



# **SATURNA (SAT) TOKEN SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT**

<b>Customer:</b>	Saturna Team ( <a href="https://saturna.co/">https://saturna.co/</a> )
<b>Prepared on:</b>	12/05/2021
<b>Platform:</b>	Binance Smart Chain
<b>Language:</b>	Solidity
<b>Audit Type:</b>	Standard

audit@etherauthority.io

# Table of contents

Project File	4
Introduction	4
Quick Stats	5
Executive Summary	6
Code Quality	6
Documentation	7
Use of Dependencies	7
AS-IS overview	8
Severity Definitions	11
Audit Findings	12
Conclusion	16
Our Methodology	17
Disclaimers	19
Appendix	
• Code Flow Diagram	20
• Slither Report Log	21

THIS IS SECURITY AUDIT REPORT DOCUMENT AND WHICH MAY CONTAIN INFORMATION WHICH IS CONFIDENTIAL. WHICH INCLUDES ANY POTENTIAL VULNERABILITIES AND MALICIOUS CODES WHICH CAN BE USED TO EXPLOIT THE SOFTWARE. THIS MUST BE REFERRED INTERNALLY AND ONLY SHOULD BE MADE AVAILABLE TO PUBLIC AFTER ISSUES ARE RESOLVED.

## Project file

<b>Name</b>	Code Review and Security Analysis Report for Saturna (SAT) Token Smart Contract
<b>Platform</b>	BSC / Solidity
<b>File</b>	Saturna.sol
<b>File MD5 hash</b>	65871E989026D9172A08F4D3050C45A7
<b>Online Contract Code</b>	<a href="https://bscscan.com/address/0x1e446CbEa52BAdeB614FBe4Ab7610F737995fB44">https://bscscan.com/address/0x1e446CbEa52BAdeB614FBe4Ab7610F737995fB44</a>

## Introduction

We were contracted by the Saturna team to perform the Security audit of the Saturna Token smart contract code. The audit has been performed using manual analysis as well as using automated software tools. This report presents all the findings regarding the audit performed on 12/05/2021.

The Audit type was Standard Audit. Which means this audit is concluded based on Standard audit scope, which is one security engineer performing audit procedure for 2 days. This document outlines all the findings as well as an AS-IS overview of the smart contract codes.

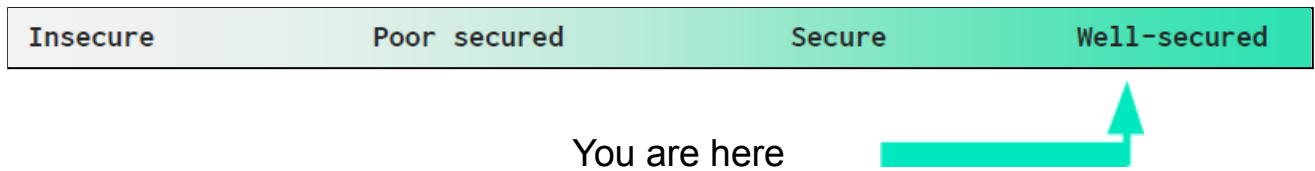
## Quick Stats:

Main Category	Subcategory	Result
Contract Programming	Solidity version not specified	Passed
	Solidity version too old	Moderated
	Integer overflow/underflow	Passed
	Function input parameters lack of check	Passed
	Function input parameters check bypass	Passed
	Function access control lacks management	Passed
	Critical operation lacks event log	Passed
	Human/contract checks bypass	Passed
	Random number generation/use vulnerability	Passed
	Fallback function misuse	Passed
	Race condition	Passed
	Logical vulnerability	Passed
	Other programming issues	Passed
Code Specification	Function visibility not explicitly declared	Passed
	Var. storage location not explicitly declared	Passed
	Use keywords/functions to be deprecated	Passed
	Other code specification issues	Passed
Gas Optimization	Assert() misuse	Passed
	High consumption 'for/while' loop	Moderated
	High consumption 'storage' storage	Passed
	"Out of Gas" Attack	Passed
Business Risk	The maximum limit for mintage not set	Passed
	"Short Address" Attack	Passed
	"Double Spend" Attack	Passed

**Overall Audit Result: PASSED**

## Executive Summary

According to the **standard** audit assessment, Customer's solidity smart contract is **Well secured**.



We used various tools like Mythril, Slither and Remix IDE. At the same time this finding is based on critical analysis of the manual audit.

All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the Audit overview section. General overview is presented in AS-IS section and all identified issues can be found in the Audit overview section.

**We found 0 critical, 0 high, 0 medium and 3 low and some very low level issues.**

## Code Quality

Saturna Token smart contract has 1 smart contract. This smart contract also contains Libraries, Smart contract inherits and Interfaces. These are compact and well written contracts.

The libraries in the Saturna Token protocol are part of its logical algorithm. A library is a different type of smart contract that contains reusable code. Once deployed on the blockchain (only once), it is assigned a specific address and its properties / methods can be reused many times by other contracts in the Saturna Token protocol.

The Saturna team has **not** provided scenario and unit test scripts, which would have helped to determine the integrity of the code in an automated way.

Overall, code parts are **not well** commented on smart contracts.

## Documentation

We were given Saturna token smart contracts code in the form of a BscScan web link. The hash of that code and that web link are mentioned above in the table.

As mentioned above, most code parts are **not well** commented. so it is difficult to quickly understand the programming flow as well as complex code logic. Comments are very helpful in understanding the overall architecture of the protocol.

Another source of information was its official website which provided rich information about the project architecture and tokenomics.

## Use of Dependencies

As per our observation, the libraries are used in this smart contract infrastructure that are based on well known industry standard open source projects. And their core code blocks are written well.

Apart from libraries, its functions are used in smart contract calls.

# AS-IS overview

Saturna is a BEP20 Token smart contract having custom features like Burning, Tax, liquidity locking, etc.

