Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

June, 2021

Audit Details

Audited project

EUROTOKEN

Deployer address

0x57bDbfDc6374297eE49551111a2eace2915BED20

Client contacts:

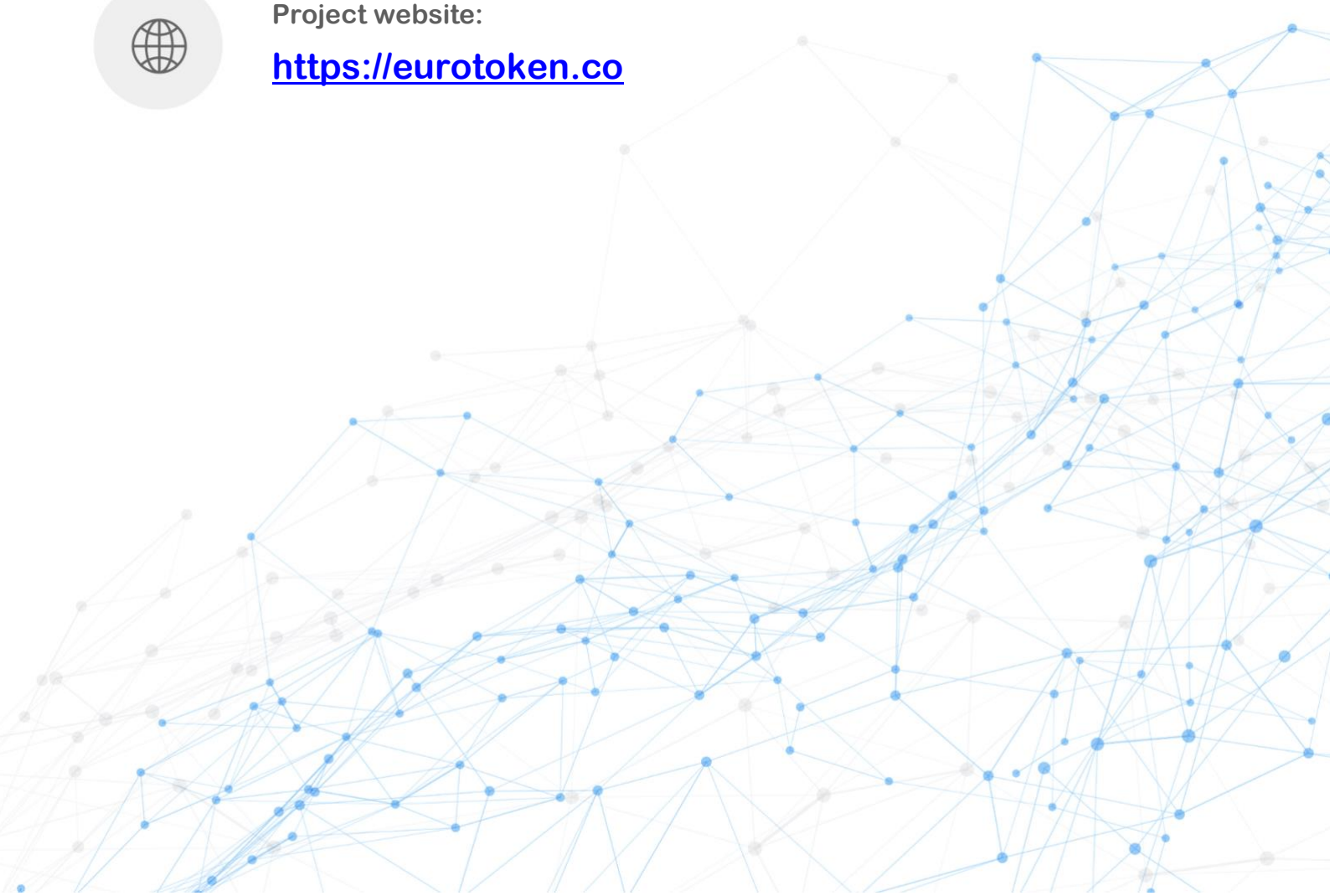
EUROTOKEN team

Blockchain

Binance Smart Chain

Project website:

https://eurotoken.co



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 below 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 TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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

TechRate was commissioned by EUROTOKEN to perform an audit of smart contracts:
https://bscscan.com/address/0x3c2C8FC79d37C97cF41d0a2E0a4C89953E49cc4e#code

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.

