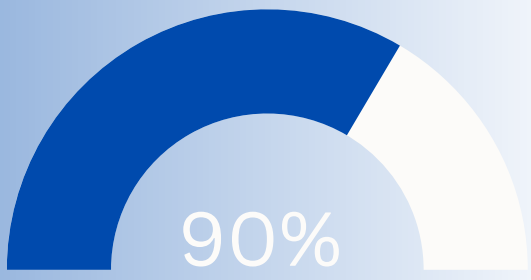
Meme audit

ERAX AUDIT REPORT

Telegram https://t.me/THE_ERAXCoin

Twitter https://x.com/Real_ERAX

MEME AUDIT



CONTRACT ADDRESS

EQDVplkPymPmbbgjBo-J6AQd4MKGgE2zTPl9jxpN1y9VD1VQ

OWNER

UQBhv7U7Jt_HH6S219IrqM4ARl6S-d_3xxgf5tbw5DgGsxch

TOKEN NAME -> ERAX

TOTAL SUPPLY -> 30,000,000,001 ERAX

BLOCKCHAIN -> TON

STANDARD -> JETTON

Meme audit has performed the automated and manual analysis of Ton contracts. Ton contracts

Status	Craitical	Majar
Opne	0	0
Acknowledged	0	0
Resovled	0	0

Important functions -> recv_internal(), mint_tokens(), burn_notification(),

TABLE OF CONTENT

MANUL REVIEW.....11

AUTOMATED REVIEW.....6

TABLE OF CONTENTS.....4

SCOPE OF WORK.....5

AUIT METHODOLOGY.....10

SCOPE OF WORK

Meme audit was consulted by Toshkin to conduct a smart contract audit of their TON source codes.

The audit scope is strictly limited to the following .fc file(s) only:

- jetton-minter.fc

🔍 Public Contract Link: https://tonscan.org/jetton/EQDVplkPymPmbbgjBo-J6AQd4MKGgE2zTPl9jxpN1y9VD1VQ#source

📄 Contract Name: jetton-minter.fc

🛠️ Compiler Version: 0.3.0

AUDIT METHODOLOGY

For a comprehensive audit of a smart contract on the TON blockchain, Meme audit follows a structured process that includes both automated and manual analysis to identify vulnerabilities, centralized points, and potential issues. Here's a breakdown of Meme audit methodology:

CONNECT:

- The onboarding team gathers source codes, specifications, and contract scope.

AUDIT

- Automated analysis detects common vulnerabilities using:
  - TON Compiler for compiling and simulating interactions.
  - TON SDK Tools for vulnerability detection.
  - Smart Contract Validators integrated with the TON VM to simulate contract behavior.
  - Blockchain Simulations to detect errors, gas inefficiencies, or potential DoS (Denial of Service) attacks.
  - A manual line-by-line audit to find vulnerabilities automated tools might miss.

Common Exploits Checked:

- Token Supply Manipulation
- Access Control and Authorization
- Ownership Control
- Message Injection

AUTOMATED REVIEW

FunctionImportanceDefinition

recv_internal()

🔴 Critical

Central function for processing incoming messages (minting, burning, providing wallet addresses, changing admin/content)

mint_tokens()

🟠 Major

Handles the minting of new tokens, affecting the total supply

burn_notification()

🟠 Major

Manages burning tokens and reducing the total supply

load_data()

🟠 Major

Responsible for loading the contract’s state, impacting total supply, admin, and content

save_data()

🟠 Major

Responsible for saving the contract’s state, impacting total supply, admin, and content

provide_wallet_address()

🟡 Medium

Provides wallet addresses and is important for user interactions

get_jetton_data()

🟢 Minor

Returns the wallet address for a given owner (state query)

get_wallet_address()

🟢 Minor

Important for user interaction but no direct impact on core contract behavior

OWNER PRIVILEGES

Centralization risk is a significant concern in the TON blockchain ecosystem. When a smart contract has a privileged role, the centralization-related risk increases, potentially leading to loss of control over assets or manipulation of the contract.