## Saturna.sol

### (1) Interfaces

- (a) IERC20
- (b) IUniswapV2Factory
- (c) IUniswapV2Pair
- (d) IUniswapV2Router01
- (e) IUniswapV2Router02

### (2) Inherited contracts

- (a) Context: Context contract.
- (b) Ownable: Ownership contract.
- (c) IERC20: IERC20 contract.

### (3) Usages

- (a) using SafeMath for uint256;
- (b) using Address for address;

### (4) Events

- (a) event Transfer(address indexed from, address indexed to, uint256 value);
- (b) event Approval(address indexed owner, address indexed spender, uint256 value);
- (c) event OwnershipTransferred(address indexed previousOwner, address indexed newOwner);



- (d) event PairCreated(address indexed token0, address indexed token1, address pair, uint);
- (e) event Approval(address indexed owner, address indexed spender, uint value);
- (f) event Transfer(address indexed from, address indexed to, uint value);
- (g) event Mint(address indexed sender, uint amount0, uint amount1);
- (h) event Burn(address indexed sender, uint amount0, uint amount1, address indexed to);
- (i) event Swap(address indexed sender, uint amount0In, uint amount1In, uint amount0Out, uint amount1Out, address indexed to );
- (j) event Sync(uint112 reserve0, uint112 reserve1);
- (k) event MinTokensBeforeSwapUpdated(uint256 minTokensBeforeSwap);
- (l) event SwapAndLiquifyEnabledUpdated(bool enabled);
- (m) event SwapAndLiquify( uint256 tokensSwapped, uint256 ethReceived, uint256 tokensIntoLiquidity );

## (5) Functions

Sl.	Functions	Type	Observation	Conclusion
1	totalSupply	read	Passed	No Issue
2	name	read	Passed	No Issue
3	symbol	read	Passed	No Issue
4	decimals	read	Passed	No Issue
5	totalSupply	read	Passed	No Issue
6	balanceOf	read	Passed	No Issue
7	transfer	write	Passed	No Issue
8	allowance	read	Passed	No Issue
9	approve	write	Passed	No Issue
10	transferFrom	write	Passed	No Issue
11	increaseAllowance	write	Passed	No Issue
12	decreaseAllowance	write	Passed	No Issue
13	isExcludedFromReward	read	Passed	No Issue
14	totalFees	read	Passed	No Issue
15	deliver	write	Passed	No Issue
16	reflectionFromToken	read	Passed	No Issue

17	tokenFromReflection	read	Passed	No Issue
18	excludeFromReward	write	access by only owner	No Issue
19	includeInReward	external	Infinite loop possibility	<b>Refer Audit Findings</b>
20	_transferBothExcluded	private	Passed	No Issue
21	excludeFromFee	write	access by only owner	No Issue
22	includeInFee	write	Passed	No Issue
23	setTaxFeePercent	external	Passed	No Issue
24	setLiquidityFeePercent	external	Passed	No Issue
25	setMaxTxPercent	external	Passed	No Issue
26	setSwapAndLiquifyEnabled	write	Passed	No Issue
27	_reflectFee	private	Passed	No Issue
28	_getValues	read	Passed	No Issue
29	_getTValues	read	Passed	No Issue
30	_getRValues	pure	Passed	No Issue
31	_getRate	read	Passed	No Issue
32	_getCurrentSupply	read	Passed	No Issue
33	takeLiquidity	write	Passed	No Issue
34	calculateTaxFee	read	Passed	No Issue
35	calculateLiquidityFee	read	Passed	No Issue
36	removeAllFee	write	Passed	No Issue
37	restoreAllFee	write	Passed	No Issue
38	isExcludedFromFee	read	Passed	No Issue
39	approve	write	Passed	No Issue
40	transfer	write	Passed	No Issue
41	swapAndLiquify	write	Passed	No Issue
42	swapTokensForEth	write	Passed	No Issue
43	addLiquidity	write	Ownership control	<b>Refer Audit Findings</b>
44	_tokenTransfer	write	Passed	No Issue
45	_transferStandard	write	Passed	No Issue
46	_transferToExcluded	write	Passed	No Issue
47	_transferFromExcluded	write	Passed	No Issue
48	_msgSender	read	Passed	No Issue
49	_msgData	read	Passed	No Issue
50	owner	read	Passed	No Issue
51	renounceOwnership	write	Passed	No Issue
52	transferOwnership	write	Passed	No Issue
53	geUnlockTime	read	Passed	No Issue

54	lock	write	Passed	No Issue
55	unlock	write	Passed	No Issue

## Severity Definitions

Risk Level	Description
<b>Critical</b>	Critical vulnerabilities are usually straightforward to exploit and can lead to tokens loss etc.
<b>High</b>	High-level vulnerabilities are difficult to exploit; however, they also have significant impact on smart contract execution, e.g. public access to crucial functions
<b>Medium</b>	Medium-level vulnerabilities are important to fix; however, they can't lead to tokens loss
<b>Low</b>	Low-level vulnerabilities are mostly related to outdated, unused etc. code snippets, that can't have significant impact on execution
<b>Lowest / Code Style / Best Practice</b>	Lowest-level vulnerabilities, code style violations and info statements can't affect smart contract execution and can be ignored.

# Audit Findings

## Critical

No critical severity vulnerabilities were found.

## High

No High severity vulnerabilities were found.

## Medium

No Medium severity vulnerabilities were found.

## Low

(1) Centralized risk in addLiquidity

```
function addLiquidity(uint256 tokenAmount, uint256 ethAmount) private {
    // approve token transfer to cover all possible scenarios
    _approve(address(this), address(uniswapV2Router), tokenAmount);

    // add the liquidity
    uniswapV2Router.addLiquidityETH{value: ethAmount}(
        address(this),
        tokenAmount,
        0, // slippage is unavoidable
        0, // slippage is unavoidable
        owner(),
        block.timestamp
    );
}
```

AddLiquidityETH function has to be addressed as owner() to get LP Tokens from Pool. At some time the owner will accumulate significant LP tokens. If the \_owner is an EOA(Externally Owned Account), mishandling of its private key can have devastating consequences to the project.

