



Audit Report for Origin Protocol - April 28, 2021

Summary

Audit Report prepared by Solidified covering the Origin NFT Ingest smart contracts.

Process and Delivery

Three (3) independent Solidified experts performed an unbiased and isolated audit of the code in several rounds. The debrief took place on 28 April 2021.

Audited Files

The source code has been supplied in the form of a GitHub repository:

<https://github.com/OriginProtocol/nft-launchpad/tree/master/contracts/contracts/ingest>

Commit number: `e55ed6029045f73c2759562990413e9f25876f2a`

The scope of the audit was limited to the following files:

```
contracts/ingest
├─ IngestImpl.sol
├─ IngestMaster.sol
├─ IngestMasterProxy.sol
├─ IngestMidProxy.sol
└─ IngestRegistry.sol
```

Intended Behavior

The smart contracts implement a mechanism to distribute proceeds from NFT sales to the artists in secure way but operator controlled way.

Code Complexity and Test Coverage

Smart contract audits are an important step to improve the security of smart contracts and can find many issues. However, auditing complex codebases has its limits and a remaining risk is present (see disclaimer).

Users of a smart contract system should exercise caution. In order to help with the evaluation of the remaining risk, we provide a measure of the following key indicators: **code complexity**, **code readability**, **level of documentation**, and **test coverage**.

Note, that high complexity or lower test coverage does equate to a higher risk. Certain bugs are more easily detected in unit testing than a security audit and vice versa. It is, therefore, more likely that undetected issues remain if the test coverage is low or non-existent.

Criteria	Status	Comment
Code complexity	Low	-
Code readability and clarity	High	-
Level of Documentation	High	-
Test Coverage	High	-



Audit Report for Origin Protocol - April 28, 2021

Issues Found

Solidified found that the Origin NFT digest contracts contain no critical issues, no major issues, 1 minor issue, in addition to 1 informational note.

We recommend all issues are amended, while the notes are up to the team's discretion, as they refer to best practices.

Issue #	Description	Severity	Status
1	IngestImpl.sol: Use of transfer() instead of call()	Minor	Pending
2	Incorrect and inconsistent spelling of the word "implementation"	Note	-

Critical Issues

No critical issues have been found.

Major Issues

No critical issues have been found.

Minor Issues

1. `IngestImpl.sol`: Use of `transfer()` instead of `call()`

The code uses `transfer()` when sending ETH to `to/sendTo`, which only forwards 2300 gas. In cases where `sendTo` address is a smart contract whose fallback function consumes more than 2300 gas, the call will always fail. This will have the side effect of potentially preventing smart contracts (e.g. DAOs) from receiving transfers.

For a more in-depth discussion of issues with `transfer()` and smart contracts, please refer to <https://diligence.consensys.net/blog/2019/09/stop-using-soliditys-transfer-now/>

Recommendation

Replace instances of `transfer()` with `call()`.

Informational Notes

2. Incorrect and inconsistent spelling of the word “implementation”

The word implementation is misspelled in variable names in the contracts `IngestImpl.sol` and `IngestRegistry.sol`:

```
address public endpointImplimentation;
```

Recommendation

Consider fixing the spelling to improve readability.



Audit Report for Origin Protocol - April 28, 2021

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of Origin Protocol or its products. This audit does not provide a security or correctness guarantee of the audited smart contract. Securing smart contracts is a multistep process, therefore running a bug bounty program as a complement to this audit is strongly recommended.

The individual audit reports are anonymized and combined during a debrief process, in order to provide an unbiased delivery and protect the auditors of Solidified platform from legal and financial liability.

Solidified Technologies Inc.