FUNDAMENTAL AND TECHNICAL AUDIT

The Official MINE Token

March 5, 2022

Table of Contents

Project Details. 2

Mission Overview. 3

Design Audit 4

Top 10 Holders Overview 5

Liquidity Pool Overview. 6

Tokenomics Overview 7

Team Overview. 8

Technical Audit Overview 9

Technical Audit Details 10

Penetration Testing 11

Accepting a project audit can be viewed as a sign of confidence and is typically the first indicator of trust for a project, but it does not guarantee that a team will not remove all liquidity, sell tokens, or engage in any other type of fraud. There is also no method to restrict private sale holders from selling their tokens. It is ultimately your obligation to read through all documentation, social media posts, and contract code for each particular project in order to draw your own conclusions and define your own risk tolerance.

DRIVENsecurity accepts no responsibility for any losses or encourages speculative investments. This audit's material is given solely for information reasons and should not be construed as investment advice.

Project Details

Project Name
The Official MINE Token

Project Type
ERC20 Token

Contract Address
0x84BB61Eb0336b309Ccf14Cc68bD1888cFa4846eA

Blockchain
Ethereum

Token Name
The Official MINE Token

Token Ticker
MINE

Decimals
9

Project Website
theofficialminetoken.io

This Audit Was Created On
March 5, 2022

Mission Overview

Real-World Mission

Yes

Realizable Mission

Yes

Innovative Idea

Yes

MISSION OVERVIEW

The Official MINE Token uses investor funds to purchase and build GPU mining rigs. They are currently operating by mining ETH, but the use of GPU mining will allow this project the ability to pivot to other cryptocurrencies which an ASIC miner would not allow. Holders earn reflections on all transactions, and the liquidity pool is supported by the amount of ETH mined.

CURRENT PROGRESS

The Official MINE Token is currently on its first phase, so this is a relatively new project. The roadmap indicates there are currently three miners in operation, however their “Hall of Rigs” is showing only two mining rigs. The team indicates they are currently working on the third miner. The roadmap is based on building more miners over time to increase the amount of cryptocurrency that is earned by the project.

CONCLUSION

The Official MINE Token has a very unique concept for a project, and since they already have two rigs running, we believe their goal is mostly achievable. The team has shown forward thinking in deciding to focus on GPU mining so they can maintain flexibility when Ethereum changes to Proof of Stake. From a business model perspective, the main concerns for this project are in scalability and benefits to the investors.

In terms of scalability, because the liquidity pool is dependent on the miners, if there is a hardware failure or some other situation, this will destabilize the liquidity for the project. In order to further stabilize and grow the liquidity, more miners will be needed to reduce potential risks associated with failure points, and that is fully dependent on volume. Because of this dependency in a volatile market, there are risks to the liquidity and we recommend a back-up plan in case something catastrophic happens.

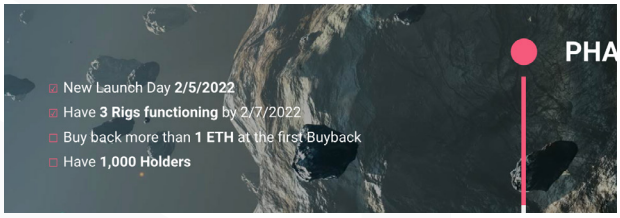
With regards to the investors, it appears the miners don’t directly benefit the holders of the token. Since the rewards from the miners are not distributed to the community, this greatly reduces the incentives for investors to want to fund the acquisition of more mining equipment. Although the stabilization of the liquidity does benefit the holders, as well as periodic buybacks of the token, this business model is similar to seed funding for a hardware company, yet there is no method of profit sharing, which would be expected in this sort of business model.

Design Audit

WEBSITE

Design Standards

For the most part, accessibility standards are not problematic on the Official Mine Token website. The use of clear imagery in the background sometimes causes some readability concerns, but overall the information is presented in a way that is legible for most users.



