



Cyberscope

# Audit Report

## **SAVELUNA**

May 2022

Source <https://github.com/savelunaclub/saveluna>  
Commit [b8f964210f47b302439bca4a50be5d36ade1ae6c](https://github.com/savelunaclub/saveluna/commit/b8f964210f47b302439bca4a50be5d36ade1ae6c)  
Audited by © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>3</b>
<b>Source Files</b>	<b>3</b>
<b>Audit Updates</b>	<b>3</b>
<b>Contract Analysis</b>	<b>4</b>
<b>ST - Stop Transactions</b>	<b>5</b>
Description	5
Recommendation	5
<b>BC - Blacklisted Contracts</b>	<b>6</b>
Description	6
Recommendation	6
<b>Contract Diagnostics</b>	<b>7</b>
<b>L01 - Public Function could be Declared External</b>	<b>8</b>
Description	8
Recommendation	8
<b>L02 - State Variables could be Declared Constant</b>	<b>9</b>
Description	9
Recommendation	9
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>10</b>
Description	10
Recommendation	10
<b>L07 - Missing Events Arithmetic</b>	<b>11</b>
Description	11
Recommendation	11
<b>L09 - Dead Code Elimination</b>	<b>12</b>
Description	12

<b>Recommendation</b>	<b>12</b>
<b>Contract Functions</b>	<b>13</b>
<b>Contract Flow</b>	<b>18</b>
<b>Domain Info</b>	<b>19</b>
<b>Summary</b>	<b>20</b>
<b>Disclaimer</b>	<b>21</b>
<b>About Cyberscope</b>	<b>22</b>

## Contract Review

<b>Github</b>	<a href="https://github.com/savelunaclub/saveluna">https://github.com/savelunaclub/saveluna</a>
<b>Commit</b>	b8f964210f47b302439bca4a50be5d36ade1ae6c

## Source Files

<b>Filename</b>	<b>SHA256</b>
<b>contract.sol</b>	e33aaf5607afb9e745234e58ceab86724a1fd0ecd0e634c479523305c28c545f

## Audit Updates

<b>Initial Audit</b>	16th May 2022
<b>Corrected</b>	

# Contract Analysis

● Critical   ● Medium   ● Minor   ● Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	OTUT	Owner Transfer User's Tokens
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling

## ST - Stop Transactions

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L1281

### Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `blacklistAmount` to zero.

```
if (blacklistEnabled && (amount > blacklistAmount || bots[sender])) {  
    revert("You're bot");  
}
```

### Recommendation

The contract could embody a check for not allowing setting the `blacklistAmount` less than a reasonable amount. A suggested implementation could check that the maximum amount should be more than a fixed percentage of the total supply.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

## BC - Blacklisted Contracts

Criticality	medium
Location	contract.sol#L1263

### Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `setBlacklists` function.

```
function setBlacklists(address _bots) external onlyOwner {  
    require(!bots[_bots]);  
    require(_bots != uniswapV2Pair, "bot address can not be pair");  
    bots[_bots] = true;  
}
```

### Recommendation

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

# Contract Diagnostics

● Critical    ● Medium    ● Minor

Severity	Code	Description
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L07	Missing Events Arithmetic
●	L09	Dead Code Elimination



## L01 - Public Function could be Declared External

**Criticality**

minor

**Location**

contract.sol#L431,439,456,463,488,501,518,541,570,597,785,794,1242,1246,1250,1259

### Description

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

```
isExcludedFromFees  
excludeFromFees  
setAmountToSwap  
setGrowthFundAddress  
transferOwnership  
renounceOwnership  
decreaseAllowance  
increaseAllowance  
transferFrom  
...
```

### Recommendation

Use the external attribute for functions never called from the contract.

## L02 - State Variables could be Declared Constant

**Criticality**

minor

**Location**

contract.sol#L1215,1216,1208

### Description

Constant state variables should be declared constant to save gas.

```
feeRate  
blacklistTime  
blacklistDuration
```

### Recommendation

Add the constant attribute to state variables that never change.

## L04 - Conformance to Solidity Naming Conventions

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L926,928,958,1002,1242,1246,1263,1333

### Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow \_ at the beginning of the mixed\_case match for private variables and unused parameters.

```
_to  
_bots  
_amount  
_address  
WETH  
MINIMUM_LIQUIDITY  
PERMIT_TYPEHASH  
DOMAIN_SEPARATOR
```

### Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>

## L07 - Missing Events Arithmetic

**Criticality**

minor

**Location**

contract.sol#L1246,1269

### Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
blacklistAmount = amount  
swapTokensAtAmount = _amount
```

### Recommendation

Emit an event for critical parameter changes.

## L09 - Dead Code Elimination

**Criticality**

minor

**Location**

contract.sol#L675

### Description

Functions that are not used in the contract, and make the code's size bigger.

