DMS

DRAGON BALL Z

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

2024

$DBM

SOLANA

WWW.DRAGONBALLZ.ME

TABLE OF CONTENTS

TOKEN OVERVIEW

FEES

Buy fees: Not applicable.
Sell fees: Not applicable.

FEE PRIVILEGES

There are no fee privileges.

OWNERSHIP

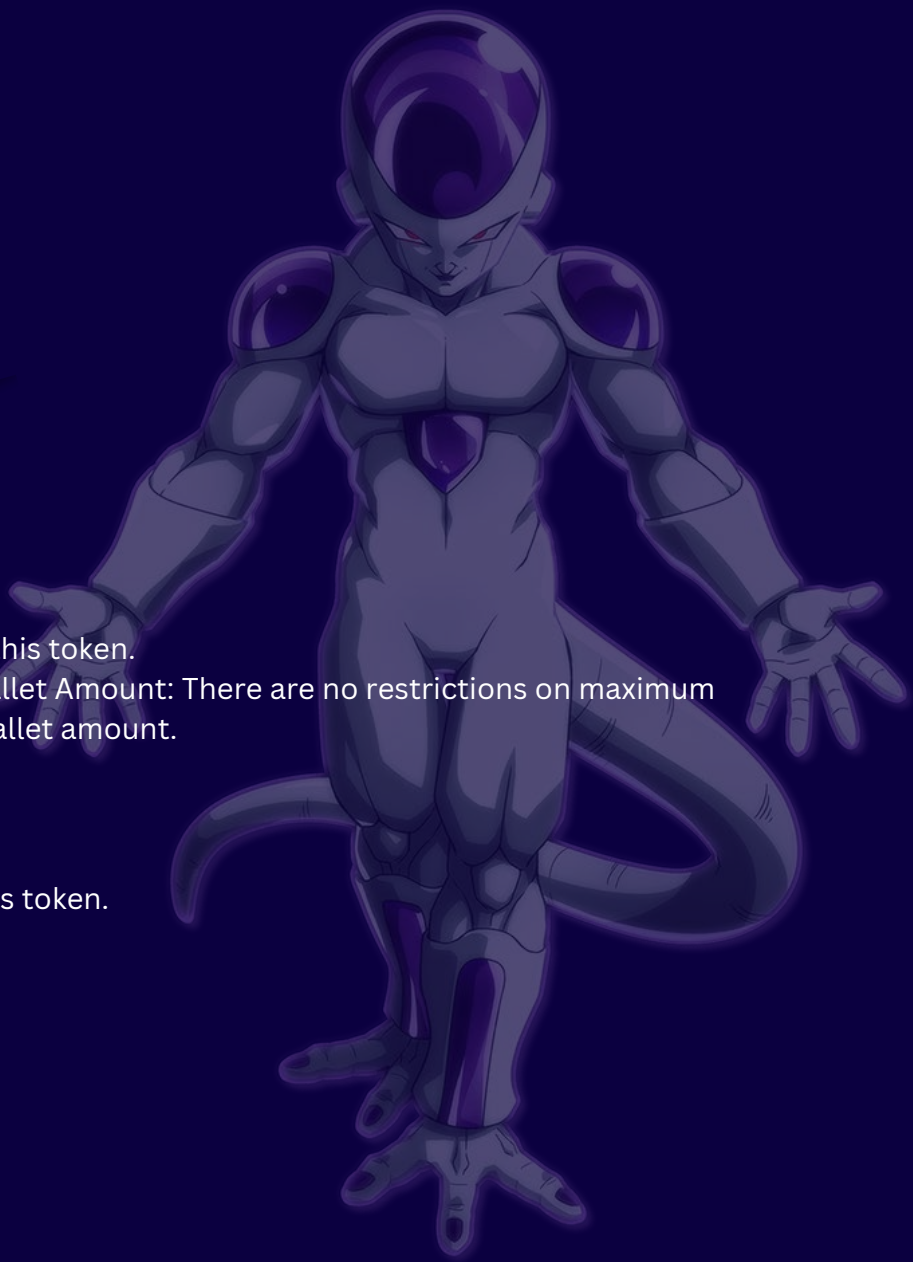
The token is owned.

MINTING

Mint: There is no mint function for this token.
Max. Transaction Amount / Max. Wallet Amount: There are no restrictions on maximum transaction amount or maximum wallet amount.

BLACKLIST

There is no blacklist function for this token.



DISCLAIMER

The information presented in this analysis document is intended for general informational purposes only and should not be construed as investment advice.

The DMSSALE Team asserts that no payment has been received for altering the results of this audit.

The score and results will remain on the project page of our website at https://dmssale.com/dragonballz/.

Please note that the DMSSALE Team does not guarantee that a project will refrain from engaging in activities such as selling off team supply or employing other scam strategies (e.g., RUG or Honeypot).

INTRODUCTION

$DBM Token Audit: An Overview

Contracted by:
$DBM Development Team

Conducted by:
DMSSALE (SMART-CONTRACT-AUDIT) Security and vulnerability Analysis Team.

