Telescr.in

Audit of smart contract DPTToken

revision 1 dated 15.09.2021

Telescr.in

Summary

Brief information

Project: DPTToken
Network: BSC
Compiler version: 0.8.7
Optimization: Enabled
Audit date: 15.09.2021

Information

The contract code was reviewed and analysed 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.

Customer did not provide a separate technical document, the audit was carried out only on the source code

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 guarantee the safety and performance of the contract DPTToken

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	Occurrence probability	Line of error
An extra restrictions	notice	low		487, 421, 417, 422, 427, 432, 438, 444, 451, 456, 563
Probably too strong restrictions	notice	low		413
Unexpected transfer to zero-address	warning	low	low	539
Implicit access modifier	notice	low	low	

A. Errors

Not found.

B. Warnings

1. Unexpected transfer to zero-address

Transfered amount adds to address(0) without an obvious reason. If it's desired behaviour it must be described in comments.

C. Notice

1. An extra restrictions

There in no need to check whether the sender is owner since it's already checked on the onlyOwner modifier.

2. Probably too strong restrictions

onlyOwner motifier on getter functions seems as too strong and useless as well restriction because data can be read from the blockchain anyway.

Recomendation: remove the modifier usage from a getter functions

3. Implicit access modifier

Storage variables _name, _symbol, _decimals and _totalsupply defined without an a access modifier.

Recommendation: Use explicit access modifier.

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.
medium	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.
medium	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 0.8.7 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:

20a2a4ff2db43bcc1bfe2913c8bb29fd462394a8

Sha1 from bytecode (non-metadata):

a80818d665c1c863b1a617323211526e7b5afb37

Contract address:

0xcAFfC5205226450444EfC7E278552E78D952d0CA

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 \nof an exit scam
        were found.  Telescr.in guarantee the safety and performance of the contract DPTToken . Sha1 of contract - 20a2a4ff2db43bcc1bfe2913c8bb29fd462394a8.
        Sha1 without meta of contract - a80818d665c1c863b1a617323211526e7b5afb37 Contract address - 0xcAFfC5205226450444EfC7E278552E78D952d0CA",
        "sig": "0xc916efedf1958e0419f556efd5d2a957784a2c084f22f4bfca155aeb23fa12175e7ac6a3ebbebcdf0c1bd1eb1859a20fc7dfd79da41f68b52867e80b0254188c1b",
        "version": "3"
}
```

Telescr.in

Check the signature