

etherauthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project: **Cornucopias**
Website: cornucopias.io
Platform: **Base Chain Network**
Language: **Solidity**
Date: **June 14th, 2024**

Table of contents

Introduction	4
Project Background	4
Audit Scope	5
Code Audit History	6
Severity Definitions	6
Claimed Smart Contract Features	7
Audit Summary	8
Technical Quick Stats	9
Business Risk Analysis	10
Code Quality	11
Documentation	11
Use of Dependencies	11
AS-IS overview	12
Audit Findings	13
Conclusion	16
Our Methodology	17
Disclaimers	19
Appendix	
• Code Flow Diagram	20
• Slither Results Log	21
• Solidity static analysis	23
• Solhint Linter	24

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.

Introduction

As part of EtherAuthority's community smart contracts audit initiatives, the Cornucopias smart contract from cornucopias.io was audited extensively. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on June 14th, 2024.

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

Website Details



- Cornucopias is an open-world MMO set in a sky-bound world, developed with Unreal Engine 5 for high-quality graphics.
- The game includes activities like crafting, commerce, combat, and racing. It emphasizes digital ownership, allowing players to acquire vehicles, land plots, and customizable domes.
- The project integrates blockchain technology and has a strong community presence on platforms like Discord and Twitter. Additionally, Cornucopias engages in philanthropic activities through its COPI Cares initiative.

Code Details

- The `LSRFactory` contract provided is a factory for creating and managing Liquid Stability Reserve (LSR) instances using the TransparentUpgradeableProxy pattern from OpenZeppelin.
- This factory contract allows for the creation and management of LSR instances, providing mechanisms to initialize them using proxy contracts, add them to a set for tracking, remove them, and interact with their functions generically.
- The use of the proxy pattern ensures that the LSR implementations can be upgraded without changing their addresses, thus maintaining the integrity of their references throughout their lifecycle.
- The ownership pattern restricts critical functions to the contract owner, ensuring controlled management.

Audit scope

Name	Code Review and Security Analysis Report for Cornucopias Smart Contract
Platform	Base Chain Network
Language	Solidity
File	LSRFactory.sol
Smart Contract Code	0xc132624055a3e6e1ef4457053c528df179b18285
Audit Date	June 14th,2024
Audit Result	Passed

Code Audit History



2
Total Findings

0
Critical






0
High

0
Medium

0
Low

2
Informational

Severity Definitions

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

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
<p>Owner Control:</p> <ul style="list-style-type: none">• Create a new LSR.• Add/Remove LSR.• Execute transaction.• Pending Owner address can be set by current owner.• Accepts the admin rights, but only for pending Owners. <p>Admin Control:</p> <ul style="list-style-type: none">• Returns the current implementation.• Changes the admin of the proxy.• Upgrade the implementation of the proxy.• Upgrade the implementation of the proxy, and then call a function from the new implementation as specified by `data`, which should be an encoded function call. This is useful to initialize new storage variables in the proxied contract.	<p>YES, This is valid.</p>

Audit Summary

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



You are here 

We used various tools like Slither, Solhint, and Remix IDE. At the same time, this finding is based on a 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. The general overview is presented in the AS-IS section and all identified issues can be found in the Audit overview section.

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

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

Overall Audit Result: **PASSED**

Business Risk Analysis

Category	Result
● Buy Tax	0%
● Sell Tax	0%
● Cannot Buy	No
● Cannot Sell	No
● Max Tax	0%
● Modify Tax	No
● Fee Check	Not Detected
● Is Honeypot	Not Detected
● Trading Cooldown	Not Detected
● Can Pause Trade?	Not Detected
● Pause Transfer?	No
● Max Tax?	No
● Is it Anti-whale?	Not Detected
● Is Anti-bot?	Not Detected
● Is it a Blacklist?	No
● Blacklist Check	No
● Can Mint?	No
● Is it a Proxy Contract?	Yes
● Is it used Open Source?	No
● External Call Risk?	No
● Balance Modifiable?	No
● Can Take Ownership?	Yes
● Ownership Renounce?	No
● Hidden Owner?	Not Detected
● Self Destruction?	Not Detected
● Auditor Confidence	High

Overall Audit Result: PASSED

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

Email: audit@EtherAuthority.io

Code Quality

This audit scope has 1 smart contract. Smart contracts contain Libraries, Smart contracts, inherits, and Interfaces. This is a compact and well-written smart contract.

The libraries in Cornucopias 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 Cornucopias.

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

Code parts are well commented on in the smart contracts. Ethereum's NatSpec commenting style is recommended.

Documentation

We were given a Cornucopias smart contract code in the form of a [basescan](#) web link.

