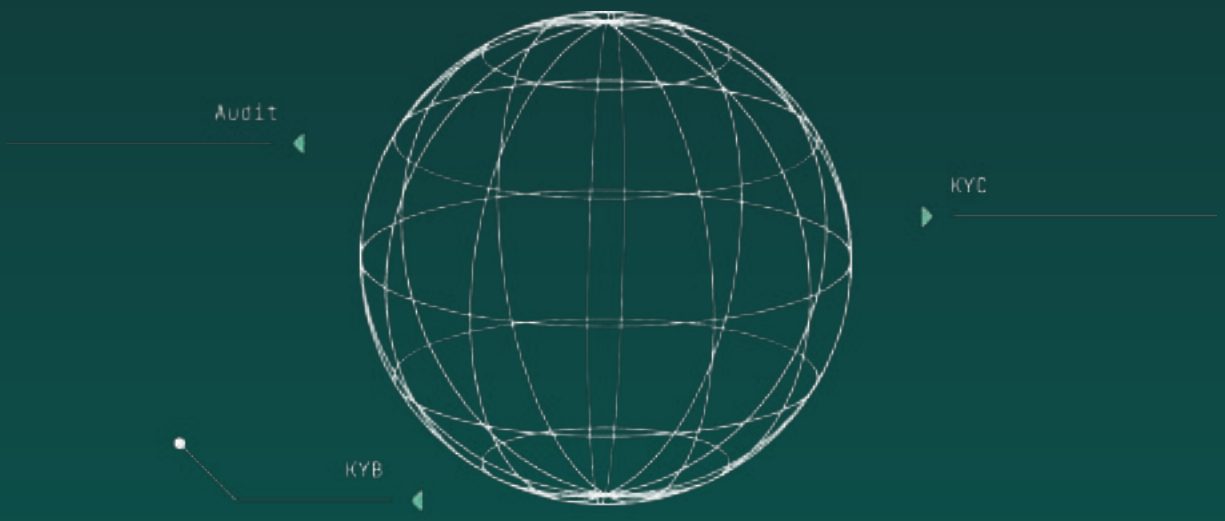
DAudit

SMART CONTRACT REVIEW AND SECURITY REPORT



MAX

COMPLETED ON

JUNE 28, 2022

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

DAudit

OVERVIEW

This audit has been prepared for MetaMAX to review their Smart Contract Code and Security. This audit report aims to help investors make an informative decision during the project research.

In this report, you will find a summarized review of the following key points:

✓ Contract's source code
✓ Contract's function
✓ Owner's wallets
✓ Important Technical Stats
✓ Good Practices
✓ Recommendation

This document may contain confidential information about IT systems and the intellectual property of the Customer as well as information about potential vulnerabilities and methods of their exploitation.

The report containing confidential information can be used internally by the Customer, or it can be disclosed publicly after all vulnerabilities are fixed — upon a decision of the Customer.

▶ This Audit report DOES NOT guarantee nor reflect the outcome and goal of the project.

▶ DAudit's audit process only guarantees that the smart contract code has been verified not to have security breaches.

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

DAudit

Table Of Content

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

DAudit

CONTRACT INFORMATION

Token Name
METAMAX

Symbol
MMAX

Contract Name
METAMAX

Type
ERC-20

Website
https://www.metamaxonline.com/

Technical Documentation
https://metamaxonline.com/wp-content/uploads/2022/05/MetaMAX-Whitepaper-2022.pdf

Contract Address
0x218558fa970eb3D34D57A196D65E61d897F731Da

Network
Binance Smart Chain

Language
Solidity

Compiler Version
v0.6.12+commit.27d51765

Optimization
Yes with 200 runs

Decimals
18

Total Supply
10,000,000,000

DAUDIT CONTRACT REVIEW PROCESS

Smart Contract Code review process:
✓ Testing the smart contracts against both common and uncommon vulnerabilities.
✓ Assessing the codebase to ensure compliance with current best practices and industry standards.
✓Ensuring contract logic meets the specifications and intentions of the client.
✓ Cross-referencing contract structure and implementation against similar smart contracts produced by industry leaders.
✓ Thorough line-by-line manual review of the entire codebase by industry experts.

