The TRONSTACK smart contract audit

Revision 2 dated 11.11.2020

Table of contents

Brief information

Project: tronstack.org
Web: TRON
Compiler version: 0.5.12
Optimization: enabled
The audit date: 11.11.2020

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.

The audit revealed:
- Logical error
- The discrepancy between declared and actual behavior
- Other comments

The detected problems full list can be found below.

General conclusion

As a result of the audit, one user warning was found, which does not affect security of funds on the contract. The exit scam clear signs - not found.

Telescr.in guarantees the TRONSTACK 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
    - 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
User warning	Warning	Informational	High

A. Errors

Not found

B. Notes

Not found

C. Warnings

1.   User warning

The investor should pay attention to the fact that he can make a maximum of 19 withdrawals, after which the user goes into the **inactive** state and further withdrawal becomes impossible.

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 0.5.12 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 (non-meta data):
                  a9fed808eacefdfdd02aaec892203aefc64cc8ac
Sha1 from bytecode (with metadata):
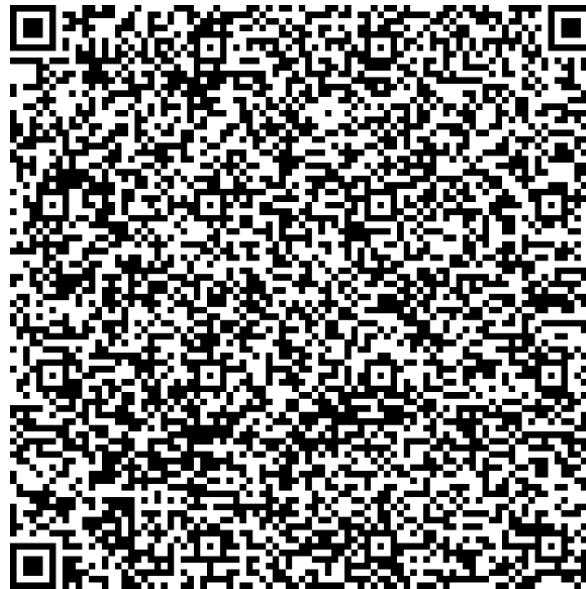   6ea6d99512234c38b904f723ce809d604847d3f3
Contract address:
                  TTpFPkjtAV9J1CA8cgxtjQ8aEorJXN2fSN

Check the digital print

Application. Digital bytecode print

Application. Signature of the audit report

{
    "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
    "msg": "As a result of the audit, one user warning was found, which does not affect security of funds on the contract. The exit scam clear signs - not found. Telescr.in guarantees the TRONSTACK contract security and performance. Sha1 from bytecode (non-meta data): a9fed808eacefdfdd02aaec892203aefc64cc8ac Sha1 from bytecode (with metadata): 6ea6d99512234c38b904f723ce809d604847d3f3 Contract address: TTpFPkjtAV9J1CA8cgxtjQ8aEorJXN2fSN",
    "sig": "0x12497d8b302e429253016e37bc30ae9804dfb897bda6f4978a8083534b64c98503db8b9044c3a6f3853f1a9e3b6fa56faa2de4356713ca9e8a933037418be8451c",
    "version": "3"
}

Check the signature