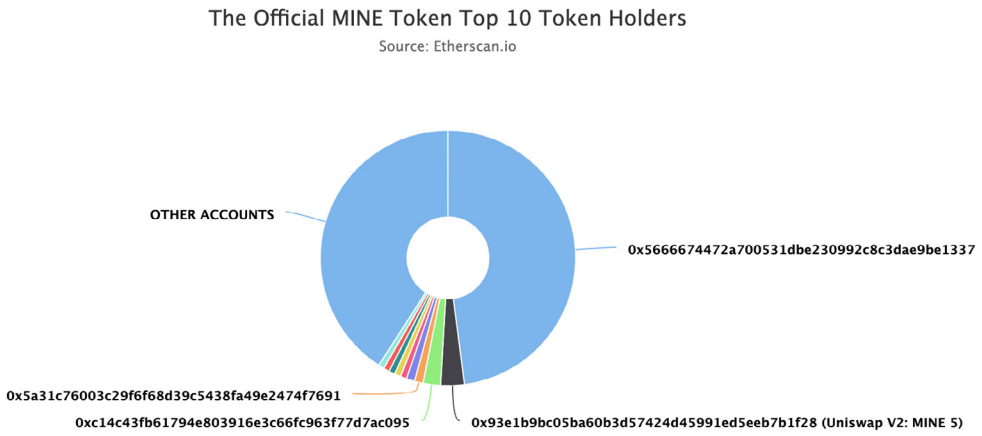
Considering the business model of this project, we feel that it would be more appropriate to leverage the brand more as a business investment than utilizing space imagery. The brand and logo mark should unify better to focus more on GPU mining than on tropes of the cryptocurrency space. The mark itself, at small sizes, takes on the appearance of an alarm clock, which is likely an unintended result.

Some more care could be taken in refinement on the site (such as the image breaking the sections between the miner and the roadmap. ***Image below***), but for the most part there are no major concerns here outside of a more formalized brand communication strategy.

SECURITY RISK ASSESSMENT: NONE

Top 10 Holders Overview

The top 10 holders collectively own 59.75% (597,530,861,917,521.00 Tokens).



1st address—Team Wallet
47.9343% of total supply.

2nd address—Uniswap V2 Liquidity Pool
3.6315% of total supply.

3rd address—Private Investor
2.2021% of the supply.

4th address—Private Investor
1.0790% of the supply.

5th address—Private Investor
1.0499% of the supply.

6th address—Private Investor
0.8050% of the supply.

7th address—Private Investor
0.8009% of the supply.

8th address—Private Investor
0.7727% of the supply.

9th address—Private Investor
0.7534% of the supply.

10th address—Private Investor
0.7242% of the supply.

CONCLUSION

The top 10 holders are in good shape overall; our only concern is the top wallet, which is managed by team members (47.9343% of the total supply). Although it is stated on the website that the wallet is locked, we discovered that it is not. We spoke with the team, and they confirmed that this is the case, ***but they also stated that they will not sell or transfer any tokens from that wallet***, which is why it is referred to as “locked”. After initial discussions, the team has made this a multi-signature wallet with multiple unique team members. Although the multi-sig wallet helps to protect this wallet from being hacked, the team still controls a large volume of the token, so we have set the risk assessment here to medum.

Liquidity Pool Overview

Liquidity locked
Yes

Locking period
5 months (06/08/2022)

Auto-liquidity function
No

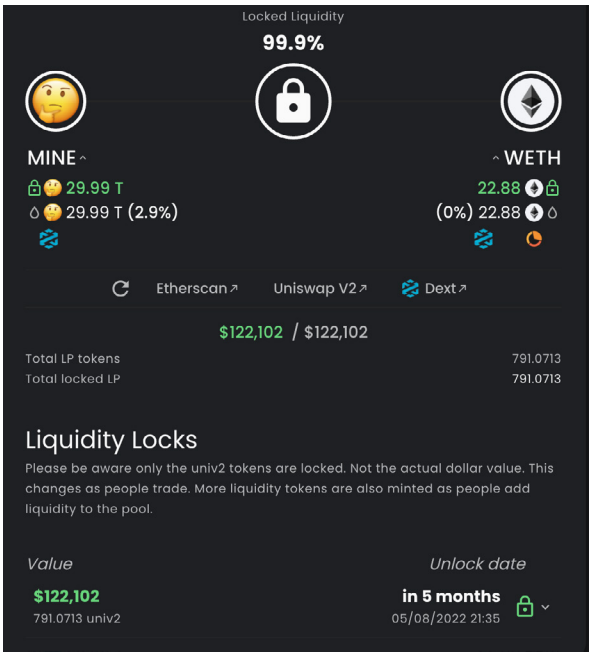
Total value locked (TVL)
$95,195 (100% of liquidity pool)