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

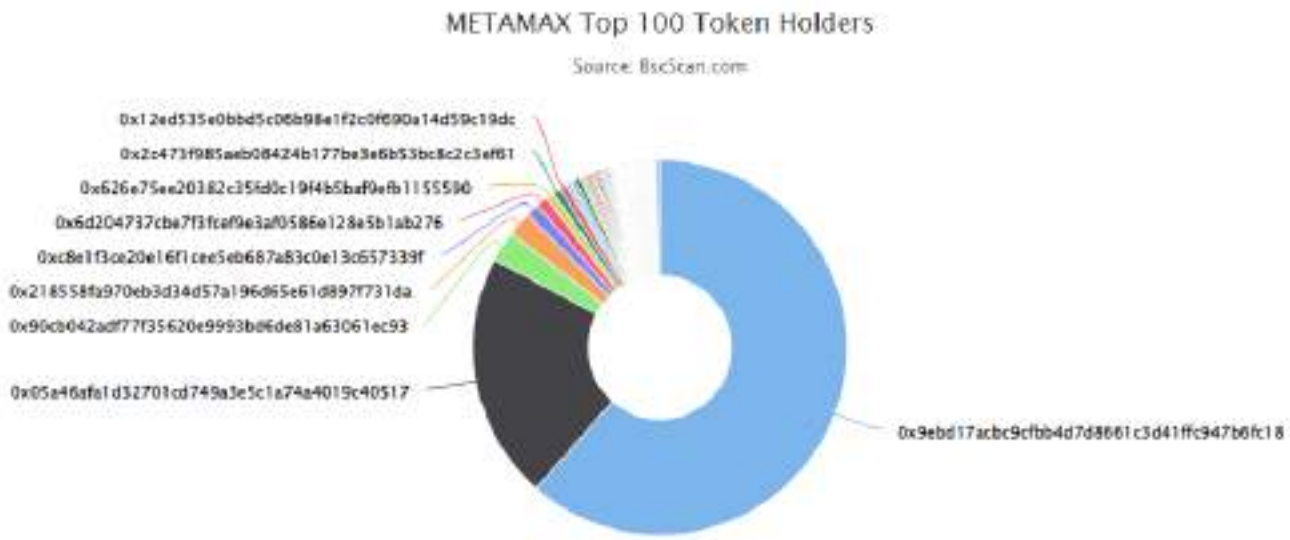
PROJECT TECHNICAL INFORMATION

(AS OF JUNE 28TH, 2022)

LIQUIDITY STATUS:

NOT ADDED YET

Owner Address	0x78C2aF9ada71B08F75dF33cbC95d1bCd248C6948
Token Total Supply	10,000,000,000
Total Token Holder	1,728



Rank	Address	Quantity (Token)	Percentage
1	[illegible]	6,148,543,615	61.4854%
2	[illegible]	2,156,316,962.8	21.5632%
3	[illegible]	265,937,500	2.6594%
4	[illegible]	211,001,948.5216	2.1100%

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

DAudit

IMPORTANT STATS

TAX
Buy tax: 8% Sell tax: 13%

OWNER CAN SET FEES
Owner can set fees up to 100%

MAX TX AMOUNT
Owner can set max tx amount

OWNERSHIP
Owner can renounce or transfer ownership

MINT FUNCTION
No mint function found

PAUSE
Owner can't pause trading

BLACKLIST
Owner can set blacklist

WHITELIST
Owner can set whitelist to avoid transaction fee

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

VULNERABILITY CHECK

CODE REVIEW

Design Logic	Passed
Compiler Warnings	Passed
Private user data leaks	Passed
Timestamp dependence	Passed
Integer overflow and underflow	Passed
Race conditions and reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle Calls	Passed
Front Running	Passed
DoS with block gas limit	Passed
DoS with Revert	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious Event Log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross function race conditions	Passed
Safe Zeppelin module	Passed
Fallback function security	Passed

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

DAudit

VULNERABILITY CHECK

FUNCTION REVIEW

Business Logics Review Functionality Checks	Passed
Access Control & Authorization	Passed
Escrow manipulation	Passed
Token Supply manipulation	Passed
Assets integrity	Passed
User Balances manipulation	Passed
Data Consistency manipulation	Passed
Kill - Switch Mechanism Operation Trails & Event Generation	Passed

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

RISK LEVELS

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

Critical

Critical vulnerabilities are usually straightforward to exploit and can lead to asset loss or data manipulations.

