Smart Contract Audit TrxEcology

Revision 1 dated 12.10.2020

Contents

Brief information

Project: tronecology.com
Web: TRON
Compiler version: 0.5.9
Optimization: enabled
The audit date: 12.10.2020

Information

The contract code was reviewed and analyzed for vulnerabilities, logical errors, and the developers' exit scams possibility. This work was carried out concerning the project source code provided by the customer.

During the audit, warning was discovered that do not directly affect the funds' safety.

The detected problems full list can be found below.

General conclusion

As the audit result, 1 warning was revealed that did not affect the users' funds security on the contract. The exit scam clear signs - not found.

Telescr.in guarantees the TrxEcology contract security and performance.

Liability disclaimer

The telescr.in team within this audit framework is not responsible for the developers or third parties' actions on the platforms associated with this project (websites, mobile applications, and so on). The audit confirms and guarantees only the smart contract correct functioning in the revision provided by the project developers (check the revision).

Confirmed by digital signature

Aggregated data

The Contract analysis was performed using the following methods:

- Static analysis
  - o Checking the code for common errors leading to the most common vulnerabilities
- Dynamic analysis
  - o The Contract launching and carrying out the attacks various kinds to identify vulnerabilities
- Code Review

Received data

Recommendation	Type	Priority	Occurrence probability
Overflow Probability	Warning	Average	Low

A. Errors

Not found

B. Remarks

Not found

C. Warnings

1. Overflow Probability

The smart contract does not use the SafeMath library for calculations. Even though the overflow probability during calculations in this method is minuscule, the general recommendation is to use SafeMath for such calculations.

Application. Error classification

Priority	
informational	This question is not directly related to functionality but may be important to understand.
low	This question has nothing to do with security, but it can affect some behavior in unexpected ways.
Average	The problem affects some functionality but does not result in an economically significant user funds loss.
high	This issue can result in the user funds loss.
Probability	
Low	It is unlikely that the system is in a state in which an error could occur or could be caused by any party.
Average	This problem may likely arise or be caused by some party.
high	It is highly likely that this problem could arise or could be exploited by some parties.

Application. Digital bytecode print

The audit was carried out for the code certain version on the compiler version 0.5.9 with the optimization enabled.

To check the contract bytecode for identity to the one that was analyzed during the audit, you must:
1. Get contract bytecode (in any block explorer)
2. Get SHA1 from bytecode string
3. Compare with reference in this report

Sha1 from bytecode:
                5db8307a6f8f38735804f1e22660105bc5f89eaf
Sha1 from bytecode (non-metadata):
                a8eb576f4da189327e99387f643645ec442978c1
Contract address:
                TX1AXMHFqDcryC793xQjU2nyHSWdsGwzGu

Check the digital print

Application. Signature of the audit report

{
  "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
  "msg": "As the audit result, 1 warning was revealed that did not affect the users' funds security on the contract. The exit scam clear signs - not found. Telescr.in guarantees the TrxEcology contract security and performance. Sha1 from bytecode: 5db8307a6f8f38735804f1e22660105bc5f89eaf Sha1 from bytecode (non-metadata): a8eb576f4da189327e99387f643645ec442978c1 Contract address: TX1AXMHFqDcryC793xQjU2nyHSWdsGwzGu",
  "sig": "0xde645c77c52fe3ae9c30862faa625c6c1413452ea5ec8846e6e150e1fb7150f027c189392584cb0e10448c14dec9fdf2e0ed1f4dbb70c68d200011dc8c9636561c",
  "version": "3"
}

Check the signature