HackSafe

# Smart Contract Security Audit Report

## Tether USD

September 2022

Security Status

★★★★½

www.hacksafe.io

# Audit Details

**Audited project**
Tether USD

**Deployer address**
THPvaUhoh2Qn2y9THCZML3H815hhFhn5YC

**Client contacts**
Tether USD

**Blockchain**
Tronchain

**Website**
https://tron.network/usdt

# Disclaimer

This is a limited report on our findings based on our analysis, in accordance with good industry practice as at the date of this report, in relation to cybersecurity vulnerabilities and issues in the framework and algorithms based on smart contracts, the details of which are set out in this report. In order to get a full view of our analysis, it is crucial for you to read the full report. While we have done our best in conducting our analysis and producing this report, it is important to note that you should not rely on this report and cannot claim against us on the basis of what it says or doesn't say, or how we produced it, and it is important for you to conduct your own independent investigations before making any decisions. We go into more detail on this in the below disclaimer below – please make sure to read it in full.

DISCLAIMER: By reading this report or any part of it, you agree to the terms of this disclaimer. If you do not agree to the terms, then please immediately cease reading this report, and delete and destroy any and all copies of this report downloaded and/or printed by you. This report is provided for information purposes only and on a non-reliance basis, and does not constitute investment advice. No one shall have any right to rely on the report or its contents, and TechRate and its affiliates (including holding companies, shareholders, subsidiaries, employees, directors, officers and other representatives) (HackSafe) owe no duty of care towards you or any other person, nor does HackSafe make any warranty or representation to any person on the accuracy or completeness of the report. The report is provided "as is", without any conditions, warranties or other terms of any kind except as set out in this disclaimer, and HackSafe hereby excludes all representations, warranties, conditions and other terms (including, without limitation, the warranties implied by law of satisfactory quality, fitness for purpose and the use of reasonable care and skill) which, but for this clause, might have effect in relation to the report. Except and only to the extent that it is prohibited by law, HackSafe hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against HackSafe, for any amount or kind of loss or damage that may result to you or any other person (including without limitation, any direct, indirect, special, punitive, consequential or pure economic loss or damages, or any loss of income, profits, goodwill, data, contracts, use of money, or business interruption, and whether in delict, tort (including without limitation negligence), contract, breach of statutory duty, misrepresentation (whether innocent or negligent) or otherwise under any claim of any nature whatsoever in any jurisdiction) in any way arising from or connected with this report and the use, inability to use or the results of use of this report, and any reliance on this report.

The analysis of the security is purely based on the smart contracts alone. No applications or operations were reviewed for security. No product code has been reviewed.

# Procedure

**Step 1 - In-Depth Manual Review**

Manual line-by-line code reviews to ensure the logic behind each function is sound and safe from various attack vectors. This is the most important and lengthy portion of the audit process (as automated tools often cannot find the nuances that lead to exploits such as flash loan attacks).

**Step 2 - Automated Testing**

Simulation of a variety of interactions with your Smart Contract on a test blockchain leveraging a combination of automated test tools and manual testing to determine if any security vulnerabilities exist.

**Step 3 – Leadership Review**

The engineers assigned to the audit will schedule meetings with our leadership team to review the contracts, any comments or findings, and ask questions to further apply adversarial thinking to discuss less common attack vectors.

**Step 4 - Resolution of Issues**

Consulting with the team to provide our recommendations to ensure the code's security and optimize its gas efficiency, if possible. We assist project team's in resolving any outstanding issues or implementing our recommendations.

**Step 5 - Published Audit Report**

Boiling down results and findings into an easy-to-read report tailored to the project. Our audit reports highlight resolved issues and any risks that exist to the project or its users, along with any remaining suggested remediation measures. Diagrams are included at the end of each report to help users understand the interactions which occur within the project.

# Background

**HackSafe was commissioned by Tether USD to perform an audit of smart contracts:**

- https://tronscan.io/#/token20/TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t/code

**The purpose of the audit was to achieve the**

- Ensutre that the smart contract functions as intended.
- Identify potential security issues with the smart contract.

The information in this report should be understand the risk exposure of the  smart contract, and as a guide to improve the security posture of the smart contract by remediating the issues that were  identified.