Solution: uniswapV2Router.addLiquidityETH function call to be replaced by address(this), and to restrict the management of the LP tokens. This will protect the LP tokens from being stolen if the \_owner account is compromised.

## (2) Infinite loop possibility

```
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;
        }
    }
}
```

If there are so many excluded wallets, then this logic will fail as it might hit the block's gas limit. If there are very limited exceptions, then this will work, but will cost more gas.

Solution: This issue is acknowledged as excluding limited wallets.

## (3) Missing Events

Following are some functions which change the state variable that should emit events.

- deliver
- excludeFromFee
- excludeFromReward
- includeInFee
- includeInReward
- setLiquidityFeePercent
- setMaxTxPercent
- setTaxFeePercent

## Very Low / Discussion / Best practices:

### (1) Solidity version

```
pragma solidity ^0.6.12;
```

Use the latest solidity version while contract deployment to prevent any compiler version level bugs.

Solution: This issue is acknowledged.

### (2) Redundant code

```
if (!_isExcluded[sender] && !_isExcluded[recipient]) {
    _transferFromExcluded(sender, recipient, amount);
} else if (!_isExcluded[sender] && _isExcluded[recipient]) {
    _transferToExcluded(sender, recipient, amount);
} else if (!_isExcluded[sender] && !_isExcluded[recipient]) {
    _transferStandard(sender, recipient, amount);
} else if (_isExcluded[sender] && _isExcluded[recipient]) {
    _transferBothExcluded(sender, recipient, amount);
} else {
    _transferStandard(sender, recipient, amount);
}
```

The condition `!_isExcluded[sender] && !_isExcluded[recipient]` is not needed, it can be included in the else condition so no need for this extra condition here.

Solution: Line no : 1118 needs to be removed.

```
} else if (!_isExcluded[sender] && !_isExcluded[recipient]) {
    _transferStandard(sender, recipient, amount);
```

(3) function and variable names do not match with bsc network

```
IUniswapV2Router02 public immutable uniswapV2Router;  
address public immutable uniswapV2Pair;
```

```
// swap tokens for ETH  
swapTokensForEth(half); // <- this breaks the ETH -> HATE swap when swap+liquify is triggered  
  
// how much ETH did we just swap into?  
uint256 newBalance = address(this).balance.sub(initialBalance);
```

This contract is for BSC, the comments and some functions have ETH text in it but it should be BNB. Some functions have used Uniswap. But it should be Pancakeswap. This naming should be changed.

Solution: Change the ETH to BNB in comments, change Uniswap to PancakeSwap to remove any confusion.

## Centralization

This smart contract has some functions which can be executed by Owner only. But the ownership is **renounced**. Which means this contract does not have any owner influenced functions.

11. owner

0x00 address

## Conclusion

We were given a contract code. And we have used all possible tests based on given objects as files. We observed some issues in the smart contract and those are fixed/ackolenged in the smart contract. **So it is good to go for the production.**

Since possible test cases can be unlimited for such extensive smart contract protocol, we provide no such guarantee of future outcomes. We have used all the latest static tools and manual observations to cover maximum possible test cases to scan everything.

Smart contracts within the scope were manually reviewed and analyzed with static analysis tools. Smart Contract's high level description of functionality was presented in As-is overview section of the report.

Audit report contains all found security vulnerabilities and other issues in the reviewed code.

Security state of the reviewed contract, based on standard audit procedure scope, is "**Well Secured**".



# Our Methodology

We like to work with a transparent process and make our reviews a collaborative effort. The goals of our security audits are to improve the quality of systems we review and aim for sufficient remediation to help protect users. The following is the methodology we use in our security audit process.

## **Manual Code Review:**

In manually reviewing all of the code, we look for any potential issues with code logic, error handling, protocol and header parsing, cryptographic errors, and random number generators. We also watch for areas where more defensive programming could reduce the risk of future mistakes and speed up future audits. Although our primary focus is on the in-scope code, we examine dependency code and behavior when it is relevant to a particular line of investigation.

## **Vulnerability Analysis:**

Our audit techniques included manual code analysis, user interface interaction, and whitebox penetration testing. We look at the project's web site to get a high level understanding of what functionality the software under review provides. We then meet with the developers to gain an appreciation of their vision of the software. We install and use the relevant software, exploring the user interactions and roles. While we do this, we brainstorm threat models and attack surfaces. We read design documentation, review other audit results, search for similar projects, examine source code dependencies, skim open issue tickets, and generally investigate details other than the implementation.

## **Documenting Results:**

We follow a conservative, transparent process for analyzing potential security vulnerabilities and seeing them through successful remediation. Whenever a potential issue is discovered, we immediately create an Issue entry for it in this document, even though we have not yet verified the feasibility and impact of the issue. This process is conservative because we document our suspicions early even if they are later shown to not represent exploitable vulnerabilities. We generally follow a process of first documenting the suspicion with unresolved questions, then confirming the issue through code analysis, live experimentation, or automated tests. Code analysis is the most tentative, and we strive to provide test code, log captures, or screenshots demonstrating our confirmation. After this we analyze the feasibility of an attack in a live system.

## **Suggested Solutions:**

We search for immediate mitigations that live deployments can take, and finally we suggest the requirements for remediation engineering for future releases. The mitigation and remediation recommendations should be scrutinized by the developers and deployment engineers, and successful mitigation and remediation is an ongoing collaborative process after we deliver our report, and before the details are made public.

