Techrate1 Techrate

TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

February, 2022

Audit Details

Audited project

Bored Floki Yacht Club

Deployer address

0x71c87346fd1c86be81fb461443f102cf67b08bfc

Client contacts:

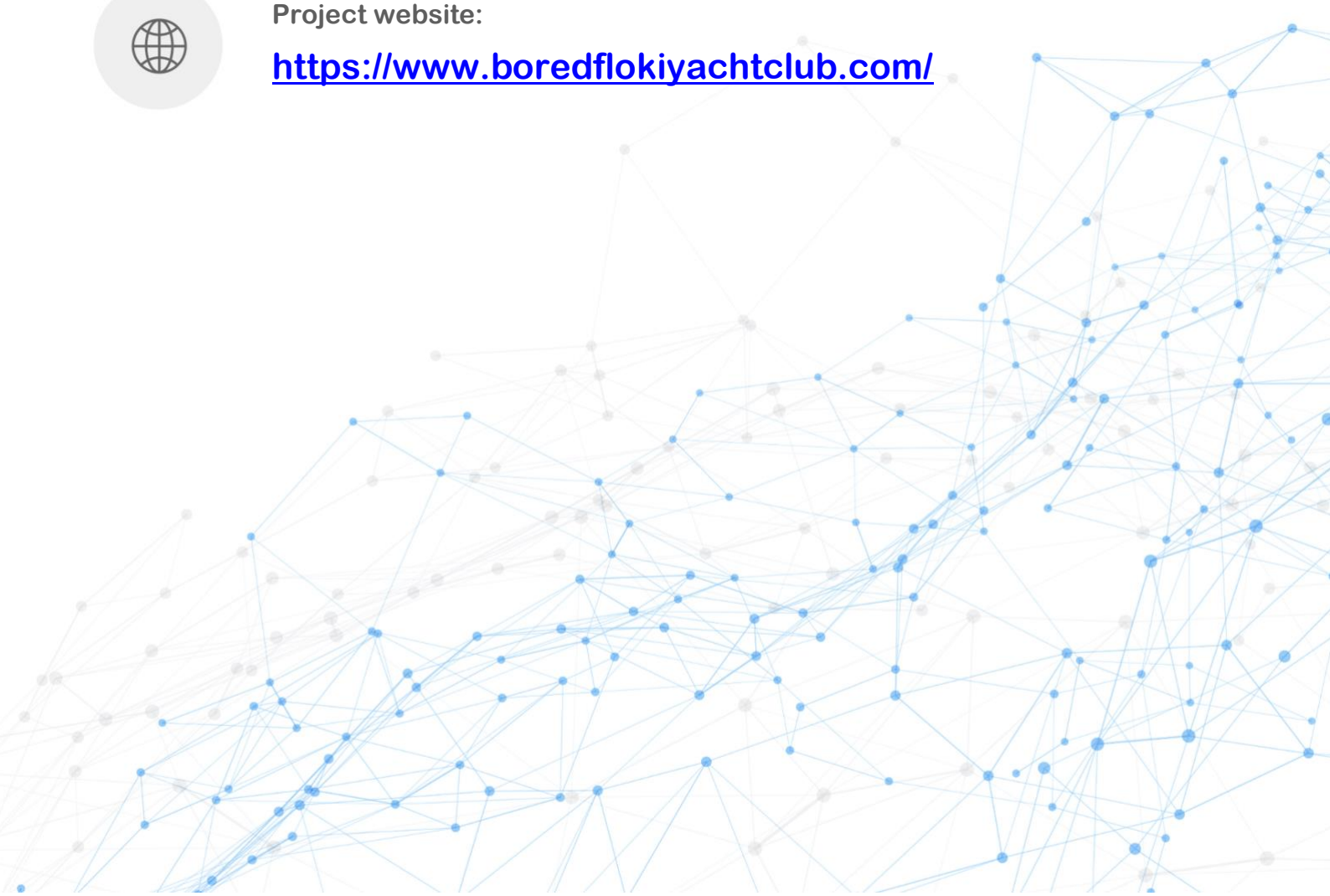
Bored Floki Yacht Club team

Blockchain

Binance Smart Chain

Project website:

https://www.boredflokiyachtclub.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 Bored Floki Yacht Club to perform an audit of smart contracts:

https://bscscan.com/address/0xa627eb25da4bcf6620dff3f3fa87e4117ec71c6d#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

