MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESSMENT

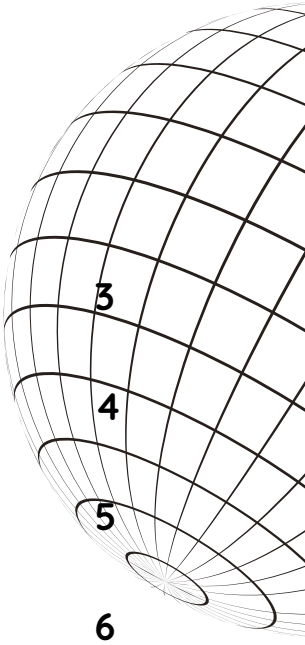
2021

MATETOKEN AUDIT REPORT

19 NOV 2021

SECURITY ASSESMENT

TABLE OF CONTENTS



SECURITY ASSESMENT

SUMMARY

This report has been prepared for MATE to discover issues and vulnerabilities in the source code of the MATE project as well as any contract dependencies that were not part of an officially recognized library. A comprehensive examination has been performed, utilizing Static Analysis, Manual Review, and Testnet Deployment techniques.

The auditing process pays special attention to the following considerations:

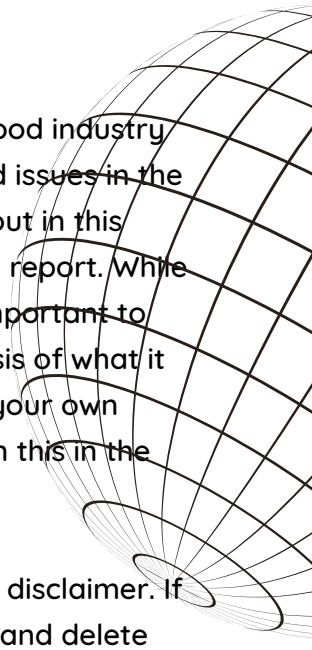
- Testing the smart contracts against both common and uncommon attack vectors.
- Assessing the codebase to ensure compliance with current best practices and industry standards.
- Ensuring contract logic meets the specifications and intentions of the client.
- Cross referencing contract structure and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

The security assessment resulted in findings that ranged from critical to informational. We recommend addressing these findings to ensure a high level of security standards and industry practices. We suggest recommendations that could better serve the project from the security perspective:

- Enhance general coding practices for better structures of source codes;
- Add enough unit tests to cover the possible use cases given they are currently missing in the repository;
- Provide more comments per each function for readability, especially contracts are verified in public;
- Provide more transparency on privileged activities once the protocol is live.

SECURITY ASSESMENT

DISCLAIMER



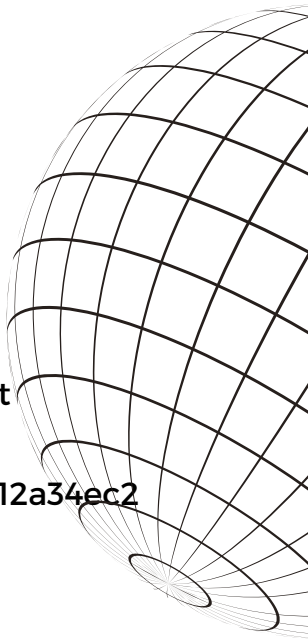
This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

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 printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and MotechAudit and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (MotechAudit) owe no duty of care towards you or any other person, nor does MotechAudit make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and MotechAudit hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, MotechAudit hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against MotechAudit, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

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.

SECURITY ASSESMENT

BACKGROUND



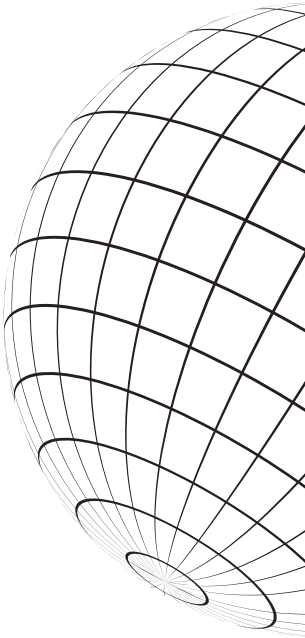
MotechAudit was commissioned by MATE to perform an audit of smart contracts:
https://bscscan.com/address/0x2198b69b36b86f250549d26d69c5957912a34ec2
The purpose of the audit was to achieve the following:

- Ensure that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be used to understand the risk exposure of the smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were identified.

