



Cyberscope

# Audit Report

## **Star of Doge**

June 2022

Type       BEP20

Network     BSC

Address     0x9402e722f0c013903ff74de572060e00880bdfd0

Audited by  © cyberscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>3</b>
<b>Audit Updates</b>	<b>3</b>
<b>Contract Analysis</b>	<b>4</b>
<b>ULTW - Unlimited Liquidity to Team Wallet</b>	<b>5</b>
Description	5
Recommendation	5
<b>Contract Diagnostics</b>	<b>6</b>
<b>FSA - Fixed Swap Address</b>	<b>7</b>
Description	7
Recommendation	7
<b>CO - Code Optimization</b>	<b>8</b>
Description	8
Recommendation	8
<b>L01 - Public Function could be Declared External</b>	<b>9</b>
Description	9
Recommendation	9
<b>L02 - State Variables could be Declared Constant</b>	<b>10</b>
Description	10
Recommendation	10
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>11</b>
Description	11
Recommendation	11
<b>L05 - Unused State Variable</b>	<b>12</b>
Description	12
Recommendation	12

<b>Contract Functions</b>	<b>13</b>
<b>Contract Flow</b>	<b>16</b>
<b>Domain Info</b>	<b>17</b>
<b>Summary</b>	<b>18</b>
<b>Disclaimer</b>	<b>19</b>
<b>About Cyberscope</b>	<b>20</b>

## Contract Review

<b>Contract Name</b>	StarOfDoge
<b>Compiler Version</b>	v0.8.4+commit.c7e474f2
<b>Optimization</b>	200 runs
<b>Licence</b>	None
<b>Explorer</b>	<a href="https://bscscan.com/token/0x9402e722f0c013903ff74de572060e00880bdfd0">https://bscscan.com/token/0x9402e722f0c013903ff74de572060e00880bdfd0</a>
<b>Symbol</b>	STARD
<b>Decimals</b>	9
<b>Total Supply</b>	8,600,000,000
<b>Domain</b>	<a href="https://stard.finance">https://stard.finance</a>

## Source Files

<b>Filename</b>	<b>SHA256</b>
<b>contract.sol</b>	6a7b59cc078d01305896e38aca3ee39fe5b29165ea99f18e5b01d133ec47843f

## Audit Updates

<b>Initial Audit</b>	23rd June 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

## ULTW - Unlimited Liquidity to Team Wallet

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L399,L405

### Description

The contract owner has the authority to transfer funds without limit to the team wallet. These funds have been accumulated from fees collected from the contract. The owner may take advantage of it by calling the `manualSend` and `manualSend`

```
function manualswap() external {
    require(_msgSender() == _developmentAddress || _msgSender() == _marketingAddress ||
    _msgSender() == owner());
    uint256 contractBalance = balanceOf(address(this));
    swapTokensForEth(contractBalance);
}

function manualsend() external {
    require(_msgSender() == _developmentAddress || _msgSender() == _marketingAddress ||
    _msgSender() == owner());
    uint256 contractETHBalance = address(this).balance;
    sendETHToFee(contractETHBalance);
}
```

### Recommendation

The contract could embody a check for the maximum amount of funds that can be swapped. Since a huge amount may volatile the token's price.

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
●	FSA	Fixed Swap Address
●	CO	Code Optimization
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L05	Unused State Variable

## FSA - Fixed Swap Address

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L190

### Description

The swap address is assigned once in the constructor and it can not be changed. The decentralized swaps sometimes create a new swap version or abandon the current. A contract that cannot change the swap address may not be able to catch-up the upgrade.

```
IUniswapV2Router02 _uniswapV2Router =  
IUniswapV2Router02(0x10ED43C718714eb63d5aA57B78B54704E256024E);
```

### Recommendation

It could be better to allow the swap address mutation in case of future swap updates.



