



TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

August, 2021

Audit Details



Audited project
BabyCosmos



Deployer address
0xeb35a4cae88d3d0cb52c8051e1989e3e21b5dc86



Client contacts:
BabyCosmos team



Blockchain
Binance Smart Chain



Project website:
www.babycosmos.net

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 BabyCosmos to perform an audit of smart contracts:

<https://bscscan.com/address/0x49febfcc9dc63069ff9f4ea47d12da741878bb48#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 21.08.2021

Contract name	BabyCosmos
Contract address	0x49fEBFcC9DC63069ff9f4Ea47D12DA741878bB48
Total supply	200,000,000
Token ticker	\$BabyCosmos
Decimals	4
Token holders	247
Transactions count	4,284
Top 100 holders dominance	96.96%
Total fee	18
Autoliquidity fee receiver	0x686f4a0bc1a63840095d54387af3046a97829c8c
Marketing fee receiver	0x686f4a0bc1a63840095d54387af3046a97829c8c
Pair	0x87ed36506800c623d637c395a31b0cf4e29cddf4
Contract deployer address	0xEB35a4Cae88D3D0Cb52C8051E1989E3e21B5dC86
Contract's current owner address	0xEB35a4Cae88D3D0Cb52C8051E1989E3e21B5dC86

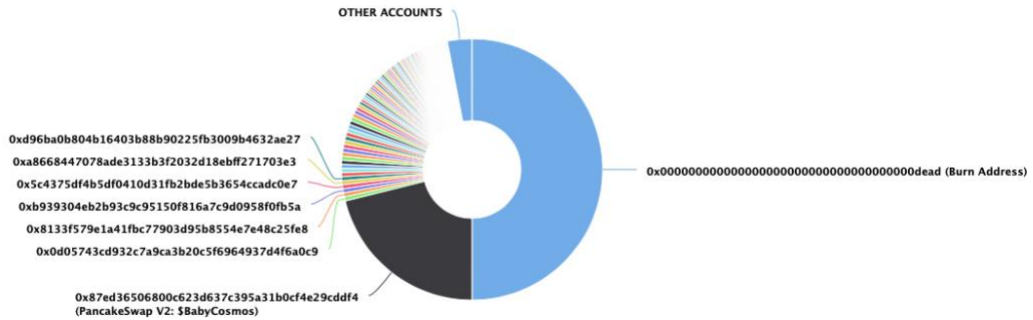
BabyCosmos Token Distribution

The top 100 holders collectively own 96.96% (193,925,500.15 Tokens) of BabyCosmos

Token Total Supply: 200,000,000.00 Token | Total Token Holders: 247

BabyCosmos Top 100 Token Holders

Source: BscScan.com



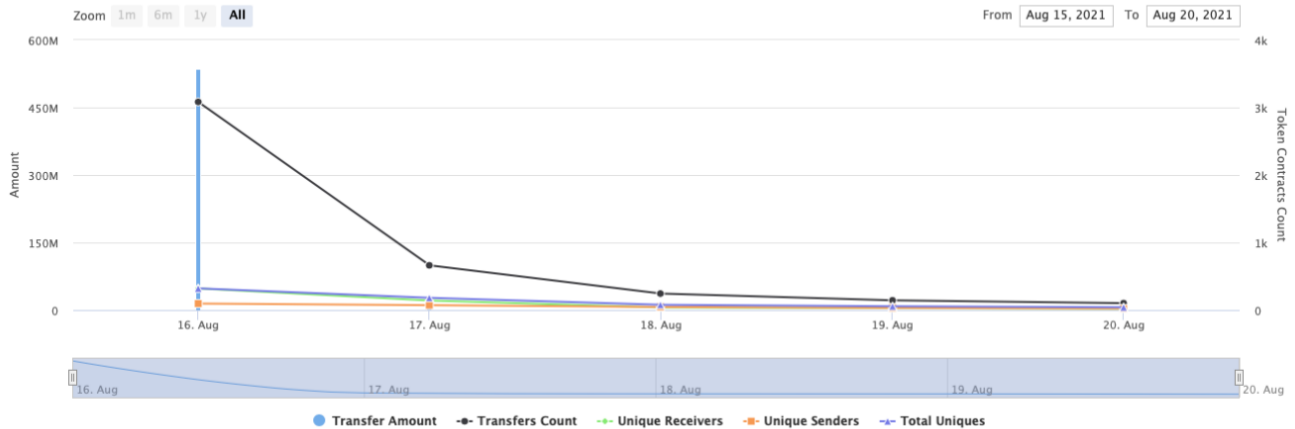
(A total of 193,925,500.15 tokens held by the top 100 accounts from the total supply of 200,000,000.00 token)