SECURITY ASSESMENT

AUDIT DETAILS



AUDITED PROJECT

MATE

DEPLOYER ADDRESS

0x47cCFF9DD0F64083E752A377c7464cBd7393E61f

CLIENT CONTACTS:

MATE Team

BLOCKCHAIN

Binance smart chain Project

WEBSITE:

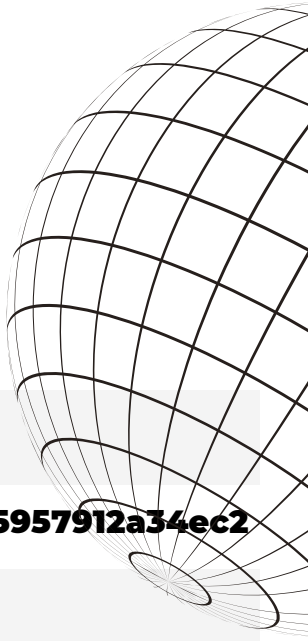
https://www.usemate.com/

MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

CONTRACT DETAILS



Token contract details for Aug-16-2021

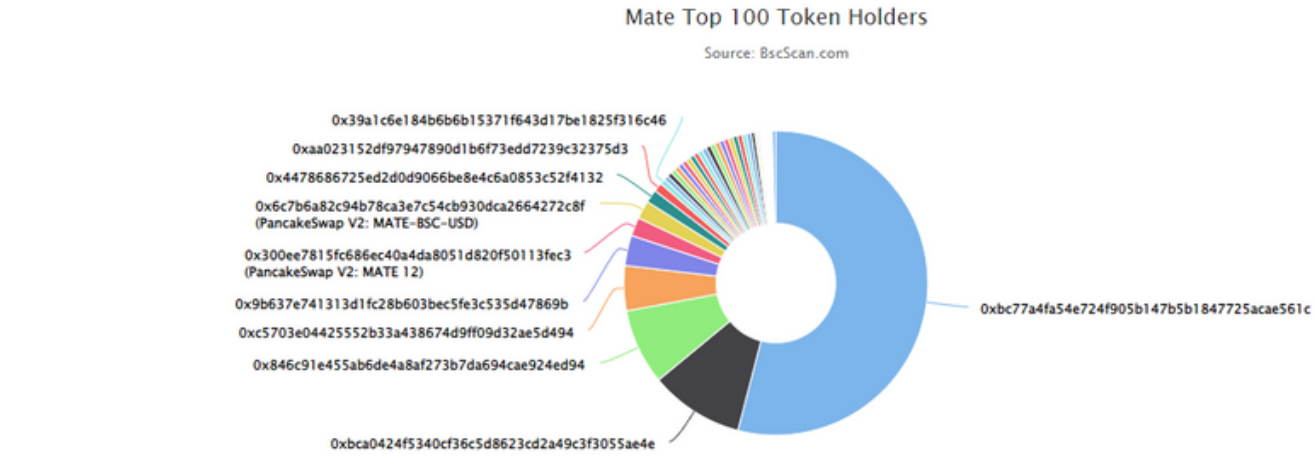
Contract name	**MATE**
Contract address	**0x2198b69b36b86f250549d26d69c5957912a34ec2**
Total supply	**100,000,000 MATE**
Token ticker	**Mate (MATE)**
Decimals	**18**
Token holders	**987**
Transactions count	**42,680**
Top 100 holders dominance	**99.0089%**
Contract deployer address	**0x47cCFF9DD0F64083E752A377c7464cBd7393E61f**
Contract's current owner address	**0x47cCFF9DD0F64083E752A377c7464cBd7393E61f**

