Cyberscope

# Audit Report

# SOEX

February 2025

| | |
|---|---|
| Network | TON |
| Address | EQCPrad8ocDulp4bAbGbxdA7BWdWE2Gs4OiAL7Yrrtu6BQMI |
| Audited by | © cyberscope |

# Analysis

● Critical ● Medium ● Minor / Informative ● Pass

| Severity | Code | Description | Status |
|---|---|---|---|
| ● | ST | Stops Transactions | Passed |
| ● | OTUT | Transfers User's Tokens | Passed |
| ● | ELFM | Exceeds Fees Limit | Passed |
| ● | MT | Mints Tokens | Passed |
| ● | BT | Burns Tokens | Passed |
| ● | BC | Blacklists Addresses | Passed |

# Table of Contents

# Risk Classification

The criticality of findings in Cyberscope's smart contract audits is determined by evaluating multiple variables. The two primary variables are:

1. **Likelihood of Exploitation**: This considers how easily an attack can be executed, including the economic feasibility for an attacker.
2. **Impact of Exploitation**: This assesses the potential consequences of an attack, particularly in terms of the loss of funds or disruption to the contract's functionality.

Based on these variables, findings are categorized into the following severity levels:

1. **Critical**: Indicates a vulnerability that is both highly likely to be exploited and can result in significant fund loss or severe disruption. Immediate action is required to address these issues.
2. **Medium**: Refers to vulnerabilities that are either less likely to be exploited or would have a moderate impact if exploited. These issues should be addressed in due course to ensure overall contract security.
3. **Minor**: Involves vulnerabilities that are unlikely to be exploited and would have a minor impact. These findings should still be considered for resolution to maintain best practices in security.
4. **Informative**: Points out potential improvements or informational notes that do not pose an immediate risk. Addressing these can enhance the overall quality and robustness of the contract.

| Severity | Likelihood / Impact of Exploitation |
|---|---|
| ● Critical | Highly Likely / High Impact |
| ● Medium | Less Likely / High Impact or Highly Likely/ Lower Impact |
| ● Minor / Informative | Unlikely / Low to no Impact |

# Review

| | |
|---|---|
| **Explorer** | https://tonscan.org/jetton/EQCPrad8ocDuIp4bAbGbxdA7BWdWE2Gs4OiAL7Yrrtu6BQMI |
| **Address** | EQCPrad8ocDuIp4bAbGbxdA7BWdWE2Gs4OiAL7Yrrtu6BQMI |
| **Network** | TON |
| **Name** | SOEX |
| **Symbol** | SOEX |
| **Decimals** | 9 |
| **Total Supply** | 800,000,000 |

## Audit Updates

| | |
|---|---|
| **Initial Audit** | 27 Feb 2025 |

## Source Files

| **Filename** | SHA256 |
|---|---|
| **jetton-minter.fc** | b93612f1f3e3d321e9695f103b1e697e97f5ba5e2da9e519987904fd667fe7ef |
| **jetton-wallet.fc** | c05aaea9eb93b705625e94d6568d64ca0499d012eb384e316e025727590c2ff3 |

# Overview

## Minter

This smart contract is a discoverable Jetton contract designed for the TON (The Open Network) blockchain. It manages the SOEX token, which is a fungible token with various functionalities essential for token operations. The contract maintains key pieces of information in its storage, including the total supply of the token, the admin address (Owner), the Jetton wallet code, and additional content related to the token.

The contract allows for minting new tokens, which can only be initiated by the owner. This process involves calculating the Jetton wallet state, determining the recipient's wallet address, and sending the minted tokens accordingly. The owner also has the authority to change the content associated with the token and can also transfer owner rights to another address.

After the initial audit, the ownership has been renounced, rendering the contract immutable and preventing any further administrative changes.

The contract supports burning tokens through a notification mechanism, which adjusts the total supply accordingly. It also includes functionality to provide wallet addresses on request, ensuring that users can retrieve their token wallet addresses when needed.

Furthermore, the contract includes a method to retrieve essential data about the token, such as the total supply, admin address (Owner), Jetton content, and wallet code. This provides a comprehensive overview of the token's current state for users and potential investors. The contract is implemented using the FunC programming language and adheres to the TON blockchain standards, ensuring compatibility and discoverability within the network.

## Wallet

The Jetton Wallet Contract is a core component of the Jetton Token system on the TON blockchain. Each wallet contract is linked to a specific Jetton Minter contract. The contract maintains the following information in the storage: Jetton balance of the owner, the owner's address, the Jetton Master contract address, and the Jetton wallet code.

