Cyberscope

# Audit Report

# ODIN Coin

April 2024

| | |
|---|---|
| Network | Stacks |
| Identifier | SP2X2Z28NXZVJFCJPBR9Q3NBVYBK3GPX8PXA3R83C.odin-tkn |
| Audited by | © cyberscope |

# Table of Contents

# Review

| | |
|---|---|
| **Explorer** | https://explorer.hiro.so/txid/0x9c94af247bb9f433011bf2ef94ac62db85078e39dde77294365016220a630b18?chain=mainnet |
| **Contract Identifier** | SP2X2Z28NXZVJFCJPBR9Q3NBVYBK3GPX8PXA3R83C.odin-tkn |
| **Network** | Stacks |
| **Symbol** | ODIN |
| **Decimals** | 6 |
| **Total Supply** | 21,000,000,000 |

## Audit Updates

| | |
|---|---|
| **Initial Audit** | 17 Apr 2024 |

## Source Files

| | |
|---|---|
| **Filename** | SHA256 |
| **odin-tkn.clar** | 13e53929de9d491193655acd1f7a475e16fb72c0025fc40faf8d8f18a58406ef |

# Overview

The Odin Token contract, deployed on the Stacks blockchain, is developed using the Clarity smart contract language, adhering to the SIP-010 standard for fungible tokens. This contract introduces a fungible token named `Odin` and includes functionalities typical of a standard token implementation such as token transfer, balance checks, and total supply management.

**Token Definition and Management**

The contract declares a fungible token `odin` and provides functions to manage its lifecycle. These include minting the initial supply, transferring tokens between accounts, and querying balances and total supply.

**Metadata Management**

The contract incorporates a feature to manage metadata through a URI, initially set to point to a JSON file hosted off-chain. This URI can be updated by the contract creator, with changes logged via custom print statements, enhancing traceability for changes to the token's metadata.

**Access Control**

Functions critical to the security and integrity of the token, such as updating the token URI, are safeguarded with access controls ensuring that only the contract creator can execute these operations.

**Transfer Functionality**

The contract includes a transfer function that allows token holders to transfer their tokens to another account. This function includes checks to ensure that transfers are authorized by the token holder.

**Batch Operations**

A `send-many` function facilitates the transfer of tokens to multiple recipients in a single transaction, which is particularly useful for distributions. This function leverages the basic transfer functionality.

# Findings Breakdown


| | |
|---|---|
| Critical | 0 |
| Medium | 0 |
| Minor / Informative | 2 |

| Severity | Unresolved | Acknowledged | Resolved | Other |
|---|---|---|---|---|
| Critical | 0 | 0 | 0 | 0 |
| Medium | 0 | 0 | 0 | 0 |
| Minor / Informative | 1 | 0 | 1 | 0 |

# Diagnostics

Critical Medium Minor / Informative

| Severity | Code | Description | Status |
|---|---|---|---|
| ● | ITA | Initial Token Allocation | Resolved |
| ● | MMCR | Metadata Mutation Centralization Risk | Unresolved |

## ITA - Initial Token Allocation

| | |
|---|---|
| **Criticality** | Minor / Informative |
| **Location** | odin-tkn.clar#81 |
| **Status** | Resolved |

### Description

During the deployment of the contract, the account `SP2X2Z28NXZVJFCJPBR9Q3NBVYBK3GPX8PXA3R83C` acquires the entire token supply of the token. This concentration of 100% of the token supply in some addresses raises significant concerns about centralization within the token's ecosystem. Such a scenario creates a risk of market manipulation and could lead to other adverse effects, potentially undermining the token's decentralized nature and the overall health of its ecosystem.

```
(begin
  (try! (ft-mint? odin u21000000000000000 contract-creator))
)
```

### Recommendation

It is recommended to distribute the tokens more broadly to achieve a more decentralized token holding structure. This can mitigate the risks associated with centralization and ensure a more stable and secure ecosystem for all participants. If the new addresses consist of a team's wallet address, then the team should carefully manage the private keys of those accounts. We strongly recommend implementing a robust security mechanism to prevent a single user from accessing the contract admin functions, such as a multi-sign wallet so that many addresses will confirm the action.

# MMCR - Metadata Mutation Centralization Risk

| | |
|---|---|
| **Criticality** | Minor / Informative |
| **Location** | odin-tkn.clar#38 |
| **Status** | Unresolved |

## Description

The contract configuration grants the contract creator exclusive control over the token-uri variable. This allows for modifications to the URI that directs users to the token's metadata. The fact that the contract creator has the authority to modify the metadata URI, leaves the token vulnerable to potential risks, as the designated address retains the capability to make changes to the metadata. This could lead to unauthorized or malicious modifications that might compromise the integrity and intended functionality of the token.

```
(define-public (set-token-uri (value (string-utf8 256)))
    (begin
        (asserts! (is-eq tx-sender contract-creator) ERR-UNAUTHORIZED)
        (var-set token-uri (some value))
        (ok (print {
              notification: "token-metadata-update",
              payload: {
                contract-id: (as-contract tx-sender),
                token-class: "ft"
              }
            })
        )
    )
)
```

## Recommendation

To address this finding and mitigate centralization risks, it is recommended to evaluate the feasibility of migrating critical configurations and functionality into the contract's codebase itself. This approach would reduce external dependencies and enhance the contract's self-sufficiency. It is essential to carefully weigh the trade-offs between external configuration flexibility and the risks associated with centralization.

# Functions Analysis

| Contract | Type | Bases | | |
|---|---|---|---|---|
| | **Function Name** | **Visibility** | **Mutability** | **Modifiers** |
| | | | | |
| **odin-tkn** | Implementation | | | |
| | | | | |
| | transfer | Public | ✓ | tx-sender |
| | get-name | Public | | - |
| | get-symbol | Public | | - |
| | get-decimals | Public | | - |
| | get-balance | Public | | - |
| | get-total-supply | Public | | - |
| | set-token-uri | Public | ✓ | contract-creator |
| | get-token-uri | Public | | - |
| | send-many | Public | ✓ | - |
| | check-err | Private | ✓ | - |
| | send-token | Private | ✓ | - |
| | send-token-with-memo | Private | ✓ | - |

# Summary

ODIN Coin implements a token mechanism on the Stacks Blockchain. This audit investigates security issues, business logic concerns and potential improvements.

# Disclaimer

The information provided in this report does not constitute investment, financial or trading advice and you should not treat any of the document's content as such. This report may not be transmitted, disclosed, referred to or relied upon by any person for any purposes nor may copies be delivered to any other person other than the Company without Cyberscope's prior written consent. 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 regarded as an indication of the economics or value of any "product" or "asset" created by any team or project that contracts Cyberscope to perform a security assessment. This document 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 represents an extensive assessment 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 Cyberscope's position is that each company and individual are responsible for their own due diligence and continuous security Cyberscope'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 Cyberscope are subject to dependencies and are 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.

# About Cyberscope

Cyberscope is a blockchain cybersecurity company that was founded with the vision to make web3.0 a safer place for investors and developers. Since its launch, it has worked with thousands of projects and is estimated to have secured tens of millions of investors' funds.

Cyberscope is one of the leading smart contract audit firms in the crypto space and has built a high-profile network of clients and partners.

**The Cyberscope team**

https://www.cyberscope.io