NOVOS

# KYC & AUDIT.

Novos is an agency specializing in blockchain technology solutions, Audits, KYC / Doxx.

NOVOS

# CERTIFICATE OF COMPLIANCE

Smart Contract Audit by NOVOS

Dofi Network

Audit Passed

August 19, 2022

NOVOS

# Table of Contents

- ❖ Audit Summary
- ❖ Project Overview
- ❖ Token Summary
- ❖ Main Contract Assessed
- ❖ Smart Contract Vulnerability Checks
- ❖ Contract Ownership
- ❖ Priviliged Functions
- ❖ Important Notes The Users
- ❖ Findings Summary
- ❖ Classification of Issues
- ❖ Findings Summary
- ❖ Classification of Issues
- ❖ Findings Table
- ❖ Public function that could be declared external
- ❖ Missing events arithmetic
- ❖ Statistics
- ❖ Liquidity
- ❖ Token Holders
- ❖ Liquidity Holders
- ❖ Liquidity Ownership

# Audit Summary

This report has been prepared for Dofi Network (DOFI) on the DOGECHAIN network. Novos provides both client-centered and user-centered examination of the smart contracts and their current status when applicable. This report represents the security assessment made to find issues and vulnerabilities on the source code along with the current liquidity and token holder statistics of the protocol.

A comprehensive examination has been performed, utilizing Cross Referencing, Static Analysis, In-House Security Tools, and line-by-line Manual Review.

The auditing process pays special attention to the following considerations:

- Ensuring contract logic meets the specifications and intentions of the client without exposing the user’s funds to risk.
- Testing the smart contracts against both common and uncommon attack vectors.
- Inspecting liquidity and holders statistics to inform the current status to both users and client when applicable.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Verifying contract functions that allow trusted and/or untrusted actors to mint, lock, pause, and transfer assets.
- Thorough line-by-line manual review of the entire codebase by industry experts.

# Project Overview

| Parameter | Result |
|---|---|
| Address | 0xF3484AE003c7ce4Dcc2fC890A9544Cd383e4199a |
| Name | Dofi Network |
| Token Tracker | DOFI |
| Decimals | 9 |
| Supply | 460,000,000 |
| Platform | DOGECHAIN |
| Compiler | v0.8.4+commit.c7e474f2 |
| Optimization | True / 200 |
| Other Settings: | default evmVersion |
| Language | Solidity |
| Codebase | https://explorer.dogechain.dog/address/0x0A85739762B9f9FEbDB0EE61ada9F71a5c9BE524/contracts |
| Url | https://dofinetwork.com/ |

# Main Contract Assessed

| Name | Contract | Live |
|---|---|---|
| **Dofi Network** | 0xF3484AE003c7ce4Dcc2fC890A9544Cd383e4199a | Yes |

NOVOS

# Smart Contract Vulnerability Checks

| Vulnerability | Automatic Scan | Manual Scan | Result |
|---|---|---|---|
| ❖ Unencrypted Private Data On-Chain | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Code With No Effects | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Message call with hardcoded gas amount | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Hash Collisions With Multiple Variable Length Arguments | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Unexpected Ether balance | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Presence of unused variables | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Right-To-Left-Override control character (U+202E) | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Typographical Error | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ DoS With Block Gas Limit | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Arbitrary Jump with Function Type Variable | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Insufficient Gas Griefing | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Incorrect Inheritance Order | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Write to Arbitrary Storage Location | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Requirement Violation | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Missing Protection against Signature Replay Attacks | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Weak Sources of Randomness from Chain Attributes | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |

NOVOS

# Smart Contract Vulnerability Checks

| Vulnerability | Automatic Scan | Manual Scan | Result |
|---|---|---|---|
| ❖ Authorization through tx.origin | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Delegatecall to Untrusted Callee | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Use of Deprecated Solidity Functions | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Assert Violation | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Reentrancy | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Unprotected SELFDESTRUCT Instruction | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Unprotected Ether Withdrawal | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Unchecked Call Return Value | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Outdated Compiler Version | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Integer Overflow and Underflow | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |
| ❖ Function Default Visibility | ✓ Complete | ✓ Complete | ✓ **Low / No Risk** |

# Contract Ownership

The contract ownership of Dofi Network is not currently renounced. The ownership of the contract grants special powers to the protocol creators, making them the sole addresses that can call sensible ownable functions that may alter the state of the protocol.

