Ether Authority

www.EtherAuthority.io
audit@etherauthority.io

SMART CONTRACT

Security Audit Report

Project:	Arbitrum Token
Website:	arbitrum.io
Platform:	Ethereum
Language:	Solidity
Date:	May 10th, 2024

Table of contents

`

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

Email: audit@EtherAuthority.io

Introduction

As part of EtherAuthority's community smart contracts audit initiatives, the Arbitrum Token smart contract from arbitrum.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 May 10th, 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

- The Arbitrum token is a Permit token registered with an Arb One and Nova counterpart.
- Arbitrum Token Contracts offer various functions such as initialize, bridge mint, bridge burn, register token on L2, and transfer from.
- This contract facilitates the bridging of an ERC20 token from Ethereum's L1 to Arbitrum's L2 chain, allowing token transfers between the two chains.

Audit scope

Name	**Code Review and Security Analysis Report for Arbitrum Token Smart Contract**
Platform	**Ethereum**
Language	**Solidity**
File	L1ArbitrumToken.sol
Smart Contract Code	0xad0c361ef902a7d9851ca7dcc85535da2d3c6fc7
Audit Date	May 10th, 2024

Claimed Smart Contract Features

Claimed Feature Detail	Our Observation
Tokenomics: • Name: Arbitrum • Symbol: ARB • Decimals: 18	**YES, This is valid.**
Ownership control: • Allow the Arb One bridge to mint tokens by only l1 arb one gateway. • Allow the Arb One bridge to burn tokens by only l1 arb one gateway.	**YES, This is valid. We suggest renouncing ownership once the ownership functions are not needed. This is to make the smart contract 100% decentralized.**

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.

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. A 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 1 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	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**

Business Risk Analysis

Category	Result
Buy Tax	0%
Sell Tax	0%
Cannot Buy	No
Cannot Sell	No
Max Tax	0%
Modify Tax	Not Detected
Fee Check	No
Is Honeypot	Not Detected
Trading Cooldown	Not Detected
Can Pause Trade?	No
Pause Transfer?	No
Max Tax?	No
Is it Anti-whale?	No
Is Anti-bot?	Not Detected
Is it a Blacklist?	Not Detected
Blacklist Check	No
Can Mint?	No
Is it a Proxy?	No
Can Take Ownership?	No
Hidden Owner?	Not Detected
Self Destruction?	Not Detected
Auditor Confidence	High

Overall Audit Result: **PASSED**

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 Arbitrum Token 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 Arbitrum Token.

The EtherAuthority team has no 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 an Arbitrum Token smart contract code in the form of an Etherscan 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.

Another source of information was its official website: arbitrum.io which provided rich information about the project architecture and tokenomics.

Use of Dependencies

As per our observation, the libraries used in this smart contract infrastructure that is 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

Functions

Sl.	Functions	Type	Observation	Conclusion
1	constructor	write	Passed	No Issue
2	initialize	write	initializer	No Issue
3	isArbitrumEnabled	external	Passed	No Issue
4	onlyArbOneGateway	modifier	Passed	No Issue
5	bridgeMint	write	Centralized risk	Refer Audit Findings
6	bridgeBurn	write	Centralized risk	Refer Audit Findings
7	registerTokenOnL2	write	Passed	No Issue
8	balanceOf	read	Passed	No Issue
9	transferFrom	write	Passed	No Issue
10	transferAndCall	write	Passed	No Issue
11	contractFallback	write	Passed	No Issue
12	isContract	write	Passed	No Issue
13	__ERC20Permit_init	internal	access only Initializing	No Issue
14	__ERC20Permit_init_unchained	internal	access only Initializing	No Issue
15	permit	write	Passed	No Issue
16	nonces	read	Passed	No Issue
17	DOMAIN_SEPARATOR	external	Passed	No Issue
18	_useNonce	internal	Passed	No Issue
19	__ERC20_init	internal	access only Initializing	No Issue
20	__ERC20_init_unchained	internal	access only Initializing	No Issue
21	name	read	Passed	No Issue
22	symbol	read	Passed	No Issue
23	decimals	read	Passed	No Issue
24	totalSupply	read	Passed	No Issue
25	balanceOf	read	Passed	No Issue
26	transfer	write	Passed	No Issue
27	allowance	read	Passed	No Issue
28	approve	write	Passed	No Issue
29	transferFrom	write	Passed	No Issue
30	increaseAllowance	write	Passed	No Issue
31	decreaseAllowance	write	Passed	No Issue
32	_transfer	internal	Passed	No Issue
33	_mint	internal	Passed	No Issue
34	_burn	internal	Passed	No Issue
35	_approve	internal	Passed	No Issue
36	_spendAllowance	internal	Passed	No Issue
37	_beforeTokenTransfer	internal	Passed	No Issue
38	_afterTokenTransfer	internal	Passed	No Issue
39	__EIP712_init	internal	access only Initializing	No Issue

