TechRate
April, 2022

SMART CONTRACTS SECURITY AUDIT REPORT

Audit Details

Audited project

Red Knight Token

Deployer address

0x29c1674ab36a29797ba7a7cd50d1fedc085017b8

Client contacts:

Red Knight Token team

Blockchain

Ethereum

Project website:

https://www.redknighttoken.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 Red Knight Token to perform an audit of smart contracts:
https://etherscan.io/address/0x1104080b3ca1F766a33C16aA890465D1A63e5078#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

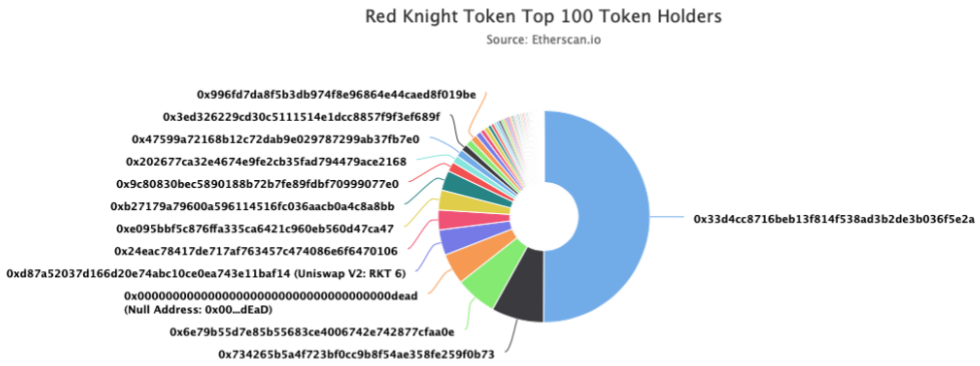
Token contract details for 15.04.2022

Contract name	Red Knight Token
Contract address	0x1104080b3ca1F766a33C16aA890465D1A63e5078
Total supply	999,000,000,000,000
Token ticker	RKT
Decimals	18
Token holders	95
Transactions count	462
Top 100 holders dominance	99.92%
Liquidity wallet	0x8c17ce0ab0dc7e3a85e19304b36e825043eab208
Base buy fees	1/4/2/3/2
Base sell fees	1/4/2/3/2
Uniswap V2 pair	0xd87a52037d166d20e74abc10ce0ea743e11baf14
Contract deployer address	0x29c1674ab36a29797ba7a7cd50d1fedc085017b8
Owner address	0x8c17ce0ab0dc7e3a85e19304b36e825043eab208

Red Knight Token Token Distribution

The top 100 holders collectively own 99.92% (998,225,106,054,932.00 Tokens) of Red Knight Token

Token Total Supply: 999,000,000,000,000.00 Token | Total Token Holders: 95

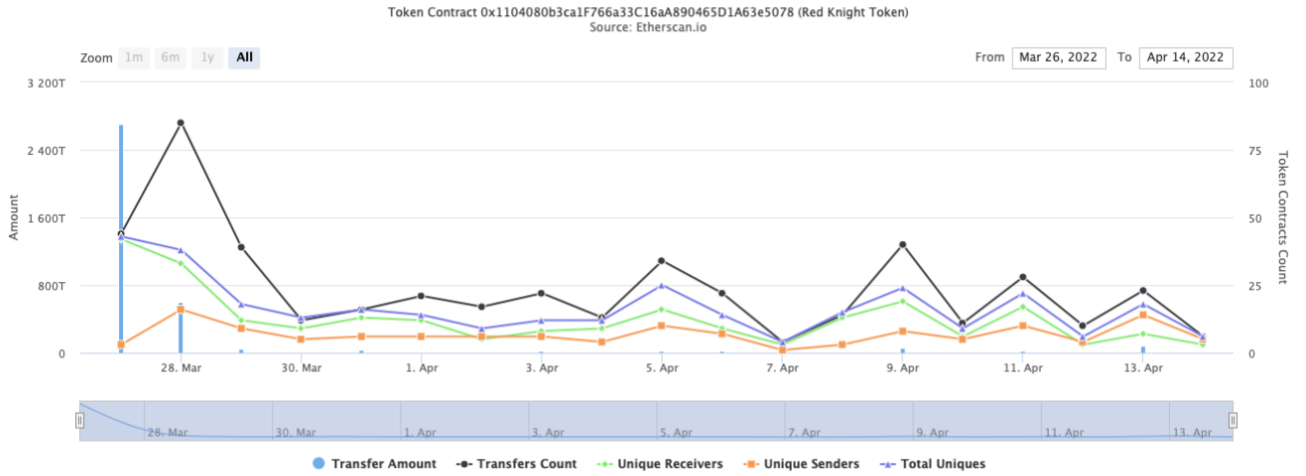


(A total of 998,225,106,054,932.00 tokens held by the top 100 accounts from the total supply of 999,000,000,000,000.00 token)

Red Knight Token Contract Interaction Details

Time Series: Token Contract Overview

Sun 27, Mar 2022 - Thu 14, Apr 2022



TECH RATE

Red Knight Token Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x33d4cc8716beb13f814f538ad3b2de3b036f5e2a	500,163,058,404,707.811262892100393054	50.0664%
2	0x734265b5a4f723bf0cc9b8f54ae358fe259f0b73	80,044,903,780,030.238956579603027624	8.0125%
3	0x6e79b55d7e85b55683ce4006742e742877cfaa0e	63,139,712,923,663.66705745726921721	6.3203%
4	Null Address: 0x00...dEaD	47,019,784,578,238.278822919319275661	4.7067%
5	Uniswap V2: RKT 6	38,656,305,187,265.356863621212998988	3.8695%
6	0x24eac78417de717af763457c474086e6f6470106	30,344,040,261,993.270668943025600095	3.0374%
7	0xe095bbf5c876ffa335ca6421c960eb560d47ca47	30,340,371,614,234.515143751607335606	3.0371%
8	0xb27179a79600a596114516fc036aacb0a4c8a8bb	30,340,371,614,234.515143751607335606	3.0371%
9	0x9c80830bec5890188b72b7fe89fdbf70999077e0	14,703,010,061,317.371349097612303393	1.4718%
10	0x202677ca32e4674e9fe2cb35fad794479ace2168	11,624,544,095,070.290564650041502027	1.1636%

