



Cyberscope

Audit Report

DogeVerseToken

June 2022

Type BEP20

Network BSC

Address 0xf5646ea3825ed14ee54237310cdb84b4cc84638e

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Audit Updates	3
Introduction	4
Source Files	5
Contract Analysis	10
Contract Diagnostics	11
BLC - Business Logic Concern	12
Description	12
Recommendation	12
FSA - Fixed Swap Address	13
Description	13
Recommendation	13
L01 - Public Function could be Declared External	14
Description	14
Recommendation	14
L04 - Conformance to Solidity Naming Conventions	15
Description	15
Recommendation	15
L07 - Missing Events Arithmetic	16
Description	16
Recommendation	16
Contract Functions	17
Contract Flow	33
Domain Info	34
Summary	35

Disclaimer**36****About Cyberscope****37**

Contract Review

Contract Name	DogeVerseToken
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200 runs
Licence	
Explorer	https://bscscan.com/token/0xF5646ea3825eD14EE54237310cdB84b4cc84638E
Domain	dogechampions.io

Audit Updates

Initial Audit	28th June 2022
Corrected	2nd July 2022

Introduction

The audited address `0xf5646ea3825ed14ee54237310cdb84b4cc84638e` implements the contract of the coin. The coin contains a dividends tracker feature that receives tokens from a specific tax on every transaction. The dividend tracker is connected with an NFT contract. It shares rewards proportional to the NFT holdings of every user. The auditing of the dividend tracker and the NFT ecosystem is **out of the scope of this audit. This audit is dedicated to coin implementation.**

During the auditing period the contract:

<https://bscscan.com/address/0xf5646ea3825ed14ee54237310cdb84b4cc84638e>

is pointed by the proxy address:

<https://bscscan.com/address/0x8925Fb1802f8974ADaaF70F190CB982c8dcFE465>

Source Files

Filename	SHA256
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	f0cbb88e6cbc994b565645eabd4320d27d529c7f1f4b3abb5fc263f3961c0a24
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	a513bea26edc02a8b2ff8b2977e953040efa7a61a752ff11ddfb057627ad7c50
@openzeppelin/contracts-upgradeable/security/ReentrancyGuardUpgradeable.sol	b6adbe9bc075b15cfb4b90f1ae020da4c78e3feada056a4c75b875350285c915
@openzeppelin/contracts-upgradeable/token/ERC1155/ERC1155Upgradeable.sol	014c5f22b0bcfac1eb7c73eff0971e9ca3f40cf3c74d6991bae2915b1e0a6ef8
@openzeppelin/contracts-upgradeable/token/ERC1155/extensions/ERC1155SupplyUpgradeable.sol	98d3570efe134810096cab2ce5d39c51323d9216e8528198fac44dd15cd3c841
@openzeppelin/contracts-upgradeable/token/ERC1155/extensions/IERC1155MetadataURIUpgradeable.sol	61e3317af2516530f091665d198fc3e27fb514038600fb07b7813913f439775f

@openzeppelin/contracts-upgradeable/token/ERC1155/IERC1155ReceiverUpgradeable.sol	7108589dbf9528c2ffe4f17fe489e8183be55c15b51af3b88c70252c13bac539
@openzeppelin/contracts-upgradeable/token/ERC1155/IERC1155Upgradeable.sol	08b1b1adbc515d850024f93e03d10ab2bd2003c999189e0c124b69bb71940240
@openzeppelin/contracts-upgradeable/token/ERC20/ERC20Upgradeable.sol	b3a6f7c65fa5c7288a65f5acde94cc2f220cce7892f41551a2f987249a955de1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/IERC20MetadataUpgradeable.sol	68bcca423fc72ec9625e219c9e36306c726a347e43f3711467c579bd3f6500c8
@openzeppelin/contracts-upgradeable/token/ERC20/IERC20Upgradeable.sol	4e09a7479aa3e7c313f8fc141c4c8fc04e0abfeb8754615ef7d78ec94c298b07
@openzeppelin/contracts-upgradeable/token/ERC721/ERC721Upgradeable.sol	91344e2805330c670623f0f8adaca28f58675a783c0d1490f83e06b93416e18d
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721EnumerableUpgradeable.sol	0b1fb4e02feef40d236a1b13acf26ab9b23736950ed3142297b1680840e491bb

@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721URIStorageUpgradeable.sol	b2627dd940804afd0a015dc10d4ea582ac4395757facf7ac7580321bed4336ac
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/IERC721EnumerableUpgradeable.sol	bb1d9c3bfcabd9561bfd84793e30332bed0da049c9fb4731f1398eaaac22d13b4
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/IERC721MetadataUpgradeable.sol	78d97961d78c8245d51fef2306c33bbc97edb18cb61159979a75187379e93c86
@openzeppelin/contracts-upgradeable/token/ERC721/IERC721ReceiverUpgradeable.sol	ad8f8e470e39cde97310b6366c8d440aaa000789a7b8c257587fc2075de7cff6
@openzeppelin/contracts-upgradeable/token/ERC721/IERC721Upgradeable.sol	9fdff069cde0011404b03bd8ec85244964685b339a07db811b25607c0bc29dde
@openzeppelin/contracts-upgradeable/utils/AddressUpgradeable.sol	44edc4d7099c781d11421cea2d82a52948e738f5f6191c8ad01dfc0f9858549c
@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol	5fb301961e45cb482fe4e05646d2f529aa449fe0e90c6671475d6a32356fa2d4

@openzeppelin/contracts-upgradeable/Utils/CountersUpgradeable.sol	5c1ac829a429b0c2ca9b4c9ed8b78d412320e9175e45f088c4e9056ef95fbf21
@openzeppelin/contracts-upgradeable/Utils/introspection/ERC165Upgradeable.sol	fd84e5284eccc479268f0ef36b830019d4f7999ceb7959430d8d8d9e602dd4ef
@openzeppelin/contracts-upgradeable/Utils/introspection/IERC165Upgradeable.sol	a39bc026ad6214e9ecd526bd4a1ddf9862d80bd4a9d0d031d9bafa4c3c147c0b
@openzeppelin/contracts-upgradeable/Utils/math/SafeMathUpgradeable.sol	4039686a509394aed475619c4e0b3a2df1df34fe59e90b9add8669de371eb731
@openzeppelin/contracts-upgradeable/Utils/StringsUpgradeable.sol	16a0e36f8dc6a83df3fec4344a11ad166ba99649d1cc52613c7ebe8015bd81a3
contracts/DogeChampionsConsumable.sol	9487f4d62b1bc7a84d3316acfb85c6f8d6c7a59aa09d545ac3b153dcebf058b6
contracts/DogeChampionsHolderRewardProtocol.sol	ae0ae96417766e842c02c17383e52081f0cf7206d2469f20e3b93b59017c5bb6
contracts/DogeChampionsNFT.sol	7ec9f452e3167129efdbfe625446799934eeec38d40755ace613d9742aebace0
contracts/DogeVerseToken.sol	096e7a4648ac57d9f017226d843e95be34e8ce4e5cf48bf7e5a951afa43f169c