40	__EIP712_init_unchained	internal	access only Initializing	No Issue
41	_domainSeparatorV4	internal	Passed	No Issue
42	_buildDomainSeparator	read	Passed	No Issue
43	_hashTypedDataV4	internal	Passed	No Issue
44	_EIP712NameHash	internal	Passed	No Issue
45	_EIP712VersionHash	internal	Passed	No Issue
46	__Context_init	internal	access only Initializing	No Issue
47	__Context_init_unchained	internal	access only Initializing	No Issue
48	_msgSender	internal	Passed	No Issue
49	_msgData	internal	Passed	No Issue
50	initializer	modifier	Passed	No Issue
51	reinitializer	modifier	Passed	No Issue
52	onlyInitializing	modifier	Passed	No Issue
53	_disableInitializers	internal	Passed	No Issue

Severity Definitions

Risk Level	Description
Critical	Critical vulnerabilities are usually straightforward to exploit and can lead to token loss etc.
High	High-level vulnerabilities are difficult to exploit; however, they also have a 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 a significant impact on execution
Lowest / Code Style / Best Practice	Lowest-level vulnerabilities, code style violations, and info statements can't affect smart contract execution and can be ignored.

Email: audit@EtherAuthority.io

Audit Findings

Critical Severity

No Critical severity vulnerabilities were found.

High Severity

No High severity vulnerabilities were found.

Medium

No Medium-severity vulnerabilities were found.

Low

No Low severity vulnerabilities were found.

Very Low / Informational / Best practices:

(1) Centralized risk:

L1ArbitrumToken.sol

The onlyArbOneGateway can call the bridgeMint function and bridgeBurn function.

Resolution: To make the smart contract 100% decentralized. We suggest renouncing ownership of the smart contract once its function is completed.

Centralization

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

L1ArbitrumToken.sol

- bridgeMint: Allow the Arb One bridge to mint tokens by only l1 arb one gateway.
- bridgeBurn: Allow the Arb One bridge to burn tokens by only l1 arb one gateway.

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

Conclusion

We were given a contract code in the form of Etherscan web links. And we have used all possible tests based on given objects as files. We observed 1 informational issue 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.

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

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 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, 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).