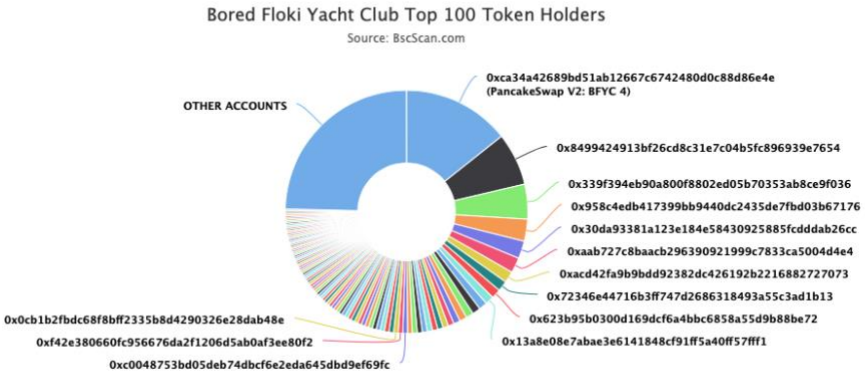
Token contract details for 04.02.2022

Contract name	Bored Floki Yacht Club
Contract address	0xa627Eb25dA4bCF6620DfF3f3fa87e4117eC71c6D
Total supply	100,000,000,000
Token ticker	BFYC
Decimals	9
Token holders	1,394
Transactions count	12,806
Top 100 holders dominance	75.38%
Autoliquidity fee receiver	0x000000000000000000000000000000000000dead
Marketing fee receiver	0x93a3a987fa2859be413e57494f1052015217edf9
Total fee	10
pair	0xca34a42689bd51ab12667c6742480d0c88d86e4e
Contract deployer address	0x71c87346fd1c86be81fb461443f102cf67b08bfc
Contract's current owner address	0x958c4edb417399bb9440dc2435de7fbd03b67176

Bored Floki Yacht Club Token Distribution

The top 100 holders collectively own 75.38% (75,382,067,078.98 Tokens) of Bored Floki Yacht Club

Token Total Supply: 100,000,000,000.00 Token | Total Token Holders: 1,394

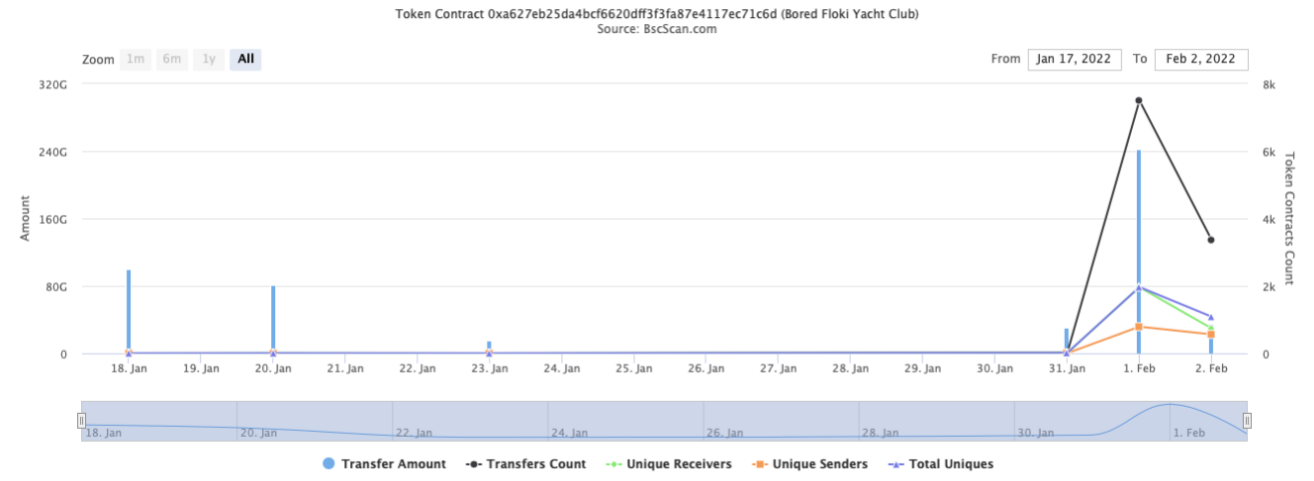


(A total of 75,382,067,078.98 tokens held by the top 100 accounts from the total supply of 100,000,000,000.00 token)

Bored Floki Yacht Club Contract Interaction Details

Time Series: Token Contract Overview

Tue 18, Jan 2022 - Wed 2, Feb 2022



Bored Floki Yacht Club Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	PancakeSwap V2: BFYC 4	14,343,142,098.990288968	14.3431%
2	0x8499424913bf26cd8c31e7c04b5fc896939e7654	7,000,000,000	7.0000%
3	0x339f394eb90a800f8802ed05b70353ab8ce9f036	4,631,448,660.757753992	4.6314%
4	0x958c4edb417399bb9440dc2435de7fbd03b67176	2,931,311,526.132285631	2.9313%
5	0x30da93381a123e184e58430925885fcdddab26cc	2,333,533,442.903743485	2.3335%
6	0xaab727c8baacb296390921999c7833ca5004d4e4	2,038,313,847.450336416	2.0383%
7	0xacd42fa9b9bdd92382dc426192b2216882727073	1,507,243,878.015088145	1.5072%
8	0x72346e44716b3ff747d2686318493a55c3ad1b13	1,379,914,825.07755913	1.3799%
9	0x623b95b0300d169dcf6a4bbc6858a55d9b88be72	1,266,148,807.882406819	1.2661%
10	0x13a8e08e7abae3e6141848cf91ff5a40ff57fff1	1,142,168,692.372035095	1.1422%