Contracts Details

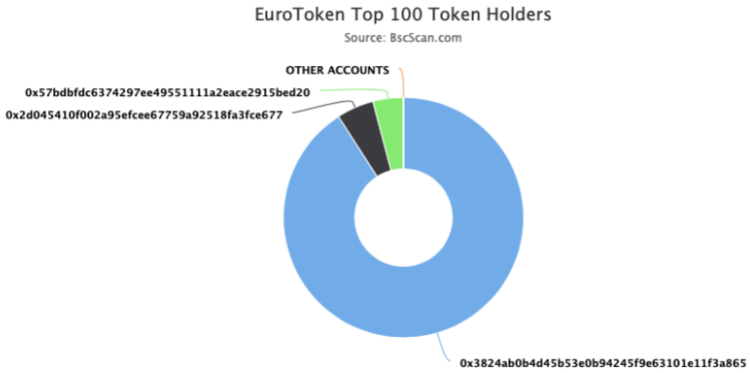
Token contract details for 08.06.2021

Contract name	EUROTOKEN
Contract address	0xe325f31a6Fe03FA1C5fC34B2D54f6C5BB04A2fA8
Total supply	1,000,000,000
Token ticker	EURO
Decimals	18
Token holders	3
Transactions count	3
Top 100 holders dominance	100.00%
Tax fee	200
Contract deployer address	0x57bDbfDc6374297eE49551111a2eace2915BED20
Contract's current owner address	0x57bdbfdc6374297ee49551111a2eace2915bed20

EUROTOKEN Token Distribution

The top 100 holders collectively own 100.00% (1,000,000,000.00 Tokens) of EuroToken

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 3

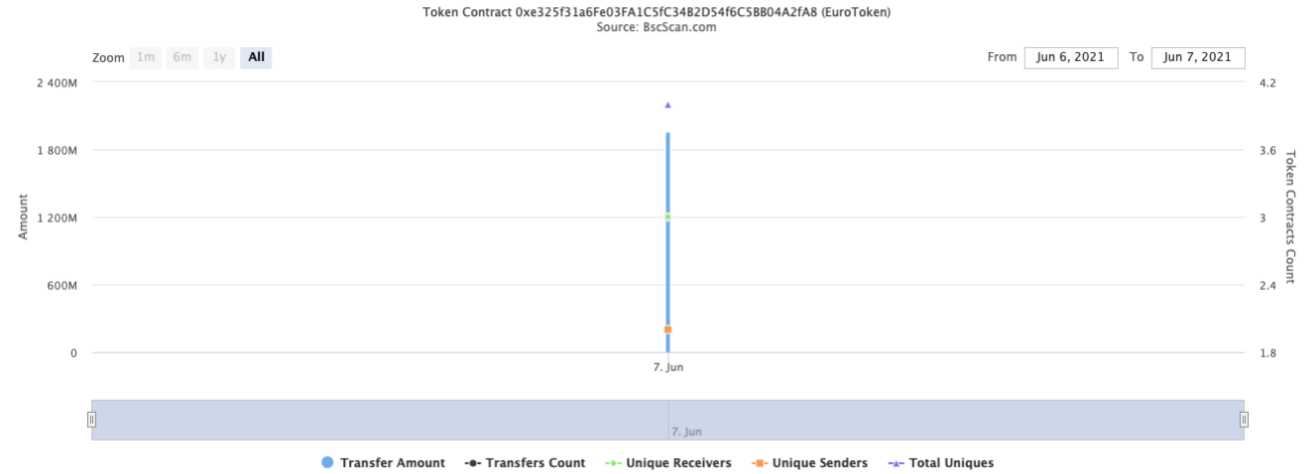


(A total of 1,000,000,000.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

EUROTOKEN Contract Interaction Details

Time Series: Token Contract Overview

Mon 7, Jun 2021 - Mon 7, Jun 2021



EUROTOKEN Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x3824ab0b4d45b53e0b94245f9e63101e11f3a865	909,000,000	90.9000%
2	0x2d045410f002a95efcee67759a92518fa3fce677	49,999,999.99999999	5.0000%
3	0x57bdbfdc6374297ee49551111a2eace2915bed20	41,000,000.00000001	4.1000%

