

Report for:

Almanac NFT

April 2023

Version 1.0

Email	Telephone
info@extropy.io	+44 1865261424

Disclaimer

The audit makes no statements or warranty about utility of the code, safety of the code, suitability of the business model, regulatory regime for the business model, or any other statements about fitness of the contracts to purpose, or their bug free status. The audit documentation is for discussion purposes only

Client Confidentiality

This document contains Client Confidential information and may not be copied without written permission.

Proprietary Information

The content of this document should be considered proprietary information.

Extropy gives permission to copy this report for the purposes of disseminating information within your organisation or any regulatory agency.

Scope

The code audited is taken from repo

https://github.com/grillolepic/almanacNFT_cairo/tree/main

at commit 44ba192d5f9defb4ceaceaf799c820cb1e9090fd

Contracts in scope

BlockTimestampHashVRF.cairo

Almanac.cairo

1. Executive Summary

This is a report of an unsolicited carried out on the Almanac NFT project.

Assessment Summary

The code is generally well written, though there are some design choices which we recommend be re considered.

Issue Count

Stage	Critical	Medium	Low	Informational
Initial Report	0	2	3	1

Technical Findings

The remainder of this document is technical in nature and provides additional detail about the items already discussed, for the purposes of remediation and risk assessment.

Assumption of function call order

Risk	Medium
Affects	Almanac.cairo

There is the assumption that function 'startShuffle' will be called before function 'finishShuffle', unexpected behaviour or reverts could result if this order is not followed.

Recommendation

Redesign the logic to combine the functions to enforce the correct ordering of statements.

Random sample design

Risk	Medium
Affects	Almanac.cairo

On chain values, no matter how used are a poor choice as a source of randomness. The main concern is manipulation from a block producer. Although this is less of a problem now because of the centralisation of the sequencer, this solution would be vulnerable if the architecture changes.

Recommendation

Use a VRF oracle service instead.

TokenURI input validation

Risk	Low
Affects	Almanac.cairo

Function 'tokenURI' should check that parameter almanacd is within an expected range, to avoid overflow and unexpected behaviour.

Recommendation

Use a simpler scheme to assign unique URIs

TokenURI calculation is over complex.

Risk	Low
Affects	Almanac.cairo

The way the tokenId is implemented means that there is a limit to the number of tokens that can be minted, the function is more complex than necessary.

Recommendation

Use a simpler scheme to assign unique URIs

Unecessary calculation

Risk	Low
Affects	Almanac.cairo

Line 429 is unnecessary, since both MAX_SUPPLY and PUBLIC_SUPPLY are constant, the value could be precalculated and defined as a constant.

```
let (maxMilestoneSupply) = uint256_sub(Uint256(MAX_SUPPLY, 0),
    Uint256(PUBLIC_SUPPLY, 0));
```

Recommendation

Replace this code with a constant.

Use pausable library

Risk	Informational
Affects	Almanac.cairo

Using the pausable library could complement the use of 'assert_only_enabled'

Recommendation

Add pausable where this is more appropriate than 'assert_only_enabled'

Appendix A

Tools used

No tools were used in this audit.

Appendix B

General Audit Goals

We audit the code in accordance with the following criteria:

Sound Architecture

This audit includes assessments of the overall architecture and design choices. Given the subjective nature of these assessments, it will be up to the development team to determine whether any changes should be made.

Smart Contract Best Practices

This audit will evaluate whether the codebase follows the current established best practices for smart contract development.

Code Correctness

This audit will evaluate whether the code does what it is intended to do.

Code Quality

This audit will evaluate whether the code has been written in a way that ensures readability and maintainability.

Security

This audit will look for any exploitable security vulnerabilities, or other potential threats to the users.

Although we have commented on the application design, issues of cryptoeconomics, game theory and suitability for business purposes as they relate to this project are beyond the scope of this audit.