contracts/interfaces/IUniswapV2Factory.sol	93bbc299c92b2a7ad33d502192e9368f5c7c7cc0db151015e2ca62b96d37445b
contracts/interfaces/IUniswapV2Pair.sol	7dc231f4e535f0bbfd837ee359765d09495c76abdd5a3b297d7578f937a43ba9
contracts/interfaces/IUniswapV2Router.sol	e377b6203035766bbba54b42dc641630ea48255c2ac0b45f8cb0bb2af8ff5727
contracts/ITournament.sol	c6f5fdc6daf3c245ab07598e2bdf5996a12e3bbebe986de1d85c40e5c3256fee

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

Contract Diagnostics

● Critical ● Medium ● Minor

Severity	Code	Description
●	BLC	Business Logic Concern
●	FSA	Fixed Swap Address
●	L01	Public Function could be Declared External
●	L04	Conformance to Solidity Naming Conventions
●	L07	Missing Events Arithmetic

BLC - Business Logic Concern

Criticality	minor
Location	contract.sol#L445

Description

When the contract sets a new reward protocol address, it is excluded from the fees and rewards. The previous reward protocol address remains excluded even if it is not used as a reward protocol.

```
function setDogeChampionsRewardProtocolAddress(address rewardProtocolAddress)
public onlyOwner {
    dogeChampionsHolderRewardProtocol =
DogeChampionsHolderRewardProtocol(rewardProtocolAddress);
    dogeChampionsRewardProtocolAddress = rewardProtocolAddress;
    _isExcludedFromFee[dogeChampionsRewardProtocolAddress] = true;
    _isExcludedFromMaxTx[dogeChampionsRewardProtocolAddress] = true;
    excludeFromReward(dogeChampionsRewardProtocolAddress);
}
```

Recommendation

The previous reward protocol address should be removed from the exclusions.

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L117

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(uniswapRouterAddress);  
    // Create a uniswap pair for this new token  
    uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory())  
        .createPair(address(this), _uniswapV2Router.WETH());  
  
    // set the rest of the contract variables  
    uniswapV2Router = _uniswapV2Router;
```

Recommendation

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

L01 - Public Function could be Declared External

Criticality	minor
Location	contracts/DogeVerseToken.sol#L133,137,141,145,154,163,168,174,179,82,184,188,192,201,259,265,296,301,399

Description

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

```
isExcludedFromFee  
setDogeChampionsRewardProtocolAddress  
setSwapAndLiquifyEnabled  
includeInFee  
excludeFromAll  
reflectionFromToken  
deliver  
totalFees  
isExcludedFromReward  
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality

minor

Location

contracts/DogeVerseToken.sol#L296,363,369,375,41,44,47,60

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.

```
_maxTxAmount  
_dogeChampionsRewardFee  
_liquidityFee  
_taxFee  
_amount  
_enabled
```

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	contracts/DogeVerseToken.sol#L269,274,279,284,291

