freshcoins

SMART CONTRACT CODE REVIEW AND SECURITY ANALYSIS REPORT

Kangeroo

$Kangeroo

27/01/2025

TOKEN OVERVIEW

Fees

- Buy fees: Not Available (0%)
- Sell fees: Not Available (0%)

Fees privileges

- Can’t set fees

Ownership

- Not Available

Minting

- Can’t mint new tokens

Max Tx Amount / Max Wallet Amount

- Not Available

Blacklist

- Not Available

Other privileges

- Not Available

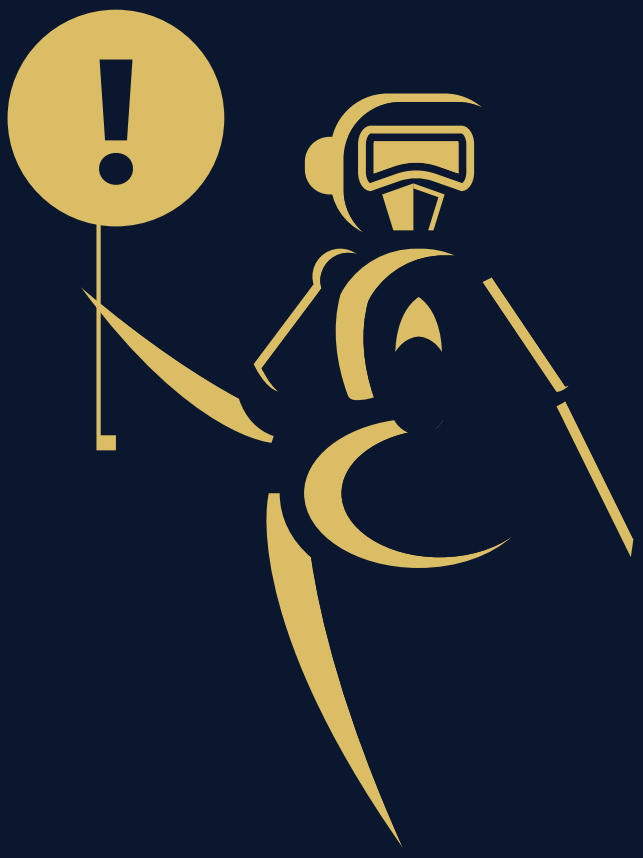
TABLE OF CONTENTS

DISCLAIMER

The information provided on this analysis document is only for general information and should not be used as a reason to invest.

FreshCoins Team will take no payment for manipulating the results of this audit.

The score and the result will stay on this project page information on our website https://freshcoins.io
FreshCoins Team does not guarantees that a project will not sell off team supply, or any other scam strategy (RUG or Honeypot etc)



INTRODUCTION

FreshCoins (Consultant) was contracted by Kangeroo (Customer) to conduct a Smart Contract Code Review and Security Analysis.

kan9jkq4MbrDTexV2gS8HT5qnvJdYyH2ZvCzPPrkMcZ

Network: Solana (SOL)

This report presents the findings of the security assessment of Customer's smart contract and its code review conducted on 27/01/2025

WEBSITE DIAGNOSTIC

https://kangeroocoin.com/

0-49 50-89 90-100

96	95	94	92	NA
Performance	Accessibility	Best Practices	SEO	Progressive Web App

Socials

X (Twitter)

https://x.com/kangeroocoin

Telegram

https://t.me/kangerooofficial

AUDIT OVERVIEW

92

Security Score

- Auditing Request
  27.01.2025
- Onboarding Process
  27.01.2025
- Audit Preview
  27.01.2025
- Audit Release
  27.01.2025

0	High
1	Medium
0	Low
0	Optimizations
0	Informational

TOKEN SUMMARY

Address:	kan9jkq4MbrDTexV2gS8HT5qnvJdYyH2ZvCzPPrkMcZ
Name:	Kangeroo
Symbol:	Kangeroo
Decimals:	9
Supply:	18,000,000,000
Platform:	Solana
Contract Name:	Kangeroo
Optimization:	Yes
License Type:	Unlicensed
Language:	Rust

PROJECT OVERVIEW

METADATA RESULTS

key:	4
updateAuthority:	masVJUNthKyG86ZsYjdMXmUA9UJSnE92BkzBsJ6v8Fd
mint:	kan9jkq4MbrDTexV2gS8HT5qnvJdYyH2ZvCzPPrkMcZ
sellerFeeBasisPoints:	0
primarySaleHappened:	0
isMutable:	0
editionNonce:	254
tokenStandard:	2

