Report Template

**Audit Firm:**

**Client Firm:**

**Prepared By:**

**Delivery Date:** October 9th, 2023

**Protocol Name** engaged **Firm Name** to review the security of its Smart Contract system. From **Begining date** to **Ending date**, a team of **X** auditors reviewed the source code in scope. All findings have been recorded in the following report.

Notice that the examined smart contracts are not resistant to external/internal exploit. For a detailed understanding of risk severity, source code vulnerability, and potential attack vectors, refer to the complete audit report below.

# Project Overview

| **Project Name** | **Project Name** |
| --- | --- |
| Language | Solidity |
| Codebase | <https://github.com/___> |
| Commit | [\_\_\_\_\_](https://github.com/___) |

| **Delivery Date** | **\_\_\_\_** |
| --- | --- |
| Audit Methodology | Static Analysis, Manual Review |

| **Vulnerability Level** | **Total** | **Pending** | **Declined** | **Acknowledged** | **Partially Resolved** | **Resolved** |
| --- | --- | --- | --- | --- | --- | --- |
| [Critical](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#Critical) | 0 | 0 | 0 | 0 | 0 | 0 |
| [High](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#High) | 0 | 0 | 0 | 0 | 0 | 0 |
| [Medium](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#Medium) | 0 | 0 | 0 | 0 | 0 | 0 |
| [Low](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#Low) | 0 | 0 | 0 | 0 | 0 | 0 |

# Audit Scope & Methodology

## Scope

| **ID** | **File** | **SHA-1 Hash** |
| --- | --- | --- |
| DPT | contracts/DividendPayingToken.sol | 4bf3ea9b168bbd1bd61d8ae8583145b342b867ba |
| TOK | contracts/Token.sol | 4bf3ea9b168bbd1bd61d8ae8583145b342b867ba |
| PRE | contracts/Presale.sol | 4bf3ea9b168bbd1bd61d8ae8583145b342b867ba |
| AIR | contracts/Airdropper.sol | 4bf3ea9b168bbd1bd61d8ae8583145b342b867ba |

## Methodology

The auditing process pays special attention to the following considerations:

* Testing the smart contracts against both common and uncommon attack vectors.
* Assessing the codebase to ensure compliance with current best practices and industry standards.
* Ensuring contract logic meets the specifications and intentions of the client.
* Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
* Thorough line-by-line manual review of the entire codebase by community auditors.

## Vulnerability Classifications

| **Vulnerability Level** | **Classification** |
| --- | --- |
| [Critical](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#Critical) | Easily exploitable by anyone, causing causing loss of assets or undermining of the protocol’s goals. |
| [High](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#High) | Arduously exploitable by a subset of addresses, causing loss of assets or undermining of the protocol’s goals. |
| [Medium](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#Medium) | Inherent risk of future exploits that may or may not impact the smart contract execution. |
| [Low](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#Low) | Minor deviation from best practices. |

# Invariants Assessed

During the course of the review, the following invariants were assesed and verified with X fuzzing runs:

* Invariant 1
* Invariant 2
* Invariant 3
* Invariant 4 (Optional)
* Invariant 5 (Optional)

# Findings & Resolutions

| **ID** | **Title** | **Category** | **Severity** | **Status** |
| --- | --- | --- | --- | --- |
| [H-01](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#H01) | A DOS can happen on XXXXXXX | DOS | HIGH | Pending |
| [H-02](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#H02) | Lack of access controls | Access Controls | HIGH | Pending |
| [M-01](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#M01) | Inherent risk of future exploits that may or may not impact the smart contract execution. | Token integration | MEDIUM | Pending |
| [M-02](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#M02) | Minor deviation from best practices. | Logic error | MEDIUM | Pending |
| [L-01](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#L01) | Low error 01 | Centralization risk | LOW | Pending |
| [L-02](https://hackmd.io/Gk0D1DoBQDKnjtcUgCBSJg#L02) | Low error 02 | Validation | LOW | Pending |

## Critical

### C-01 Title issue

<https://github.com/___/Contract.sol#L146-L160>

#### PoC:

#### Description:

#### Recommendation:

#### Resolution:

## High

### H-01 Title issue

<https://github.com/___/Contract.sol#L146-L160>

#### PoC:

#### Description:

#### Recommendation:

#### Resolution:

### H-02 Title issue

<https://github.com/___/Contract.sol#L146-L160>

#### PoC:

#### Description:

#### Recommendation:

#### Resolution:

## Medium

### M-01 Title issue

<https://github.com/___/Contract.sol#L146-L160>

#### Description:

#### Recommendation:

#### Resolution:

## Low

### L-01 Title issue

<https://github.com/___/Contract.sol#L146-L160>

#### Description:

#### Recommendation:

#### Resolution:

## Disclaimer

This report is not, nor should be considered, an “endorsement” or “disapproval” of any particular project or team. This report is not, nor should be considered, an indication of the economics or value of any “product” or “asset” created by any team or project that contracts the firm to perform a security assessment. This report does not provide any warranty or guarantee regarding the absolute bug-free nature of the technology analyzed, nor do they provide any indication of the technologies proprietors, business, business model or legal compliance.

This report should not be used in any way to make decisions around investment or involvement with any particular project. This report in no way provides investment advice, nor should be leveraged as investment advice of any sort. This report represents an extensive assessing process intending to help our customers increase the quality of their code while reducing the high level of risk presented by cryptographic tokens and blockchain technology.

Blockchain technology and cryptographic assets present a high level of ongoing risk. The firm’s position is that each company and individual are responsible for their own due diligence and continuous security. The firm’s goal is to help reduce the attack vectors and the high level of variance associated with utilizing new and consistently changing technologies, and in no way claims any guarantee of security or functionality of the technology we agree to analyze.

The assessment services provided by the firm is subject to dependencies and under continuing  
development. You agree that your access and/or use, including but not limited to any services, reports, and materials, will be at your sole risk on an as-is, where-is, and as-available basis. Cryptographic tokens are emergent technologies and carry with them high levels of technical risk and uncertainty. The assessment reports could include false positives, false negatives, and other unpredictable results. The services may access, and depend upon, multiple layers of third-parties.

Notice that smart contracts deployed on the blockchain are not resistant from internal/external exploit. Notice that active smart contract owner privileges constitute an elevated impact to any smart contract’s safety and security. Therefore, the firm does not guarantee the explicit security of the audited smart contract, regardless of the verdict.