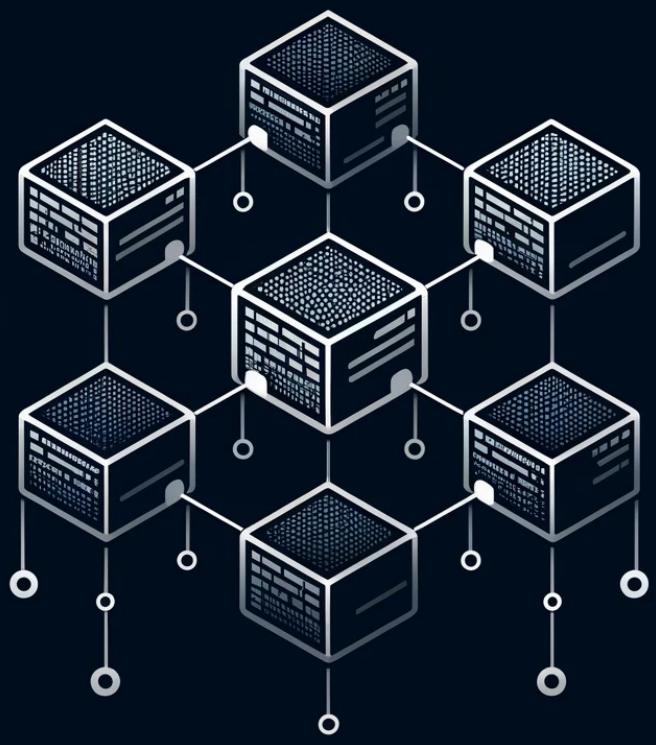
TOKENLABS NETWORK

TokenLabs Audits

ERC-20 Smart Contract Integrity and Security Evaluation

Audit Report



Token Name: Kekius Maximus

Date: January 11, 2025

ERC-20 Token Audit Disclaimer

This document provides an audit of the listed ERC-20 tokens, conducted with the purpose of identifying potential vulnerabilities in the code and assessing the overall security of the smart contracts involved. The audit has been performed by professionals experienced in blockchain security and smart contract programming.

Audit Limitations:

Limited Scope: The audit is based solely on the source code provided by the client and is limited to the evaluation of security and functionality as per the criteria established in the scope of work. It does not guarantee that all potential vulnerabilities have been identified.

Environment Dependency: The results of the audit are applicable only within the context of the environment and conditions under which the assessment was conducted. Changes in the operating environment or interactions with other contracts may alter the outcomes.

Not an Endorsement: This audit does not constitute an endorsement of the total security of the smart contract nor should it be interpreted as a guarantee of invulnerability to attacks or failures. Investors and users are advised to conduct their own due diligence before engaging with the audited tokens.

Code Updates: Any modifications to the code after the date of this audit will be invalid.

ERC-20 Token Audit Disclaimer

This document provides an audit of the listed ERC-20 tokens, conducted with the purpose of identifying potential vulnerabilities in the code and assessing the overall security of the smart contracts involved. The audit has been performed by professionals experienced in blockchain security and smart contract programming.

Audit Limitations:

1. **Limited Scope:** The audit is based solely on the source code provided by the client and is limited to the evaluation of security and functionality as per the criteria established in the scope of work. It does not guarantee that all potential vulnerabilities have been identified.

2. **Environment Dependency:** The results of the audit are applicable only within the context of the environment and conditions under which the assessment was conducted. Changes in the operating environment or interactions with other contracts may alter the outcomes.

3. **Not an Endorsement:** This audit does not constitute an endorsement of the total security of the smart contract nor should it be interpreted as a guarantee of invulnerability to attacks or failures. Investors and users are advised to conduct their own due diligence before engaging with the audited tokens.

4. **Code Updates:** Any modifications to the code after the date of this audit will invalidate the results. It is the client’s

responsibility to ensure that the audited versions of the code are those implemented on the blockchain.

Disclaimer of Liability: This document is provided "as is", without any warranties of any kind, either express or implied, including but not limited to, warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event shall the auditors be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the audited code or the use or other dealings in the tokens.

date the results. It is the client’s responsibility to ensure that the audited versions of the code are those implemented on the blockchain.

Disclaimer of Liability:

This document is provided "as is", without any warranties of any kind, either express or implied, including but not limited to, warranties of merchantability, fitness for a particular purpose, or non-infringement. In no event shall the auditors be liable for any claim, damages or other liability, whether in an action of contract, tort or otherwise, arising from, out of or in connection with the audited code or the use or other dealings in the tokens.