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.

```
_maxTxAmount = maxTxAmount
_maxTxAmount = _tTotal.mul(maxTxPercent).div(10 ** 2)
_dogeChampionsRewardFee = dogeChampionsRewardFee
_liquidityFee = liquidityFee
_taxFee = taxFee
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
OwnableUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__Ownable_init	Internal	✓	onlyInitializing
	__Ownable_init_unchained	Internal	✓	onlyInitializing
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
Initializable	Implementation			
	_disableInitializers	Internal	✓	
	_setInitializedVersion	Private	✓	
ReentrancyGuardUpgradeable	Implementation	Initializable		
	__ReentrancyGuard_init	Internal	✓	onlyInitializing
	__ReentrancyGuard_init_unchained	Internal	✓	onlyInitializing
ERC1155Upgradeable	Implementation	Initializable, ContextUpgradeable, ERC165Upgradeable, IERC1155Upgradeable, IERC1155MetadataURIUpgradeable		
	__ERC1155_init	Internal	✓	onlyInitializing
	__ERC1155_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-

	uri	Public		-
	balanceOf	Public		-
	balanceOfBatch	Public		-
	setApprovalForAll	Public	✓	-
	isApprovedForAll	Public		-
	safeTransferFrom	Public	✓	-
	safeBatchTransferFrom	Public	✓	-
	_safeTransferFrom	Internal	✓	
	_safeBatchTransferFrom	Internal	✓	
	_setURI	Internal	✓	
	_mint	Internal	✓	
	_mintBatch	Internal	✓	
	_burn	Internal	✓	
	_burnBatch	Internal	✓	
	_setApprovalForAll	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
	_doSafeTransferAcceptanceCheck	Private	✓	
	_doSafeBatchTransferAcceptanceCheck	Private	✓	
	_asSingletonArray	Private		
ERC1155SupplyUpgradeable	Implementation	Initializable, ERC1155Upgradeable		
	__ERC1155Supply_init	Internal	✓	onlyInitializing
	__ERC1155Supply_init_unchained	Internal	✓	onlyInitializing
	totalSupply	Public		-
	exists	Public		-
	_beforeTokenTransfer	Internal	✓	
IERC1155MetadataURIUpgradeable	Interface	IERC1155Upgradeable		
	uri	External		-
IERC1155Receiver	Interface	IERC165Up		

iverUpgradeable		gradeable		
	onERC1155Received	External	✓	-
	onERC1155BatchReceived	External	✓	-
IERC1155Upgradeable	Interface	IERC165Upgradeable		
	balanceOf	External		-
	balanceOfBatch	External		-
	setApprovalForAll	External	✓	-
	isApprovedForAll	External		-
	safeTransferFrom	External	✓	-
	safeBatchTransferFrom	External	✓	-
ERC20Upgradeable	Implementation	Initializable, ContextUpgradeable, IERC20Upgradeable, IERC20MetadataUpgradeable		
	__ERC20_init	Internal	✓	onlyInitializing
	__ERC20_init_unchained	Internal	✓	onlyInitializing
	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	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
IERC20MetadataUpgradeable	Interface	IERC20Upgradeable		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20Upgradeable	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
ERC721Upgradeable	Implementation	Initializable, ContextUpgradeable, ERC165Upgradeable, IERC721Upgradeable, IERC721MetadataUpgradeable		
	__ERC721_init	Internal	✓	onlyInitializing
	__ERC721_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-
	balanceOf	Public		-
	ownerOf	Public		-
	name	Public		-
	symbol	Public		-
	tokenURI	Public		-
	_baseURI	Internal		

	approve	Public	✓	-
	getApproved	Public		-
	setApprovalForAll	Public	✓	-
	isApprovedForAll	Public		-
	transferFrom	Public	✓	-
	safeTransferFrom	Public	✓	-
	safeTransferFrom	Public	✓	-
	_safeTransfer	Internal	✓	
	_exists	Internal		
	_isApprovedOrOwner	Internal		
	_safeMint	Internal	✓	
	_safeMint	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_transfer	Internal	✓	
	_approve	Internal	✓	
	_setApprovalForAll	Internal	✓	
	_checkOnERC721Received	Private	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
ERC721EnumerableUpgradeable	Implementation	Initializable, ERC721Upgradable, IERC721EnumerableUpgradeable		
	__ERC721Enumerable_init	Internal	✓	onlyInitializing
	__ERC721Enumerable_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-
	tokenOfOwnerByIndex	Public		-
	totalSupply	Public		-
	tokenByIndex	Public		-
	_beforeTokenTransfer	Internal	✓	
	_addTokenToOwnerEnumeration	Private	✓	
	_addTokenToAllTokensEnumeration	Private	✓	
	_removeTokenFromOwnerEnumeratio	Private	✓	

	n			
	_removeTokenFromAllTokensEnumeration	Private	✓	
ERC721URIStorageUpgradeable	Implementation	Initializable, ERC721Upgradable		
	__ERC721URIStorage_init	Internal	✓	onlyInitializing
	__ERC721URIStorage_init_unchained	Internal	✓	onlyInitializing
	tokenURI	Public		-
	_setTokenURI	Internal	✓	
	_burn	Internal	✓	
IERC721EnumerableUpgradeable	Interface	IERC721Upgradable		
	totalSupply	External		-
	tokenOfOwnerByIndex	External		-
	tokenByIndex	External		-
IERC721MetadataUpgradeable	Interface	IERC721Upgradable		
	name	External		-
	symbol	External		-
	tokenURI	External		-
IERC721ReceiverUpgradeable	Interface			
	onERC721Received	External	✓	-
IERC721Upgradable	Interface	IERC165Upgradable		
	balanceOf	External		-
	ownerOf	External		-
	safeTransferFrom	External	✓	-
	safeTransferFrom	External	✓	-
	transferFrom	External	✓	-

	approve	External	✓	-
	setApprovalForAll	External	✓	-
	getApproved	External		-
	isApprovedForAll	External		-
AddressUpgradable	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	verifyCallResult	Internal		
ContextUpgradable	Implementation	Initializable		
	__Context_init	Internal	✓	onlyInitializing
	__Context_init_unchained	Internal	✓	onlyInitializing
	_msgSender	Internal		
	_msgData	Internal		
CountersUpgradable	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	
	reset	Internal	✓	
ERC165Upgradable	Implementation	Initializable, IERC165Upgradable		
	__ERC165_init	Internal	✓	onlyInitializing
	__ERC165_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-

IERC165Upgradable	Interface			
	supportsInterface	External		-
SafeMathUpgradable	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		
StringsUpgradable	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
DogeChampionsConsumable	Implementation	Initializable, ERC1155Upgradable, ERC1155SupplyUpgradable, OwnableUpgradable		
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	_beforeTokenTransfer	Internal	✓	
	setMarketplaceContractAddress	Public	✓	onlyOwner