.

01

The current owner is the address 0x3745283D4cA1066F899FC470e37db66cd7D15691 which can be viewed from: HERE

02

The owner wallet has the power to call the functions displayed on the priviliged functions chart below, if the owner wallet is compromised this privileges could be exploited.

03

We recommend the team to renounce ownership at the right timing if possible, or gradually migrate to a timelock with governing functionalities in respect of transparency and safety considerations.

NOVOS

# Important Notes To The Users:

01 Contract name:

AntiBotLiquidityGeneratorToken

02 `amount` as the allowance of `spender` over the caller's tokens. Returns a boolean value indicating whether the operation succeeded.

03 Beware that changing an allowance with this method brings the risk that someone may use both the old and the new allowance by unfortunate transaction ordering. One possible solution to mitigate this race condition is to first reduce the spender's allowance to 0 and set the desired value afterwards

04 This contract is only required for intermediate, library-like contracts.

05 This version of SafeMath should only be used with Solidity 0.8 or later, because it relies on the compiler's built in overflow checks.

06 Returns the remainder of dividing two unsigned integers. (unsigned integer modulo),reverting with custom message when dividing by zero. CAUTION: This function is deprecated because it requires allocating memory for the error message unnecessarily. For custom revert reasons use {tryMod}.

07 Counterpart to Solidity's `%` operator. This function uses a `revert`opcode (which leaves remaining gas untouched) while Solidity uses an invalid opcode to revert (consuming all remaining gas).

08 It is unsafe to assume that an address for which this function returns false is an externally-owned account (EOA) and not a contract.

09 Among others, `isContract` will return false for the following types of addresses: - an externally-owned account - a contract in construction - an address where a contract will be create - an address where a contract lived, but was destroyed

10 You shouldn't rely on `isContract` to protect against flash loan attacks!

11 Preventing calls from contracts is highly discouraged. It breaks composability, breaks support for smart wallets like Gnosis Safe, and does not provide security since it can be circumvented by calling from a contract constructor.

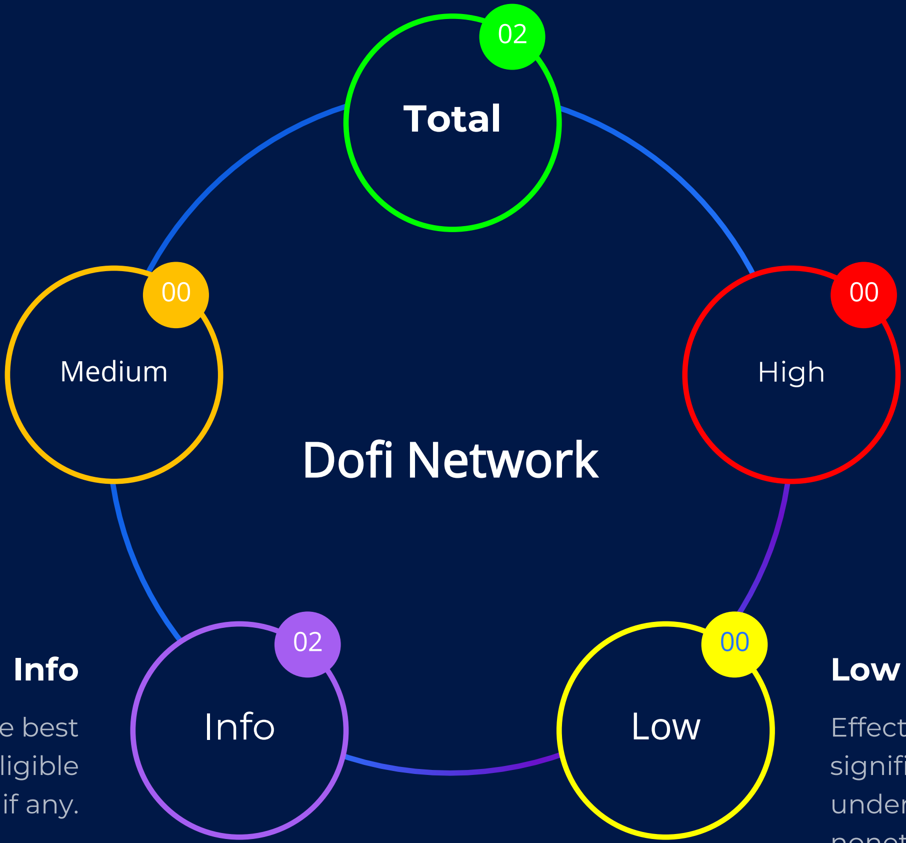
12 function removeAllFee() private { if (_taxFee == 0 && _liquidityFee == 0 && _charityFee == 0) return;