SECURITY ASSESMENT

MATE TOKEN DISTRIBUTION

The top 100 holders collectively own 99.64% (99,640,529.87 Tokens) of Mate

Token Total Supply: 100,000,000.00 Token | Total Token Holders: 987

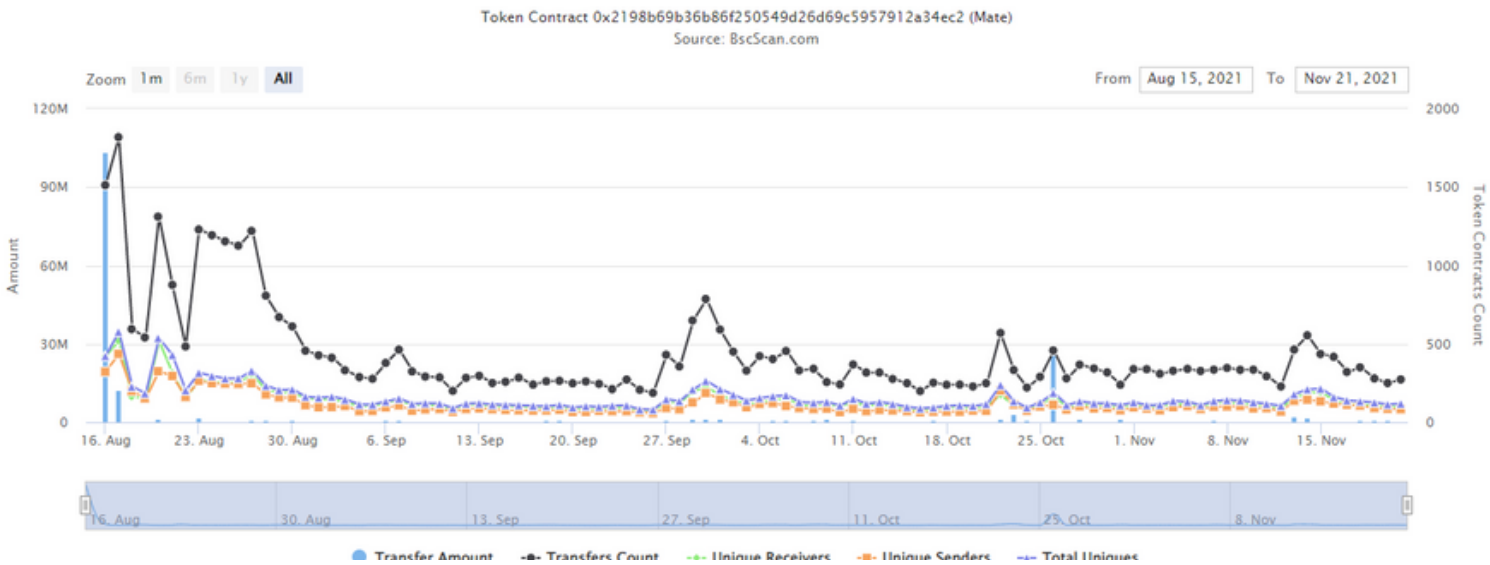


(A total of 99,640,529.87 tokens held by the top 100 accounts from the total supply of 100,000,000.00 token)

MATE TOKEN CONTRACT INTERACTION DETAILS

Time Series: Token Contract Overview

Mon 16, Aug 2021 - Sun 21, Nov 2021



MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

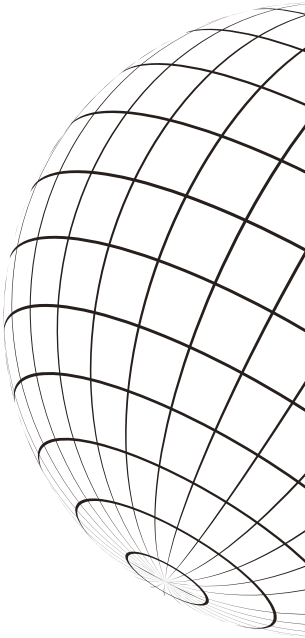
TOP 10 TOKEN HOLDERS

Rank	Address	Quantity	Percentage	Value	Analytics
1	0xbc77a4fa54e724f905b147b5b1847725acae561c	54,027,000	54.0270%	$6,741,435.03	
2	0xbca0424f5340cf36c5d8623cd2a49c3f3055ae4e	10,000,000	10.0000%	$1,247,790.00	
3	0x846c91e455ab6de4a8af273b7da694cae924ed94	8,027,679.109555169795385154	8.0277%	$1,001,685.77	
4	0xc5703e04425552b33a438674d9ff09d32ae5d494	4,800,000	4.8000%	$598,939.20	
5	0x9b637e741313d1fc28b603bec5fe3c535d47869b	3,216,616.700000000000727596	3.2166%	$401,366.22	
6	PancakeSwap V2: MATE 12	1,968,490.952409661948843424	1.9685%	$245,626.33	
7	PancakeSwap V2: MATE-BSC-USD	1,941,499.648886723742164123	1.9415%	$242,258.38	
8	0x4478686725ed2d0d9066be8e4c6a0853c52f4132	1,409,245.694703666880940174	1.4092%	$175,844.27	
9	0xaa023152df97947890d1b6f73edd7239c32375d3	949,950	0.9500%	$118,533.81	
10	0x39a1c6e184b6b6b15371f643d17be1825f316c46	581,657.5429262641830596	0.5817%	$72,578.65	

source:https://bscscan.com/

SECURITY ASSESMENT

SECURITY ISSUES



Critical Severity Issues

No high severity issues found.

High Severity Issues

No high severity issues found.