	setTournamentContract	Public	✓	onlyOwner
	setNFTContract	Public	✓	onlyOwner
	setStakeProtocolContract	Public	✓	onlyOwner
	setPremiumPrice	Public	✓	onlyOwner
	mint	Public	✓	-
	migrationMint	Public	✓	onlyOwner
	premiumMint	Public	Payable	-
	bundleMint	Public	Payable	-
	consumeFrenzyEventMint	Public	✓	-
	premiumEventMint	Public	✓	-
	rewardMint	Public	✓	onlyDogeCham pionsProtocols
	burn	Public	✓	onlyDogeCham pionsNFT
	setBundlesAvailability	Public	✓	onlyOwner
	setConsumeFrenzyEventState	Public	✓	onlyOwner
	setPremiumEventState	Public	✓	onlyOwner
	setConsumeFrenzyEventData	Public	✓	onlyOwner
	setPremiumEventData	Public	✓	onlyOwner
	setBundleDetails	Public	✓	onlyOwner
	finalizeMigration	Public	✓	onlyOwner
	getConsumeFrenzyEventProgress	Public		-
	calculateConsumableType	Internal		
DogeChampionHolderRewardProtocol	Implementation	Initializable, OwnableUp gradeable, Reentrancy GuardUpgra deable		
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	setDogeVerseTokenContract	Public	✓	onlyOwner
	setConsumableContract	Public	✓	onlyOwner
	setNFTContract	Public	✓	onlyOwner
	setClaimEnabled	Public	✓	onlyOwner
	increaseDividendPerNFT	Public	✓	onlyDogeVerse TokenAndOwn

				er
	withdrawRewards	Public	✓	-
	getRewardBalance	Public		-
DogeChampionsNFT	Implementation	Initializable, OwnableUp gradeable, ERC721URI StorageUpg radeable, ERC721Enu merableUpg radeable		
	_beforeTokenTransfer	Internal	✓	
	_burn	Internal	✓	
	tokenURI	Public		-
	supportsInterface	Public		-
	_baseURI	Internal		
	_transfer	Internal	✓	
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	configureMint	Public	✓	onlyOwner
	calculateRandomness	Internal	✓	
	validatePlayability	Public		-
	validatePlayability	Public		-
	enhanceProperty	Public	✓	-
	enhance	Internal	✓	
	publicMint	Public	Payable	-
	freeMint	Public	✓	-
	migrationMint	Public	✓	onlyOwner
	mint	Internal	✓	
	determineRarity	Internal	✓	
	determineElement	Internal	✓	
	determineBackgroundLayer	Internal	✓	
	determinePower	Internal	✓	
	determineCRTRate	Internal	✓	
	determinePassive	Internal	✓	
	pushToPlayableIds	Public	✓	onlyMarketplac

				e
	_pushToPlayableIds	Internal	✓	
	removeFromPlayableIds	Public	✓	onlyMarketplace
	_removeFromPlayableIds	Internal	✓	
	finalizeMigration	Public	✓	onlyOwner
	getAttackPowers	Public		-
	getRarity	Public		-
	getElementsAndRarities	Public		-
	getTournamentValues	Public		-
	getAllValues	Public		-
	getConsumableHistory	Public		-
	getMinterOfToken	Public		-
	getPlayableIds	Public		-
	setPropertyDeterminationRates	Public	✓	onlyOwner
	setMintPrices	Public	✓	onlyOwner
	setBaseURI	Public	✓	onlyOwner
	setIgnoreDiscountFlag	Public	✓	onlyOwner
	setContracts	Public	✓	onlyOwner
	setMintAvailability	Public	✓	onlyOwner
	setAddressToCollaboratorWhitelist	Public	✓	onlyOwner
	setAddressToDiscountWhitelist	Public	✓	onlyOwner
DogeVerseToken	Implementation	Initializable, ContextUpgradable, ERC20Upgradable, OwnableUpgradable		
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-

	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	totalFees	Public		-
	deliver	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	_transferBothExcluded	Private	✓	
	excludeFromFee	Public	✓	onlyOwner
	excludeFromMaxTx	Public	✓	onlyOwner
	excludeFromAll	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setTaxFeePercent	External	✓	onlyOwner
	setLiquidityFeePercent	External	✓	onlyOwner
	setDogeChampionsRewardFeePercent	External	✓	onlyOwner
	setMaxTxPercent	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	setDogeChampionsRewardProtocolAddress	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private	✓	
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		

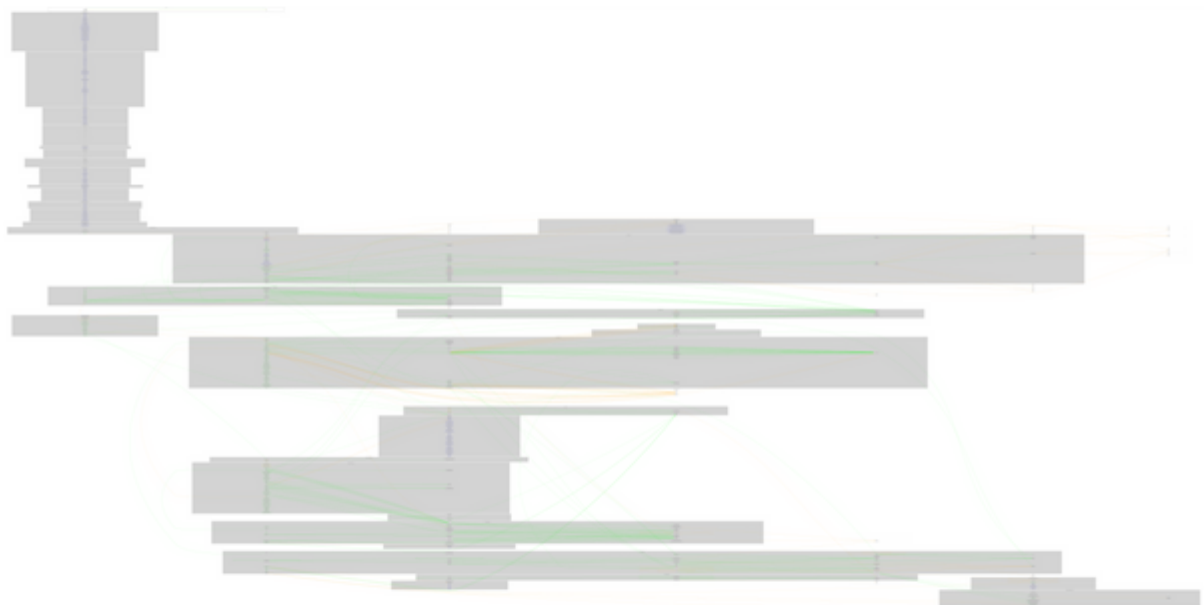
	calculateRewardFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-
	_approve	Internal	✓	
	_transfer	Internal	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	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		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IUniswapV2Router01	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		-
IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
ITournament	Interface			
	setWinnerRewardCount	External	✓	-
	setParticipationRewardCount	External	✓	-
	setNFTContract	External	✓	-
	setConsumableContract	External	✓	-
	setPaidTournamentEntranceFee	External	✓	-
	register	External	Payable	-
	setTournament	External	✓	-
	endCurrentTournament	External	✓	-
	getContractBalance	External		-
	getActiveTournaments	External		-
	getLatestEndedTournaments	External		-
	getTournament	External		-
	getTournamentWinner	External		-
	getCurrentTournament	External		-
	getPaidTournamentEntryFee	External		-
	getParticipantCount	External		-
	getRewards	External		-
	getIsJoined	External		-

	decreaseReward	External	✓	-
	decreaseConsumableReward	External	✓	-

Contract Flow



Domain Info

Domain Name	dogechampions.io
Registry Domain ID	c20b10f0013f4841bec5c5cc73b07dc2-DONUTS
Creation Date	2021-11-22T16:55:43Z
Updated Date	2021-11-27T16:56:34Z
Registry Expiry Date	2022-11-22T16:55:43Z
Registrar WHOIS Server	key-systems.net
Registrar URL	http://key-systems.net
Registrar	Key-Systems GmbH
Registrar IANA ID	269

The domain was created 5 months before the creation of the audit.

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

Summary

DogeVerseToken is an interesting project that has a friendly and growing community. The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions.

The contract is pointed by the address <https://bscscan.com/address/0x8925Fb1802f8974ADaaF70F190CB982c8dcFE465>. The proxy pointer can change any time without any warning.

The contract sends tokens to a dividend tracker. The functionality of the dividend tracker is out of the audit scope.

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>



Cyberscope

Audit Report

DogeVerseToken

June 2022

Type BEP20

Network BSC

Address 0x5198BA95447358DF6F209822A2e131D1E1989079

Audited by © cyberscope

Table of Contents

Table of Contents	1
Contract Review	3
Audit Updates	3
Introduction	4
Source Files	5
Contract Analysis	10
ST - Stop Transactions	11
Description	11
Recommendation	11
ELFM - Exceed Limit Fees Manipulation	12