# Contract Details

## Token contract details for 22.09.2022

| | |
|---|---|
| **Token Type** | : TRC20 |
| **Contract name** | : TetherToken |
| **Contract address** | : TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t |
| **Total supply** | : 34,130,268,679.280810 |
| **Circulating supply** | : 34,130,268,679.280810 |
| **Total marketcap** | : $34,132,634,195 |
| **Circulating Market Cap** | : 34,132,634,195 |
| **Liquidity** | : $254.51m |
| **Token ticker** | : USDT |
| **Decimals** | : 6 |
| **Token holders** | : 15,875,274 |
| **Transactions count** | : 595,695,442 |
| **Compiler version** | : solidity 0.4.25 |
| **Contract deployer address** | : THPvaUhoh2Qn2y9THCZML3H815hhFhn5YC |
| **Owner address** | : TBPxhVAsuzoFnKyXtc1o2UySEydPHgATto |

# Social profiles

| | |
|---|---|
| **Twitter Profile** | : https://twitter.com/Tether_to |

# Claimed Smart Contract Features

## Claimed Feature Detail

Tokenomics :

- **Name** : TetherToken
- **Symbol** : USDT
- **Decimals** : 6
- **Protocol** : TRC20
- **Total supply** : 34,130,268,679.280810
- **Contract address** : TR7NHqjeKQxGTCi8q8ZY4pL8otSzgjLj6t

## Our Observation

YES, this is valid.

# Audit Summary

According to the standard audit assessment, Customer`s solidity smart contracts are “Secure”. This token contract does contain owner control, which do not make it fully decentralized as owner does have control over smart contract.

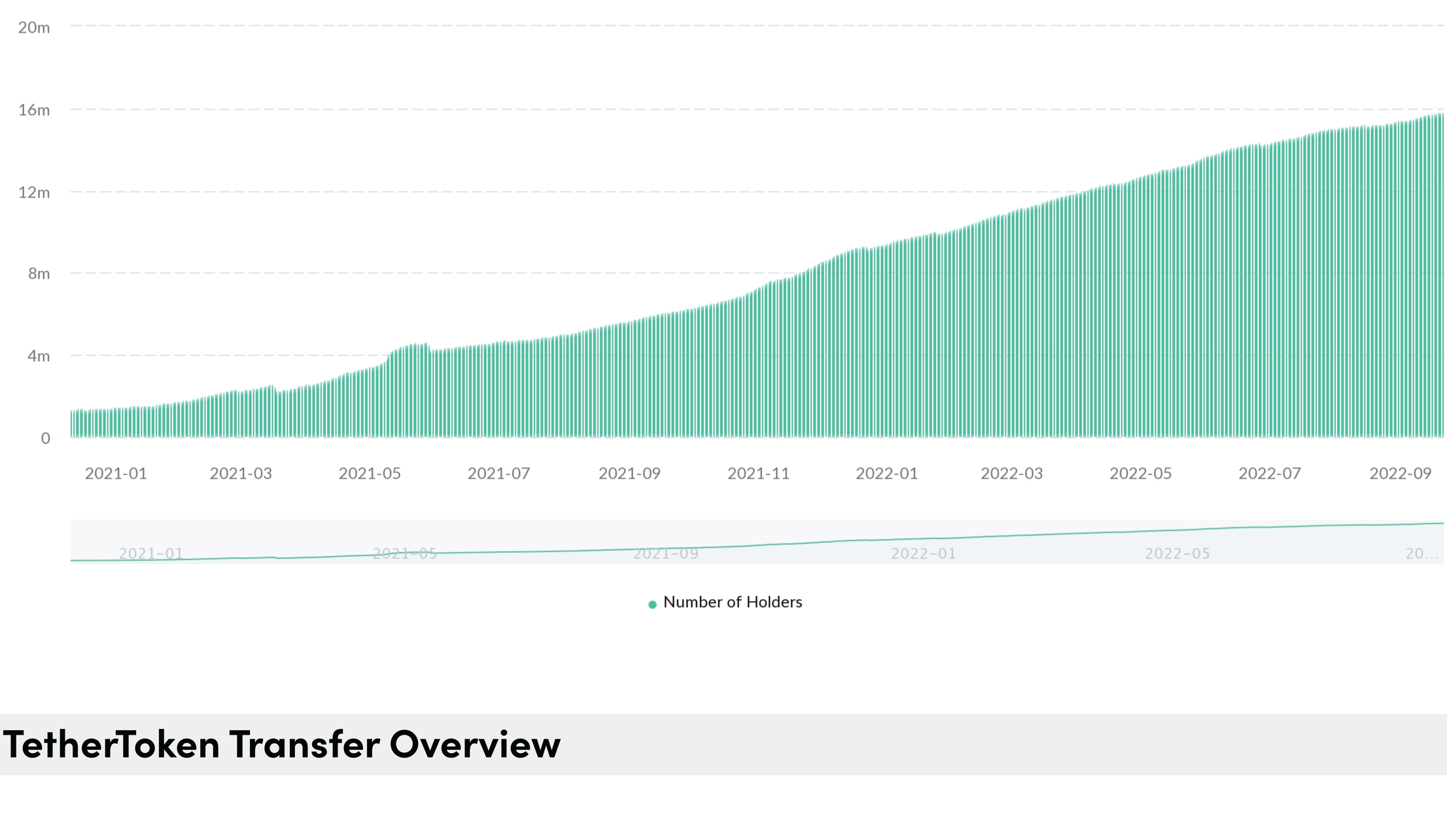
| Insecure | Poor secured | Secure | Well-secured |
|---|---|---|---|

