



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

DeFiato



Deployer address

0x93bad981c1afd0bc7b1def665a2b247ecbd8107b



Client contacts:

DeFiato team



Blockchain

Ethereum



Project website:

<https://defiato.com>

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 DeFiato to perform an audit of smart contracts:

<https://etherscan.io/address/0x1045f5ccb01daea4f8eab055f5fcbb7c0e7c89f0#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 15.02.2022

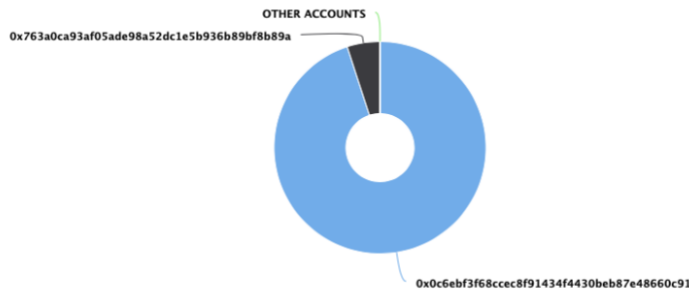
Contract name	DeFiato
Contract address	0x1045F5cCb01DAEA4f8eaB055F5FcBB7C0E7c89F0
Total supply	250,000,000
Token ticker	DFIAT
Decimals	18
Token holders	2
Transactions count	5
Top 100 holders dominance	100.00%
Contract deployer address	0x93bad981c1afd0bc7b1def665a2b247ecbd8107b
Contract's current owner address	0x3189359e6ec3b4f7ef3798458ea9b2016429983f

DeFiato Token Distribution

The top 100 holders collectively own 100.00% (250,000,000.00 Tokens) of DeFiato

Token Total Supply: 250,000,000.00 Token | Total Token Holders: 2

DeFiato Top 100 Token Holders
Source: Etherscan.io



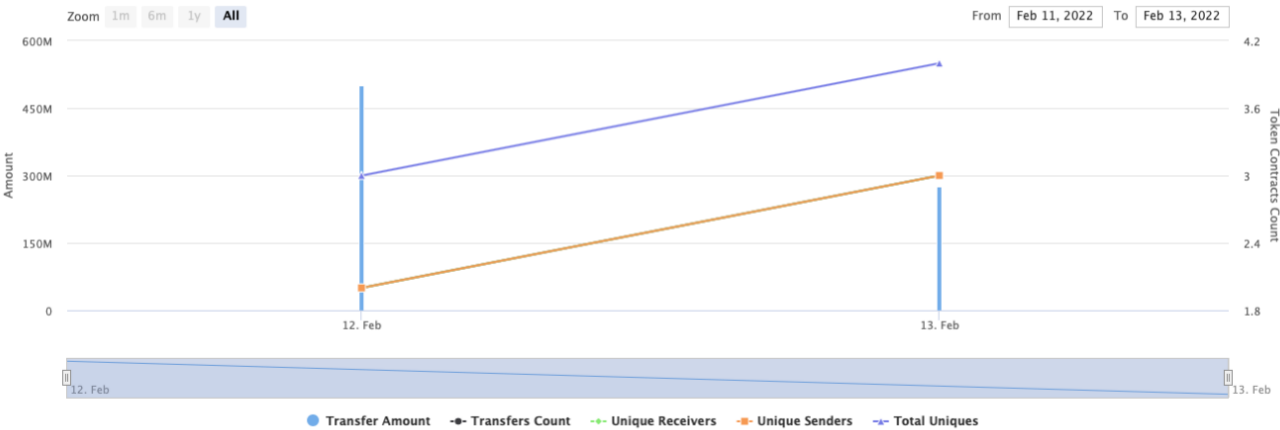
(A total of 250,000,000.00 tokens held by the top 100 accounts from the total supply of 250,000,000.00 token)

DeFiato Contract Interaction Details



Time Series: Token Contract Overview

Sat 12, Feb 2022 - Sun 13, Feb 2022

Token Contract 0x1045f5ccb01daea4f8eab055f5fcb7c0e7c89f0 (DeFiato)
Source: Etherscan.io



DeFiato Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	 0x0c6ebf3f68cc8f91434f4430beb87e48660c91	237,500,000	95.0000%
2	 0x763a0ca93af05ade98a52dc1e5b936b89bf8b89a	12,500,000	5.0000%



Contract functions details

+ [Lib] SafeMath

- [Int] add
- [Int] sub
- [Int] mul
- [Int] div

+ ERC20

- [Pub] totalSupply
- [Pub] balanceOf
- [Pub] transfer #
- [Pub] transferFrom #
- [Pub] approve #
- [Pub] allowance

+ ERC223 (ERC20)

- [Pub] transfer #
- [Pub] transfer #

+ ContractReceiver

- [Ext] tokenFallback #

+ Ownable

- [Pub] <Constructor> #
- [Pub] owner
- [Pub] renounceOwnership #
 - modifiers: onlyOwner
- [Pub] transferOwnership #
 - modifiers: onlyOwner
- [Pub] getUnlockTime
- [Pub] getTime
- [Pub] lock #
 - modifiers: onlyOwner
- [Pub] unlock #

+ BasicToken (Ownable, ERC223)

- [Pub] totalSupply
- [Pub] balanceOf
- [Prv] isContract
- [Pub] transfer #
 - modifiers: isTradable
- [Pub] transfer #
 - modifiers: isTradable
- [Pub] transfer #
 - modifiers: isTradable
- [Pub] transferFrom #
 - modifiers: isTradable
- [Pub] approve #
- [Pub] allowance
- [Pub] updateAdmin #
 - modifiers: onlyOwner
- [Pub] turnOnTradable #

- modifiers: onlyOwner

+ **DEFIATO** (BasicToken)

- **[Pub]** <Constructor> **#**
- **[Pub]** <Fallback> **(\$)**
- **[Pub]** withdraw **#**
 - modifiers: onlyOwner
- **[Pub]** transferAnyERC20Token **#**

(\$) = 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.

Notes:

- To receive tokens by the contract it should have tokenFallback function to be realized.
- There are some dangers in using send: The transfer fails if the call stack depth is at 1024 (this can always be forced by the caller) and it also fails if the recipient runs out of gas. So in order to make safe Ether transfers, always check the return value of send, use transfer or even better: Use a pattern where the recipient withdraws the money.

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

- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.
- Owner can change admin address.
- Owner can enable trading.
- Owner can withdraw contract balance.
- Anybody could transfer contract ERC20 tokens to owner's address.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

Liquidity locking details NOT provided by the team.

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.



[Techrate1](#)



[Techrate](#)



[Techrate_audits](#)