Description	12
Recommendation	12
Contract Diagnostics	13
BLC - Business Logic Concern	14
Description	14
Recommendation	14
FSA - Fixed Swap Address	15
Description	15
Recommendation	15
L01 - Public Function could be Declared External	16
Description	16
Recommendation	16
L04 - Conformance to Solidity Naming Conventions	17
Description	17
Recommendation	17
L07 - Missing Events Arithmetic	18

Description	18
Recommendation	18
Contract Functions	19
Contract Flow	35
Domain Info	36
Summary	37
Disclaimer	38
About Cyberscope	39

Contract Review

Contract Name	DogeVerseToken
Compiler Version	v0.8.4+commit.c7e474f2
Optimization	200 runs
Licence	
Explorer	https://bscscan.com/token/0x5198BA95447358DF6F209822A2e131D1E1989079
Symbol	
Decimals	0
Total Supply	-
Domain	dogechampions.io

Audit Updates

Initial Audit	28th June 2022
Corrected	

Introduction

The audited address `0x5198BA95447358DF6F209822A2e131D1E1989079` implements the contract of the coin. The coin contains a dividends tracker feature that receives tokens from a specific tax on every transaction. The dividend tracker is connected with an NFT contract. It shares rewards proportional to the NFT holdings of every user. The auditing of the dividend tracker and the NFT ecosystem is **out of the scope of this audit. This audit is dedicated to coin implementation.**

During the auditing period the contract:

<https://bscscan.com/address/0x5198ba95447358df6f209822a2e131d1e1989079>

is pointed by the proxy address:

<https://bscscan.com/address/0x8925Fb1802f8974ADaaF70F190CB982c8dcFE465>

Source Files

Filename	SHA256
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	f0cbb88e6cbc994b565645eabd4320d27d529c7f1f4b3abb5fc263f3961c0a24
@openzeppelin/contracts-upgradeable/proxy/utils/Initializable.sol	a513bea26edc02a8b2ff8b2977e953040efa7a61a752ff11ddfb057627ad7c50
@openzeppelin/contracts-upgradeable/security/ReentrancyGuardUpgradeable.sol	b6adbe9bc075b15cfb4b90f1ae020da4c78e3feada056a4c75b875350285c915
@openzeppelin/contracts-upgradeable/token/ERC1155/ERC1155Upgradeable.sol	014c5f22b0bcfac1eb7c73eff0971e9ca3f40cf3c74d6991bae2915b1e0a6ef8
@openzeppelin/contracts-upgradeable/token/ERC1155/extensions/ERC1155SupplyUpgradeable.sol	98d3570efe134810096cab2ce5d39c51323d9216e8528198fac44dd15cd3c841
@openzeppelin/contracts-upgradeable/token/ERC1155/extensions/IERC1155MetadataURIUpgradeable.sol	61e3317af2516530f091665d198fc3e27fb514038600fb07b7813913f439775f

@openzeppelin/contracts-upgradeable/token/ERC1155/IERC1155ReceiverUpgradeable.sol	7108589dbf9528c2ffe4f17fe489e8183be55c15b51af3b88c70252c13bac539
@openzeppelin/contracts-upgradeable/token/ERC1155/IERC1155Upgradeable.sol	08b1b1adbc515d850024f93e03d10ab2bd2003c999189e0c124b69bb71940240
@openzeppelin/contracts-upgradeable/token/ERC20/ERC20Upgradeable.sol	b3a6f7c65fa5c7288a65f5acde94cc2f220cce7892f41551a2f987249a955de1
@openzeppelin/contracts-upgradeable/token/ERC20/extensions/IERC20MetadataUpgradeable.sol	68bcca423fc72ec9625e219c9e36306c726a347e43f3711467c579bd3f6500c8
@openzeppelin/contracts-upgradeable/token/ERC20/IERC20Upgradeable.sol	4e09a7479aa3e7c313f8fc141c4c8fc04e0abfeb8754615ef7d78ec94c298b07
@openzeppelin/contracts-upgradeable/token/ERC721/ERC721Upgradeable.sol	91344e2805330c670623f0f8adaca28f58675a783c0d1490f83e06b93416e18d
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721EnumerableUpgradeable.sol	0b1fb4e02feef40d236a1b13acf26ab9b23736950ed3142297b1680840e491bb

@openzeppelin/contracts-upgradeable/token/ERC721/extensions/ERC721URIStorageUpgradeable.sol	b2627dd940804afd0a015dc10d4ea582ac4395757facf7ac7580321bed4336ac
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/IERC721EnumerableUpgradeable.sol	bb1d9c3bfcabd9561bfd84793e30332bed0da049c9fb4731f1398eaaac22d13b4
@openzeppelin/contracts-upgradeable/token/ERC721/extensions/IERC721MetadataUpgradeable.sol	78d97961d78c8245d51fef2306c33bbc97edb18cb61159979a75187379e93c86
@openzeppelin/contracts-upgradeable/token/ERC721/IERC721ReceiverUpgradeable.sol	ad8f8e470e39cde97310b6366c8d440aaa000789a7b8c257587fc2075de7cff6
@openzeppelin/contracts-upgradeable/token/ERC721/IERC721Upgradeable.sol	9fdff069cde0011404b03bd8ec85244964685b339a07db811b25607c0bc29dde
@openzeppelin/contracts-upgradeable/utils/AddressUpgradeable.sol	44edc4d7099c781d11421cea2d82a52948e738f5f6191c8ad01dfc0f9858549c
@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol	5fb301961e45cb482fe4e05646d2f529aa449fe0e90c6671475d6a32356fa2d4

@openzeppelin/contracts-upgradeable/Utils/CountersUpgradeable.sol	5c1ac829a429b0c2ca9b4c9ed8b78d412320e9175e45f088c4e9056ef95fbf21
@openzeppelin/contracts-upgradeable/Utils/introspection/ERC165Upgradeable.sol	fd84e5284eccc479268f0ef36b830019d4f7999ceb7959430d8d8d9e602dd4ef
@openzeppelin/contracts-upgradeable/Utils/introspection/IERC165Upgradeable.sol	a39bc026ad6214e9ecd526bd4a1ddf9862d80bd4a9d0d031d9bafa4c3c147c0b
@openzeppelin/contracts-upgradeable/Utils/math/SafeMathUpgradeable.sol	4039686a509394aed475619c4e0b3a2df1df34fe59e90b9add8669de371eb731
@openzeppelin/contracts-upgradeable/Utils/StringsUpgradeable.sol	16a0e36f8dc6a83df3fec4344a11ad166ba99649d1cc52613c7ebe8015bd81a3
contracts/DogeChampionsConsumable.sol	9487f4d62b1bc7a84d3316acfb85c6f8d6c7a59aa09d545ac3b153dcebf058b6
contracts/DogeChampionsHolderRewardProtocol.sol	ae0ae96417766e842c02c17383e52081f0cf7206d2469f20e3b93b59017c5bb6
contracts/DogeChampionsNFT.sol	7ec9f452e3167129efdbfe625446799934eeec38d40755ace613d9742aebace0
contracts/DogeVerseToken.sol	4dceda653643dd6eec821216d830d989545704b611397ed56e7f8186bc3c375c

contracts/interfaces/IUniswapV2Factory.sol	93bbc299c92b2a7ad33d502192e9368f5c7c7cc0db151015e2ca62b96d37445b
contracts/interfaces/IUniswapV2Pair.sol	7dc231f4e535f0bbfd837ee359765d09495c76abdd5a3b297d7578f937a43ba9
contracts/interfaces/IUniswapV2Router.sol	e377b6203035766bbba54b42dc641630ea48255c2ac0b45f8cb0bb2af8ff5727
contracts/ITournament.sol	c6f5fdc6daf3c245ab07598e2bdf5996a12e3bbebe986de1d85c40e5c3256fee

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

Criticality	medium
Location	contract.sol#L410

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 `_maxTxAmount` to zero.

