soken

SMART CONTRACT SECURITY AUDIT

Foundation

Scan and check this report was posted at Soken Github

November, 2022

Website: soken.io

Table of Contents

Disclaimer

This is a comprehensive report based on our automated and manual examination of cybersecurity vulnerabilities and framework flaws of the project's smart contract.

Reading the full analysis report is essential to build your understanding of project's security level. It is crucial to take note, though we have done our best to perform this analysis and report, that you should not rely on the our research and cannot claim what it states or how we created it.

Before making any judgments, you have to conduct your own independent research.

We will discuss this in more depth in the following disclaimer - please read it fully.

DISCLAIMER: You agree to the terms of this disclaimer by reading this report or any portion thereof. Please stop reading this report and remove and delete any copies of this report that you download and/or print if you do not agree to these conditions. Scan and verify report's presence in the GitHub repository by a qr-code at the title page. This report is for non-reliability information only and does not represent investment advice. No one shall be entitled to depend on the report or its contents, and Soken and its affiliates shall not be held responsible to you or anyone else, nor shall Soken provide any guarantee or representation to any person with regard to the accuracy or integrity of the report.

Without any terms, warranties or other conditions other than as set forth in that exclusion and Soken excludes hereby all representations, warrants, conditions and other terms (including, without limitation, guarantees implied by the law of satisfactory quality, fitness for purposes and the use of reasonable care and skills).

The report is provided as "as is" and does not contain any terms and conditions. Except as legally banned, Soken disclaims all responsibility and responsibilities and no claim against Soken is made to any amount or type of loss or damages (without limitation, direct, indirect, special, punitive, consequential or pure economic loses or losses) that may be caused by you or any other person, or any damages or damages, including without limitations (whether innocent or negligent).

Security analysis is based only on the smart contracts. No applications or operations were reviewed for security. No product code has been reviewed.

Procedure

Our analysis contains following steps:

1. Project Analysis;

2. Manual analysis of smart contracts:
   - Deploying smart contracts on any of the network(Ropsten/Rinkeby) using Remix IDE
   - Hashes of all transaction will be recorded
   - Behaviour of functions and gas consumption is noted, as well.

3. Unit Testing:
   - Smart contract functions will be unit tested on multiple parameters and under multiple conditions to ensure that all paths of functions are functioning as intended.
   - In this phase intended behaviour of smart contract is verified.
   - In this phase, we would also ensure that smart contract functions are not consuming unnecessary gas.
   - Gas limits of functions will be verified in this stage.

4. Automated Testing:
   - Mythril
   - Oyente
   - Manticore
   - Solgraph

Terminology

We categorize the finding into 4 categories based on their vulnerability:

- Low-severity issue — less important, must be analyzed
- Medium-severity issue — important, needs to be analyzed and fixed
- High-severity issue —important, might cause vulnerabilities, must be analyzed and fixed
- Critical-severity issue —serious bug causes, must be analyzed and fixed.

Limitations

The security audit of Smart Contract cannot cover all vulnerabilities. Even if no vulnerabilities are detected in the audit, there is no guarantee that future smart contracts are safe. Smart contracts are in most cases safeguarded against specific sorts of attacks. In order to find as many flaws as possible, we carried out a comprehensive smart contract audit. Audit is a document that is not legally binding and guarantees nothing.

Basic Security Recommendation

Unlike hardware and paper wallets, hot wallets are connected to the internet and store private keys online, which exposes them to greater risk. If a company or an individual holds significant amounts of cryptocurrency in a hot wallet, they should consider using MultiSig addresses. Wallet security is enhanced when private keys are stored in different locations and are not controlled by a single entity.
More info: **https://blog.soken.io/how-to-gnosis-multisig-1c6c0860586f**