Total liquidity value
18.17 WETH

Liquidity lock platform
UniCrypt

Liquidity pool holders
1 (UniCrypt locking contract)

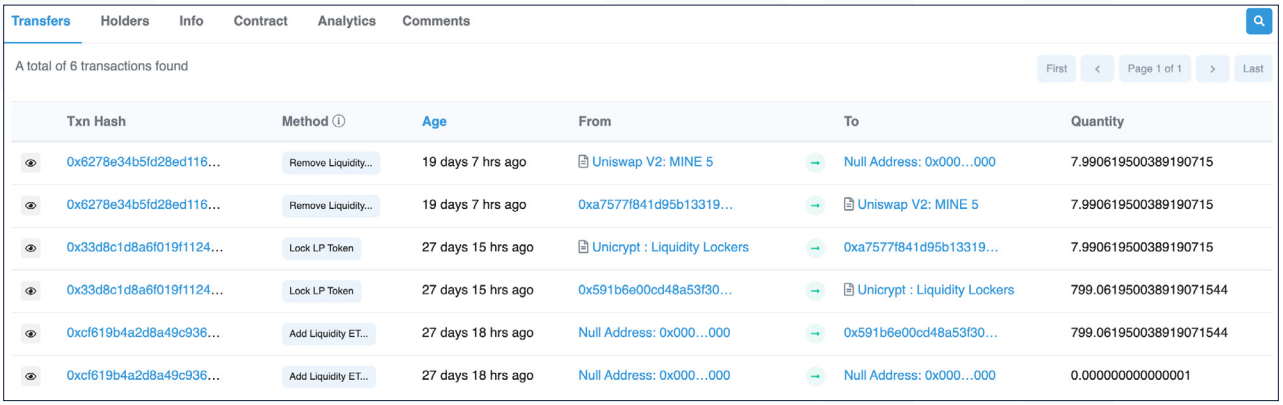
Liquidity owner
0x663a5c229c09b049e36dcc11a9b0d4a8eb9db214



Liquidity lock from UniCrypt

CONCLUSION

Developers initially added 10 ETH to the liquidity pool, which is now sitting at 18.17 ETH in the liquidity pool, with 100% of the liquidity locked for a period of 5 months. The contract does not have an auto liquidity function, but the developers claim that additional ETH will be added to the liquidity pool from the ETH mined by their mining rigs (the team indicates the first buyback will occur on March 13, 2022). In the long run, if new ETH isn't added to the liquidity pool, the token's stability may be put at risk, but for now, it's fine.



Liquidity Transactions

SECURITY RISK ASSESSMENT: LOW

Tokenomics Overview

Total supply
1,000,000,000,000,000

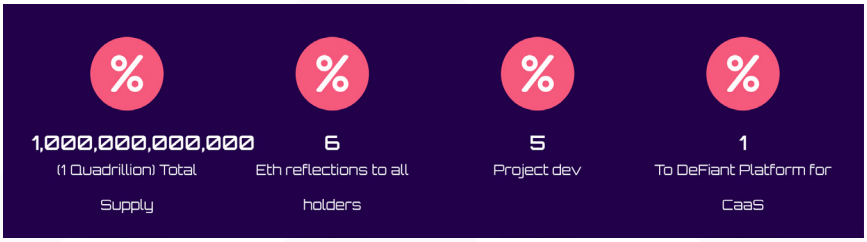
Tax applied on every transaction
Yes

Tax distribution

- 6% Reflection to holders
- 5.25% Development
- 0.75% DeFiant Platform for CaaS

Addresses that are excluded from ETH reflections:

- 0x84BB61Eb0336b309Ccf14Cc68bD1888cFa4846eA
- 0x93E1b9Bc05bA60b3D57424d45991ED5EEB7B1F28



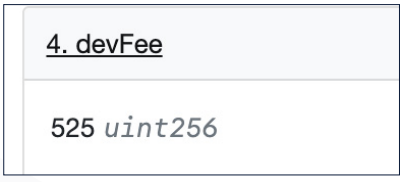
CONCLUSION

These tokenomics are definitely appealing to investors due to the large portion of tokenomics that is assigned for the distribution of ETH reflections, but we believe that 5.25% is a large amount of tax for the development and that it should be considered to be reduced in the future, as the contract is still under developer ownership. We believe that the contract is missing an auto liquidity function, which could cause issues in the long run if developers are unable to generate enough ETH for a liquidity pool by mining with their rigs.

