Cyberscope

Audit Report

NFTDistributor

August 2022

Table of Contents

Contract Review

Contract Name	NFTDistributor
Test Deploy	https://testnet.bscscan.com/address/0x24D66Bd5855 10daCa4B1365da9d39E945ad413f9
Domain	https://battleworld.game

Source Files

Filename	SHA256
contract.sol	b848192e9e5a1ac25fa886c82f298d2d727751e34512f 2dcd212ef8da8b0818f

Audit Updates

Initial Audit	4th August 2022
Corrected	

Introduction

The NFTDistributor contract implements a NFT purchase mechanism. The users can deposit their tickets in order to receive NFTs. During the purchase process, the corresponding tickets are burned from the user's balance. The ratio between NFTs and tickets is defined off-chain. The in-chain method is responsible for burning the deposited amount and minting the NFTs. The users have to provide the token ids, the amounts of tokens and a message that must be verified in order to proceed with the transaction.

Request Verification

The verification process is based on an off-chain configuration. The contract owners are responsible for updating the in-chain factor in order to validate correctly the provided message.

The verification algorithm is using the markle tree mechanism.

https://github.com/protofire/zeppelin-solidity/blob/master/contracts/MerkleProof.sol

According to the markle algorithm, the off-chain mechanism pre-defines all the `index, recipient, amount` combinations.

Hence, only pre-defined users have the ability to redeem tickets in specific amounts.

Contract Roles

Role owner:

- The contract owners can pause the purchase mechanism.
- The contract owners can invalidate the validation factor and reset the saved address that mint Nfts.

Contract Diagnostics

● Critical   ● Medium   ● Informative

Severity	Code	Description
●	USB	User Sufficient Balance
●	L04	Conformance to Solidity Naming Conventions

USB - User Sufficient Balance

Criticality	informative
Location	contract.sol#L333

Description

The contract is based on the fact that the burnFrom method from the raffleTicket will revert in case that the user's balance is insufficient.

```
require(
        IRaffleTicket(RAFFLE_TICKET_ADDRESS).burnFrom(
          _msgSender(),
          rafflecount
        ),
        "NFTDistributor#claimNFT: Burning Raffle Ticket Failed"
    );
```

Recommendation

The contract could proactively check if the user's ticket balance is sufficient.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L136,134,135

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.

```
NFT_ADDRESS
RAFFLE_TICKET_ADDRESS
ClaimMerkleRoot
```

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**
MerkleProof	Library			
	verify	Internal		
	processProof	Internal		
	_efficientHash	Private		
INFT1155	Interface			
	mint	External	✓	-
	mintBatch	External	✓	-
IRaffleTicket	Interface			
	burnFrom	External	✓	-
NFTDistributor	Implementation			
	<Constructor>	Public	✓	-
	_msgSender	Internal		
	isOwner	Public		-
	paused	Public		-
	pause	External	✓	onlyOwner
	unpause	External	✓	onlyOwner
	isContract	Internal		
	setClaimMerkleRoot	External	✓	onlyOwner
	isClaimed	Public		-
	_setClaimed	Private	✓	
	claimNFT	External	✓	whenNotPaused

Contract Flow
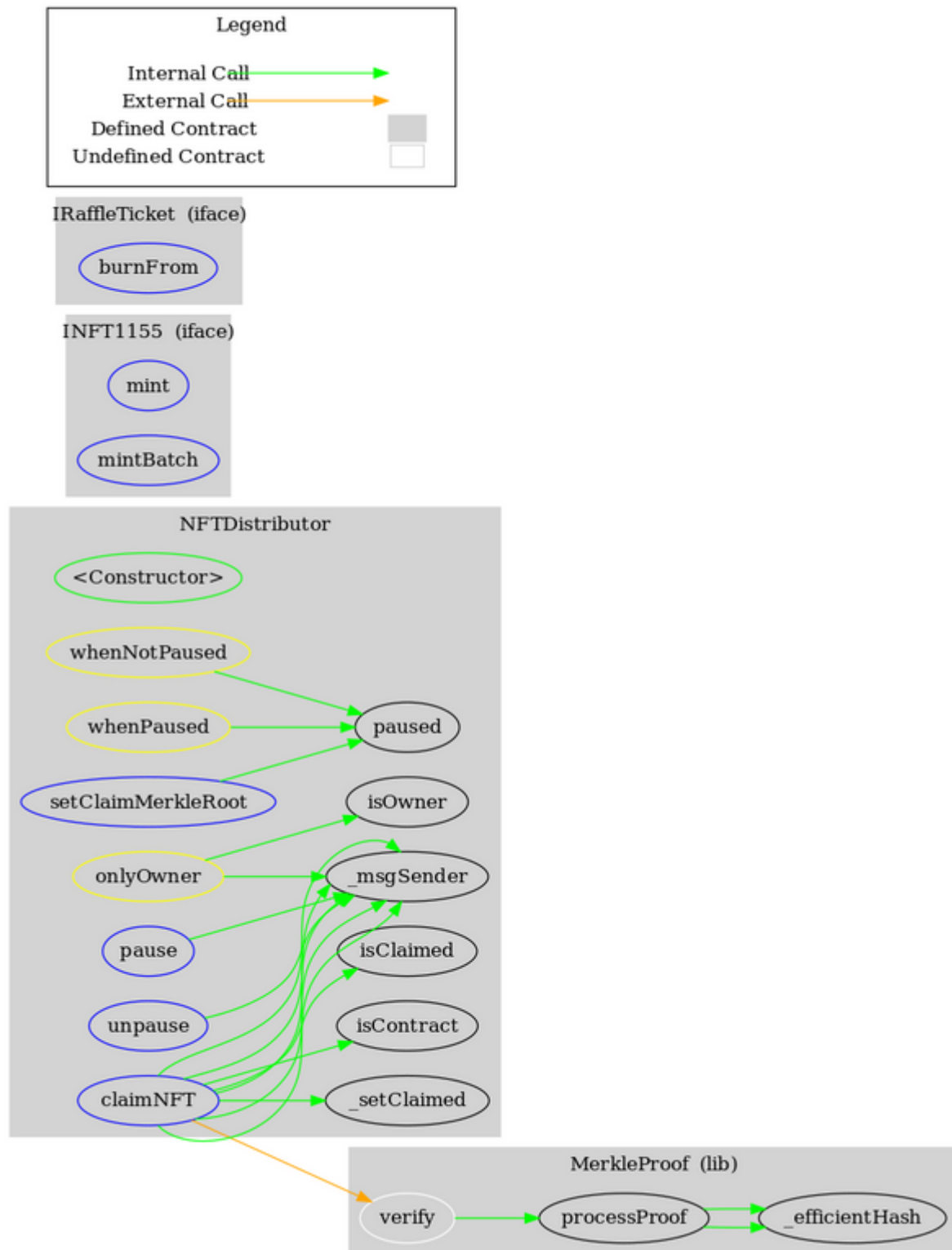
Summary

The Vault contract implements a purchase mechanism. It provides functionality to purchase Nfts by burning the corresponding tickets.The contract should thoroughly check balances before every transaction. The audit investigates the main features, mentions security recommendation, performance improvements and potential optimizations.

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