SOLIDIFIED

Audit Report for Animoca - April 19, 2022

Summary

Audit Report prepared by Solidified covering the Tower Token Payout smart contracts.

Process and Delivery

Three (3) independent Solidified experts performed an unbiased and isolated audit of the code. The debrief was on 19 April 2021.

Audited Files

The source code has been supplied as files. The sha 256 hash of those files are:

NFTPayoutClaim.sol:
`eedbc5c68ae67d5c80c80a03507ab2740a63adcc0d775d737c77e85363773644`

PayoutClaimDistributor.sol:
`02c8eec55a2fcfa900aa3151a4f5d59a9492ce24ffd5fb9ae5d002bbc09a0669`

Intended Behavior

The smart contracts implement a payout claim functionality using merkle proofs.

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 have their 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	-	-

SOLIDIFIED

Audit Report for Animoca - April 19, 2022

Issues Found

Solidified found that the Tower Token Payout 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	PayoutClaimDistributor.sol: Consider updating solidity version	Note	

Critical Issues

No issues found

Major Issues

No issues found

Minor Issues

No issues found

Notes

1. PayoutClaimDistributor.sol: Consider updating solidity version

The contract uses the solidity compiler version less than `0.8.0`. The recent Solidity releases include several bug fixes which are missing from the version used in this contract.

```
2| pragma solidity >=0.7.6 <0.8.0;
```

Recommendation
Consider updating the compiler version to `0.8.4` or greater.

Disclaimer

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

Oak Security GmbH