

TRONexWorld contract audit

Revision 3 of 10.28.2020

Table of contents

TRONexWorld contract audit	1
Table of contents	2
Brief information	3
Data	3
General conclusion	3
Liability disclaimer	3
Aggregated data	4
Received data	4
A. Errors.....	4
B. Remarks.....	4
C. Improvements.....	4
Appendix. Error classification	5
Appendix. Bytecode hash sum	6
Appendix. Audit summary signature	7

Brief information

Project: tronex.world
Web: TRON
Compiler version: 0.5.10 + commit.a1d534e
Optimization: enabled
The audit date: 10.28.2020

Data

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.

The audit revealed:

- Logical error
- The discrepancy between declared and actual behaviour
- Other comments

The detected problems full list can be found below.

General conclusion

As the audit result is contract without errors and comments. There was no exit scam obvious signs (*exit scam - a situation in which contract developers have controlled access to participants' funds and can perform withdrawal operations without their knowledge*). No bugs or security breach were found either.

Telescr.in guarantees the TRONexWorld 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](#)).

[Digitally signed.](#)

Aggregated data

The Contract analysis was performed using the following methods:

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

Received data

Recommendation	Type	Priority	Occurrence probability
Not found			

A. Errors

No errors were found.

B. Remarks

The code improvements recommended in the previous revision have been applied by the developers in this revision.

C. Improvements

The code improvements recommended in the previous revision have been applied by the developers in this revision.

Appendix. Error classification

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

Appendix. Bytecode hash sum

The audit was carried out for the code certain version on the compiler version 0.5.10 + commit.a1d534e with the optimization enabled.

To check the contract bytecode for identity to the one that was analysed 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:

16a39493c3747483dcedf703e5907b68b8c2ab6a (no metadata)

ceb835f4d3e899892e2bea3e1c60eba39b71a307 (with metadata)

address: TYQwgKgKGnZ7Ja4JR2b7hs7hLQbXn84oNY

[Check hash sum](#)

Appendix. Audit summary signature

```
{
  "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
  "msg": "As the audit result is contract without errors and comments.
There was no exit scam obvious signs (exit scam - a situation in which
contract developers have controlled access to participants' funds and can
perform withdrawal operations without their knowledge). No bugs or
security breach were found either. Telescr.in guarantees the TRONexWorld
contract security and performance. Actual for bytecode with sha1:
16a39493c3747483dcedf703e5907b68b8c2ab6a (no metadata),
ceb835f4d3e899892e2bea3e1c60eba39b71a307 (with metadata), address:
TYQwgKgKGnZ7Ja4JR2b7hs7hLQbXn84oNY",
  "sig":
"0x44deaad5c2a3f5472240d5cf4fc8b9e39fa50f782ccc8b3122b2a4f573cdec4678832e0
808fd83cda2bbb1666178a406f2399ec21a55af9f0d5e5e33e03cd69c1c",
  "version": "3"
}
```

[Check signature](#)