The top wallet, which holds 47.9343% of the token supply, is not excluded from ETH reflections, which means that 47% of the total ETH reflection pool is going to the top wallet. Our recommendation is to exclude this wallet from reflections so that token holders can benefit more from holding The Official MINE Token.

The important thing to note is that tax is applied to all transactions, which means that tax will be applied even if you move your tokens from one wallet to another.

It's also worth noting that the smart contract's development fee is set at 5.25 %, but the website reports it as a 5% fee. The team has indicated this is done for simplicity on the website.



Dev Fee set to 5.25% in contract

SECURITY RISK ASSESSMENT: LOW

Team Overview

Core Team Members
5

Doxxed Team
Doxxed to us but not publicly doxxed

Existing AMAs
Yes

Team members have previous experience:
The team members have experience with other projects both inside and outside of the MCU ecosystem (in which The Official MINE Token resides).

CONCLUSION

The Official MINE Token team is not publicly doxxed, but they decided to doxx us without hesitation. We verified their identification, so if they make any fraudulent moves that harm investors, we will make their identification public. This is not an uncommon practice for some development teams.

Technical Audit Overview

GENERAL ISSUES

- Security issues: **PASSED**
- Gas & Fees issues: **PASSED**
- ERC errors: **PASSED**
- Compilation errors: **PASSED**
- Design logic: **PASSED**
- Timestamp dependence: **PASSED**
- Buy & sell: ***The owner cannot enable/disable swapping for certain users***

SECURITY AGAINST CYBER ATTACKS

- Private user's data: **SECURED**
- Reentrancy: **SECURED**
- Cross-function Reentrancy: **PASSED**
- Front Running: **PASSED**
- Taxonomy attacks: **PASSED**
- Integer Overflow and Underflow: **PASSED**
- DoS (Denial of Service) with Unexpected revert: **PASSED**
- DoS (Denial of Service) with Block Gas Limit: **PASSED**
- Insufficient gas griefing: **PASSED**
- Forcibly Sending ETH to a Contract: **PASSED**

Technical Audit Details

IMPORTANT VARIABLES

Fees:

- rewardsFee: 6%
- launchSellFee: 8% (available for 3 days after launch)
- devFee: 5.25%

Fee receivers

- _platformWalletAddress: 0xDfA14c05571bb126BFaF7e3E87BA375e7690dbb0
- _devWalletAddress: 0x579d8da6a0efc9d99E4Ae9551D2d550ac3Adec1d

Control on Transactions/Rewards

- excludeFromFees (function) - exclude address from paying fees;
- excludeFromRewards (function) - exclude address from receiving rewards;
- includeInFee (function) - include address in paying fees;
- includeInRewards (function) - include address in receiving rewards;
- setMaxTxPercent (function) - set the max amount that is allowed in one transfer;

Control on Fees

- setFees (function with “newDevFee” and “newRewarsFee” as arguments) - set the fees that are paid in transactions;
- setLaunchSellFee (function) - set the sell fee for people that sell on launch day + 3 days;
- setUseGenericTransfer (function) - this function set the “useGenericTransfer” to True or False. When it’s settled to true, there are not fees on transfers;

Set Fee Receivers

- setDevWallet;
- _platformWalletAddress: 0xDfA14c05571bb126BFaF7e3E87BA375e7690dbb0 is hardcoded in the Smart Contract and can’t be changed;

Booleans

- swapAndRedirectEthFeesEnabled - when this variable is seated to true, the transfers have applied fees;
- currentlySwapping - used in the modifier as a mutex to avoid re-entrancy attacks;

Modifiers

- lockTheSwap;

The following functions have this modifier:

- swapAndRedirectEthFees;

CONCLUSION AND RECOMMENDATIONS:

The logic of the smart contract is well-designed. There are no errors or hidden issues.

Penetration Testing

RE-ENTRANCY

What is Re-Entrancy?

A re-entrancy attack can arise when you write a function that calls another untrusted contract before resolving any consequences. If the attacker has authority over the untrusted contract, he can initial a recursive call back to the original function, repeating interactions that would otherwise not have occurred after the effects were resolved.

Attackers can take over the smart contract's control flow and make modifications to the data that the calling function was not anticipating.

To avoid this, make sure that you do not call an external function until the contract has completed all of the internal work.