As mentioned above, code parts are well commented on. And the logic is straightforward. So it is easy to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

-

Use of Dependencies

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

Apart from libraries, its functions are not used in external smart contract calls.

AS-IS overview

LSRFactory.sol

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initialize	write	initializer	No Issue
3	_createLSR	external	access only owner	No Issue
4	_addLSR	write	Public and External Functions with Leading Underscores	Refer Audit Findings
5	_removeLSR	write	Gas Optimization, Public and External Functions with Leading Underscore	Refer Audit Findings
6	execute	internal	Passed	No Issue
7	_executeTransaction	external	Public and External Functions with Leading Underscores	Refer Audit Findings
8	getAllLSRs	internal	Passed	No Issue
9	_getLSRInfo	internal	Passed	No Issue
10	getAllLSRs	external	Passed	No Issue
11	initializer	modifier	Passed	No Issue
12	onlyOwner	modifier	Passed	No Issue
13	Ownable init	internal	Passed	No Issue
14	_setPendingOwner	external	access only owner	No Issue
15	acceptOwner	external	Passed	No Issue

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No Medium-severity vulnerabilities were found.

Low

No Low-severity vulnerabilities were found.

Very Low / Informational / Best practices:

[I-01] Gas Optimization:

Description:

These 'public' functions like `_removeLSR()` that are never called by the contract could be declared external functions.

Recommendation: We suggest declare these function external for better Gas optimization.

[I-02] Public and External Functions with Leading Underscores:

```
function _executeTransaction(  
    address _target,  
    string memory _signature,  
    bytes memory _data  
) external onlyOwner {  
    _execute(_target, _signature, _data);  
}
```

```

}

function _addLSR(address _lsr) public onlyOwner {
    require(ILSR(_lsr).mpr() != address(0), "_addLSR: is LSR
contract");
    require(lsrs_.add(_lsr), "it has been sold");
    emit AddLSR(_lsr);
}

function _removeLSR(address _lsr) public onlyOwner {
    require(lsrs_.remove(_lsr), "_removeLSR: _lsr does not
exist");
    emit RemoveLSR(_lsr);
}

```

Description:

The following functions are marked as public or external, making them accessible from outside the contract. However, their names start with an underscore (_), which conventionally suggests they are intended for internal use: `_createLSR()`, `_addLSR()`, `_removeLSR()`, `_executeTransaction()`

Recommendation: we suggest the Solidity naming convention guidelines, the codebase increases the readability, and maintainability, and makes it easier to work with Find more information on the Solidity documentation like:-

<https://docs.soliditylang.org/en/v0.8.17/style-guide.html#naming-convention>

Centralization

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

Centralized

Decentralized

You are here



The following are Owner functions:

LSRFactory.sol

- `_createLSR`: Create a new LSR by the owner.
- `_addLSR`: Add an LSR by the owner.
- `_removeLSR`: Remove an LSR by the owner.
- `_executeTransaction`: Execute transaction by the owner.

TransparentUpgradeableProxy.sol

- `admin`: Only the admin can call this function.
- `implementation`: Returns the current implementation
- `changeAdmin`: Changes the admin of the proxy.
- `upgradeTo`: Upgrade the implementation of the proxy.
- `upgradeToAndCall`: Upgrade the implementation of the proxy, and then call a function from the new implementation as specified by ``data``, which should be an encoded function call. This is useful to initialize new storage variables in the proxied contract.

Ownable.sol

- `_setPendingOwner`: The Pending Owner address can be set by the current owner.
- `_acceptOwner`: Accepts the admin rights, but only for pending Owner.

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

Conclusion

We were given a contract code in the form of a [basescan](#) web link. And we have used all possible tests based on given objects as files. We observed 2 Informational issues in the smart contracts. but those are not critical. So, **it's good to go for the production.**

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 the 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.

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

The security state of the reviewed smart contract, based on standard audit procedure scope, is **“Secured”**.

Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of the 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 white box penetration testing. We look at the project's website to get a high-level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

Documenting Results:

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

Suggested Solutions:

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

Disclaimers

EtherAuthority.io Disclaimer

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

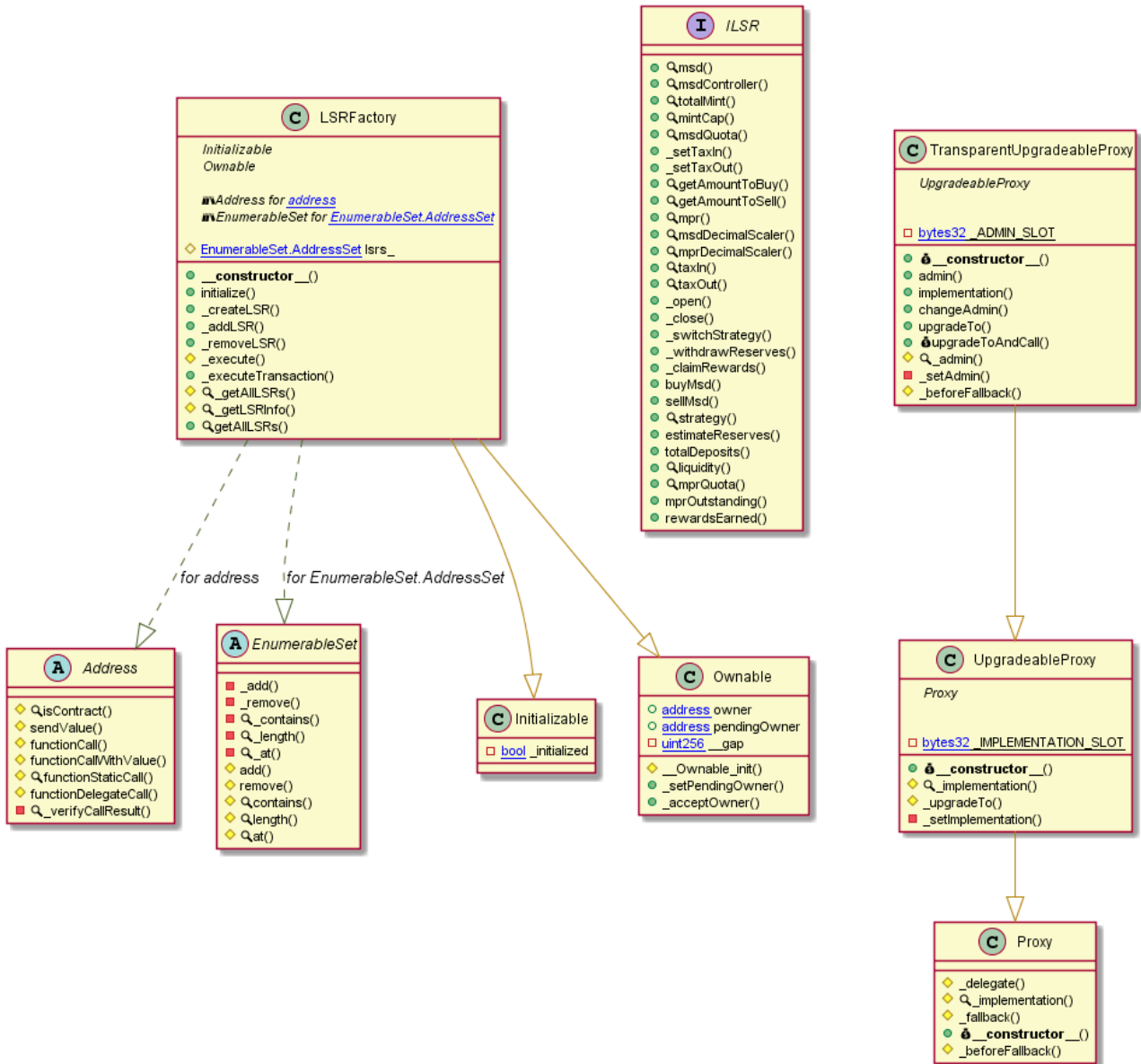
Due to the fact that the total number of test cases is unlimited, the audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status or any other statements of the contract. While 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 the explicit security of the audited smart contracts.

Appendix

Code Flow Diagram - Cornucopias



Slither Results Log

Slither is a Solidity static analysis framework that uses vulnerability detectors, displays contract details, and provides an API for writing custom analyses. It helps developers identify vulnerabilities, improve code comprehension, and prototype custom analyses quickly. The analysis includes a report with warnings and errors, allowing developers to quickly prototype and fix issues.

We did the analysis of the project altogether. Below are the results.

