Smart Contract Security Audit

Audit details:

Audited project:	Shopaneum
Deployer address:	0xf30844fab91dc0eabeb33fe41130dc4ca73bd825
Client contacts:	Shopaneum team
Blockchain:	Binance Smart Chain
Project website:	Not provided

May, 2021

TechRate

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 Shopaneum to perform an audit of smart contracts:

- *https://bscscan.com/address/0xff749e976358791a3799262b8fccedf8d0888563#code*

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

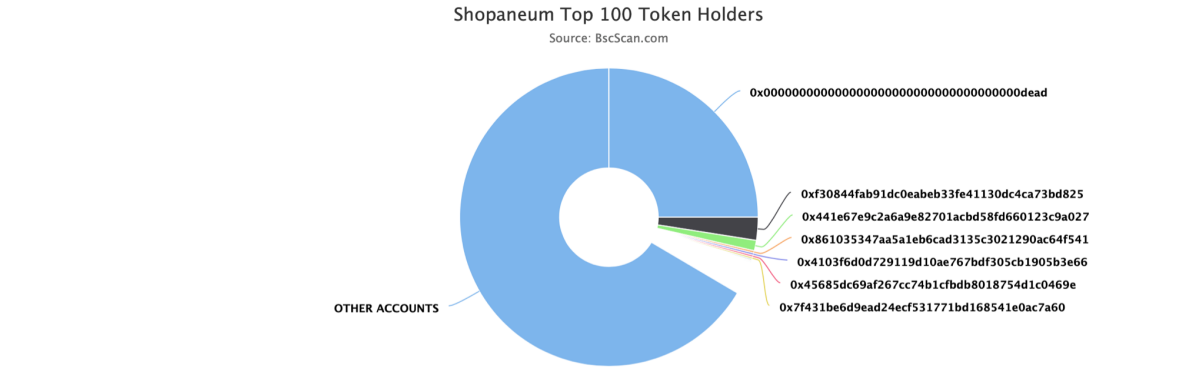
Token contract details for 05.05.2021.

Contract name:	Shopaneum
Contract address:	0xff749e976358791a3799262b8fccedf8d0888563
Total supply:	100_000_000_000_000_000_000_000_000_000
Token ticker:	SPN
Decimals:	18
Token holders:	826
Transactions count:	2885
Top 100 holders dominance:	33.48 %
Compiler version:	v0.4.26+commit.4563c3fc
Contract deployer address:	0xf30844fab91dc0eabeb33fe41130dc4ca73bd825
Contract’s current owner address:	Private field

Shopaneum token distribution

The top 100 holders collectively own 33.48% (33,483,178,130.18 Tokens) of Shopaneum

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 826



(A total of 33,483,178,130.18 tokens held by the top 100 accounts from the total supply of 100,000,000,000.00 token)

Shopaneum top 10 token holders

Rank	Address	Quantity (Token)	Percentage
1	0x000000000000000000000000000000000000dead	25,000,000,000	25.0000%
2	0xf30844fab91dc0eabeb33fe41130dc4ca73bd825	2,500,000,000	2.5000%
3	0x441e67e9c2a6a9e82701acbd58fd660123c9a027	1,125,000,000	1.1250%
4	0x861035347aa5a1eb6cad3135c3021290ac64f541	240,750,000	0.2408%
5	0x4103f6d0d729119d10ae767bdf305cb1905b3e66	238,950,000	0.2390%
6	0x45685dc69af267cc74b1cfbdb8018754d1c0469e	225,000,000	0.2250%
7	0x7f431be6d9ead24ecf531771bd168541e0ac7a60	205,083,076.347439619625	0.2051%
8	0x7be506e23f88047d69290d3a0f3586650793c256	143,013,594.999979777627711514	0.1430%
9	0xd12e723c61297a244b510779c078f54708d8462c	131,475,465	0.1315%
10	0x2d53459684ff9171088571764bba4b6ea594bebd	121,500,000	0.1215%

Contract functions details

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

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

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

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

+ Shopaneum (BEP20)
  - [Pub] <Constructor> #
  - [Pub] transferOwnership #
    - modifiers: onlyOwner
  - [Pub] finishDistribution #
    - modifiers: onlyOwner,canDistr
  - [Prv] distr #
    - modifiers: canDistr
  - [Int] doAirdrop #
  - [Pub] adminClaimAirdrop #
    - modifiers: onlyOwner
  - [Pub] adminClaimAirdropMultiple #
    - modifiers: onlyOwner
  - [Pub] updateTokensPerEth #
    - 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] withdraw #
  - modifiers: onlyOwner
- [Pub] burn #
  - modifiers: onlyOwner
- [Pub] withdrawAltcoinTokens #
  - 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.	Passed
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.	Medium issues
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 medium severity issues found.

Medium Severity Issues

1. More than total supply distribution

Issue:

There is a possibility that the distributed tokens amount will be more than total supply. So the users balance sum will be more than total supply. Same for the payable getTokens function, there is possibility of buying more tokens than the total supply

Recommendation:

Please add checking in functions distr and that the sum of total distributed and newly distributed amount will be less than total supply before sending the tokens.

Low Severity Issues

1. No equal arrays

Issue:

There is a possibility that receivers and amounts arrays will have different sizes in the adminClaimAirdropMultiple function.

Recommendation:

Please check that arrays sizes are equal.

Owner privileges

- Owner can change the tokens per eth value.
- Owner can withdraw the mistakenly sent tokens and BNBs from the contract (Not an issue as this is the sale contract).

Conclusion

Smart contracts contain medium severity issues.

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.