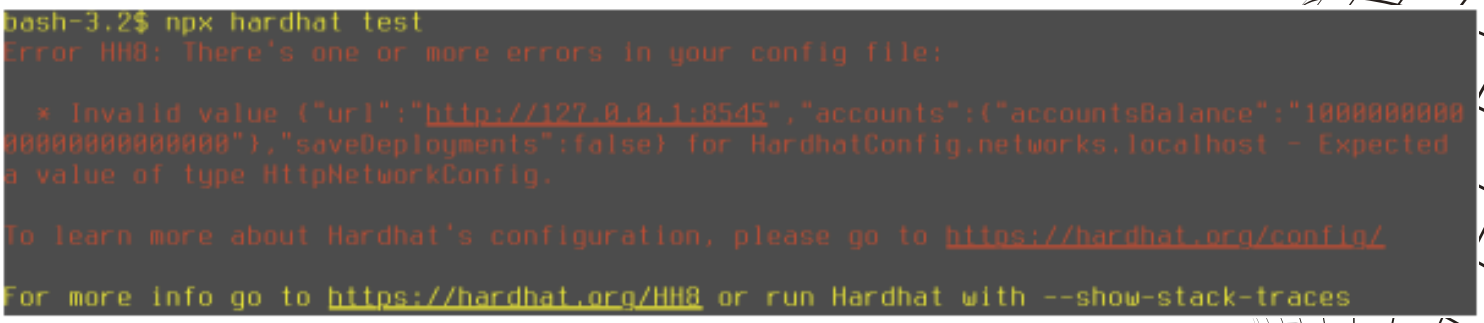
Medium Severity Issues

Tests could not be run First of all, npm install doesn't work as-is.

```
bash-3.2$ npm install
npm ERR! code ERESOLVE
npm ERR! ERESOLVE could not resolve
npm ERR!
npm ERR! While resolving: @mateproject/contracts@1.0.0
npm ERR! Found: @nomiclabs/hardhat-ethers@0.3.0-beta.10
npm ERR! node_modules/@nomiclabs/hardhat-ethers
npm ERR!   dev @nomiclabs/hardhat-ethers@"npm:hardhat-deploy-ethers" from the root project
npm ERR!
npm ERR! Could not resolve dependency:
npm ERR! dev @nomiclabs/hardhat-waffle@"^2.0.1" from the root project
npm ERR!
npm ERR! Conflicting peer dependency: @nomiclabs/hardhat-ethers@2.0.2
npm ERR! node_modules/@nomiclabs/hardhat-ethers
npm ERR!   peer @nomiclabs/hardhat-ethers@"^2.0.0" from @nomiclabs/hardhat-waffle@2.0.1
npm ERR!   node_modules/@nomiclabs/hardhat-waffle
npm ERR!     dev @nomiclabs/hardhat-waffle@"^2.0.1" from the root project
npm ERR!
npm ERR! Fix the upstream dependency conflict, or retry
npm ERR! this command with --force, or --legacy-peer-deps
npm ERR! to accept an incorrect (and potentially broken) dependency resolution.
npm ERR!
npm ERR! See /Users/helios/.npm/eresolve-report.txt for a full report.
```

After fixing package.json and successfully run npm install, we've received an error located at hardhat.config.json

SECURITY ISSUES



Recommendation: Please make sure all tests could be executed and there is a script or description of how to run them. Also, please make sure your tests are cover at least 95% of code branches.

Low Severity Issues

Tests could not be run First of all, npm install doesn't work as-is.

1. Block timestamp

   Dangerous usage of block.timestamp. block.timestamp can be manipulated by miners. Some contracts are fully related on the block.timestamp

   Contracts: UniswapHandler.sol, OrderBook.sol, MateCore.sol

   Recommendation: Please consider relying on the block.number instead

2. A public function that could be declared external

   public functions that are never called by the contract should be declared external to save gas.

   Contracts: StakingPool.sol, OrderBook.sol

   Functions: enter, leave, getOrder

   Recommendation: Use the external attribute for functions never called from the contract.

SECURITY ASSESMENT

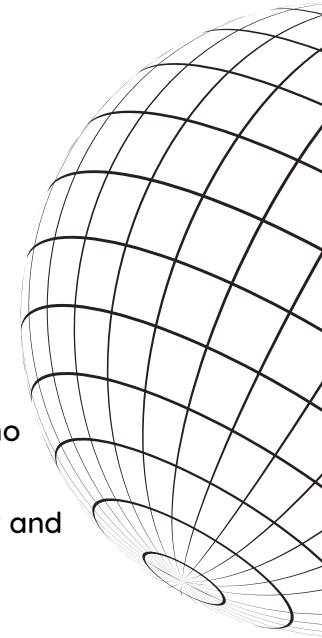
TOKEN LOGO

MOTECH AUDIT

SMART CONTRACT SECURITY AUDIT

SECURITY ASSESMENT

CONCLUSION



Smart contracts contain owner privileges!

Motech Audit note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.