SOLIDITY AUDIT

MECHA NFT MINING

“0xbdc7a55C0141AB451C53ef74dBf0413233b6Eba3”

Contents

Project Information

Project Name: MECHA NFT MINING

Network: POLYGON MATIC

Contract Address:
0xbdc7a55C0141AB451C53ef74dBf0413233b6Eba3

Type: NFT MINING

Max amount: 300 MATIC

Min amount: 10 MATIC

Dev fee: 5%

Owner fee: 5%

Withdraw fee: 0%

Withdraw system:

Plan 1,2,3 – Withdraw Anytime

Plan 4,5,6 – Unlocked 20 Days

Referral: 5%, 3%, 1%

Withdraw referral: Automatic

Max Referral: Unlimited

Reward system: Daily from 6.5%-9%

Bonus Reward: 0.1 – 1%

Scope of Audit

The scope of this audit was to analyze and document the Mecha NFT Mining smart contract codebase for quality, security, and correctness. Any error or incorrect will fixed by our team.

Check Vulnerabilities

We scanned and check those commonly known and specific vulnerabilities base on the solidity code of the project. Here are some of the commonly known vulnerabilities that we considered.

- **Compiler**
- **Struct**
- **Plan**
- **Functions**
- **Users Checkpoint**
- **Timestamp**
- **Gas Limit and Loops**
- **Byte array**
- **Backdoor**
- **Transfer forward**
- **Redundant fallback**

Issue Categories

Every issue in this report has been assigned to a severity level. There are four levels of severity, and each of them has been explained below.

Risk-level	Description
High	A high severity issue or vulnerability means that your smart contract can be exploited. Issue on this level is critical to the smart contract's performance of functionality and we recommended these issues be fixed before moving to the public.
Medium	The issues marked as medium severity usually arise because of errors and deficiencies in the smart contract code. Issues on his level could potentially bring problems, and they should still be fixed.
Low	Low level severity issues can cause minor impact and or are just warnings that can remain unfixed for now. It would be better to fix these issues at some point in the future.
Informational	These are severity issues that indicate an improvement request, a general question, a cosmetic or documentation error, or a request for information there is a lot-to-no-impact.

Number of issues per severity

Type	High	Medium	Low	Informational
Open	0	0	0	0
Acknowledge	0	0	2	1
Closed	0	0	2	1

Transaction Code

There are few transactions code base of the smart contract of this project. Each transaction will be written on the blockchain, and no one can be manipulated or change.

1. Launch

```
87      function launch() public {
88          require(msg.sender == developerWallet);
89          startUNIX = block.timestamp;
90
91
92      }
```

2. Mint / Invest

```
94
95      function invest(address payable referrer,uint8 plan) public payable {
96          _invest(referrer, plan, msg.sender, msg.value);
97
98      }
99
100
101     function _invest(address payable referrer, uint8 plan, address payable sender, uint256 value) private {
102         require(value >= INVEST_MIN_AMOUNT);
103         require(plan < 6, "Invalid plan");
104         require(startUNIX < block.timestamp, "contract hasn`t started yet");
105
```

3. Withdraw

```
167
168     function withdraw() public {
169         User storage user = users[msg.sender];
170
171         uint256 totalAmount = getUserDividends(msg.sender);
172
```

Overall function transaction will be seen at write contract overview. No backdoor or further function can cause of draining the contract.

1. **Launch**
2. **Mint / Invest**
3. **Withdraw**

Compiler Test

Compiled and tested under 3rd party solidity compiler.

0.5.8+commit.23d335f2	SUCCESS
No Warning Detected	SUCCESS
Compiled Success	SUCCESS

Contract Testing

Contract deployed and tested with our team before we released the audited report.

Network:

Polygon Testnet Mumbai

Deployed:

08.08.22

Contract Link:

https://mumbai.polygonscan.com/address/0x2D480cC3bbf57B7fA10c8bf0dd66Df14FAdfc845

Result

No major issue was found. Some false positive errors were reported by the tool. All the other issues have been categorized according to their level of severity, team improved and fixed it before the publicity of the project.

Closing Summary

Overall, smart contract is very well written and adhered to guidelines. Minor issues were discovered during the audit has been fixed.