Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

September, 2021

Audit Details

Audited project

USD SMART

Deployer address

0x242cd507e22a2c587e43dfa0bc6ac57e69173853

Client contacts:

USD SMART team

Blockchain

Binance Smart Chain

Project website:

https://usdsmart.com/

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) (TechRate) owe no duty of care towards you or any other person, nor does TechRate 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 TechRate 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, TechRate hereby excludes all liability and responsibility, and neither you nor any other person shall have any claim against TechRate, 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.

Background

TechRate was commissioned by USD SMART to perform an audit of smart contracts:

https://bscscan.com/token/0x303de4bdb189b951f875eb4a8ecde2985138161e

The purpose of the audit was to achieve the following:

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

The information in this report should be used to 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.

Contracts Details

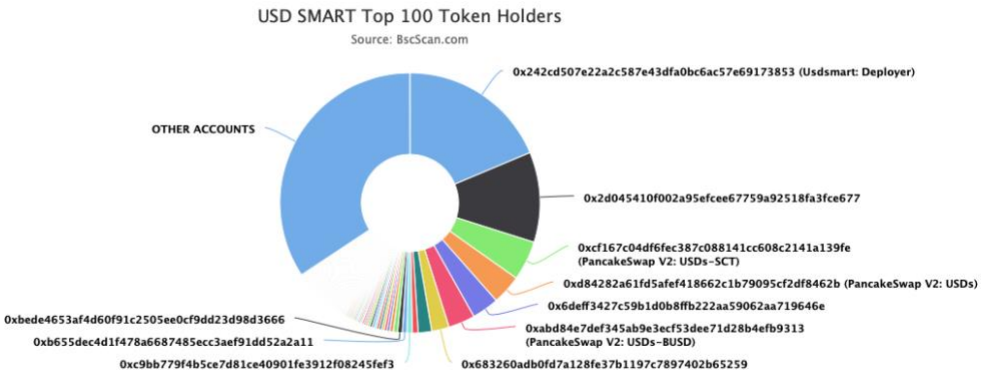
Token contract details for 14.09.2021

Contract name	USD SMART
Contract address	0x303dE4bdb189B951F875eB4A8ECDe2985138161e
Total supply	90,000,000
Token ticker	USDs
Decimals	18
Token holders	16,143
Transactions count	42,303
Top 100 holders dominance	65.69%
Contract deployer address	0x242cd507e22a2c587e43dfa0bc6ac57e69173853
Contract's current owner address	0x0000000000000000000000000000000000000000

USD SMART Token Distribution

The top 100 holders collectively own 65.69% (59,123,975.57 Tokens) of USD SMART

Token Total Supply: 90,000,000.00 Token | Total Token Holders: 16,143

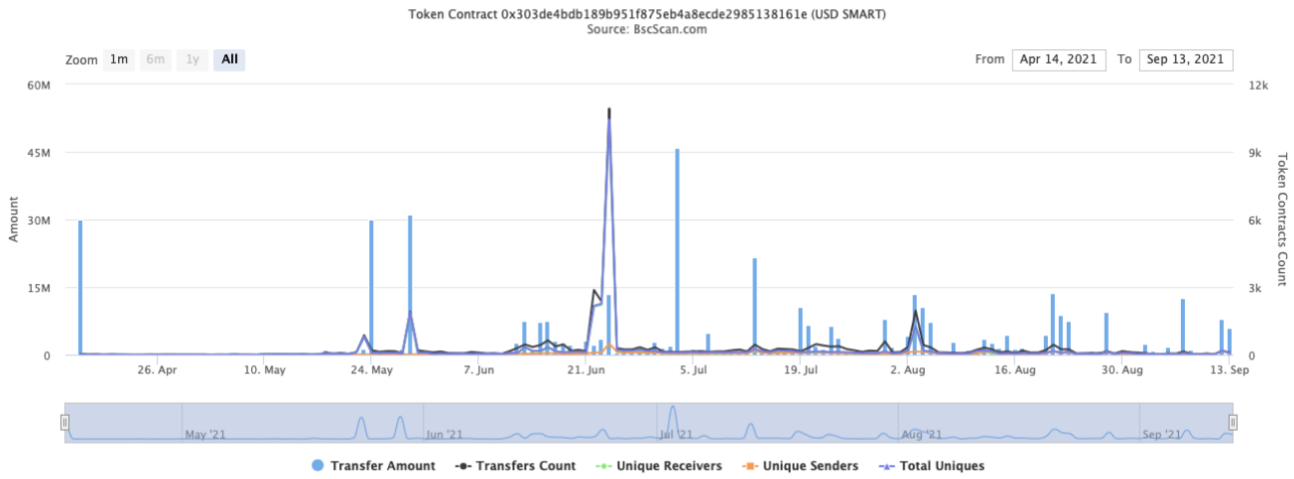


(A total of 59,123,975.57 tokens held by the top 100 accounts from the total supply of 90,000,000.00 token)