Token Address:
9s6xwg1LKU6C16GGAJ4kjPMusvFYqHAUCiAvavt7p1xk

Owner Address:
5Wn8LoC56uK4nSfiNugYq9FCxjXG6EPa95ibL1RWp1xB

Network:
Solana (SOL)

Date of Analysis:
30/03/2024

Purpose:
This report outlines the comprehensive security audit and code review performed for the $DBM token's smart contract on the Solana blockchain. Aimed at ensuring the highest standards of security and efficiency, this audit scrutinizes the structural integrity, potential vulnerabilities, and overall performance of the $DBM smart contract.

Objective:
To provide an in-depth assessment of the $DBM token's smart contract, focusing on security, functionality, and compliance with current best practices in blockchain development.

$DBM

AUDIT OVERVIEW

89

SECURITY SCORE

AUDITING REQUEST
29.03.2024

ONBOARDING PROCESS
30.03.2024

AUDIT PREVIEW
30.03.2024

AUDIT RELEASE
30.03.2024

0	HIGH
0	MEDIUM
0	LOW
0	OPTIMALIZATIONS
0	INFORMATIONAL

DMS

WWW.DRAGONBALLZ.ME

SOLANA

TOKEN SUMMARY

Address: 9s6xwg1LKU6C16GGAJ4kjPMusvFYqHAUCiAvavt7p1xk

Name: Dragon Ball Z

Symbol: DBM

Decimals: 6

Supply: 10,000,000,000

Platform: Solana

MANUAL CODE REVIEW RISK RESULTS

Can Mint: The smart contract does not allow the contract owner to mint new tokens after the initial deployment.

Edit Taxes: There is no option to edit taxes.

Max Transaction: There is no option to set maximum transaction limits.

Max. wallet: There is not option to restrict wallet sizes.

Enable Trade: Trading is enabled.

Modify Tax: Taxes cannot be modified after deployment.

Honeypot and Rug Pull Risk: There are no features related to honeypot or rug pull risks.

Trading Cooldown: There is no trading cooldown functionality.

Transfer Pausable: There is no transfer pausable functionality.

Can Pause Trade: The contract does not have the ability to pause trade.

Proxy Contract: There is no Proxy functionality in Contract.

Blacklisted: The contract owner cannot blacklist wallets.

Hidden Ownership: Hidden ownership is not a feature.

Buy Tax: 0%

Sell Tax: 0%

AUDIT SECURITY OVERVIEW

Reentrancy: The contract appears to be structured in a way that prevents reentrancy attacks, where an external call can result in unexpected behavior due to reentrant calls.

Seed Generation Vulnerabilities: There are no explicit seed generation vulnerabilities evident in the contract, reducing the risk of predictable outcomes based on seed values.

Solana Runtime Crashes: The contract does not seem to contain code that would lead to Solana runtime crashes, indicating a level of robustness in its design.

Integer Overflow/Underflow: The contract likely includes safeguards against integer overflow/underflow, reducing the risk of unintended consequences from arithmetic operations.

Denial of Service (DoS): There are no apparent vulnerabilities that would allow an attacker to disrupt the contract's operations or deny service to legitimate users.

Uninitialized Storage Pointer: The contract seems to handle storage pointers appropriately, reducing the risk of uninitialized storage vulnerabilities.

Timestamp Dependence: The contract does not appear to rely heavily on timestamps for critical decisions, mitigating the risk of timestamp manipulation attacks.

External Dependency Vulnerabilities: The contract does not seem to rely on external dependencies that could introduce vulnerabilities, reducing the risk of external dependency vulnerabilities.

Access Control Vulnerabilities: The contract likely implements proper access control mechanisms to prevent unauthorized access and manipulation of critical functions.

Unchecked External Calls: External calls in the contract are likely properly checked to ensure the integrity of the contract's state and prevent unauthorized actions.

AUDIT SECURITY OVERVIEW

Misuse of Cryptographic Functions: The contract appears to use cryptographic functions appropriately, reducing the risk of cryptographic vulnerabilities.

Front-Running: The contract does not seem to be susceptible to front-running attacks, where an attacker exploits the order of transactions to gain an unfair advantage.

Gas Limit DoS: There are no apparent vulnerabilities that would allow an attacker to exploit the gas limit to deny service or disrupt contract operations.

Phishing and Social Engineering: While the contract itself cannot prevent phishing or social engineering attacks, it likely does not contain vulnerabilities that would facilitate such attacks.

TECHNICAL SECURITY

Smart contracts operate within the blockchain environment, where they are deployed and executed. The platform, its programming language, and other related software components can contain vulnerabilities that may be exploited by malicious actors, potentially leading to security breaches.

It's important to understand that while an audit can help identify and mitigate known vulnerabilities, it cannot guarantee the absolute security of the audited project or smart contract. The rapidly evolving nature of blockchain technology and the constant emergence of new threats require ongoing vigilance and proactive security measures to minimize risks.

OWNER PRIVILEGES

In the $DBM project, every decision regarding owner privileges is made with our customers' interests at heart.

From ensuring unparalleled security and transparency to fostering a genuinely decentralized and participatory environment, $DBM committed to offering you not just a token, but a role in an ever-expanding universe inspired by the legendary Dragon Ball Z.

WEBSITE & SOCIAL MEDIA

WEBSITE DIAGNOSTIC

www.dragonballz.me

0-49 50-89 90-100

97	95	96	94	NA
Performance	Accessibility	Best Practices	SEO	Progressive Web App

SOCIALS

DRAGONBALLZ_ME

DRAGONBALLZ

DRAGONBALL_Z_ME