You are here 

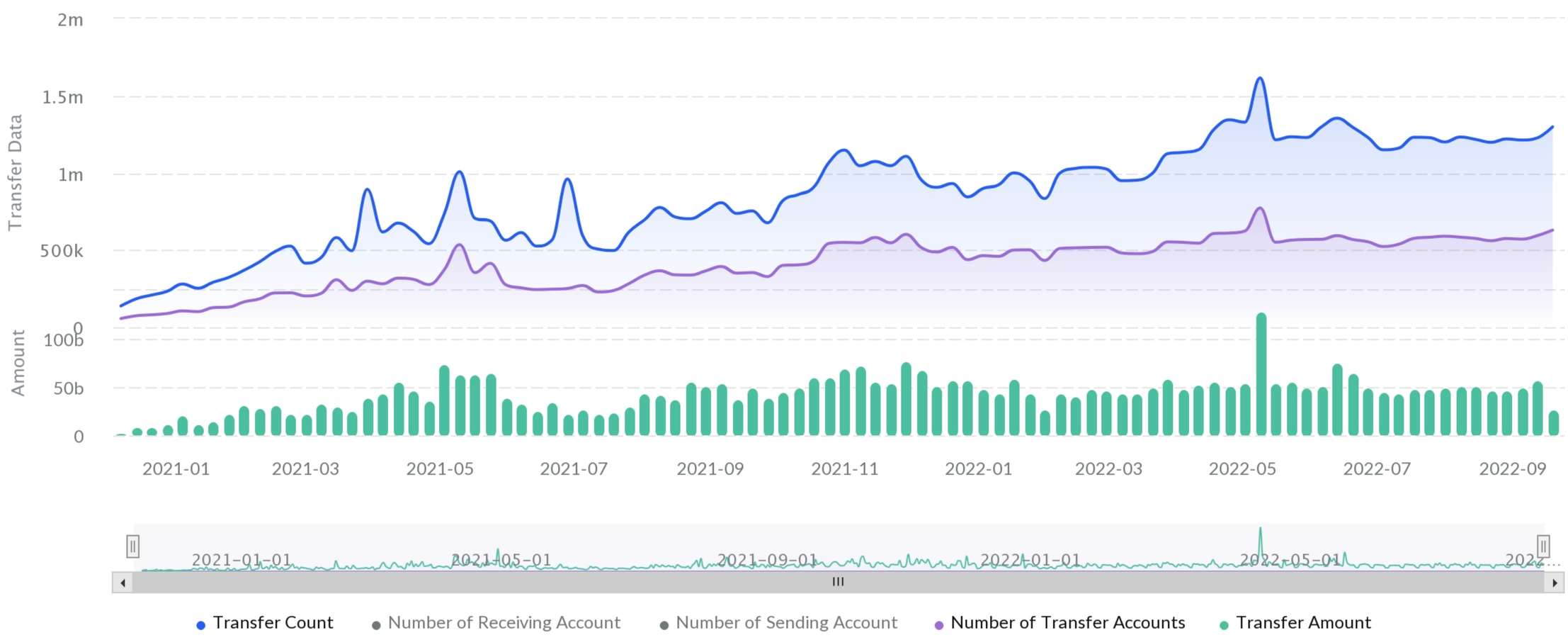
We used various tools like Slither, Mythril and Remix IDE. At the same time this finding is based on critical analysis of the manual audit. All issues found during automated analysis were manually reviewed and applicable vulnerabilities are presented in the issues checking status.