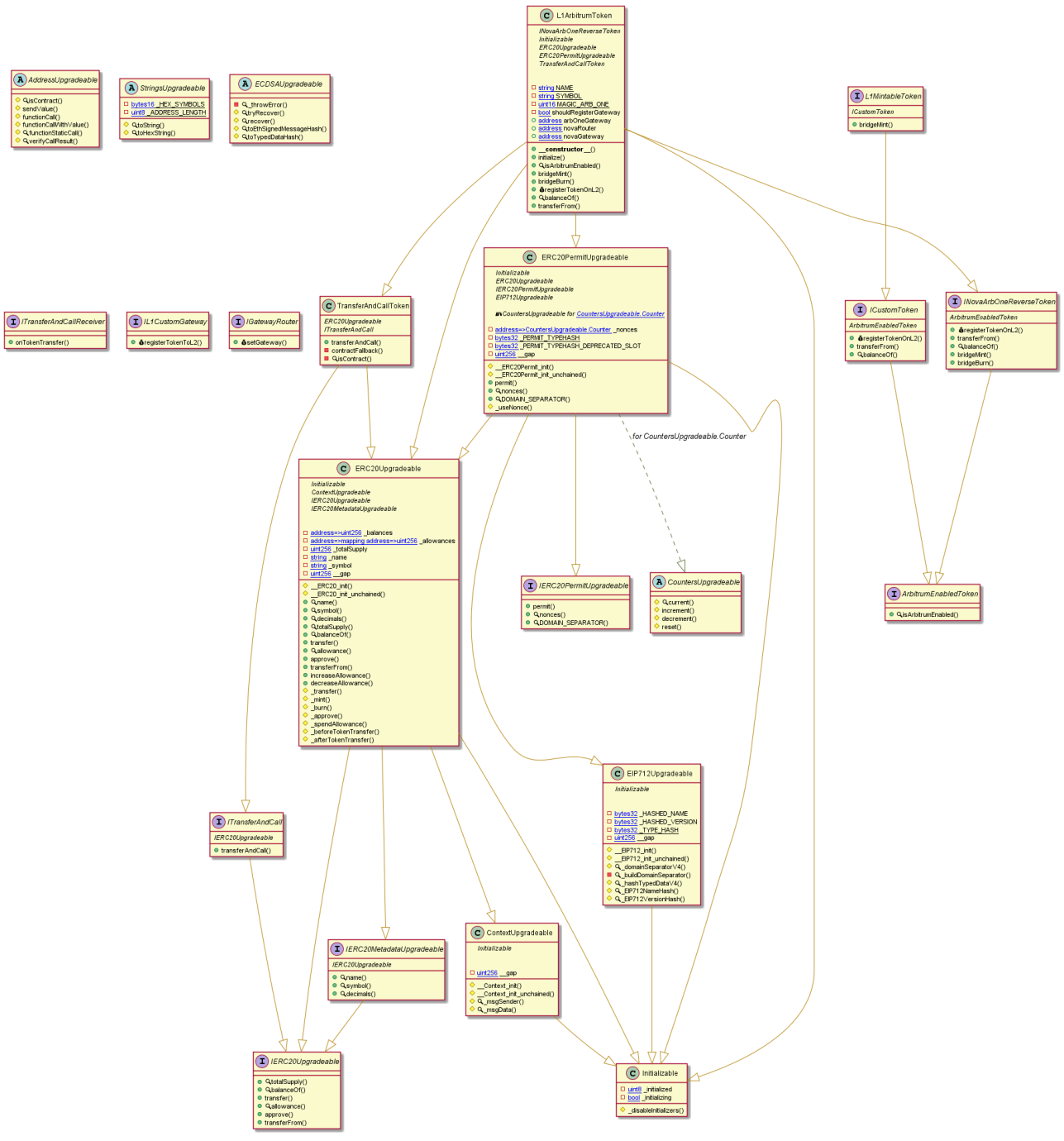
Due to the fact that the total number of test cases is unlimited, the audit makes no statements or warranties on the security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bug-free status, or any other statements of the contract. While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

Appendix

Code Flow Diagram - Arbitrum Token



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.