```
_burn
```

### Recommendation

Remove unused functions.

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>SafeMath</b>	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		
<b>IERC20Metadata</b>	Interface	IERC20		

	name	External		-
	symbol	External		-
	decimals	External		-
<b>ERC20</b>	Implementation	Context, IERC20, IERC20Met adata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Internal	✓	
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
<b>ReentrancyGuard</b>	Implementation			
	<Constructor>	Internal	✓	

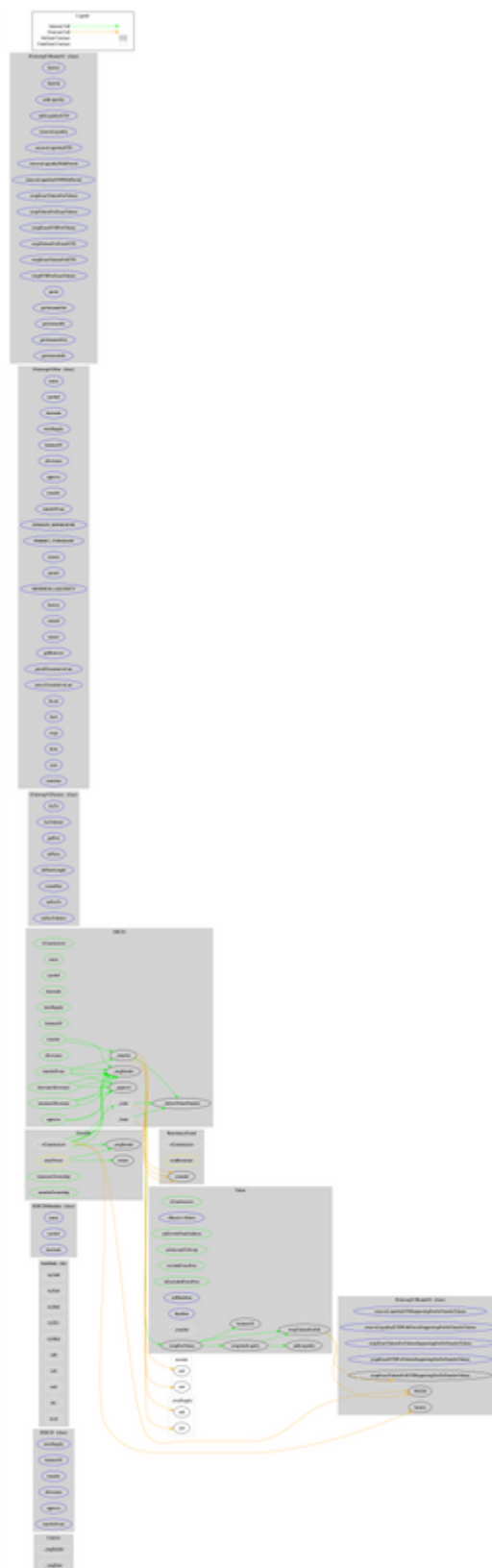
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
<b>IUniswapV2Pair</b>	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	burn	External	✓	-
	swap	External	✓	-



	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
<b>IUniswapV2Router01</b>	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-

Token	Implementation	Ownable, ERC20, Reentrancy Guard		
	<Constructor>	Public	✓	ERC20
	<Receive Ether>	External	Payable	-
	setGrowthFundAddress	Public	✓	onlyOwner
	setAmountToSwap	Public	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner
	isExcludedFromFees	Public		-
	setBlacklists	External	✓	onlyOwner
	blacklist	External	✓	onlyOwner
	_transfer	Internal	✓	
	swapFeeToken	Private	✓	
	swapAndLiquify	Private	✓	
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	

# Contract Flow



## Domain Info

<b>Domain Name</b>	saveluna.club
<b>Registry Domain ID</b>	D2B44E707F6124D60B8BAF4606B7258E6-GDREG
<b>Creation Date</b>	2022-05-14T08:38:09Z
<b>Updated Date</b>	2022-05-15T00:54:20Z
<b>Registry Expiry Date</b>	2023-05-14T08:38:09Z
<b>Registrar WHOIS Server</b>	whois.namecheap.com
<b>Registrar URL</b>	<a href="http://www.namecheap.com">http://www.namecheap.com</a>
<b>Registrar</b>	NameCheap, Inc.
<b>Registrar IANA ID</b>	1068

The domain has been created 2 days before the creation of the audit. It will expire in 12 months.

There is no public billing information, the creator is protected by the privacy settings.

## Summary

There are some functions that can be abused by the owner like stopping transactions and blacklisting addresses. The fees are 10% and can't be changed, and 5% of each transaction is burned. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

## Disclaimer

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment.

Cyberscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Cyberscope team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools. Under no circumstances did Cyberscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always Do your own research and protect yourselves from scams. This document should not be presented as a reason to buy or not buy any particular token.

The Cyberscope team disclaims any liability for the resulting losses.

## About Cyberscope

Coinscope audit and K.Y.C. service has been rebranded to Cyberscope.

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Cyberscope and Coinscope are aiming to make crypto discoverable and efficient globally. They provides all the essential tools to assist users draw their own conclusions.



The Cyberscope team

<https://www.cyberscope.io>