Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

February, 2022

Audit Details

Audited project

Saitanobi

Deployer address

0xe1d8e50e2d8a066dd92578099f8c0b16d0647635

Client contacts:

Saitanobi team

Blockchain

Ethereum

Project website:

https://saitanobi.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 Saitanobi to perform an audit of smart contracts:

https://etherscan.io/address/0x5e9f35e8163c44cd7e606bdd716abed32ad2f1c6#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.

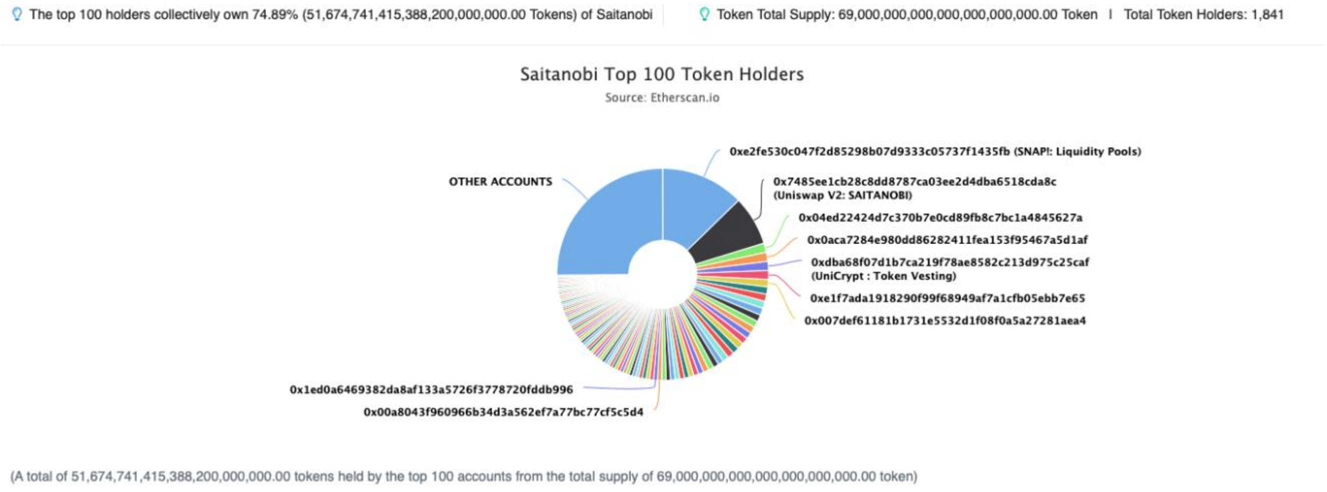
The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

Contracts Details

Token contract details for 20.02.2022

Contract name	Saitanobi
Contract address	0x5e9F35E8163c44cD7e606BdD716AbED32AD2F1C6
Total supply	69,000,000,000,000,000,000,000
Token ticker	SAITANOBI
Decimals	9
Token holders	1,841
Transactions count	6,059
Top 100 holders dominance	74.89%
Liquidity fee	12
Tax fee	1
Total fees	4708504585115537457056895073690
Uniswap V2 pair	0x7485ee1cb28c8dd8787ca03ee2d4dba6518cda8c
Contract deployer address	0xe1d8e50e2d8a066dd92578099f8c0b16d0647635
Contract's current owner address	0xe1d8e50e2d8a066dd92578099f8c0b16d0647635

Saitanobi Token Distribution



The top 100 holders collectively own 74.89% (51,674,741,415,388,200,000,000.00 Tokens) of Saitanobi

Token Total Supply: 69,000,000,000,000,000,000,000.00 Token | Total Token Holders: 1,841

