SOLIDIFIED

Audit Report for BlockZero - May 17, 2021

Summary

Audit Report prepared by Solidified covering the Dropzero smart contracts.

Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the code in several rounds. The debrief took place on 10 May 2021.

Audited Files

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

https://github.com/BlockzeroLabs/dropzero-contracts

Commit number: `ffc659391be0667064cb1c67681cf91c4837ad28`

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

```
contracts
├── Drop.sol
├── DropFactory.sol
└── interfaces
    └── IDropFactory.sol
```

Intended Behavior

The smart contracts implement airdrop claim functionality for the Blockzero project. Airdrops for ERC-20 tokens can be registered, and users can claim them by submitting a Merkle proof.

SOLIDIFIED

Audit Report for BlockZero - May 17, 2021

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	-

Test Coverage Report

```
----------------------|----------|----------|----------|----------|----------------|
File                  |  % Stmts | % Branch |  % Funcs |  % Lines |Uncovered Lines |
----------------------|----------|----------|----------|----------|----------------|
 contracts/           |      100 |    84.38 |      100 |      100 |                |
  Drop.sol            |      100 |    83.33 |      100 |      100 |                |
  DropFactory.sol     |      100 |     87.5 |      100 |      100 |                |
 contracts/interfaces/ |      100 |      100 |      100 |      100 |                |
  IDropFactory.sol    |      100 |      100 |      100 |      100 |                |
----------------------|----------|----------|----------|----------|----------------|
All files             |      100 |    84.38 |      100 |      100 |                |
----------------------|----------|----------|----------|----------|----------------|
```

Issues Found

Solidified found that the Dropzero 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	Drop.sol: The start date of a drop can be zero	Minor	Acknowledged
2	DropFactory.sol: Constructor allows the fee to be more than 20%	Note	-

SOLIDIFIED

Audit Report for BlockZero - May 17, 2021

Critical Issues

No critical issues have been found.

Major Issues

No major issues have been found.

Minor Issues

1. Drop.sol: The start date of a drop can be zero

The start date for a drop can be set to zero in function `addDropData()`. This would allow anyone to overwrite the drop data.

Recommendation
It is recommended to check if the start date is greater than or equal to the current time.

Team Reply
This is intentional.

Informational Notes

2. DropFactory.sol: Constructor allows the fee to be more than 20%

The DropFactory contract allows the constructor to set the fee to be more than 20%, unlike the `updateFee()` method.

Recommendation
It is recommended to update the constructor to check if the fee is less than or equal to 20% for consistency.

Audit Report for BlockZero - May 17, 2021

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of BlockZero 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.