## CO - Code Optimization

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L319

### Description

There are code segments that could be optimized. A segment may be optimized so that it becomes a smaller size, consumes less memory, executes more rapidly, or performs fewer operations. The function `_tokenTransfer` can be removed.

```
function _tokenTransfer(address sender, address recipient, uint256 amount) private {  
    _transferStandard(sender, recipient, amount);  
}
```

### Recommendation

Rewrite some code segments so the runtime will be more performant.

## L01 - Public Function could be Declared External

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L216,238,130,320,212,229,418,208,136,233,326,422,333,224,407,204

### Description

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

```
name
setFee
transfer
setNewMarketingAddress
excludeMultipleAccountsFromFees
setNewDevAddress
approve
transferOwnership
symbol
...
```

### Recommendation

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

## L02 - State Variables could be Declared Constant

**Criticality**

minor

**Location**

contract.sol#L113

### Description

Constant state variables should be declared constant to save gas.

```
_previousOwner
```

### Recommendation

Add the constant attribute to state variables that never change.

## L04 - Conformance to Solidity Naming Conventions

**Criticality**

minor

**Location**

contract.sol#L418,325,152,54,166,319,320,167,332,165

### 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.

```
_name  
marketingAddressUpdated  
_to  
_decimals  
_tokenAddr  
_amount  
tokensRescued  
_symbol  
WETH  
...
```

### Recommendation

Follow the Solidity naming convention.

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

## L05 - Unused State Variable

**Criticality**

minor

**Location**

contract.sol#L113,147

### Description

There are segments that contain unused state variables.

```
_tOwned  
_previousOwner
```

### Recommendation

Remove unused state variables.

# Contract Functions

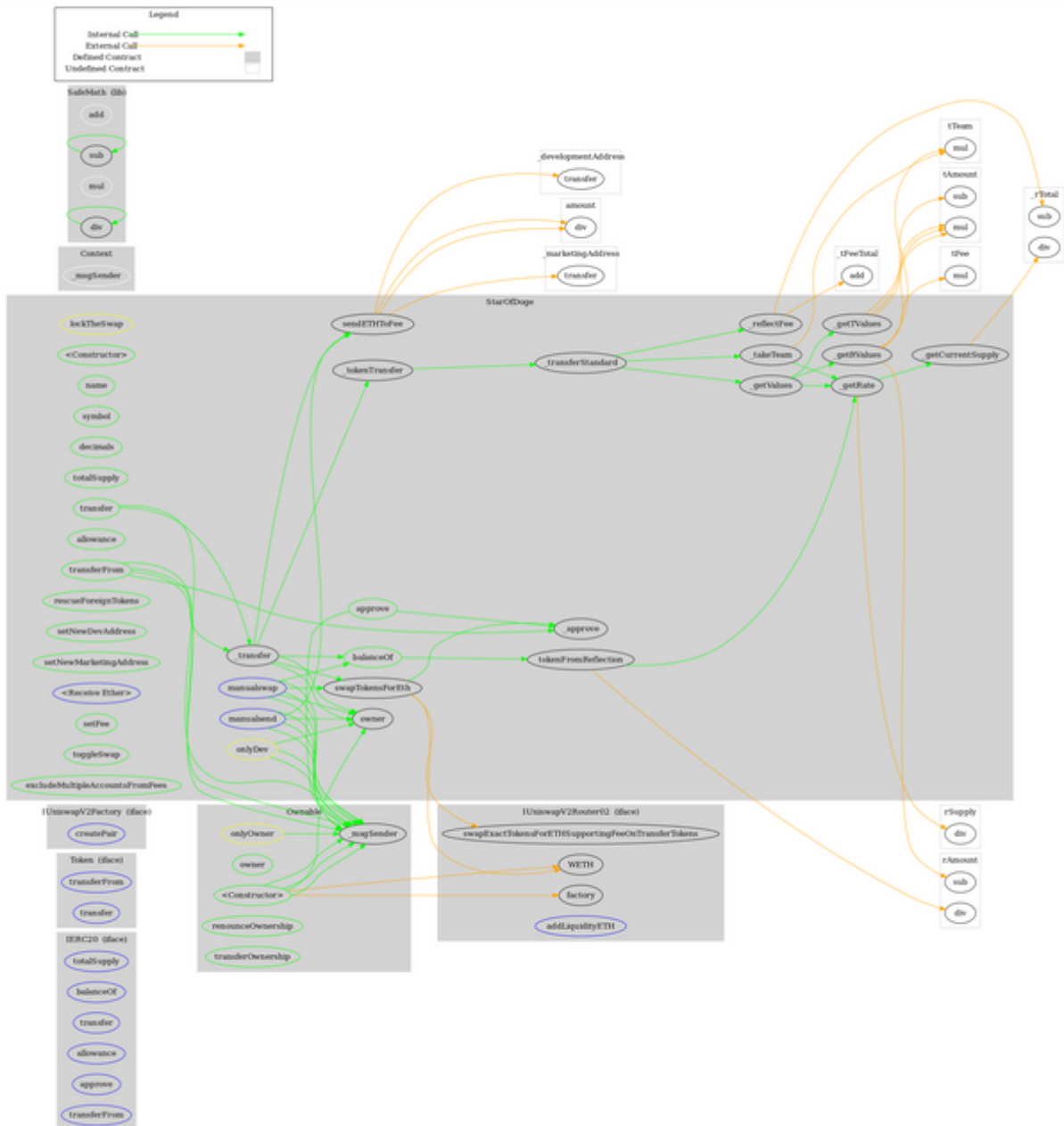
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>Token</b>	Interface			
	transferFrom	External	✓	-
	transfer	External	✓	-
<b>IUniswapV2Factory</b>	Interface			
	createPair	External	✓	-
<b>IUniswapV2Router02</b>	Interface			
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
	factory	External		-
	WETH	External		-
	addLiquidityETH	External	Payable	-
<b>Context</b>	Implementation			
	_msgSender	Internal		
<b>SafeMath</b>	Library			
	add	Internal		
	sub	Internal		

