



# Audit Report

## **Dungeons & Dens Token v2**

February 2022

Type           BEP20

Network       BSC

Address       0x0aeFAc5dcfB401FFF88ff904fD2B8Ab227341B4c

Audited by   © coinscope

# 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>ELFM - Exceed Limit Fees Manipulation</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>L04 - Conformance to Solidity Naming Conventions</b>	<b>9</b>
Description	9
Recommendation	9
<b>L09 - Dead Code Elimination</b>	<b>10</b>
Description	10
Recommendation	10
<b>L07 - Missing Events Arithmetic</b>	<b>11</b>
Description	11
Recommendation	11
<b>Contract Functions</b>	<b>12</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 Coinscope</b>	<b>20</b>

# Contract Review

<b>Contract Name</b>	DNDToken
<b>Compiler Version</b>	v0.8.6+commit.11564f7e
<b>Optimization</b>	200 runs
<b>Licence</b>	MIT
<b>Explorer</b>	<a href="https://bscscan.com/token/0x0aeFAc5dcfB401FFF88ff904fD2B8Ab227341B4c">https://bscscan.com/token/0x0aeFAc5dcfB401FFF88ff904fD2B8Ab227341B4c</a>
<b>Symbol</b>	DND
<b>Decimals</b>	18
<b>Total Supply</b>	10,000,000
<b>Source</b>	contract.sol
<b>Domain</b>	dndgamefi.com

## Audit Updates

<b>Initial Audit</b>	1st February 2022
<b>Corrected</b>	

# Contract Analysis

● Critical
 ● Medium
 ● Minor
 ● Pass

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

## ELFM - Exceed Limit Fees Manipulation

Criticality	minor
Location	contract.sol#L1220

### Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by setting the `triggerDumpProtectionAmount` to a low value.

The contract has a total of 20% fees allowed by default, but when the amount to be transferred exceeds the anti-dump amount it will tax the user with an extra 10% fee summing up to a total of 30% fees.

```
if (dumpProtectionEnabled && amount >= triggerDumpProtectionAmount) {  
    poolFeeAmount = poolFeeAmount.add(amount.mul(10).div(100));  
}
```

### Recommendation

The contract could embody a check for a minimum acceptable value of the `triggerDumpProtectionAmount` to not allow the Owner to set it too low.

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#L1

### Description

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

```
function setBlackList(address account, bool value) public onlyOwner {  
    isBlackListed[account] = value;  
}
```

### 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
●	L04	Conformance to Solidity Naming Conventions
●	L09	Dead Code Elimination
●	L07	Missing Events Arithmetic



## L01 - Public Function could be Declared External

**Criticality**

minor

**Location**

contract.sol#L1267,L1261,L1257 and 21 more

### Description

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

```
bindReferrer  
changeReferrer  
setSwapAtTokenAmount  
...
```

### Recommendation

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

## L04 - Conformance to Solidity Naming Conventions

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L34

### 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.

WETH

### Recommendation

Follow the Solidity naming convention.

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

## L09 - Dead Code Elimination

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L853,L865,L894 and 8 more

### Description

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

```
trySub  
tryMul  
tryMod  
...
```

### Recommendation

Remove unused functions.

## L07 - Missing Events Arithmetic

**Criticality**

minor

**Location**

contract.sol#L1257,L1245

### 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.

```
swapAtTokenAmount = amount  
triggerDumpProtectionAmount = value
```

### Recommendation

Emit an event for critical parameter changes.

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	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		-

