Cyberscope

Audit Report

Brett

June 2024

Network	TON
Address	EQAnmanJNfO07EHZAsHode4AyxCFboiobF1-Y04Q7UG9sinZ
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

Diagnostics

Critical Medium Minor / Informative

Severity	Code	Description	Status
	MTD	Missing Token Description	Unresolved

Table of Contents

Review

Explorer	https://tonscan.org/address/EQAnmanJNfO07EHZAsHode4AyxCFboiobF1-Y04Q7UG9sinZ
Address	EQAnmanJNfO07EHZAsHode4AyxCFboiobF1-Y04Q7UG9sinZ
Network	TON
Name	Brett
Symbol	BRETT
Decimals	9
Total Supply	8,500,000,000

Audit Updates

Initial Audit	28 Jun 2024

Source Files

Filename	SHA256
jetton-minter.fc	b93612f1f3e3d321e9695f103b1e697e97f5ba5e2da9e519987904fd667fe7ef

Overview

This smart contract is a discoverable Jetton contract designed for the TON (The Open Network) blockchain. It manages the Brett 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, 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 admin address. This process involves calculating the Jetton wallet state, determining the recipient's wallet address, and sending the minted tokens accordingly. Additionally, 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. However, since the ownership has been renounced and the admin address has been transferred to a burn address, the minting of new tokens can no longer take place.

The admin address has the authority to change the content associated with the token and can also transfer admin rights to another address. In this specific deployment, the ownership has been renounced as the admin address has been transferred to a burn address, rendering the contract immutable and preventing any further administrative changes.

Furthermore, the contract includes a method to retrieve essential data about the token, such as the total supply, admin address, 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.

Metadata

The metadata for the Brett 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 Brett token has the name "Brett" and is represented by the symbol "BRETT." It is associated with an image hosted at "https://res.cloudinary.com/coinfactory/image/upload/v1719034740/ton/o4clic7wrsxxooei629z.jpg." The token uses 9 decimal places, ensuring precise handling of fractional token amounts. Additional fields such as description, image_data, uri, amount_style, and render_type are also set to null, indicating that they are not being utilized in the current metadata structure.

The detailed metadata structure provides an overview of the Brett token's key features and its operational framework within the TON blockchain. Enhancing the metadata with additional information, particularly the description, would further benefit users and investors by offering more comprehensive insights into the token's purpose and value.


```
{
  "name": "Brett",
  "description": null,
  "image":
"https://res.cloudinary.com/coinfactory/image/upload/v1719034740/ton/o4cl
ic7wrsxxooei629z.jpg",
  "symbol": "BRETT",
  "image_data": null,
  "decimals": "9",
  "uri": null,
  "amount_style": null,
  "render_type": null
}
```

Findings Breakdown

Critical	0
Medium	0
Minor / Informative	1

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

MTD - Missing Token Description

Criticality	Minor / Informative
Location	jetton-minter.fc#L147
Status	Unresolved

Description

The smart contract's `get_jetton_data` function returns various details about the token, including its total supply, admin address, and associated content. However, upon review, it was found that the description field within the `jetton_content` is empty. The description field is an important component that provides users and potential investors with valuable information about the token, its purpose, and its unique attributes. The absence of a description can potentially hinder user engagement and investor interest.

```
(int, int, slice, cell, cell) get_jetton_data() method_id {
    (int total_supply, slice admin_address, cell content, cell
jetton_wallet_code) = load_data();
    return (total_supply, -1, admin_address, content,
jetton_wallet_code);
}
```

Recommendation

It is recommended to populate the description field in the `jetton_content` with a concise and informative summary of the token. This description should highlight the key features, intended use cases, and any other pertinent information that would help users and investors learn more about the token. Providing a detailed description not only enhances transparency but also fosters trust and interest in the token, thereby supporting its adoption and overall success.

Summary

The Brett token, built on 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 analysis reported no compiler errors or critical issues.

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