SOLIDIFIED

Audit Report for B9Labs - June 25, 2021

Summary

Audit Report prepared by Solidified covering the Swap Ethereum NFT Sale smart contracts.

Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the code below. The final debrief took place on June 25, 2021, and the results are presented here.

Audited Files

The source code has been supplied in a private source code repository:

https://git.b9lab.com/client-projects/nx-project/swap-ethereum/tree/master

Commit number: `b4272c3edbc91e0585016deabae7adc130c7070f`

Intended Behavior

The smart contracts implement a swap function that allows ERC-721 tokens to be bought with ERC-20 tokens in one atomic transaction.

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	-

Issues Found

Solidified found that the NFT swap sale contracts contains no critical issue, no major issue, no minor issues, in addtion to 1 information note.

Issue #	Description	Severity	Status
1	NFTBankedSale.sol: Contract could be misused if the bank and buyer addresses are the same	Note	-

SOLIDIFIED

Audit Report for B9Labs - June 25, 2021

Critical Issues

No critical issues have been found.

Major Issues

No major issues have been found.

Minor Issues

No minor issues have been found

Informational Notes

1. `NFTBankedSale.sol`: Contract could be misused if the bank and buyer addresses are the same

The banked sale contract could be misused by setting up a sale in which the bank and buyer address are the same.

Recommendation
Consider adding a pre-condition to the constructor ensuring that `bank != buyer`.

Audit Report for B9Labs - June 25, 2021

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of B9Labs 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.