```
if(!_isExcludedFromMaxTx[from] && !_isExcludedFromMaxTx[to])  
    require(amount <= _maxTxAmount, "Transfer amount exceeds the maxTxAmount.");
```

Recommendation

The contract could embody a check for not allowing setting the `_maxTxAmount` 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.

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L269,273,277

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setTaxFeePercent` function with a high percentage value.

```
function setTaxFeePercent(uint256 taxFee) external onlyOwner() {  
    _taxFee = taxFee;  
}
```

Recommendation

The contract could embody a check for the maximum acceptable value.

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
●	BLC	Business Logic Concern
●	FSA	Fixed Swap Address
●	L01	Public Function could be Declared External
●	L04	Conformance to Solidity Naming Conventions
●	L07	Missing Events Arithmetic

BLC - Business Logic Concern

Criticality	minor
Location	contract.sol#L445

Description

When the contract sets a new reward protocol address, it is excluded from the fees and rewards. The previous reward protocol address remains excluded even if it is not used as a reward protocol.

```
function setDogeChampionsRewardProtocolAddress(address rewardProtocolAddress)
public onlyOwner {
    dogeChampionsHolderRewardProtocol =
DogeChampionsHolderRewardProtocol(rewardProtocolAddress);
    dogeChampionsRewardProtocolAddress = rewardProtocolAddress;
    _isExcludedFromFee[dogeChampionsRewardProtocolAddress] = true;
    _isExcludedFromMaxTx[dogeChampionsRewardProtocolAddress] = true;
    excludeFromReward(dogeChampionsRewardProtocolAddress);
}
```

Recommendation

The previous reward protocol address should be removed from the exclusions.

FSA - Fixed Swap Address

Criticality	minor
Location	contract.sol#L117

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(uniswapRouterAddress);  
    // Create a uniswap pair for this new token  
    uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory())  
        .createPair(address(this), _uniswapV2Router.WETH());  
  
    // set the rest of the contract variables  
    uniswapV2Router = _uniswapV2Router;
```

Recommendation

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

L01 - Public Function could be Declared External

Criticality	minor
Location	contracts/DogeVerseToken.sol#L133,137,141,145,154,163,168,174,179,82,184,188,192,201,259,265,291,296,394

Description

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

```
isExcludedFromFee  
setDogeChampionsRewardProtocolAddress  
setSwapAndLiquifyEnabled  
includeInFee  
excludeFromAll  
reflectionFromToken  
deliver  
totalFees  
isExcludedFromReward  
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/DogeVerseToken.sol#L291,358,364,370,41,44,47,60

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.

```
_maxTxAmount  
_dogeChampionsRewardFee  
_liquidityFee  
_taxFee  
_amount  
_enabled
```

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	contracts/DogeVerseToken.sol#L269,273,277,281,287

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.

```
_maxTxAmount = maxTxAmount  
_maxTxAmount = _tTotal.mul(maxTxPercent).div(10 ** 2)  
_dogeChampionsRewardFee = dogeChampionsRewardFee  
_liquidityFee = liquidityFee  
_taxFee = taxFee
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
OwnableUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__Ownable_init	Internal	✓	onlyInitializing
	__Ownable_init_unchained	Internal	✓	onlyInitializing
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
Initializable	Implementation			
	_disableInitializers	Internal	✓	
	_setInitializedVersion	Private	✓	
ReentrancyGuardUpgradeable	Implementation	Initializable		
	__ReentrancyGuard_init	Internal	✓	onlyInitializing
	__ReentrancyGuard_init_unchained	Internal	✓	onlyInitializing
ERC1155Upgradeable	Implementation	Initializable, ContextUpgradeable, ERC165Upgradeable, IERC1155Upgradeable, IERC1155MetadataURIUpgradeable		
	__ERC1155_init	Internal	✓	onlyInitializing
	__ERC1155_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-

	uri	Public		-
	balanceOf	Public		-
	balanceOfBatch	Public		-
	setApprovalForAll	Public	✓	-
	isApprovedForAll	Public		-
	safeTransferFrom	Public	✓	-
	safeBatchTransferFrom	Public	✓	-
	_safeTransferFrom	Internal	✓	
	_safeBatchTransferFrom	Internal	✓	
	_setURI	Internal	✓	
	_mint	Internal	✓	
	_mintBatch	Internal	✓	
	_burn	Internal	✓	
	_burnBatch	Internal	✓	
	_setApprovalForAll	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
	_doSafeTransferAcceptanceCheck	Private	✓	
	_doSafeBatchTransferAcceptanceCheck	Private	✓	
	_asSingletonArray	Private		
ERC1155SupplyUpgradeable	Implementation	Initializable, ERC1155Upgradeable		
	__ERC1155Supply_init	Internal	✓	onlyInitializing
	__ERC1155Supply_init_unchained	Internal	✓	onlyInitializing
	totalSupply	Public		-
	exists	Public		-
	_beforeTokenTransfer	Internal	✓	
IERC1155MetadataURIUpgradeable	Interface	IERC1155Upgradeable		
	uri	External		-
IERC1155Receiver	Interface	IERC165Up		