# Disclaimers

## EtherAuthority.io Disclaimer

EtherAuthority team has analyzed this smart contract in accordance with the best industry practices at the date of this report, in relation to: cybersecurity vulnerabilities and issues in smart contract source code, the details of which are disclosed in this report, (Source Code); the Source Code compilation, deployment and functionality (performing the intended functions).

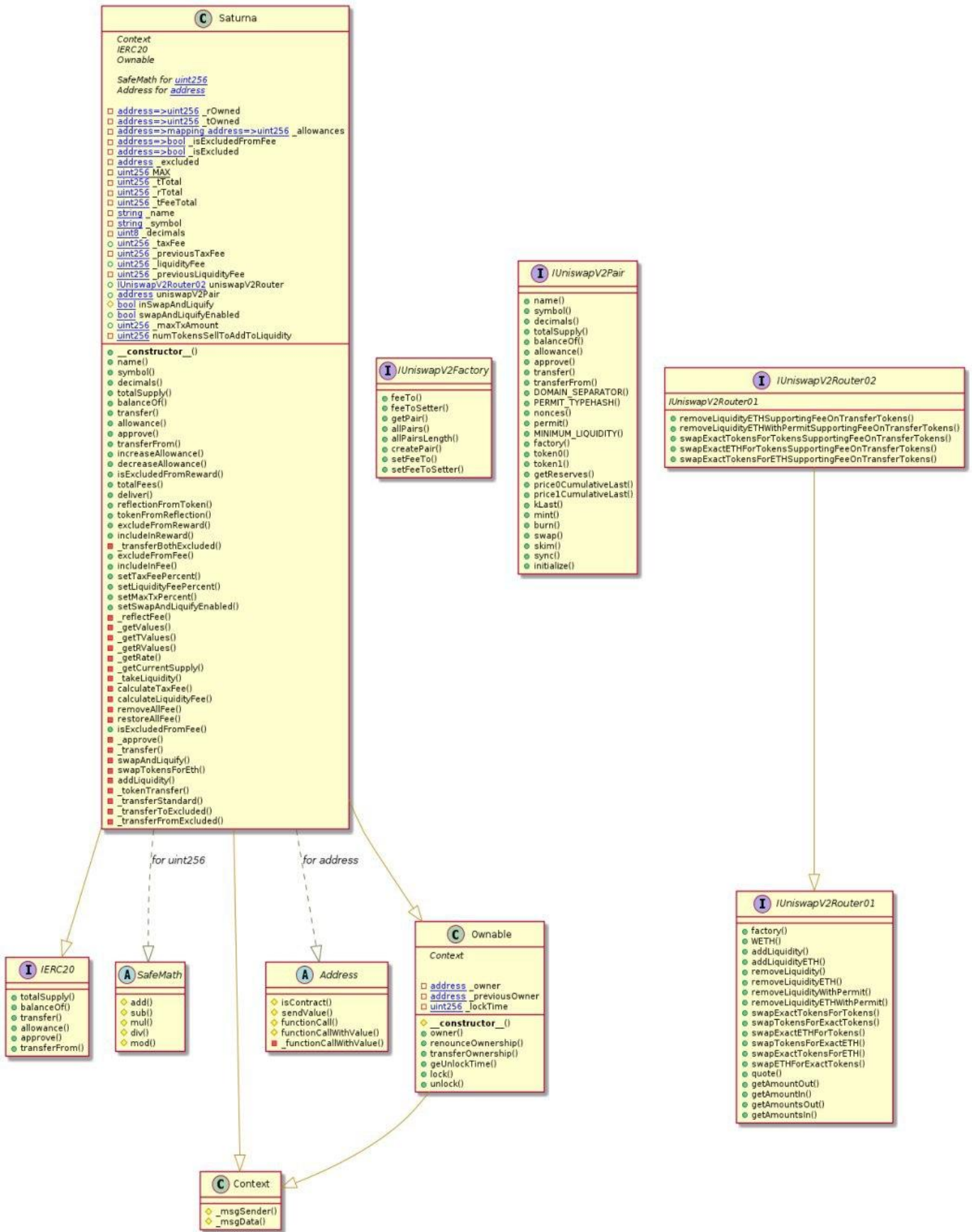
Due to the fact that the total number of test cases are unlimited, the audit makes no statements or warranties on security of the code. It also cannot be considered as a sufficient assessment regarding the utility and safety of the code, bugfree status or any other statements of the contract. While we have done our best in conducting the analysis and producing this report, it is important to note that you should not rely on this report only. We also suggest conducting a bug bounty program to confirm the high level of security of this smart contract.

## Technical Disclaimer

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have their own vulnerabilities that can lead to hacks. Thus, the audit can't guarantee explicit security of the audited smart contracts.

# Appendix

## Code Flow Diagram - Saturna (SAT) Token



This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

Email: [audit@EtherAuthority.io](mailto:audit@EtherAuthority.io)

# Slither Results Log

## >>> SLITHER REPORT Saturna.sol

xcv@xcv-ThinkPad-T410:~/tempSlither/bscContracts\$ **slither**

**Saturna.sol** INFO:Detectors:

Reentrancy in Saturna.\_transfer(address,address,uint256)

(Saturna.sol#1007-1051): External calls:

- swapAndLiquify(contractTokenBalance) (Saturna.sol#1038)

- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) -

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path, address(this),block.timestamp) (Saturna.sol#1085-1091)

External calls sending eth:

- swapAndLiquify(contractTokenBalance) (Saturna.sol#1038)

- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) State variables written after the call(s):

- \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)

- \_rOwned[address(this)] = \_rOwned[address(this)].add(rLiquidity)

(Saturna.sol#963)

- \_rOwned[sender] = \_rOwned[sender].sub(rAmount) (Saturna.sol#1141)

- \_rOwned[sender] = \_rOwned[sender].sub(rAmount) (Saturna.sol#1132)

