TechRate
March, 2022

TECH RATE

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

CrowdFi

Deployer address

0xf16f5dc443b44259f256683eb2d520d62d7eb1cb

Client contacts:

CrowdFi team

Blockchain

Ethereum

Project website:

Crowdfieth.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 CrowdFi to perform an audit of smart contracts:

https://etherscan.io/address/0xdf7852f17f831938a491e31d2e193b6381db05ad#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

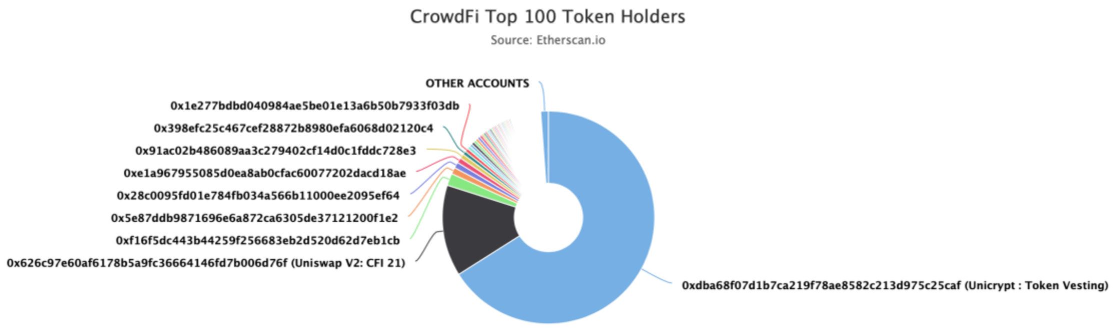
Token contract details for 16.03.2022

Contract name	CrowdFi
Contract address	0xdf7852f17F831938a491E31d2E193B6381DB05aD
Total supply	10,000,000,000
Token ticker	CFI
Decimals	18
Token holders	223
Transactions count	1,802
Top 100 holders dominance	98.83%
Early sell dev/marketing/liquidity fee	4/4/2
Total buy fees	10
Total sell fees	12
Uniswap V2 pair	0x626c97e60af6178b5a9fc36664146fd7b006d76f
Contract deployer address	0xf16f5dc443b44259f256683eb2d520d62d7eb1cb
Owner address	0xf16f5dc443b44259f256683eb2d520d62d7eb1cb

CrowdFi Token Distribution

The top 100 holders collectively own 98.83% (9,882,956,948.53 Tokens) of CrowdFi

Token Total Supply: 10,000,000,000.00 Token | Total Token Holders: 223

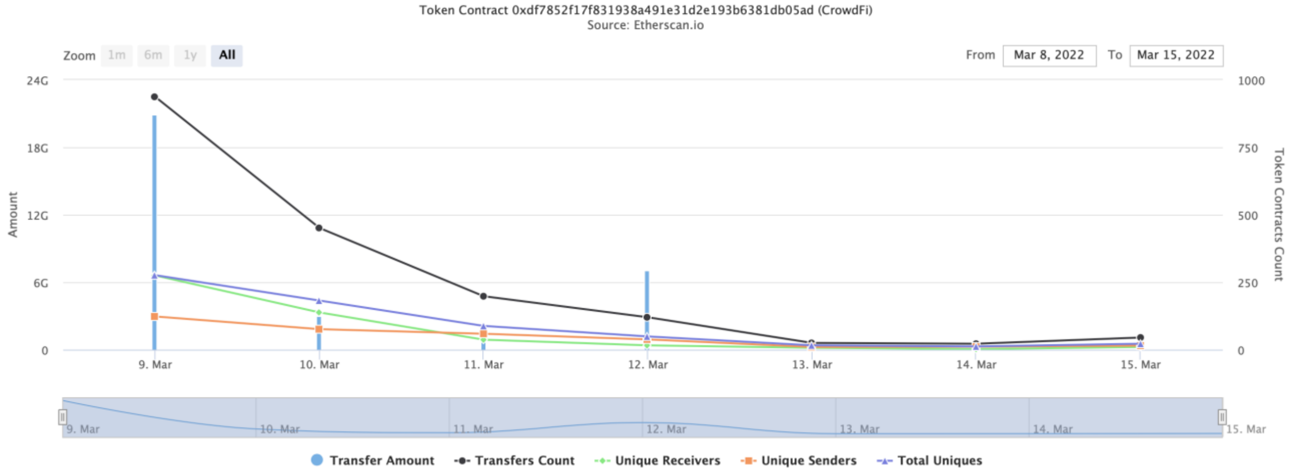


(A total of 9,882,956,948.53 tokens held by the top 100 accounts from the total supply of 10,000,000,000.00 token)

