acc

# ERC721Facet.sol

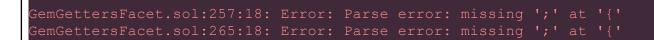
ERC721Facet.sol:2583:18: Error: Parse error: missing ';' at '{' ERC721Facet.sol:2591:18: Error: Parse error: missing ';' at '{'

### GemFacet.sol

GemFacet.sol:2398:18: Error: Parse error: missing ';' at '{' GemFacet.sol:2406:18: Error: Parse error: missing ';' at '{'

## GemGettersFacet.sol

Two, is a private and confidential document, he part of this document should be disclosed to third party without prior written permission of Ethenlatherity, Email: audit@EtherAuthority.io



# NodeLimiterFacet.sol

```
NodeLimiterFacet.sol:115:18: Error: Parse error: missing ';' at '{'
NodeLimiterFacet.sol:123:18: Error: Parse error: missing ';' at '{'
```

# OwnerFacet.sol

```
OwnerFacet.sol:230:18: Error: Parse error: missing ';' at '{'
OwnerFacet.sol:238:18: Error: Parse error: missing ';' at '{'
```

# **OwnershipFacet.sol**

OwnershipFacet.sol:2:1: Error: Compiler version ^0.8.4 does not satisfy the r semver requirement OwnershipFacet.sol:54:5: Error: Explicitly mark visibility of state OwnershipFacet.sol:88:9: Error: Avoid using inline assembly. It is acceptable only in rare cases OwnershipFacet.sol:370:50: Error: Avoid using low level calls. OwnershipFacet.sol:387:9: Error: Avoid using inline assembly. It is acceptable only in rare cases

# VaultStakingFacet.sol

VaultStakingFacet.sol:2054:18: Error: Parse error: missing ';' at '{' VaultStakingFacet.sol:2062:18: 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.

> Two, is a private and confidential document, he part of this document should be disclosed to third party without prior written permission of Etherlatherity, Email: audit@EtherAuthority.io

rear and the strain second of the



This is a private and confidential document, he part of this document should be disclosed to third party without price written permission of Otherlatherity. Ernail: audit@EtherAuthority.io

their sound. Charles and the