Cyberscope

Audit Report

3D Coin

July 2022

SHA256 37691ee485ba22053f94d2536ed1ce6c8d6f912dd25ffaeef0a6dd33013acfea

Audited by © cyberscope

Table of Contents

Contract Review

Contract Name	NFT
Test Deploy	https://testnet.bscscan.com/address/0xE3C67be8cAc94fa28a635e3DE5BB032d2ba50352
Domain	https://www.3dhoudini.com

Audit Updates

Initial Audit	16th July 2022
Corrected	

Source Files

Filename	**SHA256**
@openzeppelin/contracts/access/Ownable.sol	9353af89436556f7ba8abb3f37a6677249aa4df6024fbfaa94f79ab2f44f3231
@openzeppelin/contracts/token/ERC1155/ERC1155.sol	3a7b1481259da24728a0bac33ac9728c0faf71d436e4f198209815f732240a24
@openzeppelin/contracts/token/ERC1155/extensions/ERC1155Burnable.sol	1093c31ab9989866598a66e0d162d63aeae7e008c9cdf2b6625f113d6e30ae2b
@openzeppelin/contracts/token/ERC1155/extensions/IERC1155MetadataURI.sol	6987fbfa647d3da51e8c270371ac48c5fcd26fb046cf54644b39aa098ae30324

@openzeppelin/contracts/token/ERC1155/IERC1155.sol	fd6a1801f1f2f8af0a3ece0b254da06ec24568aec02cfe94827061379aebc6f3
@openzeppelin/contracts/token/ERC1155/IERC1155Receiver.sol	578834a1bcdac6a22de5e07ae63bbbd4d41615f35950afc6e6c068d92619b334
@openzeppelin/contracts/utils/Address.sol	1e0922f6c0bf6b1b8b4d480dcabb691b1359195a297bde6dc5172e79f3a1f826
@openzeppelin/contracts/utils/Context.sol	1458c260d010a08e4c20a4a517882259a23a4baa0b5bd9add9fb6d6a1549814a
@openzeppelin/contracts/utils/Counters.sol	2fdcb1343e5621385b62e57b5c7775607c272122b6f2dc77da8f84828aa40cd0
@openzeppelin/contracts/utils/introspection/ERC165.sol	8806a632d7b656cadb8133ff8f2acae4405b3a64d8709d93b0fa6a216a8a6154
@openzeppelin/contracts/utils/introspection/IERC165.sol	701e025d13ec6be09ae892eb029cd83b3064325801d73654847a5fb11c58b1e5
contracts/ForeverNFT.sol	37691ee485ba22053f94d2536ed1ce6c8d6f912dd25ffaeef0a6dd33013acfea
contracts/NFT/ERC1155Holder.sol	438e432bc17f841f3dad6da813e1fc498e54a6c9667aa7697563a48f72721a60
contracts/NFT/ERC1155Receiver.sol	a8fd333c2ef4c83438a940841f4412c112815efd3a8d3be114b0c2d080c26158

Introduction

The NFT contract is an nft contract where only the owner can mint tokens. In addition, there is a fixed price for each token, but there users can only buy the NFT with id 1. Lastly, Nft investments are stored in this contract.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	BLC	Business Logic Concern
	CO	Code Optimization
	L01	Public Function could be Declared External
	L04	Conformance to Solidity Naming Conventions
	L05	Unused State Variable
	L07	Missing Events Arithmetic

BLC - Business Logic Concern

Criticality	critical
Location	contract.sol#L55

Description

The business logic seems peculiar. The implementation may not follow the expected behavior.

The user can only transfer the Nft with id 1 and the value 1.

```
function buyNft() public payable returns(address){
    require(msg.value == buyPrice, "Not enough ETH sent; check price!");
    safeTransferFrom(Contract,msg.sender, 1,1 ,"");
    return msg.sender;
}
```

Recommendation

The team is advised to carefully check if the implementation follows the expected business logic.

CO - Code Optimization

Criticality	minor
Location	contract.sol#L14

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.

This code segment can be optimized. This variable does not have a specific use in the contract so it can be removed.

```
uint256 private VoucherDiscount;
```

Recommendation

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

L01 - Public Function could be Declared External

Criticality	minor
Location	contracts/ForeverNFT.sol#L85,71,79,90,100,109,95,59,53,113

Description

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

```
currentLevel
buyNft
updateSales
setAtomic
getDefaultChoice
setSuperNova
setPlasma
setNeon
_checkDiscount
...
```

Recommendation

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

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contracts/ForeverNFT.sol#L12,16,66,59,29,31,71,15,40,77,25,48,14

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.

```
VoucherDiscount
_price
nftSale
defaultChoice
_discount
_contract
Investor
_checkDiscount
Discounted
...
```

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	contracts/ForeverNFT.sol#L31,16,15,17

Description

There are segments that contain unused state variables.

```
checkLevels
Investor
Discount
Discounted
```

Recommendation

Remove unused state variables.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contracts/ForeverNFT.sol#L66