There are legitimate reasons for having privileged roles in TON **contracts:**

- Privileged roles can be granted the ability to pause recv_internal() during external threats or attacks.
- Privileged roles may use functions like add_user() or set_aux_user() to manage wallet addresses, user permissions, or transaction limits, which is useful for operational tasks such as **exchange listings.**

However, authorizing privileged roles to an externally-controlled account (EOA) can be risky, as this makes the contract vulnerable to centralized control.

RECOMMENDATION:

- Private key of a privileged role must be carefully protected to avoid potential hacks or loss of control.
- Privileged roles should be shared across multi-signature wallets to prevent single points of failure.
- Once the contract is stable, consider renouncing privileged roles to improve decentralization.
- Understand the project's initial asset distribution. Assets in liquidity pools should be locked with a release schedule.

RISK CATEGORIES

A successful external attack may allow the external attacker to directly exploit. A successful centralization-related exploit may allow the privileged role to directly exploit. All risks which are identified in the audit report are categorized:

Risk TypeDefinition

Critical

These risks pose immediate and severe threats, such as asset theft, data manipulation, or complete loss of contract functionality. They are often easy to exploit and can lead to significant, irreparable damage. Immediate fix is required.

Major

These risks can significantly impact code performance and security. They may indirectly lead to asset theft and data loss. They can allow unauthorized access or manipulation of sensitive functions if exploited. Fixing these risks is important.

Medium

These risks may create attack vectors under certain conditions. They may enable minor unauthorized actions or lead to inefficiencies that can be exploited indirectly to escalate privileges or impact functionality over time.

Minor

These should be addressed to enhance overall code quality and maintainability.

Unknown

These risks pose uncertainty specific to the contract or those that weren’t visible with it. Immediate fix is required to mitigate risk uncertainty.

All statuses which are identified in the audit report are categorized here:

Status TypeDefinition

Open

Issues that are identified but not fixed yet.

Acknowledged

Issues are acknowledged but not fixed yet.

Resolved

Issues are fixed.

DISCLAIMERS

Meme audit Network provides the easy-to-understand audit of blockchain source codes (commonly known as smart contracts).

The smart contract for this particular audit was analyzed for common contract vulnerabilities, and centralization exploits. This audit report makes no statements or warranties on the security of this contract. This audit report does not provide any warranty or guarantee regarding the absolute bug-free nature of the smart contract analyzed, nor do they provide any indication of the client's business, business model or legal compliance. This audit report does not attest to the origin, ownership, or any other data beyond the programming language, or other programming aspects that could present security risks.

Cryptographic tokens are emergent technologies, they carry high levels of technical risk and uncertainty. 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. This audit report could include false positives, false negatives, and other unpredictable results.

CONFIDENTIALITY

This report is subject to the terms and conditions (including without limitations, description of services, confidentiality, disclaimer and limitation of liability) outlined in the scope of the audit provided to the client. This report should not be transmitted, disclosed, referred to, or relied upon by any individual for any purpose without Meme audit Network's prior written consent.

NO FINANCIAL ADVICE

This audit report does not indicate the endorsement of any particular project or team, nor guarantees its security. No third party should rely on the reports in any way, including to make any decisions to buy or sell a product, service or any other asset. The information provided in this document does not constitute investment advice, financial advice, trading advice, or any other sort of advice and you should not treat any of the report's content as such. This audit report should not be used in any way.

ABOUT Meme audit NETWORK

Meme audit Network provides intelligent blockchain solutions. We provide smart contract development, testing, and auditing services. We have developed 150+ solidity codes, audited 1000+ smart contracts, and analyzed 500,000+ code lines. We have worked on major public blockchains e.g., Ethereum, Binance, Cronos, Doge, Polygon, Avalanche, Metis, Fantom, Bitcoin Cash, Velas, Oasis, etc.

Meme audit Network is built by engineers, developers, UI experts, and blockchain enthusiasts. Our team currently consists of 4 core members, and 6+ casual contributors.

- Website: https://memeaudit.site
- Email: info@memeaudit

Telegram https://t.me/memeaudit