WHITE HAT DAO

Smart Contract Audit Report

www.fragmentsnft.xyz

by - White Hat DAO
www.whitehatdao.com

Date: 29/04/2022

WHITE HAT DAO

Table of Contents

WHITE HAT DAO

Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report.

In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions.

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and White Hat DAO and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives)

White Hat DAO owes no duty of care towards you or any other person, nor does White Hat DAO make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and White Hat DAO hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report.

Except and only to the extent that it is prohibited by law, White Hat DAO hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against White Hat DAO, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on

this report. The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

This report is based on the scope of materials and documentation provided for a limited review at the time provided. Results may not be complete nor inclusive of all vulnerabilities. The review and this report are provided on an as-is, where-is, and as-available basis. You agree that your access and/or use, including but not limited to any associated services, products, protocols, platforms, content, and materials, will be at your sole risk. Blockchain technology remains under development and is subject to unknown risks and flaws. The review does not extend to the compiler layer, or any other areas beyond the programming language, or other programming aspects that could present security risks. A report does not indicate the endorsement of any particular project or team, nor guarantee its security.

No third party should rely on the reports in any way, including for the purpose of making any decisions to buy or sell a product, service or any other asset. To the fullest extent permitted by law, we disclaim all warranties, expressed or implied, in connection with this report, its content, and the related services and products and your use thereof, including, without limitation, the implied warranties of merchantability, fitness for a particular purpose, and non-infringement.

We do not warrant, endorse, guarantee, or assume responsibility for any product or service advertised or offered by a third party through the product, any open source or third-party software, code, libraries, materials, or information linked to, called by, referenced by or accessible through the report, its content, and the related services and products, any hyperlinked websites, any websites or mobile applications appearing on any advertising, and we will not be a party to or in any way be responsible for monitoring any transaction between you and any third-party providers of products or services. As with the purchase or use of a product or service through any medium or in any environment, you should use your best judgment and exercise caution where appropriate.

FOR AVOIDANCE OF DOUBT, THE REPORT, ITS CONTENT, ACCESS, AND/OR USAGE THEREOF, INCLUDING ANY ASSOCIATED SERVICES OR MATERIALS, SHALL NOT BE CONSIDERED OR RELIED UPON AS ANY FORM OF FINANCIAL, INVESTMENT, TAX, LEGAL, REGULATORY, OR OTHER ADVICE.

WHITE HAT DAO

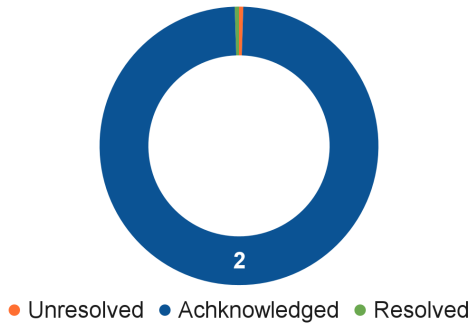
Executive Summary

White Hat DAO was contracted by "The Fragments NFTs" team to conduct a smart contract security audit. This report presents the findings of the security assessment conducted between April. 06, 2022 and April 16th, 2022. During this audit, the team manually reviewed one **(1)** smart contract and analyzed it with static analysis tools.

Based on results of the audit, the customers' smart contract safety rating is:

The White Hat DAO audit team has found 1 Informational and 1 Minor Issue. For the details of these issues please refer to the Findings section of the report.

Total Issues	2
Critical Issues	0 (0 Resolved)
Major Issues	0 (0 Resolved)
Medium Issues	0 (0 Resolved)
Minor Issues	1 Acknowledged
Informational	1 Acknowledged



WHITE HAT DAO

Summary of Findings

The most prominent audit findings were the Minor issues around the **"Use of Obsolete Function" and "Use of Insufficiently Random Values".** All issues regarding severities & vulnerabilities discovered by the audit process are listed as below:

Issue ID	Issue Title	Category	Severity	Status
FRAG-01	**Weak Source of Randomness**	Use of Insufficiently Random Values	Minor	Acknowledged
FRAG-02	**Authorization through tx.origin**	Use of Obsolete Function	informational	Acknowledged

WHITE HAT DAO

Introduction

This security audit assessment has been prepared for "Fragments NFTs". The purpose of this audit is to document and expose any safety concerns and vulnerabilities found in the source code which has been reviewed by the White Hat DAO (WHD) Audit team. This review includes any contract dependencies in scope that were not part of an officially recognized library. Comprehensive tests have been conducted, utilizing manual code review, and static analysis techniques.

