TechRate

AUDIT COMPANY

Smart Contract Security Audit

TechRate

September, 2021

Audit Details

Audited project

BabyYorkie

Deployer address

0x4eeb7a903cc5e16f5cf99e3eb2de94a51794fae9

Client contacts:

BabyYorkie team

Blockchain

Binance Smart Chain

Project website:

https://babyyorkie.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 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 BabyYorkie to perform an audit of smart contracts:

https://bscscan.com/address/0x50976c57a3a1923b55b76393451dac1e24a0a08d#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 11.09.2021

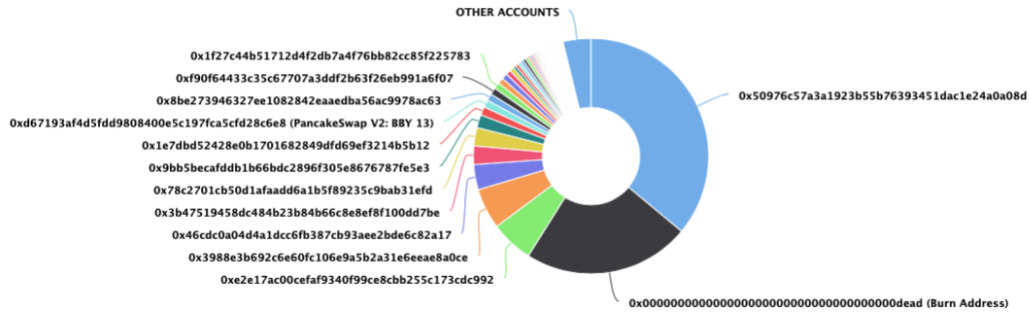|	
Contract name	BabyYorkie
Contract address	0x50976c57a3A1923B55b76393451Dac1e24A0A08d
Total supply	21,000,000,000,000
Token ticker	BBY
Decimals	9
Token holders	2,453
Transactions count	11,428
Top 100 holders dominance	96.18%
Liquidity fee	3
Tax fee	5
Total fees	2945973701950127066407
Uniswap V2 pair	0xd67193af4d5fdd9808400e5c197fca5cfd28c6e8
Contract deployer address	0x4eeb7a903cc5e16f5cf99e3eb2de94a51794fae9
Contract's current owner address	0x0000000000000000000000000000000000000000

BabyYorkie Token Distribution

BabyYorkie Top 100 Token Holders
Source: BscScan.com

OTHER ACCOUNTS

0x1f27c44b51712d4f2db7a4f76bb82cc85f225783
0xf90f64433c35c67707a3ddf2b63f26eb991a6f07
0x8be273946327ee1082842eaaedba56ac9978ac63
0xd67193af4d5fdd9808400e5c197fca5cfd28c6e8 (PancakeSwap V2: BBY 13)
0x1e7dbd52428e0b1701682849dfd69ef3214b5b12
0x9bb5becafddb1b66bdc2896f305e8676787fe5e3
0x78c2701cb50d1afaadd6a1b5f89235c9bab31efd
0x3b47519458dc484b23b84b66c8e8ef8f100dd7be
0x46cdc0a04d4a1dcc6fb387cb93aee2bde6c82a17
0x3988e3b692c6e60fc106e9a5b2a31e6eeae8a0ce
0xe2e17ac00cefaf9340f99ce8cbb255c173cdc992

0x50976c57a3a1923b55b76393451dac1e24a0a08d

0x0000000000000000000000000000000000000dead (Burn Address)

(A total of 20,197,474,819,355.50 tokens held by the top 100 accounts from the total supply of 21,000,000,000,000.00 token)

