



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

Virgo Dex Finance



Deployer address

0xaac21b3be576ad01e5b35914b5bb3e704672760c



Client contacts:

Virgo Dex Finance team



Blockchain

Binance Smart Chain



Project website:

<http://www.virgodex.io>

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 Virgo Dex Finance to perform an audit of smart contracts:

<https://bscscan.com/address/0xc825868c6a35a3018cc38080d3dbd24b4d3530d7#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 23.09.2021

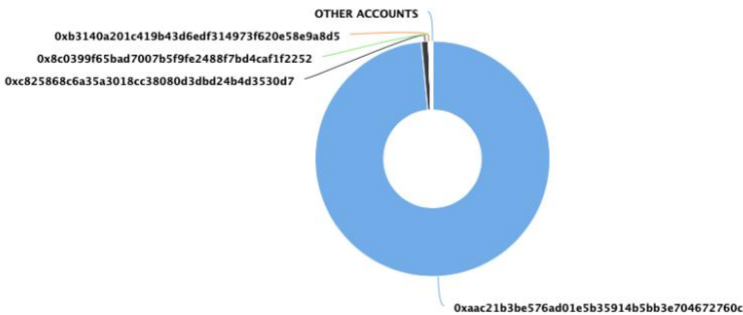
Contract name	Virgo Dex Finance
Contract address	0xC825868c6a35A3018cc38080D3DBd24B4d3530D7
Total supply	500,000,000
Token ticker	VDF
Decimals	18
Token holders	119
Transactions count	132
Top 100 holders dominance	99.98%
Contract deployer address	0xaac21b3be576ad01e5b35914b5bb3e704672760c
Contract's current owner address	0xaac21b3be576ad01e5b35914b5bb3e704672760c

Virgo Dex Finance Token Distribution

The top 100 holders collectively own 99.98% (499,904,586.00 Tokens) of Virgo Dex Finance

Token Total Supply: 500,000,000.00 Token | Total Token Holders: 119

Virgo Dex Finance Top 100 Token Holders
Source: BscScan.com



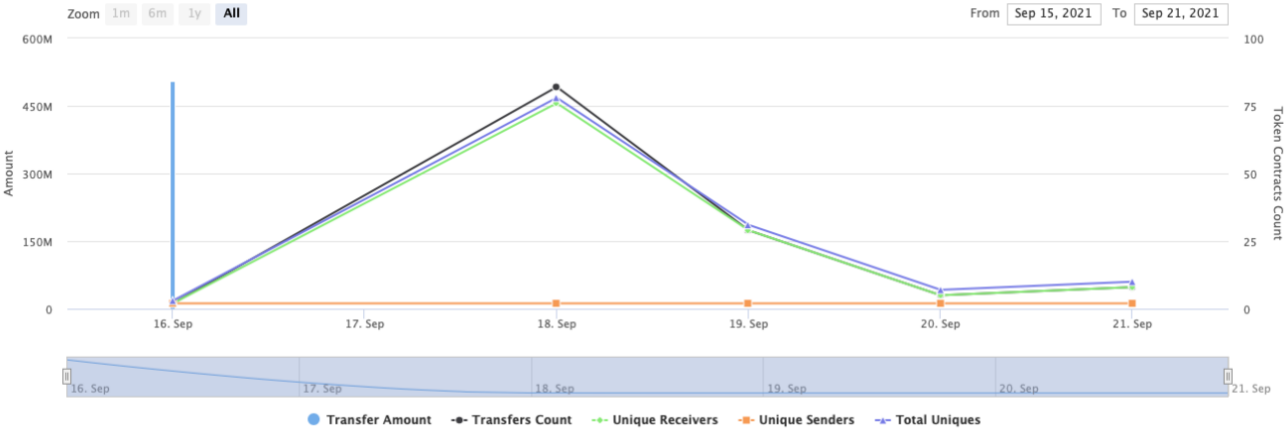
(A total of 499,904,586.00 tokens held by the top 100 accounts from the total supply of 500,000,000.00 token)