The auditing process pays special attention to the following considerations:

- Testing the smart contract(s) against both common and uncommon attack vectors
- Assessing the codebase to ensure compliance with industry standards and best practices.
- Ensuring contract logic meets the specifications and intentions of the client. Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders
- Thorough line-by-line manual review of the entire codebase by industry experts
- Reviewing unit tests to ensure full coverage of the codebase provided to White Hat DAO

The Project Summary, Scope, Audit Details and Methodology of this audit is described within this document.

The security audit results can range from critical to informational. To ensure a high level of security standards, WHD recommends the client to address the findings contained in this report. The results can be found in the Findings section.

WHITE HAT DAO

Project Summary

Project	Fragments NFTs
Description	Fragments are an NFT experiment where each fragment is an on-chain generated deflationary partial cube object. The partial cubes can be combined with other NFTs to form a full cube. The system is based on the idea to leverage the ability of its participants and usage of ETH blockchain.
Website	https://fragmentsnft.xyz/
Platform	ETHEREUM
Language used	Solidity
Codebase	https://drive.google.com/file/d/1qjpV49rRqGRgP-IGlwvF-TZuQrZzG3-Y/view?usp=sharing

Project Scope

White Hat DAO was commissioned by The Fragments NFTs to perform security assessments on the smart contract listed below:

Source Code	Acknowledgement	SHA-256
CryptoartV1.sol	Accepted	3ad3640a6830cc93e9a56fe41e7bab8901033408b82abe32a110ddfb3a589c7c

WHITE HAT DAO

Audit Details

Delivery Date	29/04/2022
Received Date	06/04/2022
Key Components	CryptoartV1.sol

Methodology

The White Hat DAO Audit team reviewed the code base provided by The Fragments NFTs team between 06/04/ 2022 and 28/04/2022.

The White Hat DAO Audit team launched the audit by analyzing the specifications of the project and focusing on the key areas of interest while evaluating the documentation. The code was then manually reviewed in an attempt to identify potential vulnerabilities and verify the code has good unit tests coverage. The White Hat DAO Audit team wrote some unit cases to test some edge cases. Automated analysis of the codebase was performed and results were reviewed.

WHITE HAT DAO

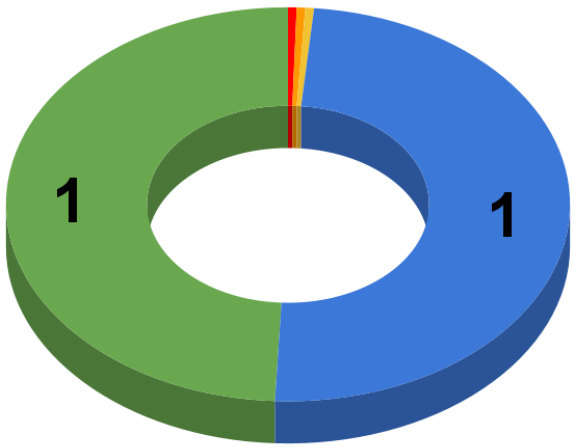
The smart contract provided by Fragment NFTs team was scanned for following list of vulnerabilities during the security assessment:

No	Vulnerability Tests	Status
# 1	Access Control	Passed
# 2	Arbitrary token minting	Passed
# 3	Business Logics Review	Passed
# 4	Centralization of power	Passed
# 5	Code clones, functionality duplication	Passed
# 6	Conditional Completion attack	Passed
# 7	Costly Loop	Passed
# 8	Ownership Takeover	Passed
# 9	Redundant fallback function	Passed
# 10	Reentrancy	Passed
# 11	Remote code execution	Passed
# 12	User Balances manipulation	Passed
# 13	Logic Flaws	Passed
# 14	Scoping and Declarations	Passed
# 15	Integer Overflow and Underflow attacks	Passed

Findings

The White Hat DAO Audit team found 1 minor and 1 informational vulnerabilities.

