TechRate
December, 2022

SMART CONTRACTS SECURITY AUDIT REPORT

Techrate_audits Techrate Techrate1

Audit Details

Audited project

Crab Market

Deployer address

0x9867cc78c4826fb8616b4a3886b0c561df313e01

Client contacts:

https://twitter.com/crabmarketcoin

Blockchain

Ethereum

Project website:

https://crab.finance

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 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 Crab Market to perform an audit of smart contracts:

https://etherscan.io/address/0x24BCeC1AFda63E622a97F17cFf9a61FFCfd9b735#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 02.12.2022

Contract name	Crab Market
Contract address	0x24BCeC1AFda63E622a97F17cFf9a61FFCfd9b735
Total supply	419,674,713.274863614665336084
Token ticker	CRAB
Decimals	18
Token holders	313
Transactions count	5,636
Top 100 holders dominance	97.41%
Burn adjust	10
poolBurnAdjust	100
TotalStaked	162214985082767575611914230
uniPool	0x90eb30Fcb70ba833cB0E7607dd017bc051DDEBEf
Contract deployer address	0x9867cc78c4826fb8616b4a3886b0c561df313e01

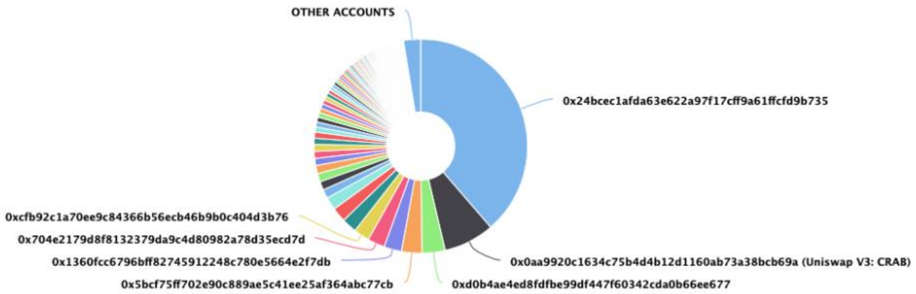
Crab Market Token Distribution

The top 100 holders collectively own 97.41% (408,813,206.75 Tokens) of Crab Market

Token Total Supply: 419,674,713.27 Token | Total Token Holders: 313

Crab Market Top 100 Token Holders

Source: Etherscan.io



(A total of 408,813,206.75 tokens held by the top 100 accounts from the total supply of 419,674,713.27 token)

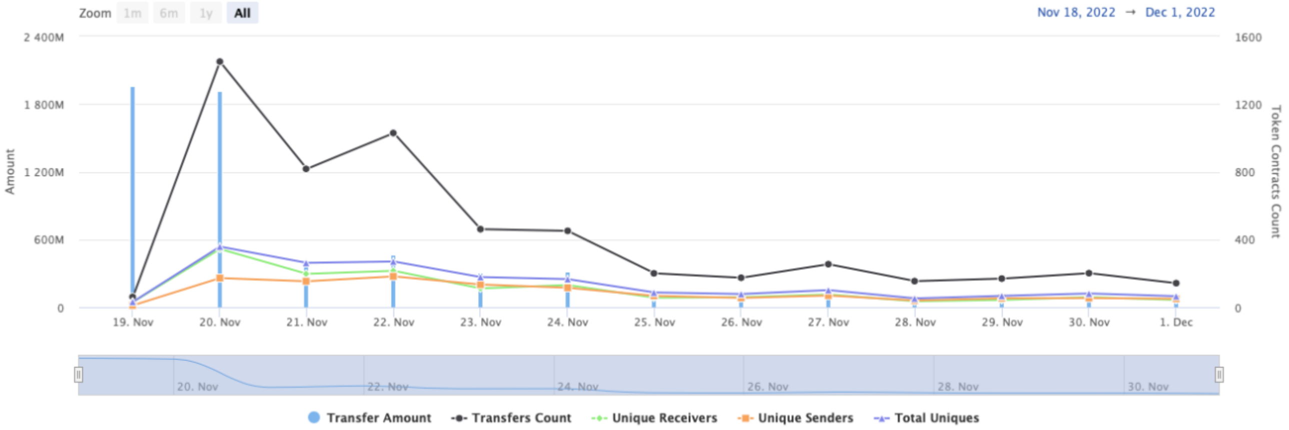
Crab Market Contract Interaction Details

