



Smart Contract Audit

Smart Contract Audit

1

About Defy Audits:

3

Project Details

4

Address

4

KYC Summary:

4

Audit Summary

5

Audit Methodology:

6

Part I: Risk Assessment

6

Summary

6

Project Overview

7

Vulnerability Assessment:

7

Part II: Concluding Remarks and Recommendations

12

Were there security vulnerabilities found?

12

Where the goals of the project met by the contract?

12

Disclaimer:

13

About Defy Audits:

We are a growing community of Solidity auditors, solidity and blockchain protocol developers who provide chain agnostic auditing services for smart contracts and DeFi applications. We perform both manual and automated testing of smart contracts. A number of open source and proprietary tools to do audits. An incomplete list of tools used in audits include the following:

- ➡ Mythx
- ➡ Slither
- ➡ Echinda Fuzzer to aid Manual testing
- ➡ Proprietary Greybox Fuzzer to aid Manual testing
- ➡ Hardhat / Python
- ➡ Rinkerby, Goril for on chain testing
- ➡ Human source code review

Project Details

| | |
|----------|---------------------|
| Platform | Binance Smart Chain |
| Version | 0.8.0 locked |
| Language | Solidity |
| Team. | PixelNFT |
| # Lines: | |

Address

 0x0a09D403D6c02A8481C343be84AC8b24709aBf98

KYC Summary:

Interview: PixelNFT is Manual Burn

The PNT used at the time of purchase are then burned manually by us, so the value of the remaining PNT tokens increases give your increase in the ecosystem back to the holder

Manual Marketing Function

The site will be promoted on all social media platforms during the project

Each sale is additionally promoted on Twitter, Telegram & Discord These pages are also advertised by third parties at cyclical intervals in order to generate even more traffic Working with social media writers to also mention the project and progress in relevant blogs

PIXEL NFT TOKEN

1.000 x 1.000 Pixel = 1.000.000 Pixel total number PNT TOKEN = 1.000.000 PNT

The more pixels are paid with PNT, the higher the value of the project token increases.

This incentive not only creates a higher reach for the NFT project but also an increase in the overall Attractiveness of the token currency.

The marketing function is also supported by the continuous increase in value of the project token another advantage achieved for the NFT project.

KYC Goals: Presale , then ICO , then Public sale

Audit Summary

Defy Finance team has performed an objective line-by-line analysis of the solidity smart contract including on-chain tests, manual analysis aided by fuzzing and static analysis. Based on evidence gathered at the time of audit completion, we can make the following risk assessment:

According to the smart contract audit:

- ❖ **PixelNFT** smart contract source code has **LOW THREAT LEVEL**.
- ❖ **PixelNFT** has **PASSED** the smart contract audit.
- ❖ **PixelNFT** has **PASSED** KYC verification.

Audit Methodology:

1. **Common vulnerabilities:** We performed a static analysis, vulnerability assessment for common vulnerabilities including *overflow, underflow, callstack depth attack, parity multis bug, timestamp dependency and re-entrancy*.

2. **Manual Review and On-chain testing:** We performed manual source code review aided by grey box fuzzing. We performed on-chain testing against common attack vectors for specific functions that have a higher attack probability based on the latest statistics we have gathered.

3. **Overall Risk Assessment:** We interviewed the team and made an overall risk assessment based on similar contracts and the intended purpose and goals of the contract.

We report analytics on critical, major and minor security vulnerabilities found and provide a holistic assessment of the overall risk of the contract. We provided a holistic risk assessment in the conclusion of this document.