Slither Log >> L1ArbitrumToken.sol

```
ERC20PermitUpgradeable.__ERC20Permit_init(string).name (L1ArbitrumToken.sol#1280) shadows:
        - ERC20Upgradeable.name() (L1ArbitrumToken.sol#907-909) (function)
        - IERC20MetadataUpgradeable.name() (L1ArbitrumToken.sol#358) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing

ERC20PermitUpgradeable.permit(address,address,uint256,uint256,uint8,bytes32,bytes32) (L1ArbitrumToken.sol#1289-1308) uses timest
amp for comparisons
        Dangerous comparisons:
        - require(bool,string)(block.timestamp <= deadline,ERC20Permit: expired deadline) (L1ArbitrumToken.sol#1298)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp

AddressUpgradeable.verifyCallResult(bool,bytes,string) (L1ArbitrumToken.sol#218-238) uses assembly
        - INLINE ASM (L1ArbitrumToken.sol#230-233)
ECDSAUpgradeable.tryRecover(bytes32,bytes) (L1ArbitrumToken.sol#515-532) uses assembly
        - INLINE ASM (L1ArbitrumToken.sol#523-527)
TransferAndCallToken.isContract(address) (L1ArbitrumToken.sol#1386-1392) uses assembly
        - INLINE ASM (L1ArbitrumToken.sol#1388-1390)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage
```

```
AddressUpgradeable.functionCall(address,bytes) (L1ArbitrumToken.sol#129-131) is never used and should be removed
AddressUpgradeable.functionCall(address,bytes,string) (L1ArbitrumToken.sol#139-145) is never used and should be removed
AddressUpgradeable.functionCallWithValue(address,bytes,uint256) (L1ArbitrumToken.sol#158-164) is never used and should be remove
d
AddressUpgradeable.functionCallWithValue(address,bytes,uint256,string) (L1ArbitrumToken.sol#172-183) is never used and should be
 removed
AddressUpgradeable.functionStaticCall(address,bytes) (L1ArbitrumToken.sol#191-193) is never used and should be removed
AddressUpgradeable.functionStaticCall(address,bytes,string) (L1ArbitrumToken.sol#201-210) is never used and should be removed
AddressUpgradeable.sendValue(address,uint256) (L1ArbitrumToken.sol#104-109) is never used and should be removed
AddressUpgradeable.verifyCallResult(bool,bytes,string) (L1ArbitrumToken.sol#218-238) is never used and should be removed
ContextUpgradeable.__Context_init() (L1ArbitrumToken.sol#762-763) is never used and should be removed
ContextUpgradeable.__Context_init_unchained() (L1ArbitrumToken.sol#765-766) is never used and should be removed
ContextUpgradeable._msgData() (L1ArbitrumToken.sol#771-773) is never used and should be removed
CountersUpgradeable.decrement(CountersUpgradeable.Counter) (L1ArbitrumToken.sol#390-398) is never used and should be removed
CountersUpgradeable.reset(CountersUpgradeable.Counter) (L1ArbitrumToken.sol#400-402) is never used and should be removed
ECDSAUpgradeable.recover(bytes32,bytes) (L1ArbitrumToken.sol#548-552) is never used and should be removed
ECDSAUpgradeable.recover(bytes32,bytes32,bytes32) (L1ArbitrumToken.sol#576-584) is never used and should be removed
ECDSAUpgradeable.toEthSignedMessageHash(bytes) (L1ArbitrumToken.sol#660-662) is never used and should be removed
ECDSAUpgradeable.toEthSignedMessageHash(bytes32) (L1ArbitrumToken.sol#646-650) is never used and should be removed
ECDSAUpgradeable.tryRecover(bytes32,bytes) (L1ArbitrumToken.sol#515-532) is never used and should be removed
ECDSAUpgradeable.tryRecover(bytes32,bytes32,bytes32) (L1ArbitrumToken.sol#561-569) is never used and should be removed
EIP712Upgradeable.__EIP712_init(string,string) (L1ArbitrumToken.sol#803-805) is never used and should be removed
ERC20PermitUpgradeable.__ERC20Permit_init_unchained(string) (L1ArbitrumToken.sol#1284) is never used and should be removed
StringsUpgradeable.toHexString(address) (L1ArbitrumToken.sol#468-470) is never used and should be removed
StringsUpgradeable.toHexString(uint256) (L1ArbitrumToken.sol#437-448) is never used and should be removed
StringsUpgradeable.toHexString(uint256,uint256) (L1ArbitrumToken.sol#453-463) is never used and should be removed
StringsUpgradeable.toString(uint256) (L1ArbitrumToken.sol#412-432) is never used and should be removed
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code
```

```
Pragma version>=0.6.9<0.9.0 (L1ArbitrumToken.sol#3) is too complex
solc-0.8.19 is not recommended for deployment
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity

Low level call in AddressUpgradeable.sendValue(address,uint256) (L1ArbitrumToken.sol#104-109):
        - (success) = recipient.call{value: amount}() (L1ArbitrumToken.sol#107)
Low level call in AddressUpgradeable.functionCallWithValue(address,bytes,uint256,string) (L1ArbitrumToken.sol#172-183):
        - (success,returndata) = target.call{value: value}(data) (L1ArbitrumToken.sol#181)
Low level call in AddressUpgradeable.functionStaticCall(address,bytes,string) (L1ArbitrumToken.sol#201-210):
        - (success,returndata) = target.staticcall(data) (L1ArbitrumToken.sol#208)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls
```

```
