BlockAudit Ai

Self Token Smart Contract

Audit Report

June, 2023

For

SELFKEY

Table of contents

1. Executive Summary

The audited contract "SelfToken'' is an ERC20 compliant token smart contract implemented on the Ethereum blockchain. The contract leverages upgradable and owner-controlled features using OpenZeppelin's upgradable and ownable contracts. The token does not have a maximum supply limit and can be paused by the owner.

2. Techniques and Methods

The audit was conducted using a combination of automated tools and manual code review. The automated tools used include Slither, Mythril, and the Solidity compiler for detecting low-level vulnerabilities. The manual code review aimed to identify architectural and logic issues.

3. Checked Vulnerabilities

The following vulnerabilities were checked:

- [x] Overflow and Underflow
- [x] Re-entrancy
- [x] Timestamp Dependence
- [x] Access Controls
- [x] Contract Upgradability
- [x] Contract Pausing

4. Issues List

No High/Mid severity issues were detected.

Low Severity

1. Unbounded Token Supply

The contract does not implement a maximum supply. Unbounded minting capabilities could lead to inflationary risks.

SelfKey comment:

The contract is owned by a multi-signature contract, which acts on behalf of the SelfKey DAO based on votes managed on our dedicated Snapshot page, thus the risk is mitigated.

5. Notes List

1. Upgradability

The contract leverages OpenZeppelin's upgradable contracts. Upgradable contracts provide the ability to fix bugs or enhance features post-deployment. However, they also introduce a level of centralization and potential for misuse, as someone with upgrade control could modify the contract for malicious intent.

SelfKey comment:

The contract is owned by a multi-signature contract, which acts on behalf of the SelfKey DAO based on votes managed on our dedicated Snapshot page, thus the risk is mitigated.

2. Owner-Only Functions

The `pause`, `unpause`, `mint` and `setAuthorizationContract` functions can only be called by the owner. This presents centralization risks as the owner has control over the contract's essential operations.

SelfKey comment:

The contract is owned by a multi-signature contract, which acts on behalf of the SelfKey DAO based on votes managed on our dedicated Snapshot page, thus the risk is mitigated.

3. No Maximum Supply

The token does not implement a maximum supply. While this could be desired depending on the use case, it also opens up potential risks of hyperinflation if not managed properly.

SelfKey comment:

The contract is owned by a multi-signature contract, which acts on behalf of the SelfKey DAO based on votes managed on our dedicated Snapshot page, thus the risk is mitigated.

4. No Rate Limiting

The contract does not incorporate rate limiting. This could open potential avenues for abuse if not properly monitored.

SelfKey comment:

The contract is owned by a multi-signature contract, which acts on behalf of the SelfKey DAO based on votes managed on our dedicated Snapshot page, thus the risk is mitigated.

6. Closing Summary

The "SelfToken" contract is well-written and adheres to many established best practices in Solidity programming. No major security issues were identified, and only minor potential concerns were noted. It is recommended to continue monitoring and ensuring good practices in contract governance, especially considering the contract's upgradeable and owner-controlled features.

7. Disclaimer

This audit is provided for informational purposes only and is based on the understanding of the contract's intended functionality at the time of the audit. It does not provide any guarantees, implied or otherwise, about the contract's reliability or security. Use at your own risk.

BlockAudit Ai

BlockAudit Ai is a secure smart contracts audit platform designed by BlockAudit Ai Technologies.

We are a team of dedicated blockchain security experts and smart contract auditors, powered by AI, determined to ensure that Smart Contract-based Web3 projects can avail the latest and best security solutions to operate in a trustworthy and risk-free ecosystem.

Request An Audit