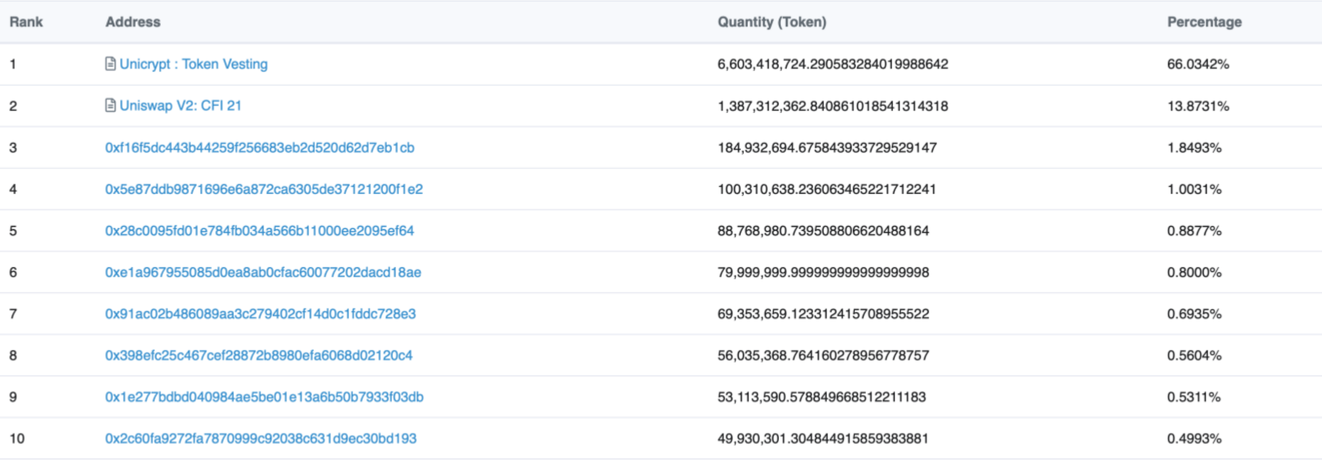
CrowdFi Contract Interaction Details

Time Series: Token Contract Overview

Wed 9, Mar 2022 - Tue 15, Mar 2022

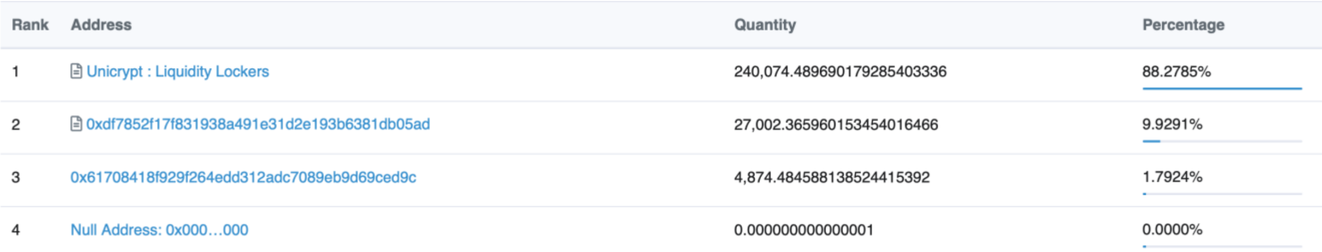


CrowdFi Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	Unicrypt : Token Vesting	6,603,418,724.290583284019988642	66.0342%
2	Uniswap V2: CFI 21	1,387,312,362.840861018541314318	13.8731%
3	0xf16f5dc443b44259f256683eb2d520d62d7eb1cb	184,932,694.675843933729529147	1.8493%
4	0x5e87ddb9871696e6a872ca6305de37121200f1e2	100,310,638.236063465221712241	1.0031%
5	0x28c0095fd01e784fb034a566b11000ee2095ef64	88,768,980.739508806620488164	0.8877%
6	0xe1a967955085d0ea8ab0cfac60077202dacd18ae	79,999,999.999999999999999998	0.8000%
7	0x91ac02b486089aa3c279402cf14d0c1fddc728e3	69,353,659.123312415708955522	0.6935%
8	0x398efc25c467cef28872b8980efa6068d02120c4	56,035,368.764160278956778757	0.5604%
9	0x1e277bdbd040984ae5be01e13a6b50b7933f03db	53,113,590.578849668512211183	0.5311%
10	0x2c60fa9272fa7870999c92038c631d9ec30bd193	49,930,301.304844915859383881	0.4993%

CrowdFi LP Token Holders



Rank	Address	Quantity	Percentage
1	Unicrypt : Liquidity Lockers	240,074.489690179285403336	88.2785%
2	0xdf7852f17f831938a491e31d2e193b6381db05ad	27,002.365960153454016466	9.9291%
3	0x61708418f929f264edd312adc7089eb9d69ced9c	4,874.484588138524415392	1.7924%
4	Null Address: 0x000…000	0.000000000000001	0.0000%

