expelee

A Secure Place For **Web3**

SMART CONTRACT AUDIT OF

Metarichs Token

Contract Address

0xbF0f0d7fe9aDDdD697F3DA6563b8756885cB1517

Audit Summary

Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analyzed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit :

Audit Result : **PASSED**

Ownership: **NOT RENOUNCED**

KYC Verification: **NOT DONE TILL AUDIT**

Audit Date: **06/05/2001**

Audit Team: **EXPELLE**

Be aware that smart contracts deployed on the blockchain aren't resistant to internal exploit, external vulnerability, or hack. For a detailed understanding of risk severity, source code vulnerability, functional hack, and audit disclaimer, kindly refer to the audit.

DISCLAMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always Do your own research and protect yourselves from being scammed. The Expelle team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.
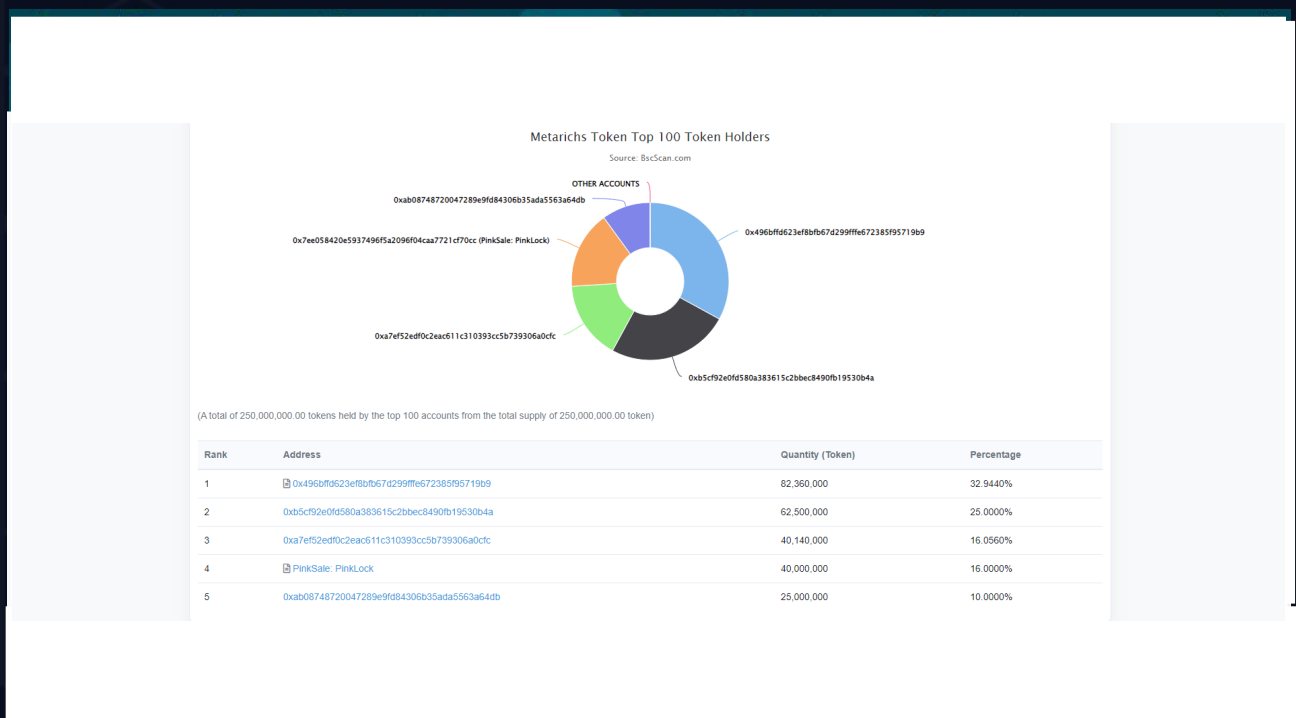
Under no circumstances did Expelle receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Always Do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelle team disclaims any liability for the resulting losses.