USD SMART Contract Interaction Details

Time Series: Token Contract Overview

Fri 16, Apr 2021 - Mon 13, Sept 2021



USD SMART Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Usdsmart: Deployer	16,817,985.009549015053427193	18.6867%
2	0x2d045410f002a95efcee67759a92518fa3fce677	10,075,000	11.1944%
3	PancakeSwap V2: USDs-SCT	4,436,531.507481829939945296	4.9295%
4	PancakeSwap V2: USDs	3,303,524.475311364055062764	3.6706%
5	0x6deff3427c59b1d0b8ffb222aa59062aa719646e	3,017,524.454566651073471326	3.3528%
6	PancakeSwap V2: USDs-BUSD	2,983,740.209034050254984141	3.3153%
7	0x683260adb0fd7a128fe37b1197c7897402b65259	1,960,603.487825796786963669	2.1784%
8	0x00202b53afb000d9ed1c00555edf60c5f2da60ff	1,500,000	1.6667%
9	0xceb9c379d86d36b2e64af096095e4df8e2e416c7	662,500	0.7361%
10	0xc9bb779f4b5ce7d81ce40901fe3912f08245fef3	582,539.600257861597236684	0.6473%

Contract functions details

```
+ [Lib] SafeMath
  - [Int] mul
  - [Int] div
  - [Int] sub
  - [Int] add

+  ForeignToken
  - [Pub] balanceOf
  - [Pub] transfer #

+  BEP20Basic
  - [Pub] balanceOf
  - [Pub] transfer #

+  BEP20 (BEP20Basic)
  - [Pub] allowance
  - [Pub] transferFrom #
  - [Pub] approve #

+  USDSMART (BEP20)
  - [Pub] <Constructor> #
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] finishDistribution #
    - modifiers: onlyOwner,canDistr
  - [Prv] distr #
    - modifiers: canDistr
  - [Int] Distribute #
    - modifiers: onlyOwner
  - [Ext] DistributeAirdrop #
    - modifiers: onlyOwner
  - [Ext] DistributeAirdropMultiple #
    - modifiers: onlyOwner
  - [Pub] updateTokensPerBsc #
    - modifiers: onlyOwner
  - [Ext] <Fallback> ($)
  - [Pub] getTokens ($)
    - modifiers: canDistr
  - [Pub] balanceOf
  - [Pub] transfer #
    - modifiers: onlyPayloadSize
  - [Pub] transferFrom #
    - modifiers: onlyPayloadSize
  - [Pub] approve #
  - [Pub] allowance
  - [Pub] getTokenBalance
  - [Pub] withdrawAll #
    - modifiers: onlyOwner
  - [Pub] withdraw #
    - modifiers: onlyOwner
  - [Pub] burn #
```

  - modifiers: onlyOwner
- [Pub] add #
  - modifiers: onlyOwner
- [Pub] withdrawForeignTokens #
  - modifiers: onlyOwner

($) = payable function
= non-constant function

Issues Checking Status

	Issue description	Checking status
1.	Compiler errors.	Passed
2.	Race conditions and Reentrancy. Cross-function race conditions.	Passed
3.	Possible delays in data delivery.	Passed
4.	Oracle calls.	Passed
5.	Front running.	Passed
6.	Timestamp dependence.	Passed
7.	Integer Overflow and Underflow.	Passed
8.	DoS with Revert.	Passed
9.	DoS with block gas limit.	Low issues
10.	Methods execution permissions.	Passed
11.	Economy model of the contract.	Passed
12.	The impact of the exchange rate on the logic.	Passed
13.	Private user data leaks.	Passed
14.	Malicious Event log.	Passed
15.	Scoping and Declarations.	Passed
16.	Uninitialized storage pointers.	Passed
17.	Arithmetic accuracy.	Passed
18.	Design Logic.	Passed
19.	Cross-function race conditions.	Passed
20.	Safe Open Zeppelin contracts implementation and usage.	Passed
21.	Fallback function security.	Passed

Security Issues

High Severity Issues

No high severity issues found.

Medium Severity Issues

No medium severity issues found.

Low Severity Issues

1. Wrong total supply restriction (Distribution finished, issue is not relevant)

   Issue:

   - The function `Distribute()` checks that totalDistributed < totalSupply, but should check totalDistributed + _amount < totalSupply.

   Recommendation:

   Check that the result will not exceed totalSupply.

2. getTokens function errors (Distribution finished, issue is not relevant)

   Issue:

   - bonusCond3 is lower than bonusCond2. “(msg.value >= bonusCond2 && msg.value < bonusCond3)” will never be true.

   Recommendation:

   Increase bonusCond3 value to be higher than bonusCond2.

   - (now >= deadline && now >= round1 && now < round2) will never be true, because deadline value higher than round2 value.

   Recommendation:

   Recheck logic of this if part.

3. Out of gas

   Issue:

   - The function `DistributeAirdropMultiple()` uses the loop for distributing tokens as airdrop.

   Recommendation:

   Check that the addresses array length is not too big.

Owner privileges (In the period when the owner is not renounced)

- Owner can increase totalSupply by calling add() function and then distribute token amount, so this is kind of minting.
- Owner can burn.
- Owner can withdraw BNBs from the contract.
- Owner can withdraw tokens from contract.
- Owner can stop distribution.
- Owner can distribute tokens.
- Owner can change tokensPerBsc value.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope. Audited only sale contract. The further transfers and operations with the funds raise are not related to this particular contract.

TechRate 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.