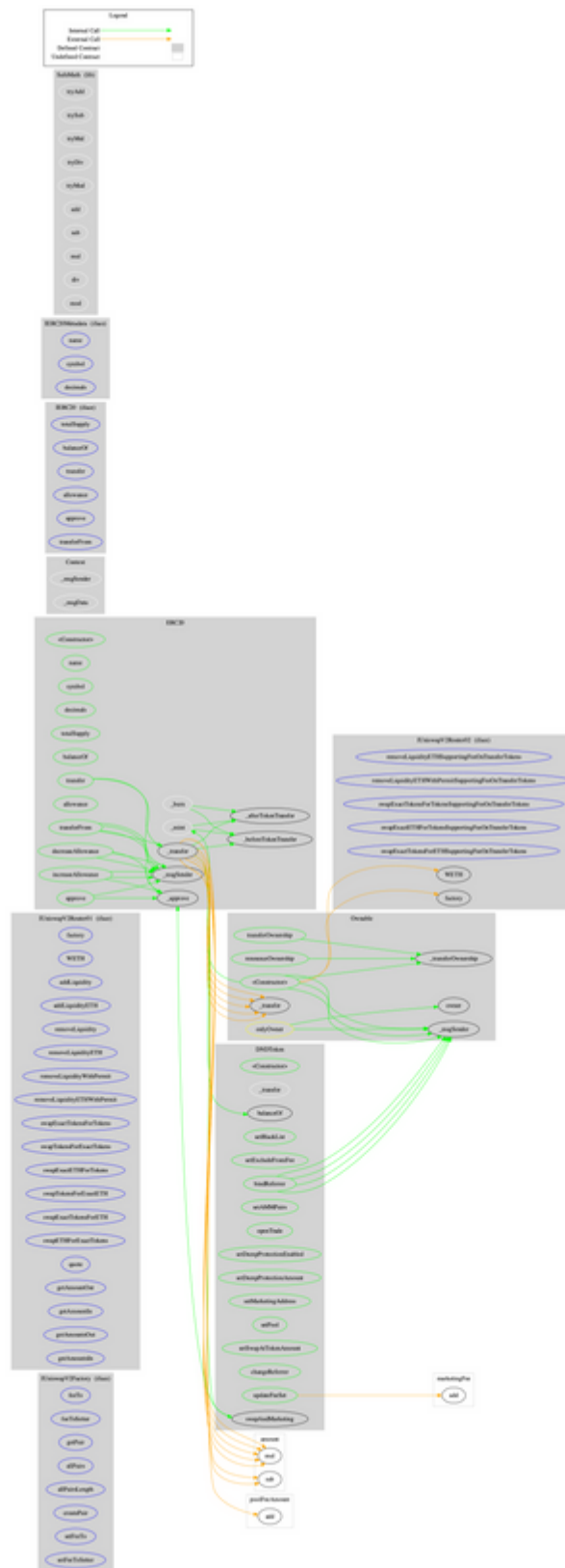
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-
<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-

<b>IERC20Metadata</b>	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>ERC20</b>	Implementation	Context, IERC20, IERC20Metadata		
	<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	✓	
	_afterTokenTransfer	Internal	✓	
<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>DNDToken</b>	Implementation	ERC20, Ownable		
	<Constructor>	Public	✓	ERC20
	_transfer	Internal	✓	
	swapAndMarketing	Private	✓	
	setBlackList	Public	✓	onlyOwner
	setExcludeFromFee	Public	✓	onlyOwner
	updateFeeSet	Public	✓	onlyOwner
	setAMMPairs	Public	✓	onlyOwner
	openTrade	Public	✓	onlyOwner
	setDumpProtectionEnabled	Public	✓	onlyOwner
	setDumpProtectionAmount	Public	✓	onlyOwner
	setMarketingAddress	Public	✓	onlyOwner
	setPool	Public	✓	onlyOwner
	setSwapAtTokenAmount	Public	✓	onlyOwner
	changeReferrer	Public	✓	onlyOwner
	bindReferrer	Public	✓	-



# Contract Flow



## Domain Info

<b>Domain Name</b>	dndgamefi.com
<b>Registry Domain ID</b>	2659776627_DOMAIN_COM-VRSN
<b>Creation Date</b>	2021-12-06T12:03:27Z
<b>Updated Date</b>	2021-12-06T13:03:33Z
<b>Registry Expiry Date</b>	
<b>Registrar WHOIS Server</b>	whois.registrar.eu
<b>Registrar URL</b>	http://www.registrar.eu
<b>Registrar</b>	Hosting Concepts B.V. d/b/a Registrar.eu
<b>Registrar IANA ID</b>	1647

The domain has been created about 2 months before the creation of the audit.

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

## Summary

DND claims to be an action-adventure sandbox game released on BSC network. The Project has a friendly and growing community. The Smart Contract analysis reported no compiler errors and only 2 issues. There are some functions that can be abused by the owner, like changing fees up to 30% and blacklisting wallets from selling. The contract has a passive anti-bot mechanism to punish snipers as well. 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.

Coinscope 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 Coinscope 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 Coinscope 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 Coinscope team disclaims any liability for the resulting losses.

## About Coinscope

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.

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



The Coinscope.co team

<https://www.coinscope.co>