TEST: PASSED

CROSS-FUNCTION RE-ENTRANCY

What is Cross-Function Re-Entrancy?

When a vulnerable function shares the state with another function that has a beneficial effect on the attacker, this cross-function re-entrancy attack is achievable. This re-entrancy issue that is the employment of intermediate functions to trigger the fallback function and a re-entrancy attack is not unusual.

Attackers can gain control of a smart contract by calling public functions that use the same state/variables as "private" or "onlyOwner" functions.

To avoid this, make sure there are no public functions that use private variables, and avoid calling routines that call external functions or use mutex (mutual exclusion).

TEST: PASSED

PENETRATION TESTING (CONTINUED)

FRONT RUNNING

What is Front Running?

Front running indicates that someone can obtain prior information of transactions from other beneficial owners by technology or market advantage, allowing them to influence the price ahead of time and result in economic benefit, which usually results in loss or expense to others

Since all transactions are visible in the block explorer for a short period of time before they are executed, network observers can see and react to an action before it is included in a block.

Attackers can front run transactions because every transaction is visible to the blockchain, even if it is in the “processing” or “indexing” state. This is a very low security vulnerability because it is based on the blockchain rather than the contract.

The only possible attack is seeing transactions made by bots. Using transaction fees, you can avoid bots.

TEST: PASSED

TAXONOMY ATTACKS

These taxation attacks can be made in 3 ways:

1. Displacement

Performed by increasing the gasPrice higher than network average, often by a multiplier of 10.

2. Insertion

Outbidding transaction in the gas price auction

3. Suppression (Block Stuffing)

The attacker sent multiple transactions with a high gasPrice and gasLimit to custom smart contracts that assert to consume all the gas and fill up the block’s gasLimit.

This type of attack occurs mainly for exchanges, so this smart contract is secured

TEST: PASSED

PENETRATION TESTING (CONTINUED)

INTEGER OVERFLOW AND UNDERFLOW

Overflow

An overflow occurs when a number gets incremented above its maximum value.

In the audited contract: uint8 private _decimals = 9;

(_decimals can't reach a value bigger than it's limit)

TEST: PASSED

Underflow

An overflow occurs when a number gets decremented below its maximum value.

(There are no decrementation functions for parameters and users can't call functions that are using uint values);

TEST: PASSED

Conclusion

This contract uses the updated version of SafeMath for Solidity 0.8 and above that will prevent Integer Overflows and Underflows.

DOS (DENIAL OF SERVICE) WITH UNEXPECTED REVERT

DoS (Denial of Service) attacks can occur in functions when you attempt to transmit funds to a user and the functionality is dependent on the successful transfer of funds.

This can be troublesome if the funds are given to a bad actor's smart contract (when they call functions like "Redeem" or "Claim"), since they can simply write a fallback function that reverts all payments.

There are no functions that deliver money to users (ACCEL Defi team is using 3rd party/external contracts in order to do that), so attackers are unable to communicate using a contract with fallBack functions.

TEST: PASSED

PENETRATION TESTING (CONTINUED)

DOS (DENIAL OF SERVICE) WITH BLOCK GAS LIMIT

Each block has an upper bound on the amount of gas that can be spent, and thus the amount of computation that can be done. This is the Block Gas Limit. If the gas spent exceeds this limit, the transaction will fail. This leads to a couple possible Denial of Service vectors.

TEST: PASSED

INSUFFICIENT GAS GRIEFING

This attack can be carried out against contracts that accept data and use it in a sub-call on another contract.

This approach is frequently employed in multisignature wallets and transaction relayers. If the sub-call fails, either the entire transaction is rolled back or execution is resumed.

TEST: PASSED—USERS CAN'T EXECUTE SUB-CALLS.

FORCIBLY SENDING ETH TO THE SMART CONTRACT

TEST: PASSED

This audit was created by

Accepting a project audit can be viewed as a sign of confidence and is typically the first indicator of trust for a project, but it does not guarantee that a team will not remove all liquidity, sell tokens, or engage in any other type of fraud. There is also no method to restrict private sale holders from selling their tokens. It is ultimately your obligation to read through all documentation, social media posts, and contract code for each particular project in order to draw your own conclusions and define your own risk tolerance.

DRIVENsecurity accepts no responsibility for any losses or encourages speculative investments. This audit's material is given solely for information reasons and should not be construed as investment advice.