# Smart contract security audit

# DIGIBLE

v.1.0

# Table of Contents

# 1.0 Introduction

## 1.1 Project engagement

During March of 2021, Digible engaged CTDSec to audit smart contracts that they created. The engagement was technical in nature and focused on identifying security flaws in the design and implementation of the contracts. Digible provided CTDSec with access to their code repository and whitepaper.

Digible is a project that aims to collect rare physical cars and NFTs.

At Digible you'll be able to buy, sell or auction your rare cards and have the option to receive them in a NFT format.

All cards will be stored safely at our DIGISAFE HQ, and you can also redeem your physical card whenever you'd like, using DIGITRACK.

## 1.2 Disclaimer

It should be noted that this audit is not an endorsement of the reliability or effectiveness of the contract, rather limited to an assessment of the logic and implementation. In order to ensure a secure contract that’s able to withstand the network’s fast-paced and rapidly changing environment, we at CTDSec recommend that Digible team put in place a bug bounty program to encourage further and active analysis of the smart contract.

# 2.0 Coverage

## 2.1 Target Code and Revision

For this audit, we performed research, investigation, and review of the Digible contract followed by issue reporting, along with mitigation and remediation instructions outlined in this report. The following code files are considered in-scope for the review:

Source:

DigiAuction.flatten.sol - 21bc54a3f9d390aecddb7997f8e6e91200bf5be11386392c71d939e613bf0e56

DigiDuel.flatten.sol - de2ea69fa6697732bc4c8813fa79cfb87af1ff3c5ad0928e10d163b7c32e5063

DigiMarket.flatten.sol - 70ef299a7a95c377de56fd6e0d0abca80c21b004e700c698f89ba9f5b61dc7fa

DigiNFT.flatten.sol - 29fafd11d6d54676ba19e7ccada52c61bb64c9ee7a1ee74933dc6439b38a9f1f

DigiNFTChild.flatten.sol - 15ad45149969795613e861bf10c30ddefb51896f2e4c01d94fdbefee71c3d6dd

DigiToken.flatten.sol - 3a12c2ba09655f45a021f174023ebc4f6e288ad5c7bed17724bf18a230faf8f5

DigiTokenChild.flatten.sol -

21d78f17bad7062be5a8c9c95d3e2912bf79dfa5a5d5c652736a21b0a516090f

## 2.2 Attacks made to the contract

In order to check for the security of the contract, we tested several attacks in order to make sure that the contract is secure and follows best practices.

| № | Issue description. | Checking status |
|---|---|---|
| 1 | Compiler warnings. | PASSED |
| 2 | Race conditions and Reentrancy. Cross-function race conditions. | PASSED |
| 3 | Possible delays in data delivery. | PASSED |
| 4 | Oracle calls. | PASSED |
| 5 | Front running. | PASSED |
| 6 | Timestamp dependence. | PASSED |
| 7 | Integer Overflow and Underflow. | PASSED |
| 8 | DoS with Revert. | PASSED |
| 9 | DoS with block gas limit. | PASSED |
| 10 | Methods execution permissions. | PASSED |
| 11 | Economy model. If application logic is based on an incorrect economic model, the application would not function correctly and participants would incur financial losses. This type of issue is most often found in bonus rewards systems, Staking and Farming contracts, Vault and Vesting contracts, etc. | PASSED |
| 12 | The impact of the exchange rate on the logic. | PASSED |
| 13 | Private user data leaks. | PASSED |
| 14 | Malicious Event log. | PASSED |
| 15 | Scoping and Declarations. | PASSED |

| | | |
|---|---|---|
| 16 | Uninitialized storage pointers. | PASSED |
| 17 | Arithmetic accuracy. | PASSED |
| 18 | Design Logic. | SOLVED BY DEV TEAM |
| 19 | Cross-function race conditions. | PASSED |
| 20 | Safe Zeppelin module. | PASSED |
| 21 | Fallback function security. | PASSED |
| 22 | Overpowered functions / Owner privileges | SOLVED BY DEV TEAM |

# 3.0 Security Issues

## 3.1 High severity issues [1]

### 1. Auction without buyers

**Issue:**

There is no function for withdrawing a token in auction, if no one participated in the auction. Also if no one participated in the auction and after its finish someone will call the claim function token will be sent to the zero address.

**Recommendation:**

Please add some function for withdrawing token from auction for token owner if auction finished without participants. Also check before claiming that someone is participating.

Fix:

Was fixed at this pull request (https://github.com/Digible/contracts/pull/1/files)

## 3.2 Medium severity issues [0]

No medium severity issues found.

## 3.3 Low severity issues [1]

### 1. Lock transfer

**Issue:**

There is a possibility of transfer in the DigiToken.flatten.sol contract even if one of the recipient or sender is locked whitelisted.

**Recommendation:**

It would be better to check that both addresses are lock whitelisted, not the only one of them.

Fix: N/A as sale it’s already done.

### Owner privileges

1. Owner can change the childChainManagerProxy address in DigiTokenChild.flatten.sol contract.
2. ChildChainManagerProxy address can mint tokens to any address using function deposit in DigiTokenChild.flatten.sol contract.
3. Owner can add and remove from the lock whitelist in DigiToken.flatten.sol contract.
4. Owner can change the childChainManagerProxy address in DigiTokenNFTChild.flatten.sol contract.
5. ChildChainManagerProxy address can mint tokens to any address using function deposit in DigiTokenNFTChild.flatten.sol contract.
6. Owner can change the purchase fee in DigiMarket.flatten.sol contract up to 100 percent.
7. Owner can change the fee in DigiDuel.flatten.sol contract up to 100 percent.
8. Owner can change the fee in DigiAuction.flatten.sol contract up to 100 percent.

Fix:

1. Solved by the dev team.
2. It is a function inherited from the Matic network so it cannot be modified directly from Digi. There is no possible solution as it is a dependency on the network.
3. N/A.
4. Solved by the dev team.
5. Same as point 2.
6. Dev team added a limit to max 30%.
7. Same as point 6.
8. Same as point 6.

# 4.0 Summary of the audit

Critical incidents have been solved, the MINT function named in the report has no danger since the DIGI team does not have access to its execution, it is only possible that it be executed from MATIC.