Cyberscope

Audit Report

NFTSport Lottery

November 2022

Gitlab	https://gitlab.com/hola-tech1/worldcup-nft/nftsport-contracts
Commit	3735ccf93cd73bcbb8f4857db4c215bf4f4ac09b
Audited by	© cyberscope

Table of Contents

Contract Review

Contract Name	Lottery
Gitlab	https://gitlab.com/hola-tech1/worldcup-nft/nftsport-contracts
Commit	3735ccf93cd73bcbb8f4857db4c215bf4f4ac09b

Audit Updates

Initial Audit	13th November 2022
Corrected	

Source Files

Filename	SHA256
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	4d148e038344167b7506ee0efd58b38f8787c6229e43800fb1129a0d4215327f
@openzeppelin/contracts-upgradeable/cryptography/MerkleProofUpgradeable.sol	38b7d647153f45309495a2713cd37536f6163ccac30717e3ecd9ac3e83200664
@openzeppelin/contracts-upgradeable/math/SafeMathUpgradeable.sol	dabaab4d3d3f03e6bfb86eec1d54f31edf0429f4bfc4dff717d5776d5231c145
@openzeppelin/contracts-upgradeable/proxy/Initializable.sol	2c3a3edc2b1a4ac2c4a8645475b51f2668b1ad5ea22df074d0c0ebd3122ce2e7
@openzeppelin/contracts-upgradeable/token/ERC721/IERC721ReceiverUpgradeable.sol	3907de7006118eb83925d21fec1a435919366b545ef8fe6363f11cf9f6273501
@openzeppelin/contracts-upgradeable/utils/AddressUpgradeable.sol	877bc9cb396d0f50330bb9c0057c029407e159739b6fab0b110f19451c8681e4
@openzeppelin/contracts-upgradeable/utils/ContextUpgradeable.sol	b9c1700bc8c28217952147b408dc67aa128eb2f71a45fceb4a8e73dff43fedac

@openzeppelin/contracts-upgradeable/utils/CountersUpgradeable.sol	5eaed54426f3286ef6ef62991c00c5c710833f12102b355dba2e8c3cda983ba4
@openzeppelin/contracts-upgradeable/utils/EnumerableSetUpgradeable.sol	634d70c2c44eda75e237be5a1f312c429475e8f3a0ab2b176aca3ae1a2d8f426
@openzeppelin/contracts-upgradeable/utils/ReentrancyGuardUpgradeable.sol	06e73664cf2eed972058697327c00d2595da4fe9a51398073bf8829e6307532a
@openzeppelin/contracts/introspection/IERC165.sol	24d63fd063d0d9e954ce1a039404b4c01d2141f787143bbd3d5090a0220a2bcc
@openzeppelin/contracts/token/ERC721/IERC721.sol	07abc5d9ae593f0dc7b854cb476fbee9e9f0df1c8f864e061f61e1532fb16357
@openzeppelin/contracts/token/ERC721/IERC721Enumerable.sol	da6fa0593fd96281d88df725727540d0c61551ed756a31a2ef6e1e8ccfbbe59d
contracts/interfaces/INFTSport.sol	74cb5baaf50a6ed63c0dff5173c9fab90d6e1f9a61ddb59ca52300b675949efb
contracts/libraries/TransferHelper.sol	bf61f5798d83a34255cdd18d52a3fd51ea3f8e3983dd9418050d0d80b997920e
contracts/lottery/Lottery.sol	56a98e8bb8d6dcb9f490f456ada8e23cd916328d9362c1633aac2915b7087ca8

Off Chain Winners Draw

The winners draw mechanism is based on an off-chain logic. The contract owner is responsible for updating the in-chain “merkleRoot” in order to validate correctly amount of native tokens that the winners will claim. The verification algorithm is using the markle tree mechanism.

https://en.wikipedia.org/wiki/Merkle_tree

According to the markle algorithm, the off-chain mechanism pre-defines the amount of native tokens that each participant will claim per round.

Audit Context

This audit focuses on the in-chain functionality. The off-chain functionality is out of the audit context.

Contract Diagnostics

● Critical ● Medium ● Minor / Informative

Severity	Code	Description	Status
●	CO	Code Optimization	Unresolved
●	L09	Dead Code Elimination	Unresolved

CO - Code Optimization

Criticality	minor / informative
Location	contract.sol
Status	Unresolved

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 `unlockTime` and `timestamp` properties are assigned with the current timestamp. Both properties cannot be changed in the contract. As a result, they will always have the same value.

```
round.unlockTime = block.timestamp;
round.result = _result;
round.timestamp = block.timestamp;
```

Recommendation

The contract could remove the `timestamp` property since it always has the same value with u`nlockTime.`

L09 - Dead Code Elimination

Criticality	minor / informative
Location	contracts/libraries/TransferHelper.sol#L27,7,17
Status	Unresolved

Description

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

```
safeTransferFrom
safeApprove
safeTransfer
```

Recommendation

Remove unused functions.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
OwnableUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__Ownable_init	Internal	✓	initializer
	__Ownable_init_unchained	Internal	✓	initializer
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
MerkleProofUpgradeable	Library			
	verify	Internal		
SafeMathUpgradeable	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		
Initializable	Implementation			