Vulnerabilities Found



Critical - 0 | Major - 0 | Medium Issue - 0 | Minor - 1 | Informational -1

WHITE HAT DAO

Severity Definitions

Severity	Definitions
Critical	Critical vulnerabilities have a catastrophic impact on the security of the project. They can lead to loss, data manipulation, take over, etc. It is strongly recommended to fix these vulnerabilities.
Major	Major vulnerabilities have a significant impact on the security of the project. They can lead to loss, data manipulation, take over, etc. It is strongly recommended to fix these vulnerabilities.
Medium	Medium vulnerabilities are important to fix. These vulnerabilities alone can't lead to asset loss or data manipulation. However, medium vulnerabilities can be chained to create a more severe vulnerability. It is highly recommended to review and address these vulnerabilities.
Minor	Minor vulnerabilities are mostly related to outdated, unused code snippets and don't have a significant impact on execution.
Informational	Informational vulnerabilities don't pose an immediate risk but are relevant to security best practices. They could be code-style violations and informational statements that don't affect smart contract execution. They may be able to be ignored.

Critical Vulnerabilities

No Critical severity vulnerabilities were found.

Major Vulnerabilities

No Major severity vulnerabilities were found.

Medium Vulnerabilities

No Medium severity vulnerabilities were found.

Minor Vulnerabilities

FRAG-01 | Weak Source of Randomness

Type: CWE-330: Use of Insufficiently Random Values
Level: Minor

Description: Ability to generate random numbers is very helpful in all kinds of applications. One obvious example is gambling DApps, where a pseudo-random number generator is used to pick the winner. However, creating a strong enough source of randomness in Ethereum is very challenging. For example, use of block.timestamp is insecure, as a miner can choose to provide any timestamp within a few seconds and still get his block accepted by others. Use of blockhash, block.difficulty and other fields is also insecure, as they're controlled by the miner. If the stakes are high, the miner can mine lots of blocks in a short time by renting hardware, pick the block that has required block hash for him to win, and drop all others.

Recommendation:

- Using a commitment scheme, e.g. RANDAO.
- Using external sources of randomness via oracles, e.g. Oraclize. Note that this approach requires trusting in oracle, thus it may be reasonable to use multiple oracles.
- Using Bitcoin block hashes, as they are more expensive to mine.

Informational Vulnerabilities

FRAG-02 | Authorization through tx.origin

Type: CWE-477: Use of Obsolete Function
Level: Informational

Description: **`tx.origin`** is a global variable in Solidity which returns the address of the account that sent the transaction. Using the variable for authorization could make a contract vulnerable if an authorized account calls into a malicious contract. A call could be made to the vulnerable contract that passes the authorization check since **`tx.origin`** returns the original sender of the transaction which in this case is the authorized account.

Recommendation: Leave as-is, this was flagged due to it being used for authentication most of the time. **`tx.origin`** is not being used for authentication in this instance, it's more for bot protection. This method also allows multi-sigs to be used like Gnoses due the calls coming from a contract where isContract() would limit all contracts and doesn't guarantee to stop the attacker.

WHITE HAT DAO

Conclusion

White Hat DAO worked with The Fragment NFTs team to perform this audit. One smart contract was reviewed during this audit. The smart contract was manually reviewed and analyzed with static analysis tools. The findings of these reviews are provided in this report.

No unit tests were provided. We constructed some unit tests to test edge cases. The code was commented well. Comments are helpful in understanding the overall architecture and the logic flow of the contracts.

During the audit of the smart contract provided by The Fragment NFTs team, the White Hat DAO audit team found a total of 2 vulnerabilities, which have been detailed in this report.

Change Log

- 13-04-2022 - Initial report. - JaxCoder
- 14-04-2022 - Initial report- CompositeFellow
- 15-04-2022 - Initial report- White Hat

Audited by

www.whitehatdao.com