



AUDIT COMPANY



LambroToken

SMART CONTRACT SECURITY AUDIT

June 2023

CheckDot



Disclaimer

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

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

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



Background

CheckDot was commissioned by Lambro to perform an audit of smart contracts:

Mainnet Deployed Contract:

<https://bscscan.com/token/0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0>

Website:

<https://lambro.io>

The purpose of the audit was to achieve the following:

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

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



Issues Checking Status

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



PASSED

LAMBRO (LAMBRO)

BSCSCAN

CHART

DOES NOT SEEM LIKE A HONEYPOT

THIS CAN ALWAYS CHANGE! DO YOUR OWN DUE DILIGENCE.

ADDRESS

0X201AF44D9DFA5464F20B8DD8AA96FC016D26E7C0

SIMULATION RESULTS

BUY TAX
3.0%

SELL TAX
3.0%

TRANSFER TAX
3.0%

BUY GAS
261,172

SELL GAS
187,920

SOURCE CODE
 OPEN SOURCE

BUY LIMIT
NONE DETECTED

SELL LIMIT
NONE DETECTED

Source code Verified on BSCscan.

5% Buy Tax (1% Charity, 1% lp, 3% between).

5% Sell Tax (1% Charity, 1% lp, 3% between).

No Buy Limit.

No Sell Limit.

Program analysis:

```

Variable(s) isExcludedFromFee (#370), _burningFee (#374), _lpFee (#375), _inbetweenFee_ (#376), _burningFeeTotal (#378), _lpFeeTotal (#379), _inbetweenFeeTotal (#380) Suspected fees in the Contract
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions

LambroToken.allowance(address,address).owner (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#423) shadows:
- Ownable.owner() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#299-301) (function)
LambroToken._approve(address,address,uint256).owner (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#448) shadows:
- Ownable.owner() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#299-301) (function)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing

Different versions of Solidity is used:
- Version used: ['0.8.19', '^0.8.0']
- ^0.8.0 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#4)
- ^0.8.0 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#234)
- ^0.8.0 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#261)
- 0.8.19 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#343)
Reference: https://github.com/crytic/slither/wiki/Detector-Documentation#different-pragma-directives-are-used

Context._msgData() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#251-253) is never used and should be removed
SafeMath.div(uint256,uint256,string) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#191-200) is never used and should be removed
SafeMath.mod(uint256,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#151-153) is never used and should be removed
SafeMath.mod(uint256,uint256,string) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#217-226) is never used and should be removed
SafeMath.tryAdd(uint256,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#22-28) is never used and should be removed
SafeMath.tryDiv(uint256,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bscscan.com-LambroToken.sol#64-69) is never used and should be removed

```

SafeMath.tryMod(uint256,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#76-81) is never used and should be removed
SafeMath.tryMul(uint256,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#47-57) is never used and should be removed
SafeMath.trySub(uint256,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#35-40) is never used and should be removed
Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#dead-code>

Pragma version<0.8.0 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#4) allows old versions
Pragma version<0.8.0 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#234) allows old versions
Pragma version<0.8.0 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#261) allows old versions
Pragma version<0.8.19 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#343) necessitates a version too recent to be trusted. Consider deploying with 0.6.12/0.7.6/0.8.7
solc-0.8.19 is not recommended for deployment
Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#incorrect-versions-of-solidity>

Function LambroToken.SellbuyCollectFee(address,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#507-537) is not in mixedCase
Function LambroToken.ExcludedFromFee(address,bool) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#556-558) is not in mixedCase
Function LambroToken.IncludeInFee(address,bool) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#560-562) is not in mixedCase
Parameter LambroToken.setLPAddress(address). _Address (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#564) is not in mixedCase
Variable LambroToken._balances (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#368) is not in mixedCase
Variable LambroToken._allowances (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#369) is not in mixedCase
Variable LambroToken._totalSupply (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#372) is not in mixedCase
Variable LambroToken._charity (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#373) is not in mixedCase
Variable LambroToken._burningFee (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#374) is not in mixedCase
Variable LambroToken._lpFee (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#375) is not in mixedCase
Variable LambroToken._inbetweenFee_ (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#376) is not in mixedCase
Variable LambroToken._charityTotal (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#377) is not in mixedCase
Variable LambroToken._burningFeeTotal (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#378) is not in mixedCase
Variable LambroToken._lpFeeTotal (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#379) is not in mixedCase
Variable LambroToken._inbetweenFeeTotal (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#380) is not in mixedCase
Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions>

LambroToken.slitherConstructorVariables() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#359-571) uses literals with too many digits:

- _totalSupply = 6942000000 * 10 ** 18 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#372)

LambroToken.slitherConstructorVariables() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#359-571) uses literals with too many digits:

- burningAddress = 0x00 (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#382)

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits>

LambroToken._burningFee (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#374) should be constant
LambroToken._charity (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#373) should be constant
LambroToken._decimals (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#365) should be constant
LambroToken._inbetweenFee_ (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#376) should be constant
LambroToken._lpFee (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#375) should be constant
LambroToken._name (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#363) should be constant
LambroToken._symbol (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#364) should be constant
LambroToken._totalSupply (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#372) should be constant
LambroToken.burningAddress (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#382) should be constant
LambroToken.charityAddress (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#381) should be constant
LambroToken.inbetweenAddress (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#384) should be constant
Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant>

renounceOwnership() should be declared external:

- Ownable.renounceOwnership() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#317-319)

transferOwnership(address) should be declared external:

- Ownable.transferOwnership(address) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#325-328)

name() should be declared external:

- LambroToken.name() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#398-400)

symbol() should be declared external:

- LambroToken.symbol() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#402-404)

decimals() should be declared external:

- LambroToken.decimals() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#406-408)

totalSupply() should be declared external:

- LambroToken.totalSupply() (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#410-412)

balanceOf(address) should be declared external:

- LambroToken.balanceOf(address) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#414-416)

transfer(address,uint256) should be declared external:

- LambroToken.transfer(address,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#418-421)

allowance(address,address) should be declared external:

- LambroToken.allowance(address,address) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#423-425)

approve(address,uint256) should be declared external:

- LambroToken.approve(address,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#427-430)

transferFrom(address,address,uint256) should be declared external:

- LambroToken.transferFrom(address,address,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#432-436)

increaseAllowance(address,uint256) should be declared external:

- LambroToken.increaseAllowance(address,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#438-441)

decreaseAllowance(address,uint256) should be declared external:

- LambroToken.decreaseAllowance(address,uint256) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#443-446)

ExcludedFromFee(address,bool) should be declared external:

- LambroToken.ExcludedFromFee(address,bool) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#556-558)

IncludeInFee(address,bool) should be declared external:

- LambroToken.IncludeInFee(address,bool) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#560-562)

setLPAddress(address) should be declared external:

- LambroToken.setLPAddress(address) (0x201af44d9dfa5464f20b8dd8aa96fc016d26e7c0.bsccscan.com-LambroToken.sol#564-568)

Reference: <https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external>



Issues Categories

Total: [0 High, 0 Medium, 0 Low]

✓ High Severity Issues

1. No issues.

✓ Medium Severity Issues

1. No issues.

✓ Low Severity Issues

1. No issues.



Owner's possibilities

Blacklist an address (blocks transfers to this address).

Whitelist an address (allows the address to be subject to no fees).



Conclusion

The LAMBRO token contract is a non-modifiable contract that only includes exclusion rights to project costs.

Nothing to report in terms of security.

CheckDot note:

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