Smart Contract Audit TokenField

Revision 1 dated 12.18.2020

Contents

Brief information

Project: tokenfield.io
Network: ETHEREUM
Compiler version: 0.7.0
Optimization: enabled
The audit date: 12.18.2020

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, no errors were found that could affect the security of the funds.

The detected problems full list can be found below.

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.

Telescr.in guarantees the TokenField 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**
Not found			

A. Errors

Not found

B. Remarks

Not found

C. Warnings

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 0.7.0 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:
abf23202e2ea8ce28fab4e1ae182a814ccd12a27
Sha1 from bytecode (non-metadata):
d8ec57a64354ec8f2f7ee13a64b636854d5fb20f
Contract address:
0x43f816682850B1e7AC8b075aa1Bd2BA309ACF5c9

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. Telescr.in guarantees the TokenField contract security and performance. sha1 bytecode: abf23202e2ea8ce28fab4e1ae182a814ccd12a27 sha1 bytecode
        (no meta): d8ec57a64354ec8f2f7ee13a64b636854d5fb20f contract address: 0x43f816682850B1e7AC8b075aa1Bd2BA309ACF5c9",
          "sig": "0x2ede1af199c45102b5f069592bc090cbb4b7215d1309f6430f5fec00796d0f123090de2c95db725915810dda6762c7b28c66caf3adf670eff8c9f5cd2794c14b1b",
          "version": "3"
}
```

Check the signature