Virgo Dex Finance Contract Interaction Details


Time Series: Token Contract Overview

Thu 16, Sept 2021 - Tue 21, Sept 2021

Token Contract 0xc825868c6a35a3018cc38080d3dbd24b4d3530d7 (Virgo Dex Finance)
Source: BscScan.com



Virgo Dex Finance Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0xaac21b3be576ad01e5b35914b5bb3e704672760c	492,459,028.888888889186	98.4918%
2	 0xc825868c6a35a3018cc38080d3dbd24b4d3530d7	4,867,171	0.9734%
3	0x8c0399f65bad7007b5f9fe2488f7bd4caf1f2252	66,667.222222221955	0.0133%
4	0xb3140a201c419b43d6edf314973f620e58e9a8d5	52,500	0.0105%
5	0xd97429ee015d22f19f70e58a092281b98500d67b	50,000	0.0100%
6	0x5a794cb38ddc72cedab709ba4546c409191e5fa6	41,692.22222222195	0.0083%
7	0x8b8daaad374184415575fd8068c5c210a904cc9	41,666.666666666664	0.0083%
8	0xd4c298ef01ced2888fa3b8193c67637bd2f6610d	41,666.666666666664	0.0083%
9	0x9437c93ec0a19f005f76633216564d700a3654a1	41,666.666666666664	0.0083%
10	0x1023e7926e76f762be7b67c1329fa73a55f65865	41,666.666666666664	0.0083%



Contract functions details

- + [Int] IBEP20
 - [Ext] totalSupply
 - [Ext] decimals
 - [Ext] symbol
 - [Ext] name
 - [Ext] getOwner
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #
- + Context
 - [Int] _msgSender
 - [Int] _msgData
- + [Lib] SafeMath
 - [Int] add
 - [Int] sub
 - [Int] sub
 - [Int] mul
 - [Int] div
 - [Int] div
 - [Int] mod
 - [Int] mod
- + Ownable (Context)
 - [Int] <Constructor> #
 - [Pub] owner
 - [Pub] renounceOwnership #
 - modifiers: onlyOwner
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Pub] recieveOwnership #
 - modifiers: onlyMidWayOwner
- + VirgoDexFinance (Context, IBEP20, Ownable)
 - [Pub] <Constructor> #
 - [Ext] getOwner
 - [Ext] decimals
 - [Ext] symbol
 - [Ext] name
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] transfer #
 - [Ext] allowance
 - [Ext] approve #
 - [Ext] transferFrom #
 - [Pub] increaseAllowance #
 - [Pub] decreaseAllowance #
 - [Int] _transfer #

- [Int] _approve #
- [Pub] tokenSale (\$)
- [Pub] viewSale
- [Pub] startSale #
 - modifiers: onlyOwner
- [Pub] clearETH #
 - 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.	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

No low severity issues found.

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

- Owner can start sell.

```
function startSale(
    uint256 _sPrice↑,
    uint256 _minDepositBNBAmount↑,
    uint256 _maxDepositBNBAmount↑,
    uint256 _saleDateStart↑,
    uint256 _saleDateEnd↑
) public onlyOwner {
    sPrice = _sPrice↑;
    minDepositBNBAmount = _minDepositBNBAmount↑;
    maxDepositBNBAmount = _maxDepositBNBAmount↑;
    saleDateStart = _saleDateStart↑;
    saleDateEnd = _saleDateEnd↑;
}
```

- Owner can withdraw BNBs (not an issue as this is the sale contract).

```
function clearETH() public onlyOwner {
    address payable _owner = msg.sender;
    _owner.transfer(address(this).balance);
}
```

Conclusion

Smart contracts do not contain high severity issues! Liquidity pair contract's security is not checked due to out of scope. tokenSale() function sells tokens from contract address, so for the proper function working contract address should have tokens on it. Audited only sale contract. The further transfers and operations with the funds raise are not related to this particular contract.

Liquidity locking details NOT provided by the team.

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.



[Techrate1](#)



[Techrate](#)



[Techrate_audits](#)