SOLIDIFIED

Audit Report for Block30 - July 23, 2021

Summary

Audit Report prepared by Solidified covering the Blocks token smart contract.

Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the code below. The final debrief took place on July 23, 2020, and the results are presented here.

Audited Files

The source code has been supplied in the form of Etherscan-verified source code:

https://etherscan.io/address/0x8a6d4c8735371ebaf8874fbd518b56edd66024eb#code

Intended Behavior

The smart contract implements a token compliant with the ERC-777 standard with the following parameters:

- Symbol: BLOCKS
- Name: BLOCKS
- Default Operators: none

The total supply of the token is minted to the deployer's account during deployment.

Findings

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 not necessarily equate to a higher risk, although certain bugs are more easily detected in unit testing than a security audit and vice versa.

Criteria	Status	Comment
Code complexity	Low	-
Code readability and clarity	High	-
Level of Documentation	High	-
Test Coverage	High	Whilst no unit tests have been provided, the codebase uses Open Zeppelin's ERC-777 implementation, which is covered by an extensive test suite.

Issues Found

Solidified found that the Paraswap contracts contain no critical issues, no major issues, no minor issues, and 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	Pragma allows for a wide range of compiler versions	Note	-

SOLIDIFIED

Audit Report for Block30 - July 23, 2021

Critical Issues

No critical issues have been found.

Major Issues

No critical issues have been found.

Minor Issues

No critical issues have been found.

Notes

1. Pragma allows for a wide range of compiler versions

The `pragma` statement allows for a wide range of compiler versions, including some versions with known bugs. In addition, the language syntax has changed since the earlier versions that are allowed.

Recommendation
Consider limiting the compiler to at least a single major version number.

Audit Report for Block30 - July 23, 2021

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of Block30 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.