Token Contract Details for 03.11.2022

Contract Name: **Foundation**

Deployed address: **0xB13d747d783BF1A9F1D65Df74C080C890045f17e**

Total Supply: **100,000,000,000**

Token Tracker: **FND**

Decimals: **7**

Token holders: **180**

Transactions count: **1968**

Top 100 holders dominance: **99.71%**

Audit Details

Project Name: **Foundation**

Language: **Solidity**

Compiler Version: **v0.8.17**

Blockchain: **Ethereum**

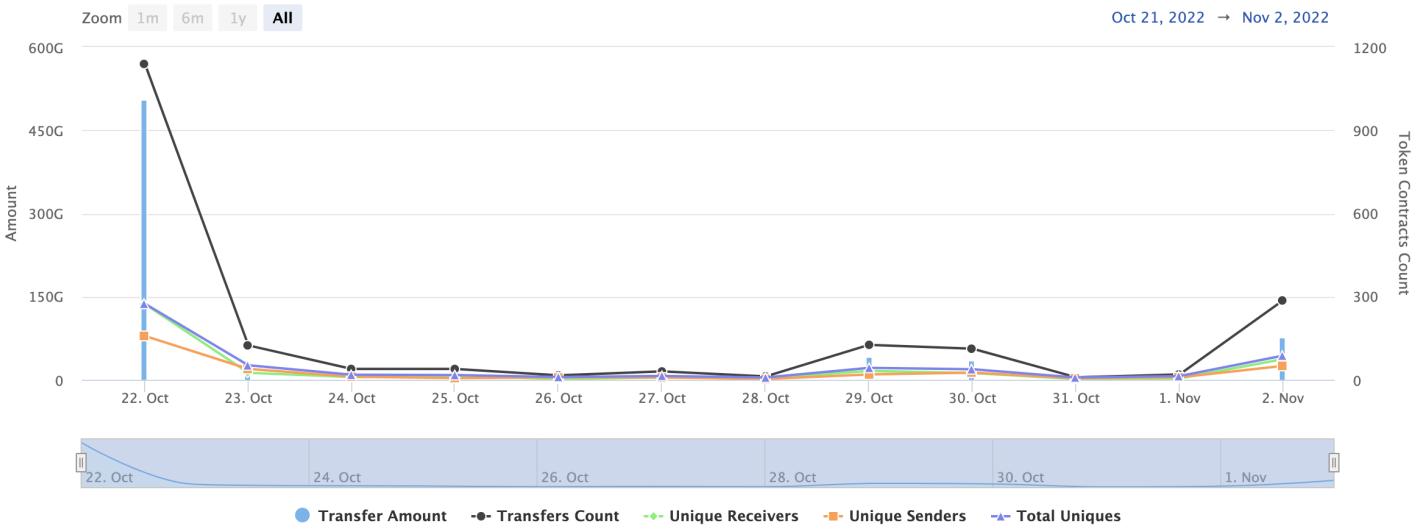
Social Profiles

Project Website: **https://foundationtoken.io/**

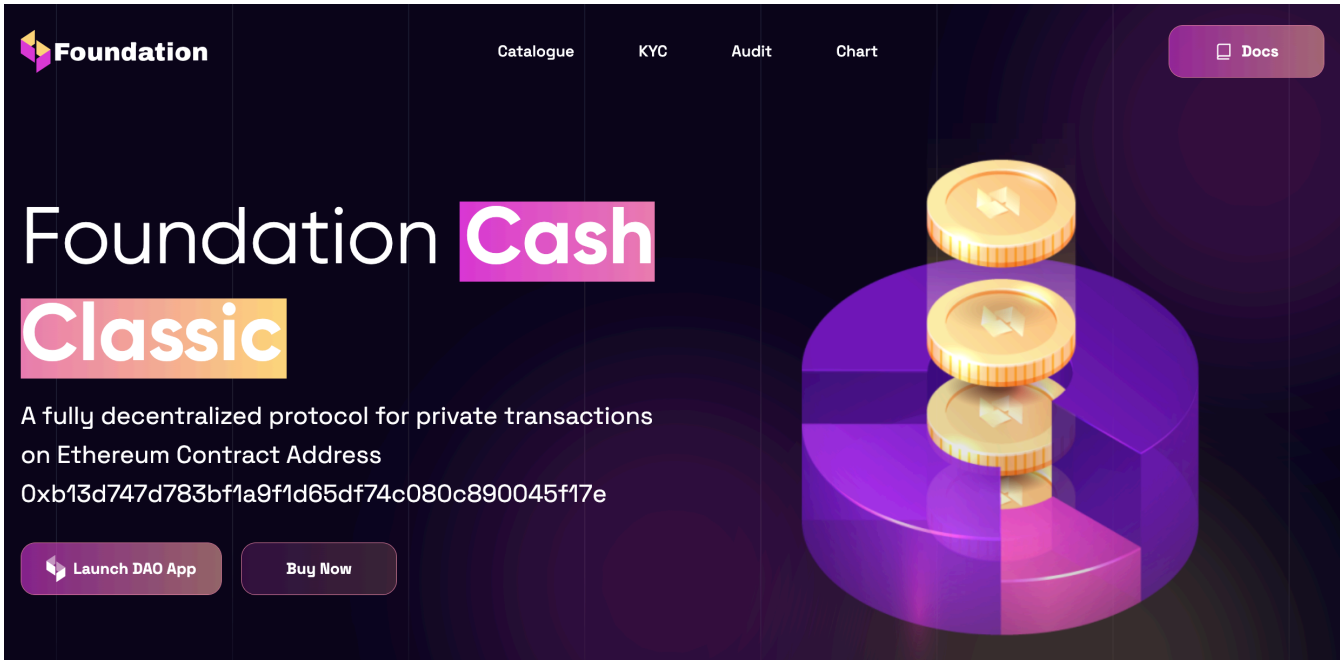
Project Twitter: **https://twitter.com/TokenFoundation**