Part I: Risk Assessment

Summary

Auditing Firm
Auditing Methodology

Defy Finance
Defy Finance Standard 1.0

Platform

Solidity

Audit Check (Mandatory)

Static, Manual

Request Date

March 28, 2022

Final Report Date

March 30, 2022

Project Overview

Language







Solidity



Contract

 0x55531463333C3A8B503E3839AD6a03A29A958D9

Source Code

Vulnerability Assessment:

- SWC-1 HoneyPot: Pass 
- SWC-2 Integer Underflow: Pass 
- SWC-3 Integer Overflow: Pass 
- SWC-4 Parity Multisig Bug: Pass 
- SWC-5 Callstack Depth Attack: Pass 
- SWC-6 Transaction-Ordering Dependency: Pass 

- SWC-7 Timestamp Dependency: Pass 
- SWC-8 Re-Entrancy: Pass 

Severity Risk Levels:

Critical: Issues marked critical need to be addressed immediately as they pose an immediate threat to contract security

Major: Need to be acknowledged as they could pose a medium threat to security

Minor: A theoretical or long-term risk, may not pose practical security risk

Informational: Negligible risk to security but may be

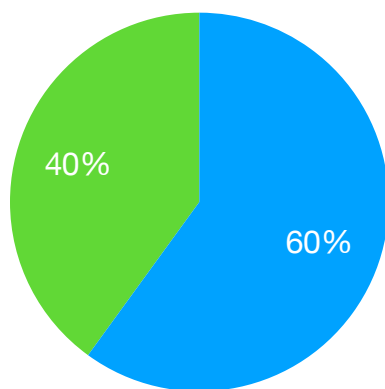
Smart Contract – Similar Contracts

| Address | Similarity Score |
|--|------------------|
| 0xd529adae263048f495a05b858c8e7c077f047813 | 0.9 |

| Address | Similarity Score |
|---|------------------|
| 0xb37f18af15bafb869a065b61fc83cf c44ed9cc27 | 0.9 |
| 0xea88c23690b9f12ac6941e8a229a a4f94c72b8db | 0.9 |

Smart Contract – Static Analysis



● Minor ● Informational ● Major
● Critical





| Function | | Line(s) affected | Severity |
|---------------------------------------|--|---|---------------|
| Deprecated code | 'throw' is deprecated in favour of 'revert()', 'require()' and 'assert()'. See line(s) 24 , 30 | Lines, 24,30 | Minor |
| Dead Code | It is recommended to remove unused or “dead” code paths. | | Minor |
| Test Coverage | Are there adequate test cases to cover business logic? | We used a generic test suite but recommend more specific test coverage. | Informational |
| Public Visibility | No visibility specified. Defaulting to 'public'. | Lines 14, 18, 22, 29 | Minor |
| Exception handling on Transfer | Calling 'send()' requires manual exception handling. Consider using 'transfer()' instead. | Lines 23 | Informational |

Smart Contract – Manual Analysis

We performed a manual code review of the following functions using fuzzing and on-chain tests to aid in vulnerability discovery. We also reviewed for gas optimizations, infinite loops that exceed block gas limits, external functions that should be internal and that each function is in line with . A pass indicates the function has passed manual inspection and is in line with intended goal(s) of the smart contract.

| Function | Description | Functions tested | Pass/Fail |
|---------------------|---|--------------------------|--|
| Total Supply | Supply of account balance of owners account | <code>tokenSupply</code> | Pass  |
| Transfer | used to transfer the tokens from the owner of the token to some other address | <code>Transfer</code> | Pass  |

| Function | Description | Functions tested | Pass/Fail |
|-----------------------|--|--|--|
| Approve | used by an address to approve the spending of a particular amount tokens by a particular address | approve | Pass  |
| _tokenTransfer | Used to send transfers to burn and marketing wallets. | treasuryAmt marketingAmt partnershipAmt exchangeAmt | Pass  |

Part II: Concluding Remarks and Recommendations

Were there security vulnerabilities found?

No critical or major issues were reported during the course of the audit. This indicates the contract meets a high standard of security and low threat risk. We only recommend some minor optimizations such as removing redundant or dead code.

Where the goals of the project met by the contract?

Additionally, there were no discrepancies found between the intended use of the contract and the implementation. We interviewed the PixelNFT team, investigated similar contracts and searched social media for additional information as part of an internal KYC process and reported no additional risk factors.

Disclaimer:

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, financial advice or legal compliance. This document should not be used in any way to make decisions around investment or involvement with any particular project.