Cyberscope

Audit Report

NFTSport BetPools

November 2022

Gitlab https://gitlab.com/hola-tech1/worldcup-nft/nftsport-contracts

Commit 3735ccf93cd73bcbb8f4857db4c215bf4f4ac09b

Audited by © cyberscope

Table of Contents

Contract Review

Contract Name	BetPools
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/AccessControlUpgradeable.sol	c5f290efee7b4156f4420d9f13b2caa990176495366b4edec4d8bc229ae1cb59
@openzeppelin/contracts-upgradeable/access/OwnableUpgradeable.sol	4d148e038344167b7506ee0efd58b38f8787c6229e43800fb1129a0d4215327f
@openzeppelin/contracts-upgradeable/math/MathUpgradeable.sol	31db49b5926d6f8eff496b0f4316a7f92f9b64274f7be94aa0b949f9d9c8112d
@openzeppelin/contracts-upgradeable/math/SafeMathUpgradeable.sol	dabaab4d3d3f03e6bfb86eec1d54f31edf0429f4bfc4dff717d5776d5231c145
@openzeppelin/contracts-upgradeable/proxy/Initializable.sol	2c3a3edc2b1a4ac2c4a8645475b51f2668b1ad5ea22df074d0c0ebd3122ce2e7
@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
contracts/bets/BetPools.sol	8ce6f7af9dc8bd545f0592f434a881b7ec64743ca4f2bb1945089f4b11380158
contracts/libraries/TransferHelper.sol	bf61f5798d83a34255cdd18d52a3fd51ea3f8e3983dd9418050d0d80b997920e

Roles

The contract has two Roles. The ADMIN_ROLE role and the UPDATER_ROLE.

ADMIN ROLE has the authority to

- Create a betting pool with the corresponding bet options.
- Finalize a pool.
- Finalize a betting pool prior to the elapsed time.
- Give UPDATER_ROLE privilege.

UPDATER_ROLE has the authority to

- Create a betting pool with the corresponding bet options.
- Finalize a pool.

Users have the authority to

- Bet on any valid option with a minimum bet value of 0.1 ethers.
- Claim and view their refund balance.
- Claim and view their rewards.
- View transaction details.
- View the deposited balance on any betting option.

Contract Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	MC	Missing Check	Unresolved
	IRD	Inconsistent Reward Distribution	Unresolved
	RSA	Rewards Sufficient Amount	Unresolved
	L04	Conformance to Solidity Naming Conventions	Unresolved

MC - Missing Check

Criticality	minor / informative
Location	contract.sol#L165
Status	Unresolved

Description

The contract is processing the variables _startTime and _endTime. These variables have not been properly sanitized and checked that they form the proper shape. These variables may produce vulnerability issues.

```
function createPool(
    string memory _title,
    string memory _description,
    string memory _thumbnail,
    uint256 _startTime,
    uint256 _endTime,
    string[] memory _options
  ) external {
    //..
    pool.startTime = _startTime;
    pool.endTime = _endTime;
    //..
}
```

Recommendation

The contract should properly check the variables according to the required specifications.

- The variable _startTime should be greater than the current timestamp.
- The variable _endTime should be greater than the _startTime variable.

IRD - Inconsistent Reward Distribution

Criticality	minor / informative
Location	contracts/bets/BetPools.sol
Status	Unresolved

Description

The contract distribute the redeem amounts during the finalization step. Users that placed a bet with the same amount in the same option may not receive the same award since the initial users are excluded from the deposit. We depict the **Case 1** where user A placed the bet initially and **Case 2** where user B placed the bet initially.

Case 1

User	Option	Bet
C	1	0.11
A	2	0.11
B	2	0.11

Finalization

User	Deposit	Refund
A	0	0.11
B	0.11	0

Case 2

User	Option	Bet
C	1	0.11

B	2	0.11
A	2	0.11

Finalization

User	Deposit	Refund
B	0	0.11
A	0.11	0

Recommendation

The redeem amount should be independent to the bet order.