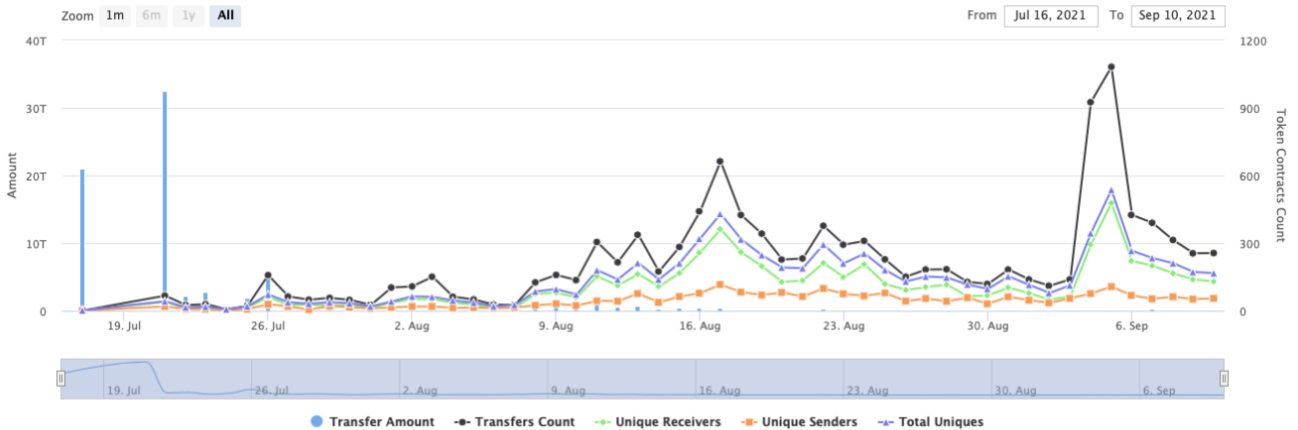# BabyYorkie Contract Interaction Details

Time Series: Token Contract Overview   Sat 17, Jul 2021 - Fri 10, Sept 2021

Token Contract 0x50976c57a3a1923b55b76393451dac1e24a0a08d (BabyYorkie)
Source: BscScan.com

Zoom 1m 6m 1y All   From Jul 16, 2021   To Sep 10, 2021

Transfer Amount   Transfers Count   Unique Receivers   Unique Senders   Total Uniques

BabyYorkie Top 10 Token Holders

Rank	Address	Quantity (Token)	Percentage
1	0x50976c57a3a1923b55b76393451dac1e24a0a08d	7,567,800,823,166.820798512	36.0371%
2	Burn Address	4,812,537,814,019.153102088	22.9168%
3	0xe2e17ac00cefaf9340f99ce8cbb255c173cdc992	1,230,888,807,921.663455967	5.8614%
4	0x3988e3b692c6e60fc106e9a5b2a31e6eeae8a0ce	1,175,789,761,464.770696095	5.5990%
5	0x46cdc0a04d4a1dcc6fb387cb93aee2bde6c82a17	722,034,630,621.695227577	3.4383%
6	0x3b47519458dc484b23b84b66c8e8ef8f100dd7be	537,254,426,346.342368485	2.5584%
7	0x78c2701cb50d1afaadd6a1b5f89235c9bab31efd	524,514,919,126.574702906	2.4977%
8	0x9bb5becafddb1b66bdc2896f305e8676787fe5e3	372,938,640,785.501676493	1.7759%
9	0x1e7dbd52428e0b1701682849dfd69ef3214b5b12	247,047,711,972.314928833	1.1764%
10	PancakeSwap V2: BBY 13	210,207,450,630.949626456	1.0010%

BabyYorkie LP Token Holders

Rank	Address	Quantity	Percentage
1	0x8655e5c4d701186d16765d1cdcef6d5287e4679a	103.668664947514394971	77.6597%
2	0x78c2701cb50d1afaadd6a1b5f89235c9bab31efd	28.528540737029831151	21.3711%
3	0xe2e17ac00cefaf9340f99ce8cbb255c173cdc992	1.203518916169087041	0.9016%
4	0x8cc7bc33f5188b1fb683bedc4dbffa77b136833b	0.079945789508684905	0.0599%
5	0x96ab1d0bd938b24ea3e61750b259e7980d4622b6	0.01023958809289424	0.0077%
6	0x0000000000000000000000000000000000000000	0.000000000000001	0.0000%