Project Telegram: **https://t.me/Foundation_Token**

Token Analytics



Project Website Overview



✓JavaScript errors hasn't been found.
✓Malware pop-up windows hasn't been detected.
✓No issues with loading elements, code, or stylesheets.

Project Website SSL Certification

Issued To

Common Name (CN)	*.foundationtoken.io
Organization (O)	<Not Part Of Certificate>
Organizational Unit (OU)	<Not Part Of Certificate>

Issued By

Common Name (CN)	R3
Organization (O)	Let's Encrypt
Organizational Unit (OU)	<Not Part Of Certificate>

Project Website Optimization for Desktop

Performance

Values are approximate and subject to change. The performance level is calculated directly from these metrics. Show calculator

▲ 0–49 ■ 50–89 ● 90–100

INDICATORS Expand

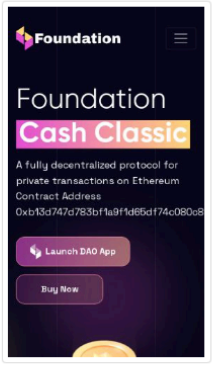
- First Contentful Paint 0.9 sec.
- Speed Index 1.1 sec.
- Largest Contentful Paint 0.9 sec.
- Time to Interactive 1.8 sec.
- Total Blocking Time 80ms
- Cumulative Layout Shift 0

Project Website Optimization for Mobile

Performance

Values are approximate and subject to change. The performance level is calculated directly from these metrics. Show calculator

▲ 0–49 ■ 50–89 ● 90–100



INDICATORS

- ▲ First Contentful Paint 3.8 sec.
- ■ Speed Index 4.6 sec.
- ▲ Largest Contentful Paint 5.0 sec.
- ▲ Time to Interactive 9.9 sec.
- ● Total Blocking Time 150ms
- ● Cumulative Layout Shift 0

Contract Function Details

- [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
- [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens
- [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens
- [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens
- [Ext] feeTo
- [Ext] feeToSetter
- [Ext] getPair
- [Ext] allPairs
- [Ext] allPairsLength
- [Ext] createPair
- [Ext] setFeeTo
- [Ext] setFeeToSetter
- [Ext] INIT_CODE_PAIR_HASH
- [Int] _msgSender
- [Int] _msgData
- [Pub] owner
- [Pub] renounceOwnership
- [Pub] transferOwnership
- [Int] _transferOwnership
- [Int] isContract
- [Int] sendValue
- [Int] functionCall
- [Int] functionCall
- [Int] functionCallWithValue
- [Int] functionCallWithValue

- [Int] functionStaticCall
- [Int] functionStaticCall
- [Int] functionDelegateCall
- [Int] functionDelegateCall
- [Int] verifyCallResult
- [Int] safeTransfer
- [Int] safeTransferFrom
- [Int] safeApprove
- [Int] safeIncreaseAllowance
- [Int] safeDecreaseAllowance
- [Prv] _callOptionalReturn
- [Ext] totalSupply
- [Ext] balanceOf
- [Ext] transfer
- [Ext] allowance
- [Ext] approve
- [Ext] transferFrom
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [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] _spendAllowance
- [Int] _beforeTokenTransfer
- [Int] _afterTokenTransfer
- [Ext] getReserves
- [Ext] setBridge
- [Ext] setMaxWallet
- [Pub] decimals
- [Pub] bridgeBalance
- [Pub] totalSupply
- [Pub] balanceOf