LSRFactory.sol

```
INFO:Detectors:
Modifier TransparentUpgradeableProxy.ifAdmin() (LSRFactory.sol#799-805) does not always
execute _; or revertReference:
https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-modifier
INFO:Detectors:
Reentrancy in LSRFactory._createLSR(address,address,bytes) (LSRFactory.sol#941-951):
  External calls:
    - _lsr = address(new TransparentUpgradeableProxy(_implementation,_proxyAdmin,_data))
      (LSRFactory.sol#946-948)
  Event emitted after the call(s):
    - AddLSR(_lsr) (LSRFactory.sol#960)
      - _addLSR(_lsr) (LSRFactory.sol#950)
    - CreateLSR(_lsr,_implementation,_proxyAdmin,_data) (LSRFactory.sol#949)
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3
INFO:Detectors:
Pragma version>=0.6.2<0.8.0 (LSRFactory.sol#3) is too complex
solc-0.7.6 is not recommended for deployment
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity
INFO:Detectors:
Function ILSR._setTaxIn(uint256) (LSRFactory.sol#473) is not in mixedCase
Function ILSR._setTaxOut(uint256) (LSRFactory.sol#475) is not in mixedCase
Function ILSR._open() (LSRFactory.sol#493) is not in mixedCase
Function ILSR._close() (LSRFactory.sol#495) is not in mixedCase
Function ILSR._switchStrategy(address) (LSRFactory.sol#497) is not in mixedCase
Function ILSR._withdrawReserves(address) (LSRFactory.sol#499) is not in mixedCase
Function ILSR._claimRewards(address) (LSRFactory.sol#501) is not in mixedCase
Function LSRFactory._createLSR(address,address,bytes) (LSRFactory.sol#941-951) is not in
mixedCase
Parameter LSRFactory._createLSR(address,address,bytes)._implementation
```

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

Email: audit@EtherAuthority.io

```
(LSRFactory.sol#942) is not in mixedCase
Parameter LSRFactory._createLSR(address,address,bytes)._proxyAdmin (LSRFactory.sol#943) is
not in mixedCase
Parameter LSRFactory._createLSR(address,address,bytes)._data (LSRFactory.sol#944) is not in
mixedCase
Function LSRFactory._addLSR(address) (LSRFactory.sol#957-961) is not in mixedCase
Parameter LSRFactory._addLSR(address)._lsr (LSRFactory.sol#957) is not in mixedCase
Function LSRFactory._removeLSR(address) (LSRFactory.sol#967-970) is not in mixedCase
Parameter LSRFactory._removeLSR(address)._lsr (LSRFactory.sol#967) is not in mixedCase
Function LSRFactory._executeTransaction(address,string,bytes) (LSRFactory.sol#996-1002) is
not in mixedCase
Parameter LSRFactory._executeTransaction(address,string,bytes)._target (LSRFactory.sol#997) is
not in mixedCase
Parameter LSRFactory._executeTransaction(address,string,bytes)._signature
(LSRFactory.sol#998) is not in mixedCase
Parameter LSRFactory._executeTransaction(address,string,bytes)._data (LSRFactory.sol#999) is
not in mixedCase
Reference:
https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-c
onventions
INFO:Slither:LSRFactory.sol analyzed (9 contracts with 93 detectors), 61 result(s) found
```

Solidity Static Analysis

Static code analysis is used to identify many common coding problems before a program is released. It involves examining the code manually or using tools to automate the process. Static code analysis tools can automatically scan the code without executing it.

LSRFactory.sol

Inline assembly:

The Contract uses inline assembly, this is only advised in rare cases. Additionally static analysis modules do not parse inline Assembly, this can lead to wrong analysis results.

Pos: 885:8:

Low level calls:

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

Pos: 164:50:

Gas costs:

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

Pos: 1038:4:

Similar variable names:

LSRFactory._getAllSRs() : Variables have very similar names "lsrs_" and "_lsrs". Note: Modifiers are currently not considered by this static analysis.

Pos: 1009:49:

Guard conditions:

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

Pos: 985:8:

Delete from dynamic array:

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

Pos: 257:12:

Solhint Linter

Linters are the utility tools that analyze the given source code and report programming errors, bugs, and stylistic errors. For the Solidity language, there are some linter tools available that a developer can use to improve the quality of their Solidity contracts.

LSRFactory.sol

```
Compiler version >=0.6.2 <0.8.0 does not satisfy the ^0.5.8 semver
requirement
Pos: 1:2
Error message for require is too long
Pos: 9:54
Error message for require is too long
Pos: 9:111
Error message for require is too long
Pos: 9:136
Error message for require is too long
Pos: 9:160
Error message for require is too long
Pos: 9:289
Error message for require is too long
Pos: 9:536
Error message for require is too long
Pos: 9:569
Function name must be in mixedCase
Pos: 5:576
Error message for require is too long
Pos: 9:590
Error message for require is too long
Pos: 9:608
Code contains empty blocks
Pos: 49:696
Error message for require is too long
Pos: 9:762
Error message for require is too long
Pos: 9:840
Error message for require is too long
Pos: 9:893
Error message for require is too long
Pos: 9:984
```

Software analysis result:

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



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

Email: audit@EtherAuthority.io