# Technical Findings Summary

## Classification of Issues

**Total**

What you should pay attention to



**Medium**

Bugs or issues with that may be subject to exploit, though their impact is somewhat limited. Issues under this classification are recommended to be fixed as soon as possible.

**High**

Exploits, vulnerabilities or errors that will certainly or probabilistically lead towards loss of funds, control, or impairment of the contract and its functions. Issues under this classification are recommended to be fixed with utmost urgency

**Info**

Consistency, syntax or style best practices. Generally pose a negligible level of risk, if any.

**Low**

Effects are minimal in isolation and do not pose a significant danger to the project or its users. Issues under this classification are recommended to be fixed nonetheless.

# Findings

## Public function that could be declared external

| ID | Severity | Contract | Function |
|---|---|---|---|
| 01 | Informational | Dofi Network | Functions: size, getKeyAtIndex, getIndexOfKey |

### Description

Gas Optimization. Public function that could be declared external

### Recommendation

Public functions that are never called by the contract should be declared external to save gas.

NOVOS

# Findings

## Missing events arithmetic

| ID | Severity | Contract | Function |
|---|---|---|---|
| 02 | Informational | Dofi Network | Missing events for setWalletBalance, setMaxBuyTransaction, setMaxSellTransaction, setSwapTokensAtAmount, setSellTransactionMultiplier |

### Description

Functions that change critical arithmetic parameters should emit an event.

### Recommendation

Emit corresponding events for critical parameter changes.

NOVOS

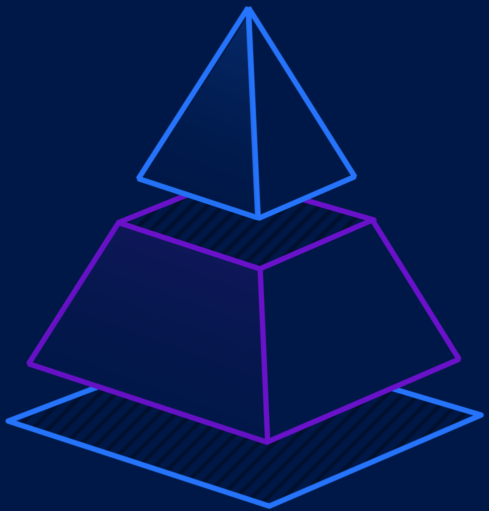
# Priviliged Functions (onlyOwner & Others)