- [Ext] setTradeStatus
- [Ext] updateMinimumTokensBeforeFeeTaken
- [Ext] setAutomatedMarketMakerPair
- [Prv] _setAutomatedMarketMakerPair
- [Ext] excludeFromFee
- [Ext] includeInFee
- [Ext] excludeFromMaxWallet
- [Ext] includeInMaxWallet
- [Ext] updateBuyFee
- [Ext] updateSellFee
- [Ext] updateTransferFee
- [Ext] updateMarketingFeeAddress
- [Ext] updateDevAddress
- [Int] _transfer
- [Prv] removeAllFee
- [Prv] restoreAllFee
- [Prv] takeFee
- [Prv] swapTokensForETH
- [Prv] addLiquidity
- [Ext] withdrawETH
- [Ext] withdrawTokens

Vulnerabilities checking

Issue Description	Checking Status
Compiler Errors	Completed
Delays in Data Delivery	Completed
Re-entrancy	Completed
Transaction-Ordering Dependence	Completed
Timestamp Dependence	Completed
Shadowing State Variables	Completed
DoS with Failed Call	Completed
DoS with Block Gas Limit	Completed
Outdated Complier Version	Completed
Assert Violation	Completed
Use of Deprecated Solidity Functions	Completed
Integer Overflow and Underflow	Completed
Function Default Visibility	Completed
Malicious Event Log	Completed
Math Accuracy	Completed
Design Logic	Completed
Fallback Function Security	Completed
Cross-function Race Conditions	Completed
Safe Zeppelin Module	Completed

Security Issues

1) Return Value of Low-level Calls: Medium-severity L1533, L1537

The functions do not check the return value of low-level calls. This can lock Ether in the contract if the call fails or may compromise the contract if the ownership is being changed. The following calls were detected without return value validations - call

Recommendation:

Ensure return value is checked using conditional statements for low-level calls. We should also ensure that we log failed calls using events.

2) Use of Floating Pragma: Informational. L21

Solidity source files indicate the versions of the compiler they can be compiled with using a pragma directive at the top of the solidity file. This can either be a floating pragma or a specific compiler version. The contract was found to be using a floating pragma which is not considered safe as it can be compiled with all the versions described. The following affected files were found to be using floating pragma: contract.sol - ^0.8.17

Recommendation:

It is recommended to use a fixed pragma version, as future compiler versions may handle certain language constructions in a way the developer did not foresee.

2) Presence of overpowered role: Informational.

L288-L290, L296-302, L1274-1278, L1280-1283, L1304-1306, L1308-1313, L1315-1322, L1328-L1330, L1332-1334, L1336-1338, L1340-1342, L1344-1359, L1361-1376, L1378-1394, L1396-1399, L1401-1404, L1581-1583, L1585-1598

The overpowered owner (i.e., the person who has too much power) is a project design where the contract is tightly coupled to their owner (or owners); only they can manually invoke critical functions. Due to the fact that this function is only accessible from a single address, the system is heavily dependent on the address of the owner. In this case, there are scenarios that may lead to undesirable consequences for investors, e.g., if the private key of this address is compromised, then an attacker can take control of the contract.

Recommendation:

We recommend designing contracts in a trust-less manner. For instance, this functionality can be implemented in the contract's constructor. Another option is to use a MultiSig wallet for this address. For systems that are provisioned for a single user, you can use [Ownable.sol](https://github.com/OpenZeppelin/openzeppelin-contracts/blob/release-v2.5.0/contracts/ownership/Ownable.sol). For systems that require provisioning users in a group, you can use [@openzeppelin/Roles.sol](https://github.com/OpenZeppelin/openzeppelin-contracts/blob/release-v2.5.0/contracts/access/Roles.sol) or [@hq20/Whitelist.sol](https://github.com/HQ20/contracts/blob/v0.0.2/contracts/access/Whitelist.sol).

Conclusion for project owner

Medium-severity and informational issues exist within smart contracts.