RSA - Rewards Sufficient Amount

Criticality	minor / informative
Location	contract.sol#L275
Status	Unresolved

Description

The contract admin has the authority to create bets with unlimited amount of options. During the reward calculation phase the deposited amount is multiplied by the number of total options. If there are many options, the contract may not have sufficient balance to cover the redeem.

```
function pendingReward(uint256 _id, address _account) public view returns
(uint256) {
if (getStatus(_id) != Status.Success || pools[_id].isClaimed[_account]) {
    return 0;
}
Pool memory pool = pools[_id];
uint256 reward =
pools[_id].options[pool.result].deposit[pool.result][_account].mul(pool.option
Count);
return reward;
}
```

Recommendation

The contract should guarantee during the finalization phase that the corresponding reward amount is sufficient to cover all the participants.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor / informative
Location	contracts/bets/BetPools.sol#L167,159,160,275,257,143,189,166,169,168,144,264,146,284,251,158,134,246,171,88,170,145,102
Status	Unresolved

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.

```
_description
_optionId
_account
_id
_title
_startTime
_thumbnail
_end
_options
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions.

Contract Functions

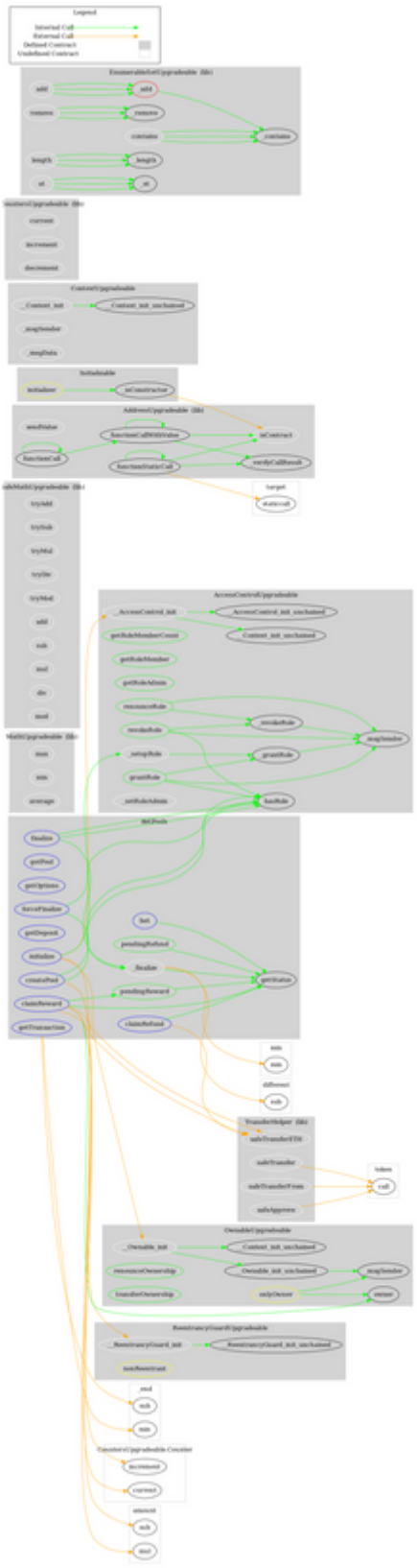
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
AccessControlUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__AccessControl_init	Internal	✓	initializer
	__AccessControl_init_unchained	Internal	✓	initializer
	hasRole	Public		-
	getRoleMemberCount	Public		-
	getRoleMember	Public		-
	getRoleAdmin	Public		-
	grantRole	Public	✓	-
	revokeRole	Public	✓	-
	renounceRole	Public	✓	-
	_setupRole	Internal	✓	
	_setRoleAdmin	Internal	✓	
	_grantRole	Private	✓	
	_revokeRole	Private	✓	
OwnableUpgradeable	Implementation	Initializable, ContextUpgradeable		
	__Ownable_init	Internal	✓	initializer
	__Ownable_init_unchained	Internal	✓	initializer
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
MathUpgradeable	Library			
	max	Internal		
	min	Internal		

	average	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		
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
BetPools	Implementation	OwnableUpgradeable, AccessControlUpgradeable, ReentrancyGuardUpgradeable		
	initialize	External	✓	initializer
	getStatus	Public		-
	getPool	External		-
	getOptions	External		-
	getTransaction	External		-
	getDeposit	External		-
	createPool	External	✓	-
	bet	External	Payable	-
	_finalize	Internal	✓	nonReentrant
	finalize	External	✓	-
	forceFinalize	External	✓	-
	pendingRefund	Public		-
	claimRefund	External	✓	-
	pendingReward	Public		-
	claimReward	External	✓	-
TransferHelper	Library			
	safeApprove	Internal	✓	
	safeTransfer	Internal	✓	
	safeTransferFrom	Internal	✓	
	safeTransferETH	Internal	✓	

Contract Flow



Summary

The BetPools contract implements a betting mechanism. This audit investigates potential vulnerabilities, improvements, and business logic concerns.

We state that admin and updater privileges are necessary and required for proper protocol operations. Thus, we emphasize the contract owner to be extra careful with the credentials.

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