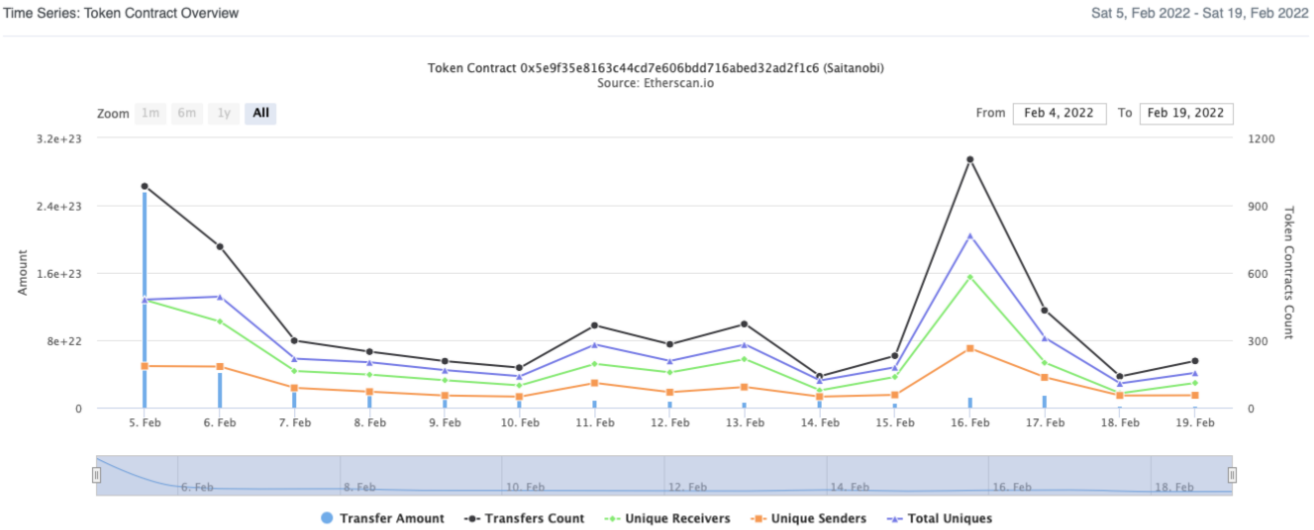
Saitanobi Top 100 Token Holders

Source: Etherscan.io

OTHER ACCOUNTS
0xe2fe530c047f2d85298b07d9333c05737f1435fb (SNAP!: Liquidity Pools)
0x7485ee1cb28c8dd8787ca03ee2d4dba6518cda8c (Uniswap V2: SAITANOBI)
0x04ed22424d7c370b7e0cd89fb8c7bc1a4845627a
0x0aca7284e980dd86282411fea153f95467a5d1af
0xdba68f07d1b7ca219f78ae8582c213d975c25caf (UniCrypt : Token Vesting)
0xe1f7ada1918290f99f68949af7a1cfb05ebb7e65
0x007def61181b1731e5532d1f08f0a5a27281aea4
0x1ed0a6469382da8af133a5726f3778720fddb996
0x00a8043f960966b34d3a562ef7a77bc77cf5c5d4

(A total of 51,674,741,415,388,200,000,000.00 tokens held by the top 100 accounts from the total supply of 69,000,000,000,000,000,000,000.00 token)

Saitanobi Contract Interaction Details



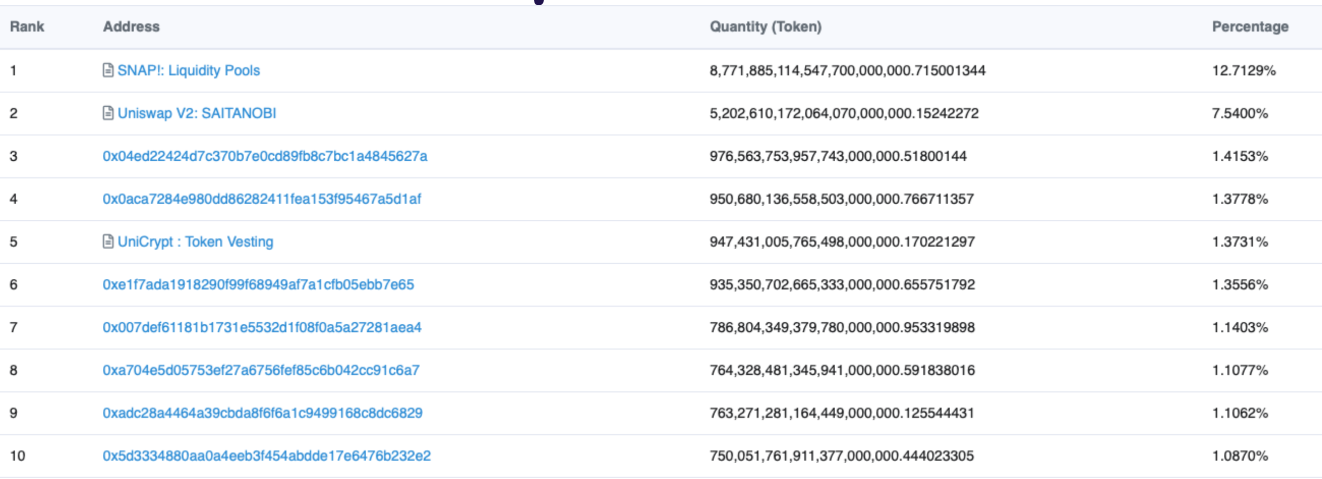
Time Series: Token Contract Overview

Sat 5, Feb 2022 - Sat 19, Feb 2022

Token Contract 0x5e9f35e8163c44cd7e606bdd716abed32ad2f1c6 (Saitanobi)