URI METADATA

Solana URI Metadata pertains to the information linked with a token, which is fetched from its Uniform Resource Identifier (URI)

https://kangeroocoin.com/metadata.json


```
{ 8 items
  key : 4
  updateAuthority : "masVJUNthKyG86ZsYjdMXmUA9UJSnE92BkzBsJ6v8Fd"
  mint : "kan9jkq4MbrDTexV2gS8HT5qnvJdYyH2ZvCzPPrkMcZ"
  data : { 4 items
    name : "Kangeroo"
    symbol : "Kangeroo"
    uri : "https://kangeroocoin.com/metadata.json"
    sellerFeeBasisPoints : 0
  }
  primarySaleHappened : 0
  isMutable : 0
  editionNonce : 254
  tokenStandard : 2
}
```

PROJECT OVERVIEW

METADATA RESULTS

key: This is an integer value that signifies the key linked to the root object

updateAuthority: This is a string value that denotes the update authority for the program

mint: This is a string value that signifies the mint address associated with the program

sellerFeeBasisPoints: This is an integer value that represents the seller fee basis points

primarySaleHappened: This is an integer value that indicates whether the primary sale of the token has occurred

isMutable: This is an integer value that indicates the mutability of the token. A value of 1 suggests that the token is mutable, while a value of 0 indicates that the token is not mutable

editionNonce: This is an integer value that denotes the edition nonce for the token

tokenStandard: This is an integer value that signifies the token standard for the program

PROJECT OVERVIEW

METAPLEX METADATA

Solana metadata encompasses supplementary information linked to a digital asset or NFT on the Solana blockchain. This information comprises details such as the asset's name, description, image, attributes, and other pertinent data

In the Solana context, metadata is usually stored in JSON format and associated with the unique identifier or token ID of assets. This metadata offers crucial information about the asset, enabling users and applications to comprehend and engage with it effectively.

TECHNICAL FINDINGS

Centralization / Privilege

During the contract deployment, all tokens are allocated to the contract deployer, presenting a potential risk of centralization. This is concerning because the deployer possesses the ability to distribute tokens without seeking consensus from the community

Recommendation

We advise the team to maintain transparency regarding the initial token distribution process

Recommendation:

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. The risk can be prevented by temporarily locking the contract or renouncing ownership.

CONCLUSION AND ANALYSIS

Smart Contracts within the scope were manually reviewed and analyzed with static tools.

Audit report overview contains all found security vulnerabilities and other issues in the reviewed code.

Found no HIGH issues during the first review.

TOKEN DETAILS

Details

Buy fees:	Not Available (0%)
Sell fees:	Not Available (0%)
Max TX:	Not Available
Max Sell:	Not Available

Honeypot Risk

Ownership:	Not Available
Blacklist:	Not detected
Modify Max TX:	Not detected
Modify Max Sell:	Not detected
Disable Trading:	Not detected

Rug Pull Risk

Liquidity:	Raydium AMM V4
Holders:	Clean

KANGEROO TOKEN ANALYTICS & TOP 10 TOKEN HOLDERS

#	Account	Token Account	Quantity	Percentage
1	hk5sMXz3VB4d4ahUyKCWc7zHeYAYykSYkb4pFNHWhje	9mg6ysWVr5vQWEn6WK6bPVPTU4B5WQLWSjcvAu5ezQGL	10,688,400,000.00	59.37%
2	EsrAoZnkRKEA2Yu4iNBMjR6Z2XL8WviyCwv1ihtWtWJX	FkK13wjnRT7cguXTKp5zxkFNr8DzFo1z5iQL1H9xHio9	3,711,600,000.00	20.61%
3	3tod4efVpW11sLNR7HPke6o5xcbpBkWerjJFvFBetWjM	4V7RczvwM4ipmyfpdZ9WKr9DeNeaS21fw8C9gKp6ar6N	3,600,000,000.00	19.99%
4	Token Owner	BBTBKm5t8kp9VRqomtcHCKVUBknR3ERUKNR4nCSYyyHz	0.00	0.00%

TECHNICAL DISCLAIMER

Smart contracts are deployed and executed on the blockchain platform. The platform, its programming language, and other software related to the smart contract can have its vulnerabilities that can lead to hacks. The audit can't guarantee the explicit security of the audited project / smart contract.