Function IERC20PermitUpgradeable.DOMAIN_SEPARATOR() (L1ArbitrumToken.sol#50) is not in mixedCase
Function ContextUpgradeable.__Context_init() (L1ArbitrumToken.sol#762-763) is not in mixedCase
Function ContextUpgradeable.__Context_init_unchained() (L1ArbitrumToken.sol#765-766) is not in mixedCase
Variable ContextUpgradeable.__gap (L1ArbitrumToken.sol#780) is not in mixedCase
Function EIP712Upgradeable.__EIP712_init(string,string) (L1ArbitrumToken.sol#803-805) is not in mixedCase
Function EIP712Upgradeable.__EIP712_init_unchained(string,string) (L1ArbitrumToken.sol#807-812) is not in mixedCase
Function EIP712Upgradeable._EIP712NameHash() (L1ArbitrumToken.sol#854-856) is not in mixedCase
Function EIP712Upgradeable._EIP712VersionHash() (L1ArbitrumToken.sol#864-866) is not in mixedCase
Variable EIP712Upgradeable._HASHED_NAME (L1ArbitrumToken.sol#785) is not in mixedCase
Variable EIP712Upgradeable._HASHED_VERSION (L1ArbitrumToken.sol#786) is not in mixedCase
Variable EIP712Upgradeable.__gap (L1ArbitrumToken.sol#873) is not in mixedCase
Function ERC20Upgradeable.__ERC20_init(string,string) (L1ArbitrumToken.sol#895-897) is not in mixedCase
Function ERC20Upgradeable.__ERC20_init_unchained(string,string) (L1ArbitrumToken.sol#899-902) is not in mixedCase
Variable ERC20Upgradeable.__gap (L1ArbitrumToken.sol#1234) is not in mixedCase
Function ERC20PermitUpgradeable.__ERC20Permit_init(string) (L1ArbitrumToken.sol#1280-1282) is not in mixedCase
Function ERC20PermitUpgradeable.__ERC20Permit_init_unchained(string) (L1ArbitrumToken.sol#1284) is not in mixedCase
Function ERC20PermitUpgradeable.DOMAIN_SEPARATOR() (L1ArbitrumToken.sol#1321-1323) is not in mixedCase
Variable ERC20PermitUpgradeable._PERMIT_TYPEHASH_DEPRECATED_SLOT (L1ArbitrumToken.sol#1273) is not in mixedCase
Variable ERC20PermitUpgradeable.__gap (L1ArbitrumToken.sol#1341) is not in mixedCase
Parameter TransferAndCallToken.transferAndCall(address,uint256,bytes)._to (L1ArbitrumToken.sol#1365) is not in mixedCase
Parameter TransferAndCallToken.transferAndCall(address,uint256,bytes)._value (L1ArbitrumToken.sol#1365) is not in mixedCase
Parameter TransferAndCallToken.transferAndCall(address,uint256,bytes)._data (L1ArbitrumToken.sol#1365) is not in mixedCase
Parameter TransferAndCallToken.contractFallback(address,uint256,bytes)._to (L1ArbitrumToken.sol#1381) is not in mixedCase
Parameter TransferAndCallToken.contractFallback(address,uint256,bytes)._value (L1ArbitrumToken.sol#1381) is not in mixedCase
Parameter TransferAndCallToken.contractFallback(address,uint256,bytes)._data (L1ArbitrumToken.sol#1381) is not in mixedCase
Parameter TransferAndCallToken.isContract(address)._addr (L1ArbitrumToken.sol#1386) is not in mixedCase
Parameter L1ArbitrumToken.initialize(address,address,address)._arbOneGateway (L1ArbitrumToken.sol#1465) is not in mixedCase
Parameter L1ArbitrumToken.initialize(address,address,address)._novaRouter (L1ArbitrumToken.sol#1465) is not in mixedCase
Parameter L1ArbitrumToken.initialize(address,address,address)._novaGateway (L1ArbitrumToken.sol#1465) is not in mixedCase
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions
L1ArbitrumToken.sol analyzed (22 contracts with 84 detectors), 68 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.

L1ArbitrumToken.sol

Check-effects-interaction:

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

more

Pos: 172:4:

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.

more

Pos: 1388:11:

Block timestamp:

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

more

Pos: 1298:19:

Low level calls:

Use of "call": should be avoided whenever possible. It can lead to unexpected behavior if return value is not handled properly. Please use Direct Calls via specifying the called contract's interface.

more

Pos: 181:50:

Gas costs:

Gas requirement of function L1ArbitrumToken.transferFrom 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: 1547:7:

Constant/View/Pure functions:

L1MintableToken.bridgeMint(address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 276:4:

Constant/View/Pure functions:

L1ArbitrumToken.transferFrom(address,address,uint256) : Potentially should be constant/view/pure but is not. Note: Modifiers are currently not considered by this static analysis.
more
Pos: 1547:7:

Similar variable names:

L1ArbitrumToken.bridgeMint(address,uint256) : Variables have very similar names "account" and "amount". Note: Modifiers are currently not considered by this static analysis.
Pos: 1498:26:

No return:

IGatewayRouter.setGateway(address,uint256,uint256,uint256,address): Defines a return type but never explicitly returns a value.
Pos: 1433:7:

Guard conditions:

Use "assert(x)" if you never ever want x to be false, not in any circumstance (apart from a bug in your code). Use "require(x)" if x can be false, due to e.g. invalid input or a failing external component.
more
Pos: 1488:11:

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.

L1ArbitrumToken.sol