Source: Etherscan.io

Saitanobi Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	SNAP!: Liquidity Pools	8,771,885,114,547,700,000,000.715001344	12.7129%
2	Uniswap V2: SAITANOBI	5,202,610,172,064,070,000,000.15242272	7.5400%
3	0x04ed22424d7c370b7e0cd89fb8c7bc1a4845627a	976,563,753,957,743,000,000.51800144	1.4153%
4	0x0aca7284e980dd86282411fea153f95467a5d1af	950,680,136,558,503,000,000.766711357	1.3778%
5	UniCrypt : Token Vesting	947,431,005,765,498,000,000.170221297	1.3731%
6	0xe1f7ada1918290f99f68949af7a1cfb05ebb7e65	935,350,702,665,333,000,000.655751792	1.3556%
7	0x007def61181b1731e5532d1f08f0a5a27281aea4	786,804,349,379,780,000,000.953319898	1.1403%
8	0xa704e5d05753ef27a6756fef85c6b042cc91c6a7	764,328,481,345,941,000,000.591838016	1.1077%
9	0xadc28a4464a39cbda8f6f6a1c9499168c8dc6829	763,271,281,164,449,000,000.125544431	1.1062%
10	0x5d3334880aa0a4eeb3f454abdde17e6476b232e2	750,051,761,911,377,000,000.444023305	1.0870%

Contract functions details

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

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

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

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Prv] _functionCallWithValue #

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] geUnlockTime
  - [Pub] lock #
    - modifiers: onlyOwner
  - [Pub] unlock #

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

  - [Ext] setFeeToSetter #

+ [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] 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 #

+ [Int] IAirdrop
  - [Ext] airdrop #

+  Saitanobi (Context, IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Pub] name
  - [Pub] symbol
  - [Pub] decimals
  - [Pub] totalSupply
  - [Pub] balanceOf
  - [Pub] transfer #
  - [Pub] allowance
  - [Pub] approve #
  - [Pub] transferFrom #
  - [Pub] increaseAllowance #
  - [Pub] decreaseAllowance #
  - [Pub] isExcludedFromReward
  - [Pub] totalFees
  - [Ext] airdrop #
    - modifiers: onlyOwner
  - [Int] airdropInternal #
  - [Ext] airdropArray #
    - modifiers: onlyOwner
  - [Pub] deliver #
  - [Pub] reflectionFromToken
  - [Pub] tokenFromReflection
  - [Pub] excludeFromReward #
    - modifiers: onlyOwner
  - [Ext] includeInReward #
    - modifiers: onlyOwner
  - [Prv] _transferBothExcluded #
  - [Pub] excludeFromFee #
    - modifiers: onlyOwner
  - [Pub] includeInFee #
    - modifiers: onlyOwner
  - [Pub] setMarketingFeePercent #
    - modifiers: onlyOwner
  - [Pub] setMarketingWallet #
    - modifiers: onlyOwner
  - [Ext] setTaxFeePercent #
    - modifiers: onlyOwner
  - [Ext] setLiquidityFeePercent #
    - modifiers: onlyOwner
  - [Ext] _setMaxWalletSizePercent #
    - modifiers: onlyOwner
  - [Ext] setMaxTxAmount #
    - modifiers: onlyOwner
  - [Ext] setSwapThresholdAmount #
    - modifiers: onlyOwner
  - [Pub] claimTokens #
    - modifiers: onlyOwner
```

- [Ext] claimOtherTokens #
  - modifiers: onlyOwner
- [Ext] clearStuckBalance #
  - modifiers: onlyOwner
- [Ext] addBotWallet #
  - modifiers: onlyOwner
- [Ext] removeBotWallet #
  - modifiers: onlyOwner
- [Pub] getBotWalletStatus
- [Ext] allowtrading #
  - modifiers: onlyOwner
- [Pub] setSwapAndLiquifyEnabled #
  - modifiers: onlyOwner
- [Ext] <Fallback> ($)
- [Prv] _reflectFee #
- [Prv] _getValues
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeLiquidity #
- [Prv] calculateTaxFee
- [Prv] calculateLiquidityFee
- [Prv] removeAllFee #
- [Prv] restoreAllFee #
- [Pub] isExcludedFromFee
- [Prv] _approve #
- [Prv] _transfer #
- [Prv] swapAndLiquify #
  - modifiers: lockTheSwap
- [Prv] swapTokensForEth #
- [Prv] addLiquidity #
- [Prv] _tokenTransfer #
- [Prv] _transferStandard #
- [Prv] _transferToExcluded #
- [Prv] _transferFromExcluded #

($) = 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.	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

1. Out of gas

Issue:

- The function includeInReward() uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

- The function _getCurrentSupply also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

Recommendation:

Check that the excluded array length is not too big.

Notes:

- Liquidity adding in wrong proportion.

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

- Owner can airdrop.
- Owner can exclude from the fee.
- Owner can change the tax, marketing and liquidity fee.
- Owner can change the maximum transaction amount.
- Owner can change marketing wallet.
- Owner can change number of tokens to add to liquidity.
- Owner can withdraw BNBs and ERC20 tokens.
- Owner can add/remove bot wallets.
- Owner can allow trading.
- Owner can change max wallet size.
- Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.

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.