	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
<b>StarOfDoge</b>	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	tokenFromReflection	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	swapTokensForEth	Private	✓	lockTheSwap
	sendETHToFee	Private	✓	
	_tokenTransfer	Private	✓	
	rescueForeignTokens	Public	✓	onlyDev
	setNewDevAddress	Public	✓	onlyDev
	setNewMarketingAddress	Public	✓	onlyDev
	_transferStandard	Private	✓	
	_takeTeam	Private	✓	

	_reflectFee	Private	✓	
	<Receive Ether>	External	Payable	-
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	manualswap	External	✓	-
	manualsend	External	✓	-
	setFee	Public	✓	onlyDev
	toggleSwap	Public	✓	onlyDev
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner



# Contract Flow



## Domain Info

<b>Domain Name</b>	stard.finance
<b>Registry Domain ID</b>	446542726d66457e9c03d22d1b81f9f6-DONUTS
<b>Creation Date</b>	2022-05-09T09:00:11Z
<b>Updated Date</b>	2022-06-09T14:41:59Z
<b>Registry Expiry Date</b>	2023-05-09T09:00:11Z
<b>Registrar WHOIS Server</b>	whois.namecheap.com
<b>Registrar URL</b>	<a href="https://www.namecheap.com/">https://www.namecheap.com/</a>
<b>Registrar</b>	NameCheap, Inc.
<b>Registrar IANA ID</b>	1068

The domain has been created 11 months before the creation of the audit.

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

## Summary

Token is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. There are some functions that can be abused by the owner, like transferring funds to the team's wallet. There is also a limit of max 16% fees. 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 provide all the essential tools to assist users draw their own conclusions.



The Cyberscope team

<https://www.cyberscope.io>