Contract functions details

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

+ [Lib] SafeMath
- [Int] tryAdd
- [Int] trySub
- [Int] tryMul
- [Int] tryDiv
- [Int] tryMod
- [Int] add
- [Int] sub
- [Int] mul
- [Int] div
- [Int] mod
- [Int] sub
- [Int] div
- [Int] mod

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

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

+ Ownable (Context)
- **[Pub]** owner
- **[Pub]** renounceOwnership **#**
  - modifiers: onlyOwner
- **[Pub]** transferOwnership **#**
  - modifiers: onlyOwner
- **[Pub]** lock **#**
  - modifiers: onlyOwner
- **[Pub]** unlock **#**

+ [Int] IUniswapV2Factory

- **[Ext]** feeTo
- **[Ext]** feeToSetter
- **[Ext]** getPair
- **[Ext]** allPairs
- **[Ext]** allPairsLength
- **[Ext]** createPair **#**
- **[Ext]** setFeeTo **#**
- **[Ext]** setFeeToSetter **#**

+ [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 **#**
- **[Ext]** initialize **#**

+ [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 **#**

+ **CoinToken (Context, IERC20, Ownable)**
  - **[Pub] <Constructor> ($)**
  - **[Pub]** name
  - **[Pub]** symbol
  - **[Pub]** decimals
  - **[Pub]** totalSupply
  - **[Pub]** balanceOf
  - **[Pub]** transfer **#**
  - **[Pub]** allowance
  - **[Pub]** approve **#**
  - **[Pub]** transferFrom **#**
  - **[Pub]** increaseAllowance **#**
  - **[Pub]** decreaseAllowance **#**
  - **[Pub]** isExcludedFromReward
  - **[Pub]** totalFees
  - **[Pub]** deliver **#**
  - **[Pub]** reflectionFromToken
  - **[Pub]** tokenFromReflection
  - **[Pub]** excludeFromReward **#**
    - modifiers: onlyOwner
  - **[Ext]** includeInReward **#**
    - modifiers: onlyOwner
  - **[Prv]** _transferBothExcluded **#**
  - **[Pub]** excludeFromFee **#**
    - modifiers: onlyOwner
  - **[Pub]** includeInFee **#**
    - modifiers: onlyOwner
  - **[Ext]** setTaxFeePercent **#**
    - modifiers: onlyOwner
  - **[Ext]** setDevFeePercent **#**
    - modifiers: onlyOwner
  - **[Ext]** setLiquidityFeePercent **#**
    - modifiers: onlyOwner
  - **[Pub]** setMaxTxPercent **#**
    - modifiers: onlyOwner
  - **[Pub]** setDevWalletAddress **#**
    - modifiers: onlyOwner
  - **[Pub]** setSwapAndLiquifyEnabled **#**
    - modifiers: onlyOwner
  - **[Ext] <Fallback> ($)**
  - **[Prv]** _reflectFee **#**
  - **[Prv]** _getValues
  - **[Prv]** _getTValues
  - **[Prv]** _getRValues

- **[Prv]** _getRate
- **[Prv]** _getCurrentSupply
- **[Prv]** _takeLiquidity **#**
- **[Prv]** _takeDev **#**
- **[Prv]** calculateTaxFee
- **[Prv]** calculateDevFee
- **[Prv]** calculateLiquidityFee
- **[Prv]** removeAllFee **#**
- **[Prv]** restoreAllFee **#**
- **[Pub]** isExcludedFromFee
- **[Prv]** _approve **#**
- **[Prv]** _transfer **#**
- **[Prv]** swapAndLiquify **#**
  - modifiers: lockTheSwap
- **[Prv]** swapTokensForEth **#**
- **[Prv]** addLiquidity **#**
- **[Prv]** _tokenTransfer **#**
- **[Prv]** _transferStandard **#**
- **[Prv]** _transferToExcluded **#**
- **[Prv]** _transferFromExcluded **#**
- **[Ext]** setRouterAddress **#**
  - modifiers: onlyOwner
- **[Ext]** setNumTokensSellToAddToLiquidity **#**
  - 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 **includeInReward()** 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.

```solidity
function includeInReward(address account↑) external onlyOwner() {
    require(_isExcluded[account↑], "Account is already excluded");
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (_excluded[i] == account↑) {
            _excluded[i] = _excluded[_excluded.length - 1];
            _tOwned[account↑] = 0;
            _isExcluded[account↑] = false;
            _excluded.pop();
            break;
        }
    }
}
```