iverUpgradeable		gradeable		
	onERC1155Received	External	✓	-
	onERC1155BatchReceived	External	✓	-
IERC1155Upgradable	Interface	IERC165Upgradable		
	balanceOf	External		-
	balanceOfBatch	External		-
	setApprovalForAll	External	✓	-
	isApprovedForAll	External		-
	safeTransferFrom	External	✓	-
	safeBatchTransferFrom	External	✓	-
ERC20Upgradable	Implementation	Initializable, ContextUpgradable, IERC20Upgradable, IERC20MetadataUpgradable		
	__ERC20_init	Internal	✓	onlyInitializing
	__ERC20_init_unchained	Internal	✓	onlyInitializing
	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	✓	
	_spendAllowance	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
IERC20MetadataUpgradeable	Interface	IERC20Upgradeable		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20Upgradeable	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
ERC721Upgradeable	Implementation	Initializable, ContextUpgradeable, ERC165Upgradeable, IERC721Upgradeable, IERC721MetadataUpgradeable		
	__ERC721_init	Internal	✓	onlyInitializing
	__ERC721_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-
	balanceOf	Public		-
	ownerOf	Public		-
	name	Public		-
	symbol	Public		-
	tokenURI	Public		-
	_baseURI	Internal		

	approve	Public	✓	-
	getApproved	Public		-
	setApprovalForAll	Public	✓	-
	isApprovedForAll	Public		-
	transferFrom	Public	✓	-
	safeTransferFrom	Public	✓	-
	safeTransferFrom	Public	✓	-
	_safeTransfer	Internal	✓	
	_exists	Internal		
	_isApprovedOrOwner	Internal		
	_safeMint	Internal	✓	
	_safeMint	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_transfer	Internal	✓	
	_approve	Internal	✓	
	_setApprovalForAll	Internal	✓	
	_checkOnERC721Received	Private	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
ERC721EnumerableUpgradeable	Implementation	Initializable, ERC721Upgradable, IERC721EnumerableUpgradeable		
	__ERC721Enumerable_init	Internal	✓	onlyInitializing
	__ERC721Enumerable_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-
	tokenOfOwnerByIndex	Public		-
	totalSupply	Public		-
	tokenByIndex	Public		-
	_beforeTokenTransfer	Internal	✓	
	_addTokenToOwnerEnumeration	Private	✓	
	_addTokenToAllTokensEnumeration	Private	✓	
	_removeTokenFromOwnerEnumeratio	Private	✓	

	n			
	_removeTokenFromAllTokensEnumeration	Private	✓	
ERC721URIStorageUpgradeable	Implementation	Initializable, ERC721Upgradable		
	__ERC721URIStorage_init	Internal	✓	onlyInitializing
	__ERC721URIStorage_init_unchained	Internal	✓	onlyInitializing
	tokenURI	Public		-
	_setTokenURI	Internal	✓	
	_burn	Internal	✓	
IERC721EnumerableUpgradeable	Interface	IERC721Upgradable		
	totalSupply	External		-
	tokenOfOwnerByIndex	External		-
	tokenByIndex	External		-
IERC721MetadataUpgradeable	Interface	IERC721Upgradable		
	name	External		-
	symbol	External		-
	tokenURI	External		-
IERC721ReceiverUpgradeable	Interface			
	onERC721Received	External	✓	-
IERC721Upgradable	Interface	IERC165Upgradable		
	balanceOf	External		-
	ownerOf	External		-
	safeTransferFrom	External	✓	-
	safeTransferFrom	External	✓	-
	transferFrom	External	✓	-

	approve	External	✓	-
	setApprovalForAll	External	✓	-
	getApproved	External		-
	isApprovedForAll	External		-
AddressUpgradable	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	verifyCallResult	Internal		
ContextUpgradable	Implementation	Initializable		
	__Context_init	Internal	✓	onlyInitializing
	__Context_init_unchained	Internal	✓	onlyInitializing
	_msgSender	Internal		
	_msgData	Internal		
CountersUpgradable	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	
	reset	Internal	✓	
ERC165Upgradable	Implementation	Initializable, IERC165Upgradable		
	__ERC165_init	Internal	✓	onlyInitializing
	__ERC165_init_unchained	Internal	✓	onlyInitializing
	supportsInterface	Public		-

IERC165Upgradable	Interface			
	supportsInterface	External		-
SafeMathUpgradable	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		
StringsUpgradable	Library			
	toString	Internal		
	toHexString	Internal		
	toHexString	Internal		
DogeChampionsConsumable	Implementation	Initializable, ERC1155Upgradable, ERC1155SupplyUpgradable, OwnableUpgradable		
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	_beforeTokenTransfer	Internal	✓	
	setMarketplaceContractAddress	Public	✓	onlyOwner

	setTournamentContract	Public	✓	onlyOwner
	setNFTContract	Public	✓	onlyOwner
	setStakeProtocolContract	Public	✓	onlyOwner
	setPremiumPrice	Public	✓	onlyOwner
	mint	Public	✓	-
	migrationMint	Public	✓	onlyOwner
	premiumMint	Public	Payable	-
	bundleMint	Public	Payable	-
	consumeFrenzyEventMint	Public	✓	-
	premiumEventMint	Public	✓	-
	rewardMint	Public	✓	onlyDogeCham pionsProtocols
	burn	Public	✓	onlyDogeCham pionsNFT
	setBundlesAvailability	Public	✓	onlyOwner
	setConsumeFrenzyEventState	Public	✓	onlyOwner
	setPremiumEventState	Public	✓	onlyOwner
	setConsumeFrenzyEventData	Public	✓	onlyOwner
	setPremiumEventData	Public	✓	onlyOwner
	setBundleDetails	Public	✓	onlyOwner
	finalizeMigration	Public	✓	onlyOwner
	getConsumeFrenzyEventProgress	Public		-
	calculateConsumableType	Internal		
DogeChampionHolderRewardProtocol	Implementation	Initializable, OwnableUp gradeable, Reentrancy GuardUpgra deable		
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	setDogeVerseTokenContract	Public	✓	onlyOwner
	setConsumableContract	Public	✓	onlyOwner
	setNFTContract	Public	✓	onlyOwner
	setClaimEnabled	Public	✓	onlyOwner
	increaseDividendPerNFT	Public	✓	onlyDogeVerse TokenAndOwn

				er
	withdrawRewards	Public	✓	-
	getRewardBalance	Public		-
DogeChampionsNFT	Implementation	Initializable, OwnableUp gradeable, ERC721URI StorageUpg radeable, ERC721Enu merableUpg radeable		
	_beforeTokenTransfer	Internal	✓	
	_burn	Internal	✓	
	tokenURI	Public		-
	supportsInterface	Public		-
	_baseURI	Internal		
	_transfer	Internal	✓	
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	configureMint	Public	✓	onlyOwner
	calculateRandomness	Internal	✓	
	validatePlayability	Public		-
	validatePlayability	Public		-
	enhanceProperty	Public	✓	-
	enhance	Internal	✓	
	publicMint	Public	Payable	-
	freeMint	Public	✓	-
	migrationMint	Public	✓	onlyOwner
	mint	Internal	✓	
	determineRarity	Internal	✓	
	determineElement	Internal	✓	
	determineBackgroundLayer	Internal	✓	
	determinePower	Internal	✓	
	determineCRTRate	Internal	✓	
	determinePassive	Internal	✓	
	pushToPlayableIds	Public	✓	onlyMarketplac

