



international crypto services agency

SMART CONTRACT

Security Audit Report



international crypto services agency

Project

MINETHEREUM



Audit Details

Project: MINETHEREUM

Blockchain: Ethereum

Project website:
Minethereum – ETH Miner

Authors: ICSA Audit team

Date: January 6th, 2023



Disclaimer

ICSA audits and reports should not be considered as a form of project's "advertisement" and does not cover any interaction and assessment from "project's contract" to "external contracts" such as Pancakeswap or similar.

ICSA does not provide any warranty on its released reports.

ICSA should not be used as a decision to invest into an audited project please do your own research. ICSA provides transparent reports to all its "clients" and to its "clients,participants" and will not claim any guarantee of bug-free code within its SMART CONTRACT.

ICSA presence is to analyze, audit and assess the client's smart contract's code. Each company or project shall be liable for its own security flaws and functionalities.

Scope of Work & Background

The main scope of this report/audit, is to document an accurate assessment of the condition of the smart contract and whether it has any security flaws in the implementation of the contract.

MINETHEREUM team agreed and provided us with the files that needed to be tested (Through Github, Etherscan, files, etc.). ICSA will be focusing on contract issues and functionalities along with the projects claims from smart contract to their website, whitepaper and repository where available, which has been provided by the project. Code is reviewed manually and with the use of software using industry best practices.

Background

ICSA was contracted by **MINETHEREUM** team to perform the security audit of the smart contract code:

- Contract Address **0xcfb305431FAA9575aFbcA68bBd31f9bCfC213Be3f**

The purpose of the audit was to achieve the following:

- Ensure that the claimed functions exist and function correctly.
- Identify any security vulnerabilities that may be present in 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.

Project Description from Dev's
Minethereum, the most robust and advanced
Ethereum miner to date. Enjoy up to 8% daily
returns, and 12% referral.

Social Media Links

Telegram: <https://t.me/minethereum>

Twitter: <https://twitter.com/Minethereumtech>

Medium:
<https://medium.com/@minethereum/minethereum-eth-miner-1a38abd7669a>

Facebook: N/A

Discord: N/A

Contracts details

Contract details for January 6th, 2023

Contract/Project name: MINETHEREUM

Description: Mining Dapp Contract

Compiler version: 0.8.17

Contract address: 0xcf305431FAA9575aFbcA68bBd31f9bCfC213Be3f

Contract deployer address: 0x21111041f4BDEBE8Bda7C8ABeC77b09d16E1FC7D

Contract's current owner address: 0x21111041f4BDEBE8Bda7C8ABeC77b09d16E1FC7D

Dev's KYC: Yes ICSA

Contract write functions details

Owner privileges:

Contract contains owner control, which does not make it fully decentralised , the owner has privileges, and has authority to make any changes now.



Centralization

This smart contract has some functions which can be executed by the Admin (Owner) only. . Following are Admin functions:

1. `buyEggs`
2. `hatchEggs`
3. `renounceOwnership`
4. `seedMarket`
5. `sellEggs`
6. `transferOwnership`

To make the smart contract 100% decentralized, we suggest renouncing ownership in the smart contract once its function is completed.

SWC Registry: Smart Contract Weakness/Vulnerabilities

<u>SWC-136</u>	Unencrypted Private Data On-Chain	PASSED
<u>SWC-135</u>	Code With No Effects	PASSED
<u>SWC-134</u>	Message call with hardcoded gas amount	PASSED
<u>SWC-133</u>	Hash Collisions with Multiple Variable Length Arguments	PASSED
<u>SWC-132</u>	Unexpected Ether balance	PASSED
<u>SWC-131</u>	Presence of unused variables	PASSED
<u>SWC-130</u>	Right-To-Left-Override control character (U+202E)	PASSED
<u>SWC-129</u>	Typographical Error	PASSED

<u>SWC-128</u>	DoS With Block Gas Limit	PASSED
<u>SWC-127</u>	Arbitrary Jump with Function Type Variable	PASSED
<u>SWC-126</u>	Insufficient Gas Griefing	PASSED
<u>SWC-125</u>	Incorrect Inheritance Order	PASSED
<u>SWC-124</u>	Write to Arbitrary Storage Location	PASSED
<u>SWC-123</u>	Requirement Violation	PASSED
<u>SWC-122</u>	Lack of Proper Signature Verification	PASSED
<u>SWC-119</u>	Shadowing State Variables	PASSED

<u>SWC-118</u>	Incorrect Constructor Name	PASSED
<u>SWC-120</u>	Weak Sources of Randomness from Chain Attributes	PASSED
<u>SWC-117</u>	Signature Malleability	PASSED
<u>SWC-116</u>	Block values as a proxy for time	LOW ISSUE
<u>SWC-115</u>	Authorization through tx.origin	PASSED
<u>SWC-114</u>	Transaction Order Dependence	PASSED
<u>SWC-121</u>	Missing Protection against Signature Replay Attacks	PASSED
<u>SWC-113</u>	DoS with Failed Call	MEDIUM SEVERITY

<u>SWC-112</u>	Delegatecall to Untrusted Callee	PASSED
<u>SWC-111</u>	Use of Deprecated Solidity Functions	PASSED
<u>SWC-110</u>	Assert Violation	PASSED
<u>SWC-109</u>	Uninitialized Storage Pointer	PASSED
<u>SWC-108</u>	State Variable Default Visibility	PASSED
<u>SWC-107</u>	Reentrancy	PASSED
<u>SWC-106</u>	Unprotected SELFDESTRUCT Instruction	PASSED
<u>SWC-105</u>	Unprotected Ether Withdrawal	PASSED

<u>SWC-104</u>	Unchecked Call Return Value	PASSED
<u>SWC-103</u>	Floating Pragma	PASSED
<u>SWC-102</u>	Outdated Compiler Version	PASSED
<u>SWC-101</u>	Integer Overflow and Underflow	PASSED

MythX passing

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

Medium severity = Medium-level vulnerabilities are more important; however, they can't lead to tokens loss

SOLHINT LINTER, Solidity Static Analysis using REMIX IDE did not find any serious issues.

Issue Checking

Manual code review is satisfactory. Although we have flagged a Medium severity issue we do not believe that will cause token loss or other problems with this particular contract.

CLOSING NOTES

Investors Advice: Technical audit of the smart contract does not guarantee the ethical nature of the project. Any owner controlled functions should be executed by the owner with responsibility. All investors/users are advised to do their due diligence before investing in the project.

Always make sure to always inspect all values and variables.

This includes, but is not limited to: • Ownership • Proper Ownership Renouncement (if any) • Any other owner-adjustable settings or variables.

OVERALL ASSESSMENT

SATISFACTORY