High

High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions

Medium

Medium-level vulnerabilities are important to fix; however, they can't lead to asset loss or data manipulations.

Low

Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution.

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

DAudit

RISK FOUND 01

CRITICAL

Owner can set fee up to 100%

Recommendation:
Total selling and buying fees should be kept at ⩽ 25%

```
function setUSDTRewardsFee(uint256 value) external onlyOwner{
    USDTRewardsFee = value;
    totalFees = USDTRewardsFee.add(liquidityFee).add(marketingFee).add(buybackFee).add(DevelopmentFee);
}

function setLiquiditFee(uint256 value) external onlyOwner{
    liquidityFee = value;
    totalFees = USDTRewardsFee.add(liquidityFee).add(marketingFee).add(buybackFee).add(DevelopmentFee);
}

function setMarketingFee(uint256 value) external onlyOwner{
    marketingFee = value;
    totalFees = USDTRewardsFee.add(liquidityFee).add(marketingFee).add(buybackFee).add(DevelopmentFee);
}

function setDevelopmentFee(uint256 value) external onlyOwner{
    DevelopmentFee = value;
    totalFees = USDTRewardsFee.add(liquidityFee).add(marketingFee).add(buybackFee).add(DevelopmentFee);
}

function setBuyBackFee(uint256 value) external onlyOwner{
    buybackFee = value;
    totalFees = USDTRewardsFee.add(liquidityFee).add(marketingFee).add(buybackFee).add(DevelopmentFee);
}
```

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

RISK FOUND 02

CRITICAL

Owner can set blacklist user, through which any user can be prohibited from trading

Recommendation:
It is recommended to use a 3rd party anti-bot service like Pinksale anti bot to ensure fairness.

```
function blacklistAddress(address account, bool value) external onlyOwner{
    _isBlacklisted[account] = value;
}
```

RISK FOUND 03

CRITICAL

Owner can set max transaction amount to 0% but can ignore some address

Recommendation:
It should be applied to all users, avoiding the case that setting to 0% makes all users unable to trade while there are still a specified number of wallets that can be traded.

```
function setMaxTxPercent(uint256 maxTxPercent) public onlyOwner() {
    _maxTxAmount = totalSupply().mul(maxTxPercent).div(10000);
}

function setExcludeFromMaxTx(address _address, bool value) public onlyOwner {
    _isExcludedFromMaxTx[_address] = value;
}
```

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

RISK FOUND 04

LOW

Owner can set whitelist to avoid transaction fee

Recommendation:
Only need to set for necessary wallets only once such as ama router, liquid pool in the initialization.