Contract functions details

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Lib] SafeMath
  - [Int] tryAdd
  - [Int] trySub
  - [Int] tryMul
  - [Int] tryDiv
  - [Int] tryMod
  - [Int] add
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] mod
  - [Int] sub
  - [Int] div
  - [Int] mod

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Prv] _verifyCallResult

+ [Lib] SafeERC20
  - [Int] safeTransfer #
  - [Int] safeTransferFrom #
  - [Int] safeApprove #
  - [Int] safeIncreaseAllowance #
  - [Int] safeDecreaseAllowance #
  - [Prv] _callOptionalReturn #

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ Ownable (Context)
  - [Int] <Constructor> #
  - [Pub] owner

  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+ ERC20 (Context, IERC20)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Int] _transfer #
  - [Int] _mint #
  - [Int] _burn #
  - [Int] _approve #
  - [Int] _setupDecimals #
  - [Int] _beforeTokenTransfer #

+ EuroToken (ERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] startAntiBot #
    - modifiers: onlyOwner
  - [Pub] cap
  - [Pub] updateTaxSender #
    - modifiers: onlyOwner
  - [Pub] updateTaxReceipt #
    - modifiers: onlyOwner
  - [Pub] updateFeeTaxAddress #
    - modifiers: onlyOwner
  - [Pub] updateFeeTax #
    - modifiers: onlyOwner
  - [Pub] mint #
    - modifiers: onlyOwner
  - [Pub] burn #
    - modifiers: onlyOwner
  - [Ext] delegates
  - [Ext] delegate #
  - [Ext] delegateBySig #
  - [Ext] getCurrentVotes
  - [Ext] getPriorVotes
  - [Int] _delegate #
  - [Int] _moveDelegates #
  - [Int] _writeCheckpoint #
  - [Int] safe32
  - [Int] getChainId

($) = payable function
= non-constant function

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

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

No low severity issues found.

Owner privileges (In the period when the owner is not renounced)

- Owner can start antibot.

```
function startAntiBot(address _lpAddress⬆) public onlyOwner {
    require(!isAntiBotActivated, "Only one time");

    lpAddress = _lpAddress⬆;
    timeAntiBotActivated = block.timestamp;
    isAntiBotActivated = true;
}
```

- Owner can change the status of tax sender and receipt.

```
ftrace | funcSig
function updateTaxSender(address sender⬆, bool status⬆) public onlyOwner {
    require(_addressesSenderTax[sender⬆] != status⬆);
    _addressesSenderTax[sender⬆] = status⬆;
}

ftrace | funcSig
function updateTaxReceipt(address receipt⬆, bool status⬆) public onlyOwner {
    require(_addressesReceiptTax[receipt⬆] != status⬆);
    _addressesReceiptTax[receipt⬆] = status⬆;
}
```

- Owner can change tax fee address.

```
ftrace | funcSig
function updateFeeTaxAddress(address _addr⬆) public onlyOwner {
    require(feeTaxAddress != _addr⬆);
    feeTaxAddress = _addr⬆;
}
```

- Owner can change tax fee.

```
ftrace | funcSig
function updateFeeTax(uint256 feeTax⬆) public onlyOwner {
    require(feeTax⬆ <= 500, "Max feeTax is 5%");
    _feeTax = feeTax⬆;
}
```

Conclusion

Smart contracts contain owner privileges! Also, mint function is internal, if this contract will be used in bind of MasterChef contract, there will be no access to mint function.

Ownership renounce details provided by the team:
https://bscscan.com/tx/0x2260694978f9558ad7afe58fc236990bb69c5420293c052a6cd46b8f1fdf8a98

TechRate 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.