				e
	_pushToPlayableIds	Internal	✓	
	removeFromPlayableIds	Public	✓	onlyMarketplace
	_removeFromPlayableIds	Internal	✓	
	finalizeMigration	Public	✓	onlyOwner
	getAttackPowers	Public		-
	getRarity	Public		-
	getElementsAndRarities	Public		-
	getTournamentValues	Public		-
	getAllValues	Public		-
	getConsumableHistory	Public		-
	getMinterOfToken	Public		-
	getPlayableIds	Public		-
	setPropertyDeterminationRates	Public	✓	onlyOwner
	setMintPrices	Public	✓	onlyOwner
	setBaseURI	Public	✓	onlyOwner
	setIgnoreDiscountFlag	Public	✓	onlyOwner
	setContracts	Public	✓	onlyOwner
	setMintAvailability	Public	✓	onlyOwner
	setAddressToCollaboratorWhitelist	Public	✓	onlyOwner
	setAddressToDiscountWhitelist	Public	✓	onlyOwner
DogeVerseToken	Implementation	Initializable, ContextUpgradable, ERC20Upgradable, OwnableUpgradable		
	<Constructor>	Public	✓	-
	initialize	Public	✓	initializer
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-

	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	totalFees	Public		-
	deliver	Public	✓	-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	Public	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	_transferBothExcluded	Private	✓	
	excludeFromFee	Public	✓	onlyOwner
	excludeFromMaxTx	Public	✓	onlyOwner
	excludeFromAll	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	setTaxFeePercent	External	✓	onlyOwner
	setLiquidityFeePercent	External	✓	onlyOwner
	setDogeChampionsRewardFeePercent	External	✓	onlyOwner
	setMaxTxPercent	External	✓	onlyOwner
	setMaxTxAmount	External	✓	onlyOwner
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	setDogeChampionsRewardProtocolAddress	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	_reflectFee	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_takeLiquidity	Private	✓	
	calculateTaxFee	Private		
	calculateLiquidityFee	Private		

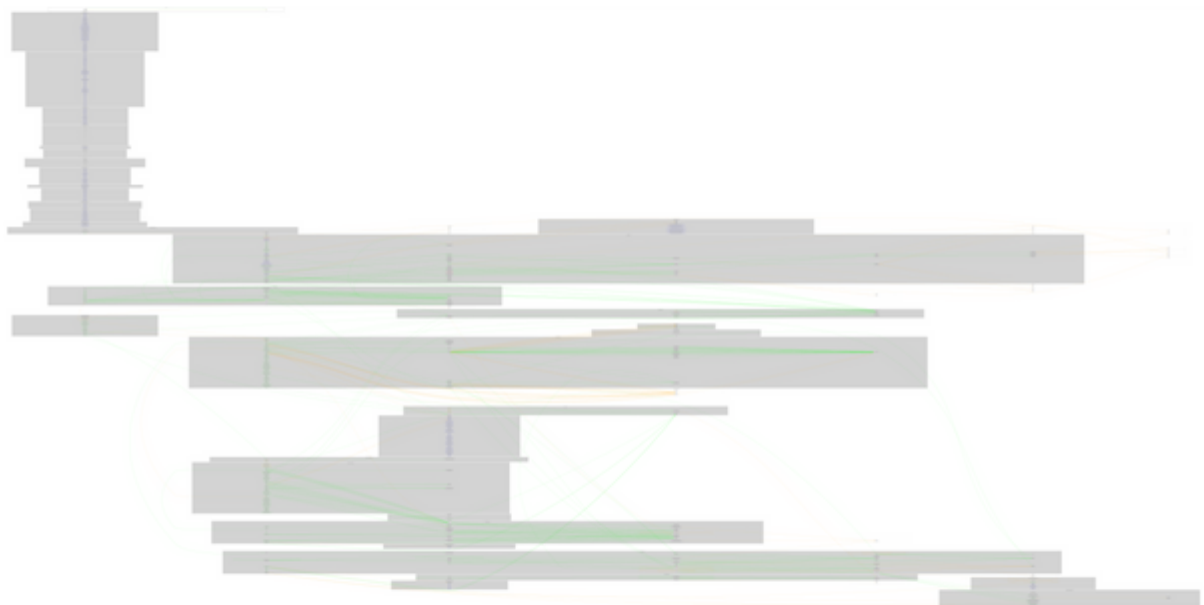
	calculateRewardFee	Private		
	removeAllFee	Private	✓	
	restoreAllFee	Private	✓	
	isExcludedFromFee	Public		-
	_approve	Internal	✓	
	_transfer	Internal	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	_tokenTransfer	Private	✓	
	_transferStandard	Private	✓	
	_transferToExcluded	Private	✓	
	_transferFromExcluded	Private	✓	
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Pair	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		-
	mint	External	✓	-
	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
IUniswapV2Router01	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		-
IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
ITournament	Interface			
	setWinnerRewardCount	External	✓	-
	setParticipationRewardCount	External	✓	-
	setNFTContract	External	✓	-
	setConsumableContract	External	✓	-
	setPaidTournamentEntranceFee	External	✓	-
	register	External	Payable	-
	setTournament	External	✓	-
	endCurrentTournament	External	✓	-
	getContractBalance	External		-
	getActiveTournaments	External		-
	getLatestEndedTournaments	External		-
	getTournament	External		-
	getTournamentWinner	External		-
	getCurrentTournament	External		-
	getPaidTournamentEntryFee	External		-
	getParticipantCount	External		-
	getRewards	External		-
	getIsJoined	External		-

	decreaseReward	External	✓	-
	decreaseConsumableReward	External	✓	-

Contract Flow



Domain Info

Domain Name	dogechampions.io
Registry Domain ID	c20b10f0013f4841bec5c5cc73b07dc2-DONUTS
Creation Date	2021-11-22T16:55:43Z
Updated Date	2021-11-27T16:56:34Z
Registry Expiry Date	2022-11-22T16:55:43Z
Registrar WHOIS Server	key-systems.net
Registrar URL	http://key-systems.net
Registrar	Key-Systems GmbH
Registrar IANA ID	269

The domain was created 5 months before the creation of the audit.

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 manipulating 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.

The contract sends tokens to a dividend tracker. The functionality of the dividend tracker is out of the audit scope.

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>