Introduction

In the rapidly evolving world of blockchain technology, the security and reliability of smart contracts are paramount, particularly for those managing valuable digital assets. ERC-20 tokens, a standard for issuing and managing tokens on the Ethereum blockchain, are widely used in a variety of applications, including utility tokens, governance tokens, and more. Given their critical role and the complexities inherent in smart contract code, conducting thorough audits is essential to ensure their integrity and security.

This audit report provides a comprehensive analysis of the ERC-20 token smart contract. The primary objective is to identify potential security vulnerabilities, ensure compliance with the latest Ethereum community standards, and assess the overall reliability of the contract mechanisms. By scrutinizing the code line by line, the audit aims to prevent potential risks such as transaction errors, token losses, or exploits that could be leveraged for attacks such as reentrancy, overflow/underflow, and unauthorized access.

The findings of this audit are intended to serve multiple stakeholders, including the token developers, project managers, and potential investors. For developers, it provides crucial insights into areas of improvement and reinforcement. For project managers, it offers an assessment of risk management and compliance adherence. For investors, it assures the technical robustness of the token, enhancing confidence in its security as a digital asset.

By addressing these key areas, the audit supports the underlying goal of fostering trust and stability in blockchain-based systems, ensuring that the ERC-20 token not only meets but exceeds the rigorous standards required for widespread adoption and use.

Sensitive Information and Potential Vulnerabilities in ERC-20 Token Smart Contracts

During the audit of an ERC-20 token smart contract, particular attention must be paid to the handling of sensitive information and the identification of potential security vulnerabilities. Smart contracts inherently contain both code and data that are visible on the blockchain to all participants, which means that certain types of sensitive information or poorly implemented functions can become significant liabilities.

Sensitive Information Exposure: Smart contracts should not contain secrets, private keys, or any personally identifiable information (PII) in the code or in the transaction logs. Exposure of such information can lead to security breaches, identity theft, and other malicious activities. During the audit, it is crucial to verify that the contract does not inadvertently expose sensitive data through its functions or event logs.

Levels of Severity in Vulnerabilities for ERC-20 Tokens

1. **Critical:**

Vulnerabilities classified as critical can lead to complete loss of funds, unauthorized creation of tokens, or total loss of contract functionality. They allow attackers to perform actions like draining the contract's balance or manipulating token supply without consent.

2. **High:**

High-severity vulnerabilities can cause significant harm such as theft of a substantial portion of funds, unauthorized access to restricted functions, or major disruptions in token operations. They might not lead to a complete system compromise but can seriously affect confidence and usability.

3. **Medium:**

Medium-severity vulnerabilities may lead to disruptions in contract behavior or exposure of sensitive information which could degrade the user experience or lead to indirect financial loss. They are often more situational and might require specific conditions to be exploited.

4. **Low:**

Low-severity vulnerabilities are considered nuisances rather than serious threats. They typically involve minor issues that have limited implications on contract functionality and user security.

These are often edge cases that are unlikely to be exploited or lead to minimal disruption.

These severity levels help stakeholders prioritize their responses and allocate resources efficiently to address the most pressing issues first. In the context of smart contracts and ERC-20 tokens, paying particular attention to the highest severity issues is critical due to the direct financial implications and the trust users place in these digital assets.

Audited Token Information

AUDIT TEAM	TokenLabs
TOKEN NAME	Kekius Maximus
TOKEN SYMBOL	KEKIUS
NETWORK	mainnet_iota
DEPLOYED CONTRACT	https://explorer.evm.iota.org//token/0xf2364cdD0dcE4630aa8af2d21Daa52b3B9c82835
AUDIT DATE	January 11, 2025
JS TEST	No
TYPE	ERC-20 Token

Token contract was tested for the following vulnerabilities:

- Reentrancy
- Ownership Takeover
- Timestamp Dependence
- Gas Limit and Loops
- DoS with (Unexpected) Throw
- DoS with Block Gas Limit
- Transaction-Ordering Dependence
- Style guide violation
- Costly Loop
- ERC20 API violation
- Unchecked external call
- Unchecked math
- Unsafe type inference
- Implicit visibility level
- Deployment Consistency
- Repository Consistency
- Data Consistency
- Business Logics Review
- Functionality Checks

- Access Control & Authorization
- Escrow manipulation
- Token Supply manipulation
- Assets integrity
- User Balances manipulation
- Data Consistency manipulation
- Kill-Switch Mechanism
- Operation Trails & Event Generation

Audit Results

According to tests results at the date of this token audition, we have found that:

1. Non**critical** vulnerability was found.
2. Non **high** vulnerability was found.
3. Non **medium** vulnerability was found.
4. Non-**low** vulnerability was found.
5. Token ownership is **not renounced.**
6. Token is **not mintable (No more tokens can be minted).**
7. Token can’t be paused.
8. Token doesn’t have any extra trading fee.
9. Token owner can’t set extra fees.