Time Series: Token Contract Overview

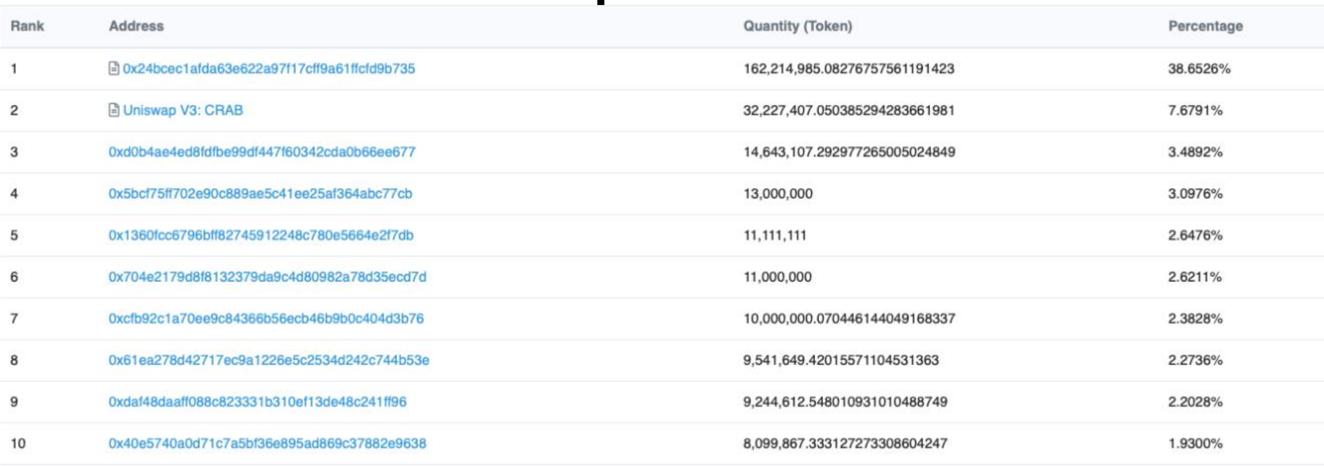
Sat 19, Nov 2022 - Thu 1, Dec 2022

Token Contract 0x24BCeC1AFda63E622a97F17cFf9a61FFCfd9b735 (Crab Market)

Source: Etherscan.io



Crab Market Top 10 Token Holders



Rank	Address	Quantity (Token)	Percentage
1	0x24bcec1afda63e622a97f17cff9a61ffcfd9b735	162,214,985.08276757561191423	38.6526%
2	Uniswap V3: CRAB	32,227,407.050385294283661981	7.6791%
3	0xd0b4ae4ed8fdfbe99df447f60342cda0b66ee677	14,643,107.292977265005024849	3.4892%
4	0x5bcf75ff702e90c889ae5c41ee25af364abc77cb	13,000,000	3.0976%
5	0x1360fcc6796bff82745912248c780e5664e2f7db	11,111,111	2.6476%
6	0x704e2179d8f8132379da9c4d80982a78d35ecd7d	11,000,000	2.6211%
7	0xcfb92c1a70ee9c84366b56ecb46b9b0c404d3b76	10,000,000.070446144049168337	2.3828%
8	0x61ea278d42717ec9a1226e5c2534d242c744b53e	9,541,649.42015571104531363	2.2736%
9	0xdaf48daaff088c823331b310ef13de48c241ff96	9,244,612.548010931010488749	2.2028%
10	0x40e5740a0d71c7a5bf36e895ad869c37882e9638	8,099,867.333127273308604247	1.9300%

Contract functions details

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

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

 + [Lib] Address
   - [Int] isContract
   - [Int] sendValue #

 + [Lib] SafeERC20
   - [Int] safeApprove #
   - [Prv] _callOptionalReturn #

 + [Int] IUniswapV2Router01
   - [Ext] factory
   - [Ext] WETH
   - [Ext] addLiquidity #
   - [Ext] addLiquidityETH ($)
   - [Ext] removeLiquidity #
   - [Ext] removeLiquidityETH #
   - [Ext] removeLiquidityWithPermit #
   - [Ext] removeLiquidityETHWithPermit #
   - [Ext] swapExactTokensForTokens #
   - [Ext] swapTokensForExactTokens #
   - [Ext] swapExactETHForTokens ($)
   - [Ext] swapTokensForExactETH #
   - [Ext] swapExactTokensForETH #
   - [Ext] swapETHForExactTokens ($)
```

```
  - [Ext] quote
  - [Ext] getAmountOut
  - [Ext] getAmountIn
  - [Ext] getAmountsOut
  - [Ext] getAmountsIn

