



Coinsult

Advanced Manual Smart Contract Audit



Project: Crypto

Website: <https://cryptomoney.bet/>

Low-risk

5 low-risk code
issues found

Medium-risk

0 medium-risk code
issues found

High-risk

0 high-risk code
issues found

Contract address

0x807F7D3Db25B4D4e2f799340D74ed6De9aa4d97D

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

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	0xf0d24558d838d972bf52e7a41d5e27bb25570001	100,000,000,000	100.000%

Source code

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

<https://bscscan.com/address/0x807f7d3db25b4d4e2f799340d74ed6de9aa4d97d#code>

Manual Code Review

● Low-risk

5 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.

```
secondsUntilAutoClaimAvailable = nextClaimTime > block.timestamp
    ? nextClaimTime.sub(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"
);
```

● **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

- Owner can exclude addresses from dividends.
- Owner can exclude addresses from fees.
- The ownership of the contract isn't renounced.
- Owner can change the router address.
- Fees can be set up to 25% for both buy and sell fees.

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

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%");
}
```

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: 79%

Rug-pull Review

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

- Locked Liquidity (no liquidity yet)
- Large unlocked wallets
 - Note: Tokens not distributed yet
- 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.