



# Smart Contract Security Audit

## Audit details:

Audited project:	Saturna
Deployer address:	0x67f7f8d9c71ef84f8b9a340b58d3e2d5b533501f
Client contacts:	Saturna team
Blockchain:	Binance Smart Chain
Project website:	<a href="https://saturna.co">https://saturna.co</a>

# 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 Saturna to perform an audit of smart contracts:

- <https://bscscan.com/address/0x1e446cbea52badeb614fbe4ab7610f737995fb44#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 09.05.2021.

Contract name:	Saturna
Contract address:	0x1e446cbea52badeb614fbe4ab7610f737995fb44
Total supply:	1000000000000000000000000
Token ticker:	SAT
Decimals:	9
Token holders:	12553
Transactions count:	26172
Top 100 holders dominance:	81.15 %
Liquidity fee:	5
Tax fee:	5
Total fees:	64063317645896689476766
Uniswap V2 pair:	0xad7db2aea6e8904347be097f920174469a64774e
Contract deployer address:	0x67f7f8d9c71ef84f8b9a340b58d3e2d5b533501f
Contract's current owner address:	0x00

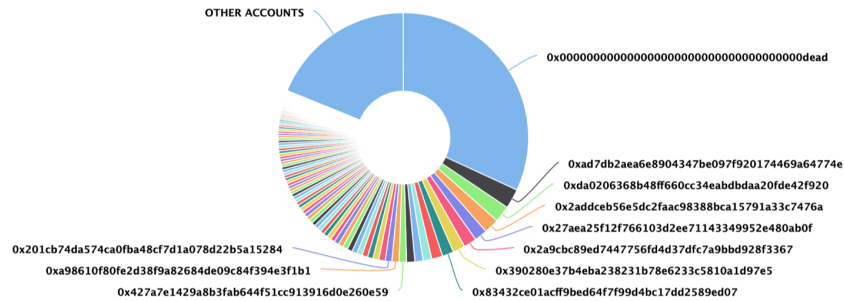
# Saturna token distribution

The top 100 holders collectively own 81.15% (811,533,748,165,695.00 Tokens) of Saturna

Token Total Supply: 1,000,000,000,000.00 Token | Total Token Holders: 12,553

Saturna Top 100 Token Holders

Source: BscScan.com



(A total of 811,533,748,165,695.00 tokens held by the top 100 accounts from the total supply of 1,000,000,000,000.00 token)


## Saturna contract interaction details

Time Series: Token Contract Overview

Thu 6, May 2021 - Sat 8, May 2021



### Saturna top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x00000000000000000000000000000000dead	319,090,632,476,320.813061563	31.9091%
2	 0xad7db2aea6e8904347be0971920174469a64774e	25,408,341,939,620.814679968	2.5408%
3	0xda0206368b48ff660cc34eabdbdaa20fde42f920	21,297,330,224,483.924037226	2.1297%
4	0x2addceb56e5dc2faac98388bca15791a33c7476a	19,500,766,740,465.659710812	1.9501%
5	0x27aea25f12f766103d2ee71143349952e480ab0f	16,768,067,225,443.908045042	1.6768%
6	0x2a9cbc89ed7447756fd4d37d1c7a9bbd928f3367	16,681,694,152,842.162673991	1.6682%
7	0x390280e37b4eba238231b78e6233c5810a1d97e5	15,672,711,640,167.506047152	1.5673%
8	0x83432ce01acff9bed64f7f99d4bc17dd2589ed07	14,866,477,429,849.985861848	1.4866%
9	0x67f7f8d9c71ef84f8b9a340b58d3e2d5b533501f	14,213,112,653,512.760902925	1.4213%
10	0x91b8795cb19cbcd4b7473411a65d8edac3c77091	11,141,036,196,477.188895466	1.1141%

## Saturna LP token holders

Rank	Address	Quantity	Percentage
1	<a href="#">0x00</a>	5,953.875986273494059241	53.1785%
2	<a href="#">0x00dead</a>	5,079.436230140754533435	45.3682%
3	<a href="#">0x07d80ae6f36a5e08dca74ce884a24d39db9934ed</a>	148.471087970255000771	1.3261%
4	<a href="#">0xd500b8462be1b5fd21faca2de1475537e8cb1115</a>	4.020964620675134439	0.0359%
5	<a href="#">0xb51d0c90dae0bf15530c039dfe43c1fc64d33c23</a>	2.461570101681645664	0.0220%
6	<a href="#">0x97712c56b8e3cca6915cd9575a54faeb28020e9</a>	1.989651647324726501	0.0178%
7	<a href="#">0xb348f09f28f8eef32774661528a8a92fac27f660</a>	1.749572253946771582	0.0156%
8	<a href="#">0x2b837fb29b4c360f9e832ffa6b787219af14fb74</a>	1.098221613781016465	0.0098%
9	<a href="#">0x92f0f7b5d87425056148e60e78e4ebf312f7787b</a>	0.797200215376053604	0.0071%
10	<a href="#">0xebfca4daed91b32a41ccfd6de4b7fd5571f0e41</a>	0.410925687761706567	0.0037%

# 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)

- [Int] <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 #

#### + Saturna (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
- [Pub] deliver #
- [Pub] reflectionFromToken
- [Pub] tokenFromReflection
- [Pub] excludeFromReward #
  - modifiers: onlyOwner
- [Ext] includeInReward #
  - modifiers: onlyOwner
- [Prv] \_transferBothExcluded #
- [Pub] excludeFromFee #
  - modifiers: onlyOwner
- [Pub] includeInFee #
  - modifiers: onlyOwner
- [Ext] setTaxFeePercent #

- modifiers: onlyOwner
- [Ext] setLiquidityFeePercent #
  - modifiers: onlyOwner
- [Ext] setMaxTxPercent #
  - 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.

```
function includeInReward(address account) external onlyOwner() {
    require(!_isExcluded[account], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account) {
            _excluded[i] = _excluded[_excluded.length - 1];
            tOwned[account] = 0;
            _isExcluded[account] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- ❑ 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.

```
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

Recommendation:

Use `EnumerableSet` instead of array or do not use long arrays.

# Conclusion

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

Liquidity burning transaction provided by the team -

<https://bscscan.com/tx/0x2e87f434cbab0d41a8bd8b5cadb139f610319c05554fde4ba868700b172778ef>

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.*