- \_rOwned[sender] = \_rOwned[sender].sub(rAmount) (Saturna.sol#879)

- \_rOwned[recipient] = \_rOwned[recipient].add(rTransferAmount)

(Saturna.sol#1133)

- \_rOwned[sender] = \_rOwned[sender].sub(rAmount) (Saturna.sol#1152)

- \_rOwned[recipient] = \_rOwned[recipient].add(rTransferAmount)

(Saturna.sol#1143)

- \_rOwned[recipient] = \_rOwned[recipient].add(rTransferAmount)

(Saturna.sol#1153)

- \_rOwned[recipient] = \_rOwned[recipient].add(rTransferAmount)

(Saturna.sol#881) - \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)

- \_rTotal = \_rTotal.sub(rFee) (Saturna.sol#918)

- \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)

- \_tOwned[address(this)] = \_tOwned[address(this)].add(tLiquidity)

(Saturna.sol#965)

- \_tOwned[sender] = \_tOwned[sender].sub(tAmount) (Saturna.sol#878)

- \_tOwned[sender] = \_tOwned[sender].sub(tAmount) (Saturna.sol#1151)

- \_tOwned[recipient] = \_tOwned[recipient].add(tTransferAmount)

(Saturna.sol#1142)

- \_tOwned[recipient] = \_tOwned[recipient].add(tTransferAmount)

(Saturna.sol#880) Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities>

INFO:Detectors:

Saturna.addLiquidity(uint256,uint256) (Saturna.sol#1094-1107) ignores return value by uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#unused-return>

INFO:Detectors:

Saturna.allowance(address,address).owner (Saturna.sol#795) shadows:

- Ownable.owner() (Saturna.sol#431-433) (function)

Saturna.\_approve(address,address,uint256).owner (Saturna.sol#999) shadows:

- Ownable.owner() (Saturna.sol#431-433) (function)

Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#local-variable-shadowing>

INFO:Detectors:

Reentrancy in Saturna.\_transfer(address,address,uint256)

(Saturna.sol#1007-1051): External calls:

- swapAndLiquify(contractTokenBalance) (Saturna.sol#1038)
- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) -

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path, address(this),block.timestamp) (Saturna.sol#1085-1091)

External calls sending eth:

- swapAndLiquify(contractTokenBalance) (Saturna.sol#1038)
- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) State variables written after the call(s):

- \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)
- \_liquidityFee = \_previousLiquidityFee (Saturna.sol#992)
- \_liquidityFee = 0 (Saturna.sol#987)
- \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)
- \_previousLiquidityFee = \_liquidityFee (Saturna.sol#984)
- \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)
- \_previousTaxFee = \_taxFee (Saturna.sol#983)
- \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)
- \_tFeeTotal = \_tFeeTotal.add(tFee) (Saturna.sol#919)
- \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)
- \_taxFee = \_previousTaxFee (Saturna.sol#991)
- \_taxFee = 0 (Saturna.sol#986)

Reentrancy in Saturna.constructor() (Saturna.sol#751-767):

External calls:

- uniswapV2Pair =

IUniswapV2Factory(\_uniswapV2Router.factory()).createPair(address(this),\_uniswapV2Router.WE TH()) (Saturna.sol#756-757)

State variables written after the call(s):

- \_isExcludedFromFee[owner()] = true (Saturna.sol#763)
- \_isExcludedFromFee[address(this)] = true (Saturna.sol#764)
- uniswapV2Router = \_uniswapV2Router (Saturna.sol#760)

Reentrancy in Saturna.swapAndLiquify(uint256)

(Saturna.sol#1053-1074): External calls:

- swapTokensForEth(half) (Saturna.sol#1065)

-

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path, address(this),block.timestamp) (Saturna.sol#1085-1091)

- addLiquidity(otherHalf,newBalance) (Saturna.sol#1071)
- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) External calls sending eth:

- addLiquidity(otherHalf,newBalance) (Saturna.sol#1071)

- uniswapV2Router.addLiquidityETH{value: ethAmount} (address(this),tokenAmount,0,0,owner(),block.timestamp) (Saturna.sol#1099-1106) State variables written after the call(s):
  - addLiquidity(otherHalf,newBalance) (Saturna.sol#1071)
    - \_allowances[owner][spender] = amount (Saturna.sol#1003)

Reentrancy in Saturna.transferFrom(address,address,uint256) (Saturna.sol#804-808): External calls:

- \_transfer(sender,recipient,amount) (Saturna.sol#805)
  - uniswapV2Router.addLiquidityETH{value: ethAmount} (address(this),tokenAmount,0,0,owner(),block.timestamp) (Saturna.sol#1099-1106) -

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path, address(this),block.timestamp) (Saturna.sol#1085-1091)

External calls sending eth:

- \_transfer(sender,recipient,amount) (Saturna.sol#805)
  - uniswapV2Router.addLiquidityETH{value: ethAmount} (address(this),tokenAmount,0,0,owner(),block.timestamp) (Saturna.sol#1099-1106) State variables written after the call(s):

-

\_approve(sender,\_msgSender(),\_allowances[sender][\_msgSender()].sub(amount,ERC20: transfer amount exceeds allowance)) (Saturna.sol#806)

- \_allowances[owner][spender] = amount (Saturna.sol#1003)

Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-2>

INFO:Detectors:

Reentrancy in Saturna.\_transfer(address,address,uint256)

(Saturna.sol#1007-1051): External calls:

- swapAndLiquify(contractTokenBalance) (Saturna.sol#1038)
  - uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) -

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path, address(this),block.timestamp) (Saturna.sol#1085-1091)

External calls sending eth:

- swapAndLiquify(contractTokenBalance) (Saturna.sol#1038)
  - uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) Event emitted after the call(s):