Contract functions details

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

+ [Int] IBEP20
  - [Ext] totalSupply
  - [Ext] decimals
  - [Ext] symbol
  - [Ext] name
  - [Ext] getOwner
  - [Ext] balanceOf
  - [Ext] transfer #
  - [Ext] allowance
  - [Ext] approve #
  - [Ext] transferFrom #

+ Auth
  - [Pub] <Constructor> #
  - [Pub] authorize #
    - modifiers: onlyOwner
  - [Pub] unauthorize #
    - modifiers: onlyOwner
  - [Pub] isOwner
  - [Pub] isAuthorized
  - [Pub] transferOwnership #
    - modifiers: onlyOwner

+ [Int] IDEXFactory
  - [Ext] createPair #

+ [Int] IDEXRouter
  - [Ext] factory
  - [Ext] WETH
  - [Ext] addLiquidity #
  - [Ext] addLiquidityETH ($)
  - [Ext] swapExactTokensForTokensSupportingFeeOnTransferTokens #
  - [Ext] swapExactETHForTokensSupportingFeeOnTransferTokens ($)
  - [Ext] swapExactTokensForETHSupportingFeeOnTransferTokens #

+ [Int] IDividendDistributor
  - [Ext] setDistributionCriteria #
  - [Ext] setShare #
  - [Ext] deposit ($)
  - [Ext] process #

+ DividendDistributor (IDividendDistributor)
  - [Pub] <Constructor> #

- [Ext] setDistributionCriteria #
  - modifiers: onlyToken
- [Ext] setShare #
  - modifiers: onlyToken
- [Ext] deposit ($)
  - modifiers: onlyToken
- [Ext] process #
  - modifiers: onlyToken
- [Int] shouldDistribute
- [Int] distributeDividend #
- [Ext] claimDividend #
- [Pub] getUnpaidEarnings
- [Int] getCumulativeDividends
- [Int] addShareholder #
- [Int] removeShareholder #

+ BoredFlokiYachtClub (IBEP20, Auth)
- [Pub] <Constructor> #
  - modifiers: Auth
- [Ext] <Fallback> ($)
- [Ext] totalSupply
- [Ext] decimals
- [Ext] symbol
- [Ext] name
- [Ext] getOwner
- [Pub] balanceOf
- [Ext] allowance
- [Pub] approve #
- [Ext] approveMax #
- [Ext] transfer #
- [Ext] transferFrom #
- [Ext] setMaxWalletPercent #
  - modifiers: onlyOwner
- [Int] _transferFrom #
- [Int] _basicTransfer #
- [Int] checkTxLimit
- [Int] shouldTakeFee
- [Int] takeFee #
- [Int] shouldSwapBack
- [Ext] clearStuckBalance #
  - modifiers: onlyOwner
- [Pub] tradingStatus #
  - modifiers: onlyOwner
- [Pub] cooldownEnabled #
  - modifiers: onlyOwner
- [Int] swapBack #
  - modifiers: swapping
- [Ext] setTxLimit #
  - modifiers: authorized
- [Ext] setIsDividendExempt #
  - modifiers: authorized
- [Ext] setIsFeeExempt #
  - modifiers: authorized
- [Ext] setIsTxLimitExempt #
  - modifiers: authorized

- [Ext] setIsTimelockExempt #
  - modifiers: authorized
- [Ext] setFees #
  - modifiers: authorized
- [Ext] setFeeReceivers #
  - modifiers: authorized
- [Ext] setSwapBackSettings #
  - modifiers: authorized
- [Ext] setSwapThresholdAmount #
  - modifiers: authorized
- [Ext] setTargetLiquidity #
  - modifiers: authorized
- [Ext] setDistributionCriteria #
  - modifiers: authorized
- [Ext] setDistributorSettings #
  - modifiers: authorized
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified

($) = 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)

- Authorized account can change the maximum transaction amount.
- Authorized account can include in and exclude from dividends.
- Authorized account can include in and exclude from fee and transaction amount.
- Authorized account can change fees.
- Authorized account can change fee receivers.
- Authorized account can change swap threshold and disable/enable swap.
- Authorized account can change target liquidity values.
- Authorized account can change distribution criteria.
- Authorized account can change distribution GAS.
- Owner can withdraw BNBs to the marketing address.
- Owner can change cooldown status.
- Owner can change trading status.
- Owner can change max wallet amount restriction.

Conclusion

Smart contracts contain owner privileges! 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.