Coinsult

Advanced Manual Smart Contract Audit

Project: 1Cent
Website: https://1centdream.online/

Low-risk	Medium-risk	High-risk
6 low-risk code issues found	0 medium-risk code issues found	0 high-risk code issues found

Contract address
0xAe4d7B8e83bacc7469615565aa0B5030f01334B5

Disclaimer

Coinsult is not responsible if a project turns out to be a scam, rug-pull or honeypot. We only provide a detailed analysis for your own research.

Coinsult is not responsible for any financial losses. Nothing in this contract audit is financial advice, please do your own research.

The information provided in this audit is for informational purposes only and should not be considered investment advice. Coinsult does not endorse, recommend, support or suggest to invest in any project.

Coinsult can not be held responsible for when a project turns out to be a rug-pull, honeypot or scam.

Tokenomics

Rank	Address	Quantity (Token)	Percentage
1	Null Address: 0xdea...069	251,843,463,423,699	50.3687%
2	0x60bbdf6287f5bca0d8480f930d823463dc29f77a (CA)	189,618,261,893,962	37.9237%
3	PinkSale: PinkLock (CA)	15,001,300,000,000	3.0003%
4	0x2608828334500e5eb3f3b86f9d0f33a636ddba0f	8,734,282,052,401.952633883813518827	1.7469%
5	0xb8fef6f92f16dee71bbd73ac0ec828ab9e1671ae	8,556,331,208,705.335700600883318666	1.7113%
6	0x135bfe77bb3207612fce36b5f01d04f42c8ec281 (CA)	2,500,000,000,000	0.5000%
7	PancakeSwap V2: 1Cent 4 (CA)	1,696,913,158,094.744549881926649344	0.3394%
8	0x5938dee0d922e6dc8f6a6e846432a2b71bc4b7ab	1,320,000,000,000	0.2640%
9	0xe8e1d7969b8c226e8bdc6f14bd993d588e0bad52	830,455,546,253.383110465327647625	0.1661%
10	0xbcc6e4a8fe389d6c0907b5d1862142f16102452c	800,000,000,000	0.1600%

Source code

Coinsult was commissioned by 1Cent to perform an audit based on the following smart contract:

https://bscscan.com/address/0xAe4d7B8e83bacc7469615565aa0B5030f01334B5#code

Manual Code Review

🟢 Low-risk

6 low-risk code issues found.
Could be fixed, will not bring problems.

- Contract contains Reentrancy vulnerabilities:
  Additional information: This combination increases risk of malicious intent. While it may be justified by some complex mechanics (e.g. rebase, reflections, buyback).
  More information: Slither

```
    function _transfer(
        address sender,
        address recipient,
        uint256 amount
    ) internal virtual {
        require(sender != address(0), "ERC20: transfer from the zero address");
        require(recipient != address(0), "ERC20: transfer to the zero address");

        _beforeTokenTransfer(sender, recipient, amount);

        uint256 senderBalance = _balances[sender];
        require(senderBalance >= amount, "ERC20: transfer amount exceeds balance");
        unchecked {
            _balances[sender] = senderBalance - amount;
        }
        _balances[recipient] += amount;

        emit Transfer(sender, recipient, amount);

        _afterTokenTransfer(sender, recipient, amount);
    }
```

- Avoid relying on block.timestamp
  block.timestamp can be manipulated by miners.

```
block.timestamp
```

- Missing zero address validation
  Check that the new address is not the zero address.

```
       function setMarketingWallet(address payable wallet) external
onlyOwner {
        _marketingWalletAddress = wallet;
    }
```

- The return value of an external transfer/transferFrom call is not checked
  Use SafeERC20, or ensure that the transfer/transferFrom return value is checked.

```
function swapAndSendToFee(uint256 tokens) private {
        uint256 initialCAKEBalance = IERC20(rewardToken).balanceOf(
            address(this)
        );

        swapTokensForCake(tokens);
        uint256 newBalance =
(IERC20(rewardToken).balanceOf(address(this))).sub(
            initialCAKEBalance
        );
        IERC20(rewardToken).transfer(_marketingWalletAddress,
newBalance);
    }
```

- Literals with many digits are difficult to read and review.
  Recommendation: Use Ether suffix, Time suffix, or The scientific notation

```
require(
            newValue >= 200000 && newValue <= 500000,
            "BABYTOKEN: gasForProcessing must be between 200,000 and
500,000"
        );
```

- Calls inside a loop might lead to a denial-of-service attack.
  _withdrawDividendOfUser() (#2141-2167) has external calls inside a loop:
  IERC20(rewardToken).transfer()

```
function _withdrawDividendOfUser(address payable user)
        internal
        returns (uint256)
    {
        uint256 _withdrawableDividend = withdrawableDividendOf(user);
        if (_withdrawableDividend > 0) {
            withdrawnDividends[user] = withdrawnDividends[user].add(
                _withdrawableDividend
            );
            emit DividendWithdrawn(user, _withdrawableDividend);
            bool success = IERC20(rewardToken).transfer(
                user,
                _withdrawableDividend
            );

            if (!success) {
                withdrawnDividends[user] =
withdrawnDividends[user].sub(
                    _withdrawableDividend
                );
                return 0;
            }

            return _withdrawableDividend;
        }
```

🟡 Medium-risk

0 medium-risk code issues found.
Should be fixed, could bring problems.

🔴 High-risk

0 high-risk code issues found
Must be fixed, and will bring problems.

Extra notes by the team

🟢 Fees can be set up to 25% for both buy and sell fees.

```
function setLiquiditFee(uint256 value) external onlyOwner {
        liquidityFee = value;
        totalFees =
tokenRewardsFee.add(liquidityFee).add(marketingFee);
        require(totalFees <= 25, "Total fee is over 25%");
    }

    function setMarketingFee(uint256 value) external onlyOwner {
        marketingFee = value;
        totalFees =
tokenRewardsFee.add(liquidityFee).add(marketingFee);
        require(totalFees <= 25, "Total fee is over 25%");
    }
```

🟡 Owner can exclude addresses from dividends.

🟡 Owner can exclude addresses from fees.

🟡 Owner can change the router address.

🟡 The ownership of the contract isn’t renounced.

Contract Snapshot

```
contract BABYTOKEN is ERC20, Ownable, BaseToken {
    using SafeMath for uint256;

    uint256 public constant VERSION = 1;

    IUniswapV2Router02 public uniswapV2Router;
    address public uniswapV2Pair;

    bool private swapping;

    BABYTOKENDividendTracker public dividendTracker;

    address public rewardToken;

    uint256 public swapTokensAtAmount;

    uint256 public tokenRewardsFee;
    uint256 public liquidityFee;
    uint256 public marketingFee;
    uint256 public totalFees;

    address public _marketingWalletAddress;

    uint256 public gasForProcessing;
```

Website Review

Coinsult checks the website completely manually and looks for visual, technical and textual errors. We also look at the security, speed and accessibility of the website. In short, a complete check to see if the website meets the current standard of the web development industry.

- 🔴 Mobile Friendly
- 🟢 Contains no jQuery errors
- 🟢 SSL Secured
- 🟢 No major spelling errors

Loading speed: 74%

Rug-pull Review

Based on the available information analyzed by us, we come to the following conclusions:

🟢 Locked Liquidity

🟢 No large unlocked wallets

🟡 No doxxed Team

Honeypot Review

Based on the available information analyzed by us, we come to the following conclusions:

🟢 Ability to sell

🟢 Owner is not able to pause the contract

🟡 Router can be changed

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 the project owner.