We found 0 critical, 0 high, 0 medium and 2 low and some very low-level issues. These issues are not critical ones.

# TetherToken Token Holders




## TetherToken Transfer Overview



# Contract functions details

BasicToken.sol
+ ERC20Basic
    -[Pub] totalSupply
    -[Pub] balanceOf
    -[Pub] transfer

+ BasicToken (ERC20Basic)
    -[Pub] transfer
    -[Pub] balanceOf

BasicToken.sol
+BlackList (Ownable)
    -[Ext] getBlackListStatus
    -[Pub] addBlackList #
      -modifiers: onlyOwner
    -[Pub] removeBlackList #
      -modifiers: onlyOwner

Migrations.sol
+Migrations
    -[Pub] Migrations
    -[Pub] setCompleted #
      -modifiers: restricted
    -[Pub] upgrade #
      -modifiers: restricted

MultiSigWallet.sol
+MultiSigWallet
    -[Pub] MultiSigWallet #
      -modifiers: validRequirement
-[Pub] addOwner #
  -modifiers: onlyWallet, ownerDoesNotExist, notNull, validRequirement
-[Pub] removeOwner #
  -modifiers: onlyWallet, ownerExists
-[Pub] replaceOwner #
  -modifiers: onlyWallet, ownerExists, ownerDoesNotExist
-[Pub] changeRequirement #
  -modifiers: onlyWallet, validRequirement
-[Pub] submitTransaction #
-[Pub] confirmTransaction #

# Contract functions details

-modifiers: ownerExists, transactionExists, notConfirmed
-[Pub] revokeConfirmation #
-modifiers: ownerExists, confirmed, notExecuted
-[Pub] executeTransaction #
-modifiers: notExecuted
-[Pub] isConfirmed
-[Int] addTransaction #
-[Pub] getConfirmationCount #
-[Pub] getTransactionCount #
-[Pub] getOwners
-[Pub] getConfirmations
-[Pub] getTransactionIds

Ownable.sol
+Ownable
-[Pub] Ownable
-[Pub] transferOwnership #
-modifiers: onlyOwner

Pausable.sol
+Pausable (Ownable)
-[Pub] pause #
-modifiers: onlyOwner, whenNotPaused
-[Pub] unpause #
-modifiers: onlyOwner, whenPaused

SafeMath.sol
+[Lib] SafeMath
-[Int] mul
-[Int] div
-[Int] sub
-[Int] add

StandardToken.sol
+ ERC20(ERC20Basic)
-[Pub] allowance
-[Pub] transferFrom
-[Pub] approve

# Contract functions details

+StandardToken (ERC20, BasicToken)

- -[Pub] transferFrom #
- -[Pub] approve #
- -[Pub] allowance
- -[Pub] increaseApproval #
- -[Pub] decreaseApproval #

StandardTokenWithFees.sol

+StandardTokenWithFees (StandardToken, Ownable)

- -calcFee
- -[Pub] transfer #
- -[Pub] transferFrom #
- -[Pub] setParams #
  - -modifiers: onlyOwner

TetherToken.sol

+TetherToken (Pausable, StandardTokenWithFees, BlackList)

- -[Pub] TetherToken
- -[Pub] transfer #
  - -modifiers: whenNotPaused
- -[Pub] transferFrom #
  - -modifiers: whenNotPaused
- -[Pub] balanceOf
- -[Pub] oldBalanceOf
- -[Pub] approve #
  - -modifiers: whenNotPaused
- -[Pub] increaseApproval #
  - -modifiers: whenNotPaused
- -[Pub] decreaseApproval #
  - -modifiers: whenNotPaused
- -[Pub] allowance
- -[Pub] deprecate #
  - -modifiers: onlyOwner
- -[Pub] totalSupply
- -[Pub] issue #
  - -modifiers: onlyOwner
- -[Pub] redeem #
  - -modifiers: onlyOwner