NOTE: Please check the disclaimer above and note, that audit makes no statements or warranties on business model, investment attractiveness or code sustainability. Contract security report for community

SECURITY REPORT
FOR COMMUNITY

Foundation

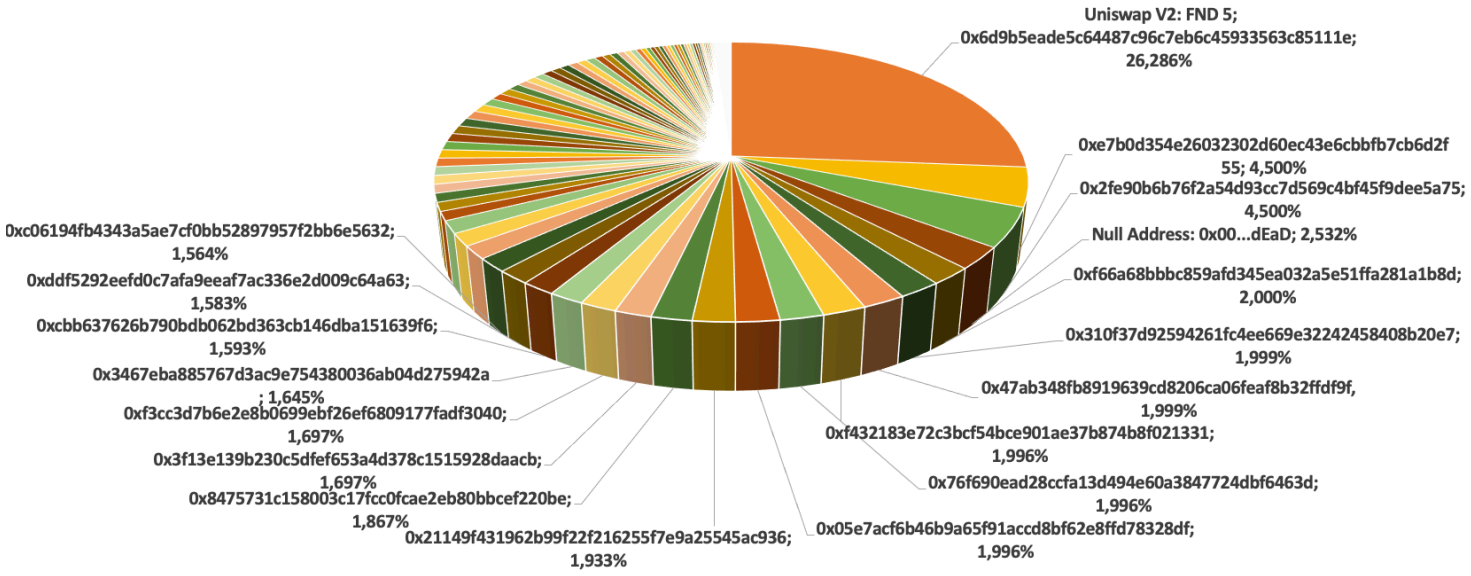
soken

Whitepaper of the project

The whitepaper of Foundation project has been verified on behalf of Soken team.

Whitepaper link: **https://github.com/DemerzelFoundation/Foundation-Token/blob/main/Foundation%20Token.pdf**

FND Token Distribution



FND Top 10 Holders

Rank	Address	Quantity (Token)	Percentage
1	Uniswap V2: FND 5	26,286,228,718.988851	26.2862%
2	0xe7b0d354e26032302d60ec43e6cbbfb7cb6d2f55	4,500,000,000	4.5000%
3	0x2fe90b6b76f2a54d93cc7d569c4bf45f9dee5a75	4,500,000,000	4.5000%
4	Null Address: 0x00...dEaD	2,532,323,510.1216769	2.5323%
5	0xf66a68bbbc859afd345ea032a5e51ffa281a1b8d	1,999,914,291.7111062	1.9999%
6	0x310f37d92594261fc4ee669e32242458408b20e7	1,999,000,000	1.9990%
7	0x47ab348fb8919639cd8206ca06feaf8b32ffdf9f	1,998,623,476.5287072	1.9986%
8	0xf432183e72c3bcf54bce901ae37b874b8f021331	1,996,372,375.1542096	1.9964%
9	0x76f690ead28ccfa13d494e60a3847724dbf6463d	1,996,276,127.4648928	1.9963%
10	0x05e7acf6b46b9a65f91accd8bf62e8ffd78328df	1,995,714,993.3112335	1.9957%

Soken Contact Info

Website: www.soken.io

Mob: (+1)416-875-4174

32 Britain Street, Toronto, Ontario, Canada

Telegram: @team_soken

GitHub: sokenteam

Twitter: @soken_team