BabyCosmos Contract Interaction Details

Time Series: Token Contract Overview

Mon 16, Aug 2021 - Fri 20, Aug 2021

Token Contract 0x49febfc9dc63069ff9f4ea47d12da741878bb48 (BabyCosmos)
Source: BscScan.com



BabyCosmos Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	Burn Address	100,000,000	50.0000%
2	PancakeSwap V2: \$BabyCosmos	42,283,600.1046	21.1418%
3	0x0d05743cd932c7a9ca3b20c5f6964937d4f6a0c9	1,000,000	0.5000%
4	0x8133f579e1a41fbc77903d95b8554e7e48c25fe8	1,000,000	0.5000%
5	0xb939304eb2b93c9c95150f816a7c9d0958f0fb5a	1,000,000	0.5000%
6	0x5c4375df4b5df0410d31fb2bde5b3654ccadc0e7	999,999.918	0.5000%
7	0xa8668447078ade3133b3f2032d18ebff271703e3	999,999.8812	0.5000%
8	0xd96ba0b804b16403b88b90225fb3009b4632ae27	999,999.702	0.5000%
9	0xdf64d86925a56404d6a891d49a3e9ca22decfc63	999,999.46	0.5000%
10	0xc64eef7a324883d7ad71f568a1dcc194c0c7a20f	999,999.18	0.5000%



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 #
- + BabyCosmos (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: onlyOwner
- [Ext] setFeeReceivers #
 - modifiers: onlyOwner
- [Ext] setSwapBackSettings #
 - modifiers: authorized
- [Ext] setTargetLiquidity #
 - modifiers: authorized
- [Ext] setDistributionCriteria #
 - modifiers: authorized
- [Ext] setDistributorSettings #
 - modifiers: authorized
- [Pub] getCirculatingSupply
- [Pub] getLiquidityBacking
- [Pub] isOverLiquified
- [Ext] airdrop #
 - 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.	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 `airdrop()` uses the loop to airdrop rewards by the list. Function will be aborted with `OUT_OF_GAS` exception if there will be a long receivers list.

```
ftrace | funcSig
function airdrop(address from↑, address[] calldata addresses↑, uint256[] calldata tokens↑) external onlyOwner {
    uint256 SCCC = 0;

    require(addresses↑.length == tokens↑.length, "Mismatch between Address and token count");

    for(uint i=0; i < addresses↑.length; i++){
        SCCC = SCCC + tokens↑[i];
    }

    require(balanceOf(from↑) >= SCCC, "Not enough tokens in wallet for airdrop");

    for(uint i=0; i < addresses↑.length; i++){
        _basicTransfer(from↑, addresses↑[i], tokens↑[i]);
        if(!isDividendExempt[addresses↑[i]]) {
            try distributor.setShare(addresses↑[i], _balances[addresses↑[i]]) {} catch {}
        }
    }

    // Dividend tracker
    if(!isDividendExempt[from↑]) {
        try distributor.setShare(from↑, _balances[from↑]) {} catch {}
    }
}
```

Recommendation:

Check that the array length is not too big.

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

- Owner can change the maximum transaction amount.
- Owner can include in and exclude from dividends.
- Owner can include in and exclude from fee and transaction amount.
- Owner can change fees.
- Owner can change fee receivers.
- Owner can change swap threshold and disable/enable swap.
- Owner can change target liquidity values.
- Owner can change distribution criteria.
- Owner can change distribution GAS.
- Owner can change setMaxWalletPercent.
- Owner can withdraw BNBs to the marketing receiver address.
- Owner can change trading status.
- Owner can change cooldown status.
- Owner can change buybackKeepItSimple value.
- Owner can change addresses' isTimelockExempt value.

Conclusion

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

Liquidity locking details provided by the team:

https://dxsale.app/app/v2_9/dxlockview?id=0&add=0xEB35a4Cae88D3D0Cb52C8051E1989E3e21B5dC86&type=lplock&chain=BSC

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.