SOLIDIFIED

Audit Report for The Sandbox Multi Giveaway Contract - March 5, 2021

Summary

Audit Report prepared by Solidified covering the Sandbox multi giveaway smart contract.

Process and Delivery

Two (2) independent Solidified experts performed an unbiased and isolated audit of the code below. The debrief took place on March 5, 2021, and the results are presented here.

Audited Files

The following contracts were covered during the audit:

https://github.com/thesandboxgame/sandbox-smart-contracts/blob/audit_multi_claim_20210222/src/solc_0.7/claims/MultiGiveaway/ClaimERC1155ERC721ERC20.sol

https://github.com/thesandboxgame/sandbox-smart-contracts/blob/audit_multi_claim_20210222/src/solc_0.7/claims/MultiGiveaway/MultiGiveaway.sol

Commit number: `6c66e05d0de7d6ae25099a326eb0854408e6127f`

Intended Behavior

The audited contracts implement functionality for users to claim multiple token giveaways by providing a merkle proof for their eligibility for the giveaway.

SOLIDIFIED

Audit Report for The Sandbox Multi Giveaway Contract - March 5, 2021

Executive Summary

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	Medium	-
Code readability and clarity	High	-
Level of Documentation	Medium	-
Test Coverage	High	-

Issues Found

Solidified found no critical issues, no major issues, no minor issue. One informational note has been added.

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

Issue #	Description	Severity	Status
1	Claim processing will fail if the claim data-structures passed by a user grow too big	Note	-

Critical Issues

No critical issues have been found.

Major Issues

No major issues have been found.

Minor Issues

No minor issues have been found.

Notes

1. Claim processing will fail if the claim data-structures passed by a user grow too big

Since claims are passed as a data-structure that contains the different claims per user in arrays, the claim processing might fail due to the block gas limit if these arrays are too large. This is unlikely to be an issue in normal use cases, but care should be taken to ensure very large claims are split up in several transactions.

Recommendation
Ensure the current system is not used with very big claims. This is mainly a note for off-chain code considerations.

Audit Report for The Sandbox Multi Giveaway Contract - March 5, 2021

Disclaimer

Solidified audit is not a security warranty, investment advice, or an endorsement of TSB GAMING LTD 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.