Contract functions details

+ [Int] IERC20
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ [Int] IFactory
  - [Ext] createPair #
  - [Ext] getPair

+ [Int] IRouter
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidityETH ($)
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

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

+ [Lib] Address
  - [Int] isContract
  - [Int] sendValue #
  - [Int] functionCall #
  - [Int] functionCall #
  - [Int] functionCallWithValue #
  - [Int] functionCallWithValue #
  - [Int] functionStaticCall
  - [Int] functionStaticCall
  - [Int] functionDelegateCall #
  - [Int] functionDelegateCall #
  - [Prv] _verifyCallResult

+ Context
  - [Int] _msgSender
  - [Int] _msgData

+ Ownable (Context)
  - [Pub] <Constructor> #
  - [Pub] owner
  - [Pub] renounceOwnership #
    - modifiers: onlyOwner
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+ RedKnightToken (IERC20, Ownable)
  - [Pub] <Constructor> #
  - [Ext] <Fallback> ($)
  - [Ext] transfer #
  - [Pub] approve #
  - [Ext] transferFrom #
  - [Ext] increaseAllowance #
  - [Ext] decreaseAllowance #
  - [Prv] _approve #
  - [Prv] _getNow
  - [Ext] launch #
    - modifiers: onlyOwner
  - [Ext] cancelLaunch #
    - modifiers: onlyOwner
  - [Ext] activateTrading #
    - modifiers: onlyOwner
  - [Ext] deactivateTrading #
    - modifiers: onlyOwner
  - [Prv] _setAutomatedMarketMakerPair #
  - [Ext] allowTradingWhenDisabled #
    - modifiers: onlyOwner
  - [Ext] excludeFromFees #
    - modifiers: onlyOwner
  - [Ext] excludeFromMaxWalletLimit #
    - modifiers: onlyOwner
  - [Ext] excludeFromMaxTransactionLimit #
    - modifiers: onlyOwner
  - [Ext] blockAccount #
    - modifiers: onlyOwner
  - [Ext] unblockAccount #
    - modifiers: onlyOwner
  - [Ext] setWallets #

  - modifiers: onlyOwner
- [Ext] setBaseFeesOnBuy #
  - modifiers: onlyOwner
- [Ext] setBaseFeesOnSell #
  - modifiers: onlyOwner
- [Ext] setLaunch2FeesOnBuy #
  - modifiers: onlyOwner
- [Ext] setLaunch2FeesOnSell #
  - modifiers: onlyOwner
- [Ext] setLaunch3FeesOnBuy #
  - modifiers: onlyOwner
- [Ext] setLaunch3FeesOnSell #
  - modifiers: onlyOwner
- [Ext] setMaxWalletAmount #
  - modifiers: onlyOwner
- [Ext] setMaxTransactionAmount #
  - modifiers: onlyOwner
- [Pub] excludeFromDividends #
  - modifiers: onlyOwner
- [Ext] setMinimumTokensBeforeSwap #
  - modifiers: onlyOwner
- [Ext] claimETHOverflow #
  - modifiers: onlyOwner
- [Ext] name
- [Ext] symbol
- [Ext] decimals
- [Ext] totalSupply
- [Pub] balanceOf
- [Ext] totalFees
- [Ext] allowance
- [Ext] isInLaunch
- [Ext] getBaseBuyFees
- [Ext] getBaseSellFees
- [Pub] tokenFromReflection
- [Ext] reflectionFromToken
- [Int] _transfer #
- [Prv] _tokenTransfer #
- [Prv] _reflectFee #
- [Prv] _getTValues
- [Prv] _getRValues
- [Prv] _getRate
- [Prv] _getCurrentSupply
- [Prv] _takeContractFees #
- [Prv] _adjustTaxes #
- [Prv] _setCustomSellTaxPeriod #

- [Prv] _setCustomBuyTaxPeriod #
- [Prv] _swapAndLiquify #
- [Prv] _swapTokensForETH #
- [Prv] _addLiquidity #

($) = 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.**	Low issues
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

1. Out of gas

Issue:

- The function `excludeFromDividends()` uses the loop to find and remove addresses from the _excluded list. Function will be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.
- The function `_getCurrentSupply()` also uses the loop for evaluating total supply. It also could be aborted with OUT_OF_GAS exception if there will be a long excluded addresses list.

Recommendation:
Check that the excluded array length is not too big.

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

- Owner can launch/stop the contract.
- Owner can enable/disable trading.
- Owner can include addresses in _isAllowedToTradeWhenDisabled array.
- Owner can exclude from fees, dividends, max wallet and transaction limit.
- Owner can block/unblock accounts.
- Owner can change all fees.
- Owner can change fee receivers addresses.
- Owner can change maxWalletAmount and maxTxAmount.
- Owner can change minimumTokensBeforeSwap.
- Owner can withdraw contract ETHs.

Conclusion

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

Liquidity locking details are provided by the team:
https://app.unicrypt.network/amm/uni-v2/pair/0xd87a52037d166d20e74abc10ce0ea743e11baf14

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.