+ [Int] IUniswapV2Router02 (IUniswapV2Router01)
  - [Ext] removeLiquidityETHSupportingFeeOnTransferTokens #
  - [Ext] removeLiquidityETHWithPermitSupportingFeeOnTransferTokens #
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IUniswapV2Pair
  - [Ext] name
  - [Ext] symbol
  - [Ext] decimals
  - [Ext] totalSupply
  - [Ext] balanceOf
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transfer #
  - [Ext] transferFrom #
  - [Ext] DOMAIN_SEPARATOR
  - [Ext] PERMIT_TYPEHASH
  - [Ext] nonces
  - [Ext] permit #
  - [Ext] MINIMUM_LIQUIDITY
  - [Ext] factory
  - [Ext] token0
  - [Ext] token1
  - [Ext] getReserves
  - [Ext] price0CumulativeLast
  - [Ext] price1CumulativeLast
  - [Ext] kLast
  - [Ext] mint #
  - [Ext] burn #
  - [Ext] swap #
  - [Ext] skim #
  - [Ext] sync #

+  TokenEvents

+  CRABMARKET (IERC20, TokenEvents)
  - [Pub] <Constructor> #
```

- [Ext] totalSupply
- [Pub] balanceOf
- [Ext] transfer #
- [Ext] allowance
- [Ext] approve #
- [Ext] transferFrom #
- [Ext] increaseAllowance #
- [Ext] decreaseAllowance #
- [Int] _transfer #
- [Int] _mint #
- [Int] _burn #
- [Int] _approve #
- [Int] _burnFrom #
- [Int] mintInitialTokens #
  - modifiers: synchronized
- [Ext] StakeTokens #
  - modifiers: synchronized
- [Ext] UnstakeTokens #
  - modifiers: synchronized
- [Ext] ClaimStakeInterest #
  - modifiers: synchronized
- [Ext] RollStakeInterest #
  - modifiers: synchronized
- [Int] rollInterest #
- [Int] claimInterest #
- [Ext] BurnCrab #
  - modifiers: synchronized
- [Pub] calcStakingRewards
- [Pub] minsPastStakeTime
- [Pub] isStakeFinished
- [Pub] crabBalance
- [Ext] setUnipool #
  - modifiers: onlyAdmins
- [Ext] setBurnAdjust #
  - modifiers: onlyAdmins
- [Ext] uniPoolBurnAdjust #
  - modifiers: onlyAdmins
- [Ext] revokeAdmin #
  - modifiers: onlyAdmins

($) = 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.

Notes:

- The function BurnCrab() burns amt from the user and poolDiv from the uniPool if poolDiv is higher than amt.

Owner privileges (In the period when the admin is not locked)

- Admin can change uniPool address.
- Admin can change burnAdjust address.
- Admin can change isLocked status.

Testnet deployment

Contracts Description Table

Contract	Type	Bases		
└	**Function Name**	**Visibility**	**Mutability**	**Modifiers**
CRABMARKET	Implementation	IERC20, TokenEvents		
└		Public ❗	🛑	NO❗
└	transfer	External ❗	🛑	NO❗
└	approve	External ❗	🛑	NO❗
└	transferFrom	External ❗	🛑	NO❗
└	increaseAllowance	External ❗	🛑	NO❗
└	decreaseAllowance	External ❗	🛑	NO❗
└	StakeTokens	External ❗	🛑	synchronized
└	ClaimStakeInterest	External ❗	🛑	synchronized
└	RollStakeInterest	External ❗	🛑	synchronized
└	BurnCrab	External ❗	🛑	synchronized
└	setUnipool	External ❗	🛑	onlyAdmins
└	setBurnAdjust	External ❗	🛑	onlyAdmins
└	uniPoolBurnAdjust	External ❗	🛑	onlyAdmins
└	revokeAdmin	External ❗	🛑	onlyAdmins

Legend

Symbol	Meaning
🛑	Function can modify state
💵	Function is payable

Conclusion

Smart contracts do not contain high 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.

Ownership renounce details are provided by the team:
https://etherscan.io/tx/0x016e70b91d5edb11b860d5d522569a1ccfca9c5addac17ad0e2c7e527e1dfaa7

Liquidity locking details are provided by the team:
https://etherscan.io/token/0x80825c93a9e7c9fbf05ee32d629636e4bfb2c9fe?a=0x9867cc78c4826fb8616b4a3886b0c561df313e01

Security score: 90.

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.