- Transfer(sender,recipient,tTransferAmount) (Saturna.sol#1136)
  - \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)
- Transfer(sender,recipient,tTransferAmount) (Saturna.sol#1156)
  - \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)
- Transfer(sender,recipient,tTransferAmount) (Saturna.sol#1146)
  - \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)
- Transfer(sender,recipient,tTransferAmount) (Saturna.sol#884)
  - \_tokenTransfer(from,to,amount,takeFee) (Saturna.sol#1050)

Reentrancy in Saturna.constructor() (Saturna.sol#751-767):

External calls:

- uniswapV2Pair =

IUniswapV2Factory(\_uniswapV2Router.factory()).createPair(address(this),\_uniswapV2Router.WE TH()) (Saturna.sol#756-757)

Event emitted after the call(s):

- Transfer(address(0),\_msgSender(),\_tTotal) (Saturna.sol#766)

Reentrancy in Saturna.swapAndLiquify(uint256)

(Saturna.sol#1053-1074): External calls:

- swapTokensForEth(half) (Saturna.sol#1065)

-

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path, address(this),block.timestamp) (Saturna.sol#1085-1091)

- addLiquidity(otherHalf,newBalance) (Saturna.sol#1071)

- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) External calls sending eth:

- addLiquidity(otherHalf,newBalance) (Saturna.sol#1071)

- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) Event emitted after the call(s):

- Approval(owner,spender,amount) (Saturna.sol#1004)

- addLiquidity(otherHalf,newBalance) (Saturna.sol#1071)

- SwapAndLiquify(half,newBalance,otherHalf) (Saturna.sol#1073)

Reentrancy in Saturna.transferFrom(address,address,uint256)

(Saturna.sol#804-808): External calls:

- \_transfer(sender,recipient,amount) (Saturna.sol#805)

- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) -

uniswapV2Router.swapExactTokensForETHSupportingFeeOnTransferTokens(tokenAmount,0,path, address(this),block.timestamp) (Saturna.sol#1085-1091)

External calls sending eth:

- \_transfer(sender,recipient,amount) (Saturna.sol#805)

- uniswapV2Router.addLiquidityETH{value: ethAmount}

(address(this),tokenAmount,0,0,owner(),block.timestamp)

(Saturna.sol#1099-1106) Event emitted after the call(s):

- Approval(owner,spender,amount) (Saturna.sol#1004)

- \_approve(sender,\_msgSender(),\_allowances[sender]

[\_msgSender()].sub(amount,ERC20: transfer amount exceeds allowance))

(Saturna.sol#806) Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#reentrancy-vulnerabilities-3>

INFO:Detectors:

Ownable.unlock() (Saturna.sol#478-483) uses timestamp for comparisons

Dangerous comparisons:

- require(bool,string)(now > \_lockTime,Contract is locked until 7 days)

(Saturna.sol#480) Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#block-timestamp>

INFO:Detectors:

Address.isContract(address) (Saturna.sol#283-292) uses assembly

- INLINE ASM (Saturna.sol#290)

Address.\_functionCallWithValue(address,bytes,uint256,string)

(Saturna.sol#376-397) uses assembly

- INLINE ASM (Saturna.sol#389-392)

Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#assembly-usage>

INFO:Detectors:

Saturna.\_rTotal (Saturna.sol#715) is set pre-construction with a non-constant



function or state variable:

- (MAX - (MAX % \_tTotal))

Saturna.\_previousTaxFee (Saturna.sol#723) is set pre-construction with a non-constant function or state variable:

- \_taxFee

Saturna.\_previousLiquidityFee (Saturna.sol#726) is set pre-construction with a non-constant function or state variable:

- \_liquidityFee

Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#function-initializing-state-variables>

INFO:Detectors:

Low level call in Address.sendValue(address,uint256)

(Saturna.sol#310-316): - (success) = recipient.call{value: amount}{}  
(Saturna.sol#314)

Low level call in Address.\_functionCallWithValue(address,bytes,uint256,string)  
(Saturna.sol#376- 397):

- (success,returndata) = target.call{value: weiValue}(data)

(Saturna.sol#380) Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#low-level-calls>

INFO:Detectors:

Function IUniswapV2Pair.DOMAIN\_SEPARATOR() (Saturna.sol#522) is not in mixedCase  
Function IUniswapV2Pair.PERMIT\_TYPEHASH() (Saturna.sol#523) is not in mixedCase  
Function IUniswapV2Pair.MINIMUM\_LIQUIDITY()

(Saturna.sol#540) is not in mixedCase  
Function IUniswapV2Router01.WETH()

(Saturna.sol#562) is not in mixedCase  
Parameter

Saturna.setSwapAndLiquifyEnabled(bool).\_enabled (Saturna.sol#909) is not in mixedCase

Parameter Saturna.calculateTaxFee(uint256).\_amount (Saturna.sol#968) is not in mixedCase  
Parameter Saturna.calculateLiquidityFee(uint256).\_amount

(Saturna.sol#974) is not in mixedCase  
Variable Saturna.\_taxFee (Saturna.sol#722) is not in mixedCase

Variable Saturna.\_liquidityFee (Saturna.sol#725) is not in mixedCase

Variable Saturna.\_maxTxAmount (Saturna.sol#734) is not in mixedCase

Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#conformance-to-solidity-naming-conventions>

INFO:Detectors:

Redundant expression "this (Saturna.sol#256)" inContext (Saturna.sol#250-259)

Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#redundant-statements>

INFO:Detectors:

Variable

IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountADesired (Saturna.sol#567) is too similar to

IUniswapV2Router01.addLiquidity(address,address,uint256,uint256,uint256,uint256,address,uint256).amountBDesired (Saturna.sol#568)

Variable

Saturna.\_transferFromExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1150) is too similar to