```
Error message for require is too long
Pos: 9:107
Error message for require is too long
Pos: 9:177
Error message for require is too long
Pos: 9:205
Avoid using inline assembly. It is acceptable only in rare cases
Pos: 17:229
Error message for revert is too long
Pos: 13:488
Error message for revert is too long
Pos: 13:490
Avoid using inline assembly. It is acceptable only in rare cases
Pos: 13:522
Error message for require is too long
Pos: 9:700
Error message for require is too long
Pos: 9:728
Error message for require is too long
Pos: 9:741
Error message for require is too long
Pos: 9:752
Function name must be in mixedCase
Pos: 5:761
Code contains empty blocks
Pos: 57:761
Function name must be in mixedCase
Pos: 5:764
Code contains empty blocks
Pos: 67:764
Function name must be in mixedCase
Pos: 5:802
Function name must be in mixedCase
Pos: 5:806
Function name must be in mixedCase
Pos: 5:853
Function name must be in mixedCase
Pos: 5:863
Function name must be in mixedCase
Pos: 5:894
Function name must be in mixedCase
Pos: 5:898
Error message for require is too long
Pos: 9:1048
```

```
Error message for require is too long
Pos: 9:1075
Error message for require is too long
Pos: 9:1076
Error message for require is too long
Pos: 9:1081
Error message for require is too long
Pos: 9:1125
Error message for require is too long
Pos: 9:1130
Error message for require is too long
Pos: 9:1159
Error message for require is too long
Pos: 9:1160
Code contains empty blocks
Pos: 24:1206
Code contains empty blocks
Pos: 24:1226
Function name must be in mixedCase
Pos: 5:1279
Function name must be in mixedCase
Pos: 5:1283
Code contains empty blocks
Pos: 84:1283
Avoid making time-based decisions in your business logic
Pos: 17:1297
Avoid using inline assembly. It is acceptable only in rare cases
Pos: 9:1387
Explicitly mark visibility in function (Set ignoreConstructors to
true if using solidity >=0.7.0)
Pos: 5:1460
Error message for require is too long
Pos: 9:1468
Error message for require is too long
Pos: 9:1469
Error message for require is too long
Pos: 9:1470
Error message for require is too long
Pos: 9:1482
Error message for require is too long
Pos: 9:1487
```

Software analysis result:

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

Email: audit@EtherAuthority.io