| Function Name | Parameters | Visibility |
|---|---|---|
| ✓ renounceOwnership | ▪ none | ▪ **external** |
| ✓ transferOwnership | ▪ address newOwner | ▪ **public** |
| ✓ prepareForPartherOrExchang eListing | ▪ address_partnerOrExchangeAddress | ▪ **external** |
| ✓ setWalletBalance | ▪ uint256 _maxWalletBalance | ▪ **external** |
| ✓ setMaxBuyTransaction | ▪ uint256 _maxTxn | ▪ **external** |
| ✓ setMaxSellTransaction | ▪ uint256 _maxTxn | ▪ **external** |
| ✓ updateBusdDividendToken | ▪ address _newContract | ▪ **external** |
| ✓ updateMarketingWallet | ▪ address _newWallet | ▪ **external** |
| ✓ setSwapTokensAtAmount | ▪ uint256 _swapAmount | ▪ **external** |
| ✓ setSellTransactionMultiplier | ▪ uint256 _multiplier | ▪ **external** |
| ✓ setTradingIsEnabled | ▪ none | ▪ **external** |
| ✓ setBusdDividendEnabled | ▪ bool _enabled | ▪ **external** |
| ✓ setMarketingEnabled | ▪ bool _enabled | ▪ **external** |
| ✓ setSwapAndLiquifyEnabled | ▪ bool _enabled | ▪ **external** |
| ✓ updatebusdDividendTracker | ▪ address newAddress | ▪ **external** |
| ✓ updateUniswapV2Router | ▪ address newAddress | ▪ **external** |

NOVOS

# Priviliged Functions (onlyOwner & Others)

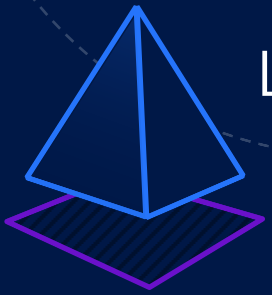
| Function Name | Parameters | Visibility |
|---|---|---|
| ✓ excludeFromFees | ▪ address account, bool excluded | ▪ **public** |
| ✓ excludeFromDividend | ▪ address account | ▪ **public** |
| ✓ setAutomatedMarketMakerP air | ▪ address pair, bool value | ▪ **external** |
| ✓ updateGasForProcessing | ▪ uint256 newValue | ▪ **external** |
| ✓ updateMinimumBalanceForDi vidends | ▪ uint256 newMinimumBalance | ▪ **external** |
| ✓ updateClaimWait | ▪ uint256 claimWait | ▪ **external** |
| ✓ processDividendTracker | ▪ uint256 gas | ▪ **external** |