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.

```
VoucherDiscount = _discount
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

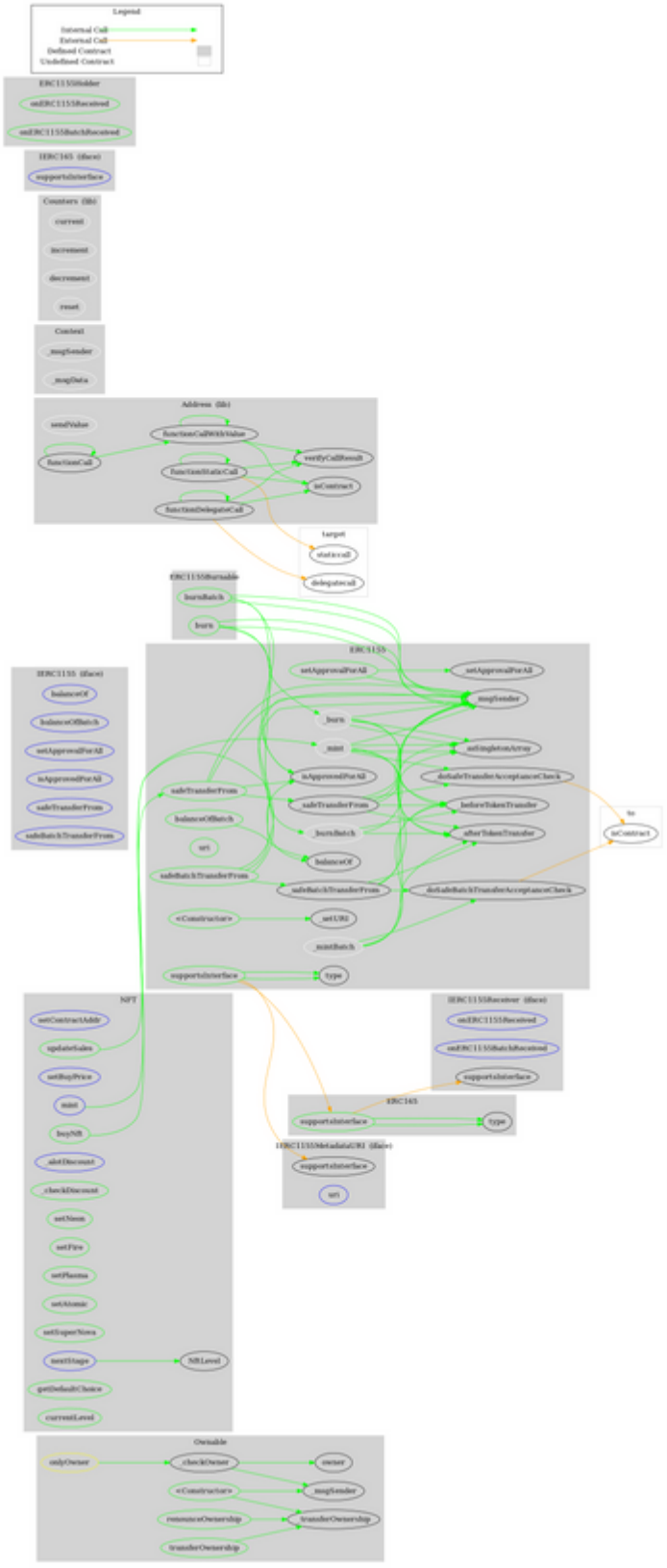
Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	_checkOwner	Internal		
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_transferOwnership	Internal	✓	
ERC1155	Implementation	Context, ERC165, IERC1155, IERC1155MetadataURI		
	<Constructor>	Public	✓	-
	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		
ERC1155Burnable	Implementation	ERC1155		
	burn	Public	✓	-
	burnBatch	Public	✓	-
IERC1155MetadataURI	Interface	IERC1155		
	uri	External		-
IERC1155	Interface	IERC165		
	balanceOf	External		-
	balanceOfBatch	External		-
	setApprovalForAll	External	✓	-
	isApprovedForAll	External		-
	safeTransferFrom	External	✓	-
	safeBatchTransferFrom	External	✓	-
IERC1155Receiver	Interface	IERC165		
	onERC1155Received	External	✓	-
	onERC1155BatchReceived	External	✓	-
Address	Library			
	isContract	Internal		
	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	

	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Counters	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	
	reset	Internal	✓	
ERC165	Implementation	IERC165		
	supportsInterface	Public		-
IERC165	Interface			
	supportsInterface	External		-
NFT	Implementation	ERC1155, Ownable, ERC1155Burnable, ERC1155Holder		
	<Constructor>	Public	Payable	ERC1155
	supportsInterface	Public		-
	setContractAddr	External	✓	onlyOwner
	mint	External	✓	onlyOwner
	setBuyPrice	External	✓	onlyOwner
	buyNft	Public	Payable	-
	updateSales	Public	✓	-
	_alotDiscount	External	✓	onlyOwner
	_checkDiscount	Public		-

	setNeon	Public	✓	-
	setFire	Public	✓	-
	setPlasma	Public	✓	-
	setAtomic	Public	✓	-
	setSuperNova	Public	✓	-
	nextStage	External	✓	onlyOwner
	getDefaultChoice	Public		-
	currentLevel	Public		-
ERC1155Holder	Implementation	ERC1155Receiver		
	onERC1155Received	Public	✓	-
	onERC1155BatchReceived	Public	✓	-
ERC1155Receiver	Implementation	ERC165, IERC1155Receiver		
	supportsInterface	Public		-

Contract Flow



Domain Info

Domain Name	3dhoudini.com
Registry Domain ID	2410837419_DOMAIN_COM-VRSN
Creation Date	2019-07-09T05:11:00.00Z
Updated Date	2022-06-07T07:52:34.00Z
Registry Expiry Date	2023-07-09T05:11:36.00Z
Registrar WHOIS Server	WHOIS.DREAMHOST.COM
Registrar URL	WWW.DREAMHOST.COM
Registrar	DREAMHOST
Registrar IANA ID	431

The domain has been created in 12 months before the creation of the audit.

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

Summary

The Smart Contract analysis reported one critical issue and no compiler error. The users can only buy NFT with id 1. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions.

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