Contract Review

Contract Name	Metarichs Token
Compiler Version	v0.8.10+commit.fc410830
Optimization	Yes with 200 runs
License	None (default bsc license)
Explorer	BSC
Symbol	MRC
Decimals	18
Total Supply	250,000,000
Domain	metarichs.finance

Tokenomics

Metarichs Token Top 100 Token Holders

Source: BscScan.com

(A total of 250,000,000.00 tokens held by the top 100 accounts from the total supply of 250,000,000.00 token)

Rank	Address	Quantity (Token)	Percentage
1	0x496bffd623ef8bfb67d299fffe672385f95719b9	82,360,000	32.9440%
2	0xb5cf92e0fd580a383615c2bbec8490fb19530b4a	62,500,000	25.0000%
3	0xa7ef52edf0c2eac611c310393cc5b739306a0cfc	40,140,000	16.0560%
4	PinkSale: PinkLock	40,000,000	16.0000%
5	0xab08748720047289e9fd84306b35ada5563a64db	25,000,000	10.0000%

Project Review

Token Name Metarichs Token

Web Site metarichs.finance

Twitter twitter.com/Metarichs

Telegram t.me/MetarichsOfficialGroup

Contract Address 0xbF0f0d7fe9aDDdD697F3DA6 563b8756885cB1517

Platform BINANCE SMART CHAIN

Token Type BEP 20

Language SOLIDITY

Audit Methodology

The scope of this report is to audit the smart contract source code of AlcarLand. Inter has scanned the contract and reviewed the project for common vulnerabilities, exploits, hacks, and back-doors. Below is the list of commonly known smart contract vulnerabilities, exploits, and hacks:

Category

Smart Contract Vulnerabilities

- Re-entrancy
- Unhandled Exceptions
- Transaction Order Dependency
- Integer Overflow
- Unrestricted Action
- Incorrect Inheritance Order
- Typographical Errors
- Requirement Violation

Source Code Review

- Ownership Takeover
- Gas Limit and Loops
- Deployment Consistency
- Repository Consistency
- Data Consistency
- Token Supply Manipulation

Functional Assessment

- Access Control & Authorization
- Operations Trail & Event Generation
- Assets Manipulation
- Liquidity Access

Vulnerability Checklist

No.	Description	Result
1	Compiler warnings	Passed
2	Race conditions and Re-entrancy. Cross-function race conditions.	Passed
3	Possible delays in data delivery	Passed
4	Oracle calls	Passed
5	Front running	Passed
6	Timestamp dependence	Passed
7	Integer Overflow and Underflow	Passed
8	DoS with Revert	Passed
9	DoS with block gas limit	Passed
10	Methods execution permissions	Passed
11	Economy model	Passed
12	The impact of the exchange rate on the logic	Passed
13	Private user data leaks	Passed
14	Malicious Event log.	Passed
15	Scoping and Declarations	Passed
16	Uninitialized storage pointers	Passed
17	Arithmetic accuracy	Passed
18	Design Logic	Passed
19	Cross-function race conditions	Passed
20	Safe Zeppelin module	Passed
21	Fallback function security	Passed

Important Points To Consider

✔ The owner cannot mint tokens after intial deployment.

✔ The owner cannot stop Trading.

✘ The owner cannot change the max tx amount.

✔ The contract is verified

✘ The owner can enable/disable PinkSale Antibot and autoLiquidity.

✔ The owner can change the fees with no restrictions.

About Expelee

Expellee is a community driven organisation dedicated to fostering an anti-rug movement. We're here to keep investment safe from fraudsters. We've encountered several rug pulls and know how it feels to be duped, which is why we don't want anybody else to go through the same experience. We are here to raise awareness through our services so that the future of cryptocurrency
can be rug-free.

The auditing process focuses to the following considerations with collaboration of an expert team :

- Functionality test of the Smart Contract to determine if proper logic has been followed throughout the whole process.
- Manually detailed examination of the code line by line by experts.
- Live test by multiple clients using Testnet.
- Analysing failure preparations to check how the Smart Contract performs in case of any bugs and vulnerabilities.
- Checking whether all the libraries used in the code are on the latest version.
- Analysing the security of the on-chain data.

Social Media

@Expelee

@ExpeleeOfficial

@expelee-co