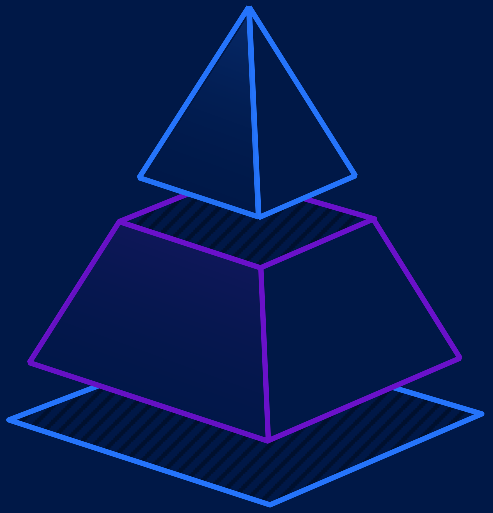


NOVOS

# Statistics

## Liquidity Info





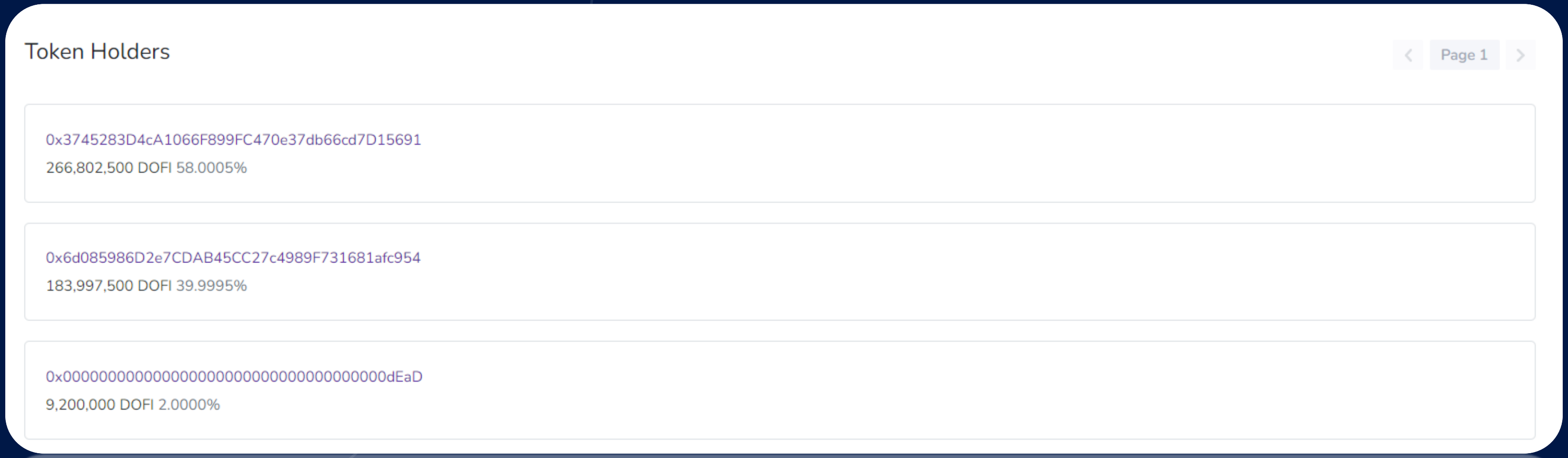
| Parameter | Result |
|---|---|
| Pair Address | 0xa461e64402c693b6a953faf37aefbf19674cf225 |
| DOFI Reserves | 0 DOFI |
| Reserves, wDoge | 0 wDoge |
| Liquidity Value | $ 0 |

NOVOS

# Statistics

## Token (DOFI) Holders Info

| Parameter | Result |
|---|---|
| DOFI Percentage Burnt | 2 % |
| DOFI Amount Burnt | 9,200,000 DOFI |
| Top 10 Percentage Own | 98 % |
| Top 10 Amount Owned | 450,800,000 DOFI |



Token Holders

0x3745283D4cA1066F899FC470e37db66cd7D15691
266,802,500 DOFI 58.0005%

0x6d085986D2e7CDAB45CC27c4989F731681afc954
183,997,500 DOFI 39.9995%

0x000000000000000000000000000000000000dEaD
9,200,000 DOFI 2.0000%

NOVOS

# Disclaimer

Novos has conducted an independent audit to verify the integrity of and highlight any vulnerabilities or errors, intentional or unintentional, that may be present in the codes that were provided for the scope of this audit. This audit report does not constitute agreement, acceptance or advocation for the Project that was audited, and users relying on this audit report should not consider this as having any merit for financial advice in any shape, form or nature. The contracts audited do not account for any economic developments that may be pursued by the Project in question, and that the veracity of the findings thus presented in this report relate solely to the proficiency, competence, aptitude and discretion of our independent auditors, who make no guarantees nor assurance that the contracts are completely free of exploits, bugs, vulnerabilities or deprecation of technologies.

All information provided in this report does not constitute financial or investment advice, nor should it be used to signal that any persons reading this report should invest their funds without sufficient individual due diligence regardless of the findings presented in this report. Information is provided 'as is', and Novos is under no covenant to the completeness, accuracy or solidity of the contracts audited. In no event will Novos or its partners, employees, agents or parties related to the provision of this audit report be liable to any parties for, or lack thereof, decisions and/or actions with regards to the information provided in this audit report.

The assessment services provided by Novos is subject to dependencies and under continuing development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where- is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.