



TechRate
AUDIT COMPANY

Smart Contract Security Audit

Audit Details



Audited project

Titan War



Deployer address

0x70224d8813ba9e5c85fefb4d0a68344405fe0746



Client contacts:

Titan War team



Blockchain

Binance Smart Chain



Project website:

Not provided by Titan War team

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 Titan War to perform an audit of smart contracts:

<https://bscscan.com/address/0x76f34cd142ca4a5ea2e197ebffbf5234a1c29268#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 28.08.2021

Contract name	Titan War
Contract address	0x76F34cd142ca4a5ea2E197ebffbF5234A1c29268
Total supply	1,000,000,000
Token ticker	TITAN
Decimals	8
Token holders	10,180
Transactions count	15,655
Top 100 holders dominance	1.64%
Contract deployer address	0x70224d8813ba9e5c85fefb4d0a68344405fe0746

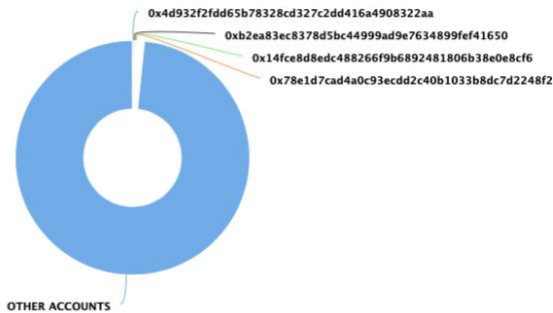
Titan War Token Distribution

The top 100 holders collectively own 1.64% (16,415,288.59 Tokens) of Titan War

Token Total Supply: 1,000,000,000.00 Token | Total Token Holders: 10,180

Titan War Top 100 Token Holders

Source: BscScan.com



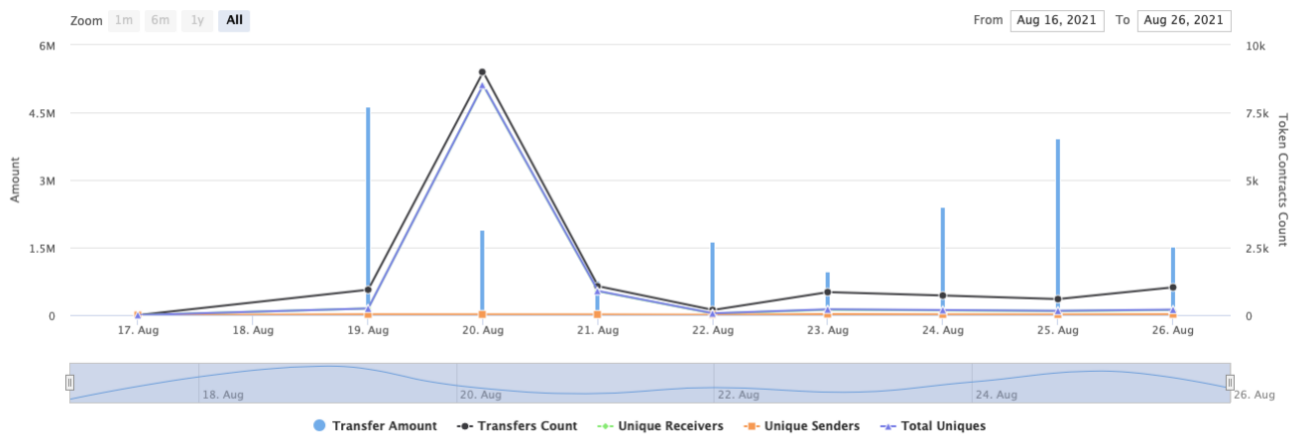
(A total of 16,415,288.59 tokens held by the top 100 accounts from the total supply of 1,000,000,000.00 token)

Titan War Contract Interaction Details

Time Series: Token Contract Overview

Tue 17, Aug 2021 - Thu 26, Aug 2021

Token Contract 0x76f34cd142ca4a5ea2e197ebffb5234a1c29268 (Titan War)
Source: BscScan.com



Titan War Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x4d932f2fdd65b78328cd327c2dd416a4908322aa	1,822,643	0.1823%
2	0xb2ea83ec8378d5bc44999ad9e7634899fe41650	1,746,100	0.1746%
3	0x14fce8d8edc488266f9b6892481806b38e0e8cf6	1,285,400	0.1285%
4	0x78e1d7cad4a0c93ecdd2c40b1033b8dc7d2248f2	717,620	0.0718%
5	0xded0eaadcba4ac4e0834f09ef87922040bc7ac76	585,000	0.0585%
6	0xaaede87806c0f8a3ed671f104cb927dfb5daf2a9	511,682.26774931	0.0512%
7	0xa56aef26d692d8a51c9e17a08db294a888f8e975	500,000	0.0500%
8	0x0d1bfaa3813782497299150b9c1213072587066c	430,125.908742	0.0430%
9	0xd62066aece60187785fd62e5c2c9f840852573af	428,300	0.0428%
10	0x1a45dd52f59356f26b57ba6c3a3c6aa00ba0725e	360,000	0.0360%



Contract functions details

- + [Int] IERC20
 - [Ext] totalSupply
 - [Ext] balanceOf
 - [Ext] allowance
 - [Ext] transfer #
 - [Ext] approve #
 - [Ext] transferFrom #
- + [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 #
- + TitanWar (BEP20)
 - [Pub] <Constructor> #
 - [Ext] setTaxFeePercent #
 - modifiers: onlyOwner
 - [Prv] calculateTaxFee
 - [Prv] removeAllFee #
 - [Prv] restoreAllFee #
 - [Ext] setLiquidityFeePercent #
 - modifiers: onlyOwner
 - [Prv] calculateLiquidityFee
 - [Pub] transferOwnership #
 - modifiers: onlyOwner
 - [Pub] finishDistribution #
 - modifiers: onlyOwner,canDistr
 - [Prv] distr #
 - modifiers: canDistr
 - [Pub] totalFees
 - [Int] Distribute #
 - modifiers: onlyOwner
 - [Ext] DistributeAirdrop #
 - modifiers: onlyOwner
 - [Ext] DistributeAirdropMultiple #
 - 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] withdrawAll #
 - modifiers: onlyOwner
- [Pub] withdraw #
 - modifiers: onlyOwner
- [Pub] burn #
 - 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.	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 high severity issues found.

✓ Medium Severity Issues

1. Wrong total supply restriction

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

Issue:

- `bonusCond1 = bonusCond2 = bonusCond3`, so all the conditions will not work as expected.

Recommendation:

Recheck logic of this part of the contract.

✓ Low Severity Issues

3. Wrong total supply restriction

Issue:

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

Recommendation:

Check that the result will not exceed `totalSupply`.

4. 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.

Notes:

- Functions `setTaxFeePercent`, `calculateTaxFee`, `removeAllFee`, `restoreAllFee`, `setLiquidityFeePercent`, `calculateLiquidityFee` are not used.

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

- 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 `tokensPerEth` value.

Conclusion

Smart contracts contain low severity issues! Liquidity pair contract's security is not checked due to out of scope.

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](#)