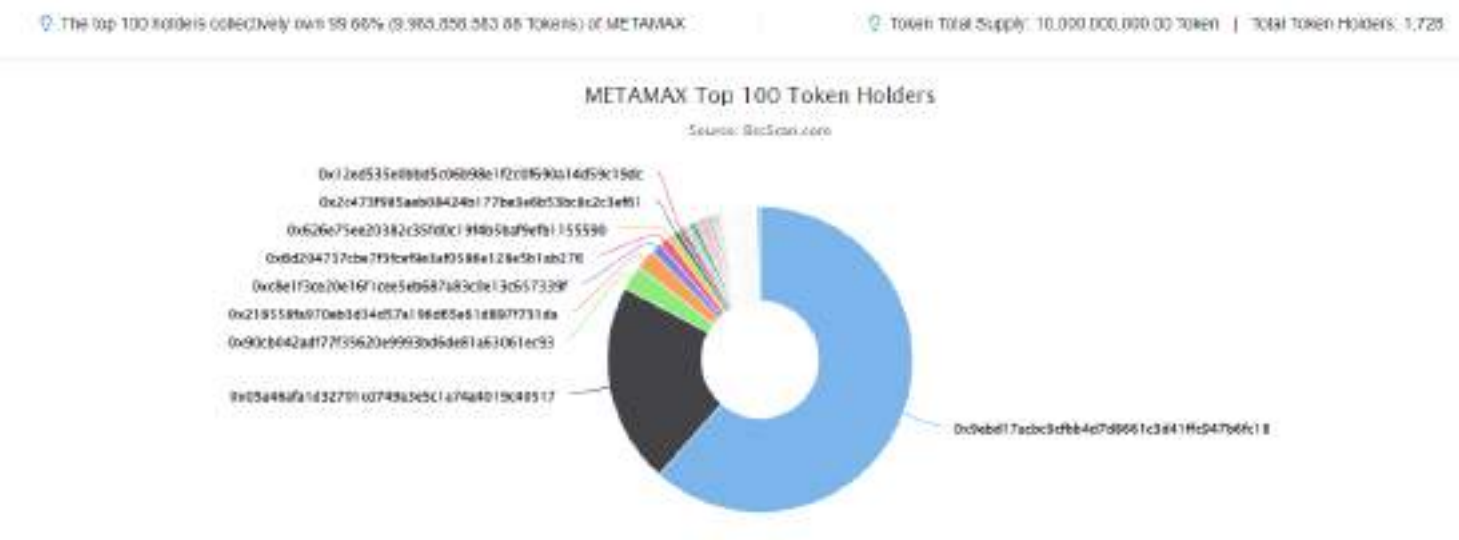
```
function excludeFromFees(address account, bool excluded) public onlyOwner {
    require(_isExcludedFromFees[account] != excluded, "Account is already the value of 'excluded'");
    _isExcludedFromFees[account] = excluded;
    emit ExcludeFromFees(account, excluded);
}

function excludeMultipleAccountsFromFees(address[] memory accounts, bool excluded) public onlyOwner {
    for(uint256 i = 0; i < accounts.length; i++) {
        _isExcludedFromFees[accounts[i]] = excluded;
    }

    emit ExcludeMultipleAccountsFromFees(accounts, excluded);
}
```

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

RISK FOUND 05

LOW

There are 1,728 wallets that already hold tokens before the presale



METAMAX GOOD PRACTICES FOUND

1

The owner cannot mint new tokens after deployment.

2

The owner cannot stop or pause the contract.

DECENTRALAB PTE.LTD.
160 Robinson Road, #14-04 Singapore
Singapore (068914)
support@daudit.org

DAudit

ABOUT DAUDIT

DAudit offers Smart Contract vulnerability and quality testing services at a rapid pace to ensure that projects do not fall behind the market.

Experienced	Fast	Careful	Affordable
A group of experienced blockchain developers built many successful DApp applications and are familiar with security flaws.	Within 6 hours, the audit report will be on your desk! We also have professional consultation and support staff available around the clock.	We deeply analyze the smart contracts line by line and cover the smart contracts with both automated and manual testing.	Affordable We provide the most competitive price in the industry, with audit reports ranging from $500 to $1,000, KYC services start at $1000, and KYB services start at $2,000

CONTACT US

Email

support@daudit.org

Support 24/7

@daudit (Mr.Drake)
@vietdn (Mr.Viet)

DISCLAIMER

DAudit Disclaimer

By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or prin and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice.

The smart contracts submitted for audit were examined in accordance with best industry practices at the time of this report in terms of cybersecurity vulnerabilities and issues in smart contract source code, which are detailed in this report (Source Code); the Source Code compilation, deployment, and functionality (performing the intended functions).

The audit makes no claims or guarantees about the code's security. It also cannot be deemed an adequate appraisal of the code's utility and safety, bug-free status, or any other contractual assertions. While we did our best in completing the study and generating this report, it is crucial to emphasize that you should not rely only on this report; we advocate doing many independent audits and participating in a public bug bounty program to assure smart contract security.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed

Technical Disclaimer

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