Contract functions details

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

 + [Int] IUniswapV2Pair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #
  - [Ext] initialize #

 + [Int] IUniswapV2Factory
  - [Ext] feeTo
  - [Ext] feeToSetter
  - [Ext] getPair
  - [Ext] allPairs
  - [Ext] allPairsLength
  - [Ext] createPair #
  - [Ext] setFeeTo #
```

  - [Ext] setFeeToSetter #

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

+ [Int] IERC20Metadata (IERC20)
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals

+ ERC20 (Context, IERC20, IERC20Metadata)
  - [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] _beforeTokenTransfer #

+ [Lib] SafeMath
  - [Int] add
  - [Int] sub
  - [Int] sub
  - [Int] mul
  - [Int] div
  - [Int] div
  - [Int] mod
  - [Int] mod

+ Ownable (Context)

```
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
+ [Lib] SafeMathInt
  - [Int] mul
  - [Int] div
  - [Int] sub
  - [Int] add
  - [Int] abs
  - [Int] toUint256Safe
+ [Lib] SafeMathUint
  - [Int] toInt256Safe
+ [Int] IUniswapV2Router01
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] removeLiquidity #
  - [Ext] removeLiquidityETH #
  - [Ext] removeLiquidityWithPermit #
  - [Ext] removeLiquidityETHWithPermit #
  - [Ext] swapExactTokensForTokens #
  - [Ext] swapTokensForExactTokens #
  - [Ext] swapExactETHForTokens ($)
  - [Ext] swapTokensForExactETH #
  - [Ext] swapExactTokensForETH #
  - [Ext] swapETHForExactTokens ($)
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn
+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+  CrowdFi (ERC20, Ownable)
  - [Pub] <Constructor> #
    - modifiers: ERC20
```

- [Ext] <Fallback> ($)
- [Ext] enableTrading #
  - modifiers: onlyOwner
- [Ext] removeLimits #
  - modifiers: onlyOwner
- [Ext] disableTransferDelay #
  - modifiers: onlyOwner
- [Ext] setEarlySellTax #
  - modifiers: onlyOwner
- [Ext] updateSwapTokensAtAmount #
  - modifiers: onlyOwner
- [Ext] updateMaxTxnAmount #
  - modifiers: onlyOwner
- [Ext] updateMaxWalletAmount #
  - modifiers: onlyOwner
- [Pub] excludeFromMaxTransaction #
  - modifiers: onlyOwner
- [Ext] updateSwapEnabled #
  - modifiers: onlyOwner
- [Ext] updateBuyFees #
  - modifiers: onlyOwner
- [Ext] updateSellFees #
  - modifiers: onlyOwner
- [Pub] excludeFromFees #
  - modifiers: onlyOwner
- [Pub] blacklistAccount #
  - modifiers: onlyOwner
- [Pub] setAutomatedMarketMakerPair #
  - modifiers: onlyOwner
- [Prv] _setAutomatedMarketMakerPair #
- [Ext] updateMarketingWallet #
  - modifiers: onlyOwner
- [Ext] updateDevWallet #
  - modifiers: onlyOwner
- [Pub] isExcludedFromFees
- [Int] _transfer #
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] swapBack #
- [Ext] Airdrop #
  - modifiers: onlyOwner

($) = 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.**	Low issues
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.**	Low issues
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

1. Out of gas

Issue:

- The function Airdrop() uses the loop to airdrop amounts to addresses from list. Function will be aborted with OUT_OF_GAS exception if there will be a long addresses list.
- The function Airdrop() do not compare recipients length and values length to be equal.

Recommendation:

Check that the array's length is not too big and array's length are equal.

Notes:

- Sell fee depends on type of transferring.
- Sell fee changes in transfer function but not changes back.

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

- Owner can enable trading.
- Owner can remove limits.
- Owner can disable transfer delay.
- Owner can enable/disable enableEarlySellTax.
- Owner can change swapTokensAtAmount.
- Owner can change maxTransactionAmount and maxWallet.
- Owner can exclude from maxTransactionAmount.
- Owner can enable/disable swapEnabled.
- Owner can change all fees.
- Owner can exclude addresses from fees.
- Owner can blacklist address.
- Owner can include addresses in automatedMarketMakerPairs.
- Owner can change marketing and dev wallets.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. The further transfers and operations with the funds raise are not related to this particular contract. Liquidity adding in wrong proportion.

Liquidity locking details are provided by the team:
https://app.unicrypt.network/amm/uni-v2/pair/0x626c97e60af6178b5a9fc36664146fd7b006d76f

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.