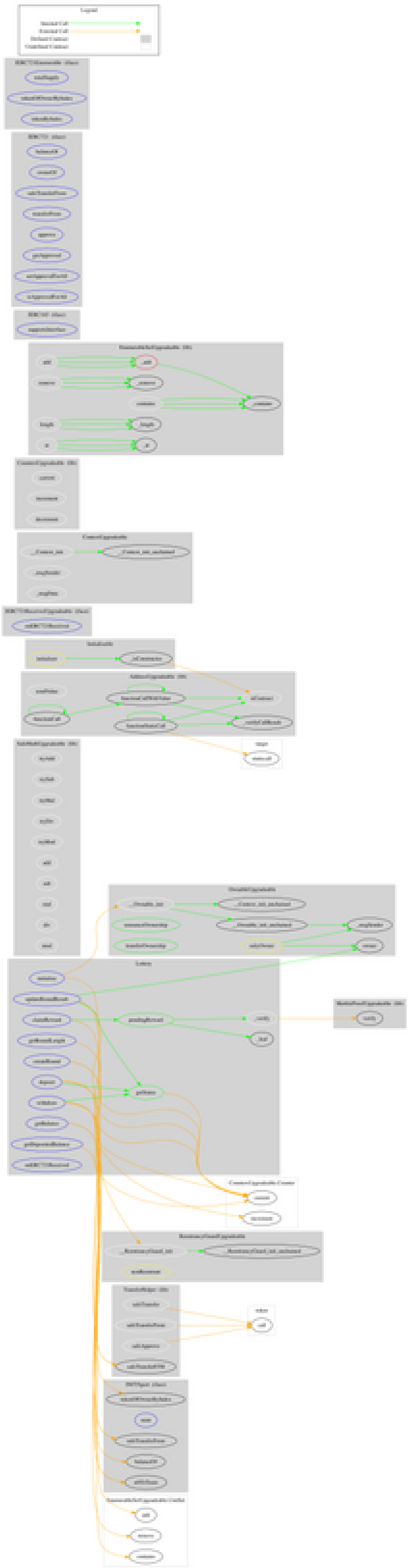
	_isConstructor	Private		
IERC721ReceiverUpgradeable	Interface			
	onERC721Received	External	✓	-
AddressUpgradeable	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	_verifyCallResult	Private		
ContextUpgradeable	Implementation	Initializable		
	__Context_init	Internal	✓	initializer
	__Context_init_unchained	Internal	✓	initializer
	_msgSender	Internal		
	_msgData	Internal		
CountersUpgradeable	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	
EnumerableSetUpgradeable	Library			
	_add	Private	✓	
	_remove	Private	✓	
	_contains	Private		

	_length	Private		
	_at	Private		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
ReentrancyGuardUpgradeable	Implementation	Initializable		
	__ReentrancyGuard_init	Internal	✓	initializer
	__ReentrancyGuard_init_unchained	Internal	✓	initializer
IERC165	Interface			
	supportsInterface	External		-
IERC721	Interface	IERC165		
	balanceOf	External		-
	ownerOf	External		-
	safeTransferFrom	External	✓	-
	transferFrom	External	✓	-
	approve	External	✓	-
	getApproved	External		-
	setApprovalForAll	External	✓	-
	isApprovedForAll	External		-

	safeTransferFrom	External	✓	-
IERC721Enumerable	Interface	IERC721		
	totalSupply	External		-
	tokenOfOwnerByIndex	External		-
	tokenByIndex	External		-
INFTSport	Interface	IERC721, IERC721Enumerable		
	nftToTeam	External		-
	mint	External	✓	-
TransferHelper	Library			
	safeApprove	Internal	✓	
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeTransferETH	Internal	✓	
Lottery	Implementation	IERC721ReceiverUpgradeable, OwnableUpgradeable, ReentrancyGuardUpgradeable		
	initialize	External	✓	initializer
	getStatus	Public		-
	getRoundLength	External		-
	createRound	External	Payable	onlyOwner
	updateRoundResult	External	✓	onlyOwner
	getBalance	External		-
	getDepositedBalance	External		-
	deposit	External	✓	-
	withdraw	External	✓	-
	_leaf	Internal		
	_verify	Internal		

	pendingReward	Public		-
	claimReward	External	✓	-
	onERC721Received	External	✓	-

Contract Flow



Summary

The Lottery contract implements a lottery mechanism based on NFTs contribution. This audit investifgates potential vulnerabilities, improvements and business logic concerns.

Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope’s prior written consent. This report is not nor should be considered an “endorsement” or “disapproval” of any particular project or team. This report is not nor should be regarded as an indication of the economics or value of any “product” or “asset” created by any team or project that contracts Cyberscope to perform a security assessment. This document does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors' business, business model or legal compliance. This report should not be used in any way to make decisions around investment or involvement with any particular project. This report represents an extensive assessment process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk Cyberscope’s position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies and in no way claims any guarantee of security or functionality of the technology we agree to analyze. The assessment services provided by Cyberscope are subject to dependencies and are under continuing development. You agree that your access and/or use including but not limited to any services reports and materials will be at your sole risk on an as-is where-is and as-available basis Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives false negatives and other unpredictable results. The services may access and depend upon multiple layers of third parties.

About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

The Cyberscope team

https://www.cyberscope.io