# Contract functions details

-[Pub] destroyBlackFunds #

-modifiers: onlyOwner

($) = payable function
# = non-constant function

# Issues Checking Status

| No. | Title | Status |
|---|---|---|
| 1. | Unlocked Compiler Version | Low issue |
| 2. | Missing Input Validation | Passed |
| 3. | Race conditions and Reentrancy. Cross-function race conditions. | Passed |
| 4. | Possible delays in data delivery | Passed |
| 5. | Oracle calls. | Passed |
| 6. | Timestamp dependence. | Passed |
| 7. | Integer Overflow and Underflow | Passed |
| 8. | DoS with Revert. | Passed |
| 9. | DoS with block gas limit. | Passed |
| 10. | Methods execution permissions. | Passed |
| 11. | Economy model of the contract. | Passed |
| 12. | Private use data leaks. | Passed |
| 13. | Malicious Event log. | Passed |
| 14. | Scoping and Declarations. | Passed |
| 15. | Uninitialized storage pointers. | Passed |
| 16. | Arithmetic accuracy. | Passed |
| 17. | Design Logic. | Passed |
| 18. | Safe Open Zeppelin contracts implementation and usage. | Passed |
| 19. | Incorrect Naming State Variable | Passed |
| 20. | Too old version | Low issue |

# Severity Definitions

| Risk Level | Description |
| --- | --- |
| Critical | Critical vulnerabilities are usually straightforward to exploit and can lead to assets loss or data manipulations. |
| High | High-level vulnerabilities are difficult to exploit; however, they also have a significant impact on smart contract execution, e.g., public access to crucial functions |
| Medium | Medium-level vulnerabilities are important to fix; however, they can't lead to assets loss or data manipulations. |
| Low | Low-level vulnerabilities are mostly related to outdated, unused, etc. code snippets that can't have a significant impact on execution. |

# Security Issues

**Critical Severity Issues**

No critical severity issue found.

**High Severity Issues**

No high severity issues found.

**Medium Severity Issues**

No medium severity issues found.

**Low Severity Issues**

Two low severity issue found.

## 1. Old Compiler Version.

- **Description**

  Contract has been deployed using too old solidity version.

- **Recommendation**

  It is advisable to deploy contract using any of the latest version of solidity.

## 2. Unlocked Compiler Version.

- **Description**

  The contract utilizes an unlocked compiler version. An unlocked compiler version in the contract's source code permits the user to compile it at or above a particular version. This, in turn, leads to differences in the generated bytecode between compilations due to differing compiler version numbers. This can lead to ambiguity when debugging as compiler-specific bugs may occur in the codebase that would be difficult to identify over a span of multiple compiler versions rather than a specific one.

- **Recommendation**

  It is advisable that the compiler version is alternatively locked at the lowest version possible so that the contract can be compiled. For example, for version ^0.4.18 the contract should contain the following line:

  pragma solidity 0.4.25;

# Centralization

## Owner Privileges :

- Tether USD Contract:
    - Owner can transfer ownership.
    - Owner can pause and unpause functions of contract.
    - Owner can add and remove addresses from blacklist.
    - Owner can issue and burn tokens.
    - Owner can deprecate black funds.
    - Owner can set params.

This smart contract has some functions which can be executed by the Admin (Owner) only. If the admin wallet private key would be compromised, then it would create trouble as smart contract ownership has not been renounced. Following are Admin functions functions:

- Addblacklist
- Removeblacklist
- Transferownership
- Pause
- Unpause
- Setparams
- Deprecate
- Issue
- Redeem
- Destroyblackfunds

# Conclusion

Smart contract contains low severity issues! The further transfer and operations with the fund raised are not related to this particular contract.

HackSafe note: Please check the disclaimer above and note, the audit makes no statements or warranties on business model, investment attractiveness or code sustainability. The report is provided for the only contract mentioned in the report and does not include any other potential contracts deployed by Owner.