Saturna.\_transferStandard(address,address,uint256).tTransferAmount

(Saturna.sol#1131) Variable

Saturna.\_transferFromExcluded(address,address,uint256).rTransferAmount

(Saturna.sol#1150) is too similar to  
Saturna.\_transferToExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1140) Variable  
Saturna.\_transferFromExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1150) is too similar to  
Saturna.\_transferBothExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#877) Variable  
Saturna.\_transferFromExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1150) is too similar to Saturna.\_getTValues(uint256).tTransferAmount  
(Saturna.sol#931)  
Variable  
Saturna.\_transferFromExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1150) is too similar to  
Saturna.\_transferFromExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1150)  
Variable  
Saturna.\_transferToExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1140) is too similar to  
Saturna.\_transferToExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1140) Variable  
Saturna.\_transferBothExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#877) is too similar to  
Saturna.\_transferBothExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#877) Variable Saturna.reflectionFromToken(uint256,bool).rTransferAmount  
(Saturna.sol#843) is too similar to  
Saturna.\_transferStandard(address,address,uint256).tTransferAmount (Saturna.sol#1131)  
Variable Saturna.\_getRValues(uint256,uint256,uint256,uint256).rTransferAmount  
(Saturna.sol#939) is too similar to  
Saturna.\_transferStandard(address,address,uint256).tTransferAmount (Saturna.sol#1131)  
Variable Saturna.\_getValues(uint256).rTransferAmount (Saturna.sol#924) is too  
similar to  
Saturna.\_transferBothExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#877) Variable Saturna.\_getValues(uint256).rTransferAmount  
(Saturna.sol#924) is too similar to  
Saturna.\_transferToExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1140) Variable  
Saturna.\_transferToExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1140) is too similar to  
Saturna.\_transferBothExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#877) Variable Saturna.\_getValues(uint256).rTransferAmount  
(Saturna.sol#924) is too similar to  
Saturna.\_transferStandard(address,address,uint256).tTransferAmount  
(Saturna.sol#1131) Variable  
Saturna.\_transferFromExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1150) is too similar to Saturna.\_getValues(uint256).tTransferAmount  
(Saturna.sol#923)  
Variable Saturna.\_getRValues(uint256,uint256,uint256,uint256).rTransferAmount  
(Saturna.sol#939) is too similar to  
Saturna.\_transferBothExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#877)  
Variable Saturna.\_getRValues(uint256,uint256,uint256,uint256).rTransferAmount  
(Saturna.sol#939) is too similar to  
Saturna.\_transferToExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1140)

Variable

Saturna.\_transferBothExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#877) is too similar to

Saturna.\_transferStandard(address,address,uint256).tTransferAmount  
(Saturna.sol#1131) Variable

Saturna.\_transferToExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1140) is too similar to

Saturna.\_transferStandard(address,address,uint256).tTransferAmount  
(Saturna.sol#1131) Variable

Saturna.\_transferStandard(address,address,uint256).rTransferAmount  
(Saturna.sol#1131) is too similar to

Saturna.\_transferStandard(address,address,uint256).tTransferAmount  
(Saturna.sol#1131)

Variable Saturna.\_getRValues(uint256,uint256,uint256,uint256).rTransferAmount  
(Saturna.sol#939) is too similar to Saturna.\_getTValues(uint256).tTransferAmount  
(Saturna.sol#931) Variable

Saturna.\_transferToExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1140) is too similar to Saturna.\_getValues(uint256).tTransferAmount  
(Saturna.sol#923)

Variable Saturna.reflectionFromToken(uint256,bool).rTransferAmount  
(Saturna.sol#843) is too similar to

Saturna.\_transferFromExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1150)

Variable Saturna.\_transferStandard(address,address,uint256).rTransferAmount  
(Saturna.sol#1131) is too similar to

Saturna.\_transferFromExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1150)

Variable Saturna.\_transferBothExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#877) is too similar to Saturna.\_getValues(uint256).tTransferAmount  
(Saturna.sol#923)

Variable Saturna.reflectionFromToken(uint256,bool).rTransferAmount  
(Saturna.sol#843) is too similar to

Saturna.\_transferToExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1140)

Variable

Saturna.\_transferBothExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#877) is too similar to

Saturna.\_transferFromExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1150) Variable

Saturna.reflectionFromToken(uint256,bool).rTransferAmount (Saturna.sol#843) is too  
similar to Saturna.\_getTValues(uint256).tTransferAmount (Saturna.sol#931) Variable

Saturna.reflectionFromToken(uint256,bool).rTransferAmount (Saturna.sol#843) is too  
similar to Saturna.\_transferBothExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#877)

Variable

Saturna.\_transferBothExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#877) is too similar to

Saturna.\_getTValues(uint256).tTransferAmount (Saturna.sol#931)

Variable Saturna.reflectionFromToken(uint256,bool).rTransferAmount  
(Saturna.sol#843) is too similar to Saturna.\_getValues(uint256).tTransferAmount  
(Saturna.sol#923)

Variable

Saturna.\_transferToExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1140) is too similar to