The Jetton Wallet supports receiving, sending, and burning Jettons. Transfers are initiated by the wallet owner and involve the calculation of the recipient's Jetton Wallet address before executing the transfer. Only the wallet owner is able to transfer their Jettons and the wallet enforces balance checks before processing transactions. The contract also supports the burning of the owner's tokens. After the burn, the Jetton Minter updates the total supply of the token.

The contract includes a fail-safe mechanism for handling bounced transactions. If a transfer fails, the Jettons are returned to the sender's balance, preventing accidental loss of tokens. The contract also has methods to retrieve the Jetton balance, the owner's address and the associated Jetton Minter contract.

The Jetton Wallet contract supports the Minter, trying to achieve compatibility, security, and efficiency in token transactions within the TON network.

# Metadata

The metadata for the SOEX token on the TON blockchain provides essential details about this digital asset, facilitating its integration and operation within the TON ecosystem. The metadata includes crucial information that defines the token's characteristics and ensures its seamless functionality across the network. The metadata reveals that the token has the name "SOEX" and is represented by the symbol "SOEX." It is associated with the hosted image. The token uses 9 decimal places, ensuring precise handling of fractional token amounts.

The detailed metadata structure provides an overview of the SOEX token's key features and its operational framework within the TON blockchain, as they benefit users and investors by offering more comprehensive insights into the token's purpose and value.

```
{
 "address": "0:8fada77ca1c0ee229e1b01b19bc5d03b0567561361ace0e8802fb62baedbba05",
 "name": "SOEX",
 "symbol": "SOEX",
 "decimals": "9",
 "image": "https://static.shelterofexiles.com/soex-square_256.png",
 "description": "SOEX is utility token powering Shelter of Exiles gaming ecosystem"
}
```

# Findings Breakdown

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

# MA - Mint Authority

| | |
|---|---|
| **Criticality** | Passed |
| **Location** | jetton-minter.fc#L70 |
| **Status** | Resolved |

## Description

The contract Owner has the authority to mint tokens at their discretion, allowing them to create new tokens at any time without restriction. This centralizes control over the token supply, as the Owner can increase the total supply at will. Such a design underscores the importance of trust in the owner's actions and transparency in their decision-making, as these actions can directly influence the token's scarcity, value, and overall ecosystem.

The contract has renounced the ownership so it no longer has an assigned owner and consequently, the owner's privileges and authority are revoked. As a result, the owner is unable to execute any methods that are designated exclusively for owner access.

```
if (op == op::mint()) {
    throw_unless(73, equal_slices(sender_address,
admin_address));
    slice to_address = in_msg_body~load_msg_addr();
    int amount = in_msg_body~load_coins();
    cell master_msg = in_msg_body~load_ref();
    slice master_msg_cs = master_msg.begin_parse();
    master_msg_cs~skip_bits(32 + 64); ;; op + query_id
    int jetton_amount = master_msg_cs~load_coins();
    mint_tokens(to_address, jetton_wallet_code, amount,
master_msg);
    save_data(total_supply + jetton_amount, admin_address,
content, jetton_wallet_code);
    return ();
}
```

## UA - Update Authority

| | |
|---|---|
| **Criticality** | Passed |
| **Location** | jetton-minter.fc#L138 |
| **Status** | Resolved |

### Description

The contract includes functionality that allows the Owner to modify the content or metadata of tokens at their discretion. This provides centralized control over token properties. This feature introduces the risk of misuse changes that may undermine trust in the token's integrity or utility.

The contract has renounced the ownership so it no longer has an assigned owner and consequently, the owner's privileges and authority are revoked. As a result, the owner is unable to execute any methods that are designated exclusively for owner access.

```
if (op == 4) { ;; change content, delete this for immutable
tokens
    throw_unless(73, equal_slices(sender_address,
admin_address));
    save_data(total_supply, admin_address,
in_msg_body~load_ref(), jetton_wallet_code);
    return ();
}
```

# Summary

The SOEX token and wallet that is built for the TON network, leverages a solid architecture. This audit rigorously evaluates its performance, security, and compliance with best practices. The investigation aims to identify and address any operational vulnerabilities, performance bottlenecks, and areas for optimization, ensuring the token's robustness and reliability in the TON ecosystem.

The contract has renounced the ownership so it no longer has an assigned owner and consequently, the owner's privileges and authority are revoked. As a result, the owner is unable to execute any methods that are designated exclusively for owner access. By relinquishing ownership, the contract eliminates the potential risks associated with centralized authority, reducing the possibility of the owner misusing their privileges or becoming a single point of failure. It is important to note that renouncing ownership is an irreversible action, and once executed, it cannot be undone.

The ownership has been renounced on this transaction:

https://tonscan.org/tx/6a920f14eddbdd9654eee88c8fa9ef10560ea89609fe4076f970d8133700087b

# 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**

cyberscope.io