Audit of smart contracts UltronCash

Revision 2 dated 03.25.2021

Contents

Brief information

Project: UltronCash
Network: TRON
Compiler version: ^0.6.12
Optimization: enabled
The audit date: 03.25.2021

Information

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

During the audit neither errors that can affect the security of funds nor exit scam possibility was detected.

General conclusion

As a result of the audit, no errors were found that affect the security of users' funds on the contract. No obvious signs of an exit scam were found. No backdoors found either.

Telescr.in guarantees the safety and performance of the UltronCash contract.

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.

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	Probability of occurrence	Line
Decreasing of withdrawing value	Notice	Low	N/a	205

A. Errors

Not found in this revision.

B. Warnings

Not found in this revision.

C. Notice

1. Decreasing of withdrawing value

Line 205
When toSend > savingPool then less trx will be sent to the user. But the old value of toSend was already set as withdrawn of deposits.

D. Remarks

Not found.

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 ^0.6.12 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:
      be218a13224dc81763b23d2b82e2a698583ee690 - UltronCashTrx
      c70756b477966081139b89ae847376d2e73cb441 - UltronCashBtt
Sha1 from bytecode (non-metadata):
      eeb545f48469fb7c43080f03420a797963571050 - UltronCashTrx
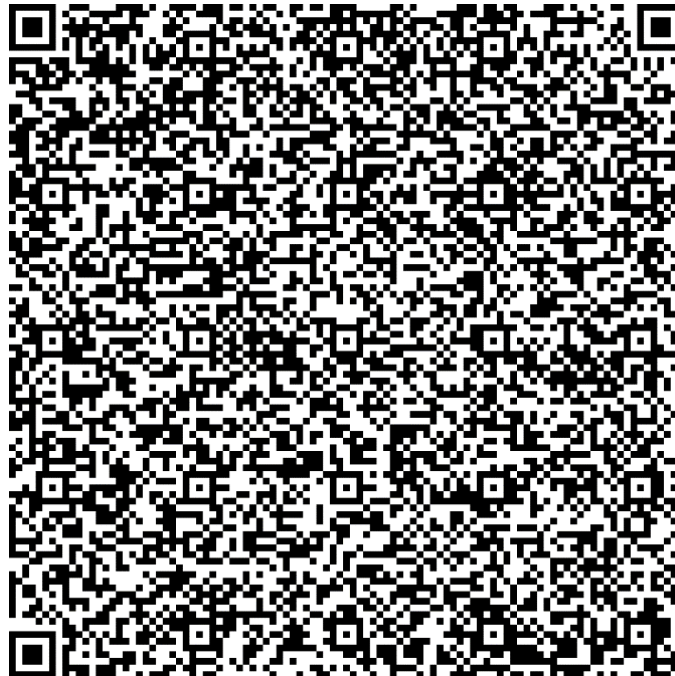   cc3e38baae37c6279cbba7352e74e3ddc4119b68 - UltronCashBtt
Contract address:
      TJLoSAT7h5HZmptHx3VZxjm93qZhPkMHUQ - UltronCashTrx
      TMbbYAvr5YaxJYjov8v77U1QARLcdwLhCv - UltronCashBtt

Check the digital print

Application. Signature of the audit report

{
    "address": "0x505ade8cea4db608250e503a5e8d4cb436044d2e",
    "msg": "As a result of the audit, no errors were found that affect the security of users' funds on the contract. No obvious signs of an exit scam were found. No backdoors found either. Telescr.in guarantees the safety and performance of the UltronCash contract. Sha1 from bytecode: be218a13224dc81763b23d2b82e2a698583ee690 - UltronCashTrx c70756b477966081139b89ae847376d2e73cb441 - UltronCashBtt Sha1 from bytecode (non-metadata): eeb545f48469fb7c43080f03420a797963571050 - UltronCashTrx cc3e38baae37c6279cbba7352e74e3ddc4119b68 - UltronCashBtt Contract address: TJLoSAT7h5HZmptHx3VZxjm93qZhPkMHUQ - UltronCashTrx TMbbYAvr5YaxJYjov8v77U1QARLcdwLhCv - UltronCashBtt",
    "sig": "0x00907b2ba8fa2a8dc54c1a55de040abf8cf418ba38f1cc9252375bd5df999d46214a7c96d96eac664b0cd3ae71aeb2c22b40e582c923aa6e7110afe834818aee1c",
    "version": "3"
}

[Check the signature](#)