- 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.

```solidity
function _getCurrentSupply() private view returns (uint256, uint256) {
    uint256 rSupply = _rTotal;
    uint256 tSupply = _tTotal;
    for (uint256 i = 0; i < _excluded.length; i++) {
        if (
            _rOwned[_excluded[i]] > rSupply ||
            _tOwned[_excluded[i]] > tSupply
        ) return (_rTotal, _tTotal);
        rSupply = rSupply.sub(_rOwned[_excluded[i]]);
        tSupply = tSupply.sub(_tOwned[_excluded[i]]);
    }
    if (rSupply < _rTotal.div(_tTotal)) return (_rTotal, _tTotal);
    return (rSupply, tSupply);
}
```

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

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

- Owner can change the tax, dev and liquidity fee.

```
ftrace | funcSig
function setTaxFeePercent(uint256 taxFee⬆) external onlyOwner() {
    _taxFee = taxFee⬆;
}


ftrace | funcSig
function setDevFeePercent(uint256 devFee⬆) external onlyOwner() {
    _devFee = devFee⬆;
}


ftrace | funcSig
function setLiquidityFeePercent(uint256 liquidityFee⬆) external onlyOwner() {
    _liquidityFee = liquidityFee⬆;
}
```

- Owner can change the maximum transaction amount.

```
function setMaxTxPercent(uint256 maxTxPercent⬆) public onlyOwner {
    _maxTxAmount = maxTxPercent⬆  * 10 ** _decimals;
}
```

- Owner can exclude from the fee.

```
function excludeFromFee(address account⬆) public onlyOwner {
    _isExcludedFromFee[account⬆] = true;
}
```

- Owner can change dev address.

```
function setDevWalletAddress(address _addr⬆) public onlyOwner {
    _devWalletAddress = _addr⬆;
}
```

- Owner can change router address.

```
function setRouterAddress(address newRouter⬆) external onlyOwner {
    IUniswapV2Router02 _uniswapV2Router = IUniswapV2Router02(newRouter⬆);
    uniswapV2Pair = IUniswapV2Factory(_uniswapV2Router.factory()).createPair(address(this), _uniswapV2Router.WETH());
    uniswapV2Router = _uniswapV2Router;
}
```

- Owner can minimum number of tokens to add to liquidity.

```
function setNumTokensSellToAddToLiquidity(uint256 amountToUpdate⬆) external onlyOwner {
    numTokensSellToAddToLiquidity = amountToUpdate⬆;
}
```

- **Owner can lock and unlock. By the way, using these functions the owner could retake privileges even after the ownership was renounced.**

```solidity
    //Locks the contract for owner for the amount of time provided
function lock(uint256 time↑) public virtual onlyOwner {
    _previousOwner = _owner;
    _owner = address(0);
    _lockTime = time↑;
    emit OwnershipTransferred(_owner, address(0));
}


//Unlocks the contract for owner when _lockTime is exceeds
function unlock() public virtual {
    require(_previousOwner == msg.sender, "You don't have permission to unlock.");
    require(block.timestamp > _lockTime , "Contract is locked.");
    emit OwnershipTransferred(_owner, _previousOwner);
    _owner = _previousOwner;
}
```

Conclusion

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

Liquidity locking details are NOT provided by the team.

Ownership renounce details are provided by the team:
https://bscscan.com/address/0x50976c57a3a1923b55b76393451dac1e24a0a08d#readContract

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.