Saturna.\_transferFromExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1150) Variable  
Saturna.\_transferBothExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#877) is too similar to  
Saturna.\_transferToExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1140) Variable  
Saturna.\_transferStandard(address,address,uint256).rTransferAmount  
(Saturna.sol#1131) is too similar to Saturna.\_getValues(uint256).tTransferAmount  
(Saturna.sol#923) Variable Saturna.\_getValues(uint256).rTransferAmount  
(Saturna.sol#924) is too similar to  
Saturna.\_transferFromExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1150) Variable Saturna.\_getValues(uint256).rTransferAmount  
(Saturna.sol#924) is too similar to Saturna.\_getTValues(uint256).tTransferAmount  
(Saturna.sol#931)  
Variable Saturna.\_transferStandard(address,address,uint256).rTransferAmount  
(Saturna.sol#1131) is too similar to Saturna.\_getTValues(uint256).tTransferAmount  
(Saturna.sol#931) Variable  
Saturna.\_transferToExcluded(address,address,uint256).rTransferAmount  
(Saturna.sol#1140) is too similar to Saturna.\_getTValues(uint256).tTransferAmount  
(Saturna.sol#931)  
Variable Saturna.\_getRValues(uint256,uint256,uint256,uint256).rTransferAmount  
(Saturna.sol#939) is too similar to Saturna.\_getValues(uint256).tTransferAmount  
(Saturna.sol#923) Variable  
Saturna.\_transferStandard(address,address,uint256).rTransferAmount (Saturna.sol#1131)  
is too similar to Saturna.\_transferBothExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#877)  
Variable Saturna.\_getValues(uint256).rTransferAmount (Saturna.sol#924) is too  
similar to Saturna.\_getValues(uint256).tTransferAmount (Saturna.sol#923)  
Variable Saturna.\_getRValues(uint256,uint256,uint256,uint256).rTransferAmount  
(Saturna.sol#939) is too similar to  
Saturna.\_transferFromExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1150)  
Variable Saturna.\_transferStandard(address,address,uint256).rTransferAmount  
(Saturna.sol#1131) is too similar to  
Saturna.\_transferToExcluded(address,address,uint256).tTransferAmount  
(Saturna.sol#1140)

Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#variable-names-are-too-similar>

INFO:Detectors:

Saturna.slitherConstructorVariables() (Saturna.sol#700-1158) uses literals with too many digits: -  $\_tTotal = 1000000000 * 10^{**6} * 10^{**9}$  (Saturna.sol#714)

Saturna.slitherConstructorVariables() (Saturna.sol#700-1158) uses literals with too many digits:

-  $\_maxTxAmount = 5000000 * 10^{**6} * 10^{**9}$  (Saturna.sol#734)

Saturna.slitherConstructorVariables() (Saturna.sol#700-1158) uses literals with too many digits: -  $numTokensSellToAddToLiquidity = 500000 * 10^{**6} * 10^{**9}$

(Saturna.sol#735) Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#too-many-digits>

INFO:Detectors:

Saturna.\_decimals (Saturna.sol#720) should be constant

Saturna.\_name (Saturna.sol#718) should be constant

Saturna.\_symbol (Saturna.sol#719) should be constant

Saturna.\_tTotal (Saturna.sol#714) should be constant

Saturna.numTokensSellToAddToLiquidity (Saturna.sol#735) should be constant  
Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#state-variables-that-could-be-declared-constant>

INFO:Detectors:

renounceOwnership() should be declared external:

- Ownable.renounceOwnership() (Saturna.sol#450-453)

transferOwnership(address) should be declared external:

- Ownable.transferOwnership(address) (Saturna.sol#459-463)

geUnlockTime() should be declared external:

- Ownable.geUnlockTime() (Saturna.sol#465-467)

lock(uint256) should be declared external:

- Ownable.lock(uint256) (Saturna.sol#470-475)

unlock() should be declared external:

- Ownable.unlock() (Saturna.sol#478-483)

name() should be declared external:

- Saturna.name() (Saturna.sol#769-771)

symbol() should be declared external:

- Saturna.symbol() (Saturna.sol#773-775)

decimals() should be declared external:

- Saturna.decimals() (Saturna.sol#777-779)

totalSupply() should be declared external:

- Saturna.totalSupply() (Saturna.sol#781-783)

transfer(address,uint256) should be declared external:

- Saturna.transfer(address,uint256) (Saturna.sol#790-793)

allowance(address,address) should be declared external:

- Saturna.allowance(address,address) (Saturna.sol#795-797)

approve(address,uint256) should be declared external:

- Saturna.approve(address,uint256) (Saturna.sol#799-802)

transferFrom(address,address,uint256) should be declared external:

- Saturna.transferFrom(address,address,uint256) (Saturna.sol#804-808)

increaseAllowance(address,uint256) should be declared external:

- Saturna.increaseAllowance(address,uint256) (Saturna.sol#810-813)

decreaseAllowance(address,uint256) should be declared external:

- Saturna.decreaseAllowance(address,uint256) (Saturna.sol#815-818)

isExcludedFromReward(address) should be declared external:

- Saturna.isExcludedFromReward(address) (Saturna.sol#820-822)

totalFees() should be declared external:

- Saturna.totalFees() (Saturna.sol#824-826)

deliver(uint256) should be declared external:

- Saturna.deliver(uint256) (Saturna.sol#828-835)

reflectionFromToken(uint256,bool) should be declared external:

- Saturna.reflectionFromToken(uint256,bool) (Saturna.sol#837-846)

excludeFromReward(address) should be declared external:

- Saturna.excludeFromReward(address) (Saturna.sol#854-862)

excludeFromFee(address) should be declared external:

- Saturna.excludeFromFee(address) (Saturna.sol#887-889)

includeInFee(address) should be declared external:

- Saturna.includeInFee(address) (Saturna.sol#891-893)

setSwapAndLiquifyEnabled(bool) should be declared external:

- Saturna.setSwapAndLiquifyEnabled(bool) (Saturna.sol#909-912)

isExcludedFromFee(address) should be declared external:

- Saturna.isExcludedFromFee(address) (Saturna.sol#995-997)

Reference:

<https://github.com/crytic/slither/wiki/Detector-Documentation#public-function-that-could-be-declared-external>

INFO:Slither:Saturna.sol analyzed (10 contracts with 72 detectors), 106 result(s) found  
INFO:Slither:Use <https://crytic.io/> to get access to additional detectors and Github integration  
xcv@xcv-ThinkPad-T410:~/tempSlither/bscContracts\$



This is a private and confidential document. No part of this document should be disclosed to third party without prior written permission of EtherAuthority.

**Email: [audit@EtherAuthority.io](mailto:audit@EtherAuthority.io)**