

SKELETON ECOSYSTEM

SMART CONTRACT AUDIT



BALDO INU
(BALDO INU)
ERC20

0x5a132d92D5566AD1e2495a5AaD4770b9F438



Table of Contents

| | |
|---------------------------------------|----|
| Table of Contents | 1 |
| Disclaimer | 2 |
| Overview | 3 |
| Creation/Audit Date | 3 |
| Verified Socials | 3 |
| Contract Functions Analysis | 4 |
| Contract Safety and Weakness | 8 |
| Detected Vulnerability Description | 12 |
| Contract Flow Graph | 16 |
| Contract Interaction Graph | 17 |
| Inheritance Graph | 18 |
| Contract Descriptions | 19 |
| Audit Scope | 31 |

Global Disclaimer

This document serves as a disclaimer for the crypto smart contract audit conducted by Skeleton Ecosystem. The purpose of the audit was to review the codebase of the smart contracts for potential vulnerabilities and issues. It is important to note the following:

Limited Scope: The audit is based on the code and information available up to the audit completion date. It does not cover external factors, system interactions, or changes made after the audit. The audit itself can not guarantee 100% safety and can not detect common scam methods like farming and developer sell-out.

No Guarantee of Security: While we have taken reasonable steps to identify vulnerabilities, it is impossible to guarantee the complete absence of security risks or issues. The audit report provides an assessment of the contract's security as of the audit date.

Continued Development: Smart contracts and blockchain technology are evolving fields. Updates, forks, or changes to the contract post-audit may introduce new risks that were not present during the audit.

Third-party Code: If the smart contract relies on third-party libraries or code, those components were not thoroughly audited unless explicitly stated. Security of these dependencies is the responsibility of their respective developers.

Non-Exhaustive Testing: The audit involved automated analysis, manual review, and testing under controlled conditions. It is possible that certain vulnerabilities or issues may not have been identified.

Risk Evaluation: The audit report includes a risk assessment for identified vulnerabilities. It is recommended that the development team carefully reviews and addresses these risks to mitigate potential exploits.

Not Financial Advice: This audit report is not intended as financial or investment advice. Decisions regarding the use, deployment, or investment in the smart contract should be made based on a comprehensive assessment of the associated risks.

By accessing and using this audit report, you acknowledge and agree to the limitations outlined above. Skeleton Ecosystem and its auditors shall not be held liable for any direct or indirect damages resulting from the use of the audit report or the smart contract itself.

Please consult with legal, technical, and financial professionals before making any decisions related to the smart contract.

Overview

| | |
|-----------------------|---|
| Contract Name | BALDO_INU |
| Ticker/Symbol | BALDO INU |
| Blockchain | Ethereum ERC20 BASE |
| Contract Address | 0x5a132d92D5566AD1e2495a5AaD4770b9F4388927 |
| Creator Address | 0xFdb9ebD5331eDa60becF6FFc3A46fA0A0e6D437a |
| Current Owner Address | 0x00 |
| Contract Explorer | https://basescan.org/token/0x5a132d92d5566ad1e2495a5aad4770b9f4388927#code |
| Compiler Version | v0.8.19+commit.7dd6d404 |
| License | None |
| Optimisation | Yes with 200 Runs |
| Total Supply | 1,000,000 BALDO INU |
| Decimals | 9 |

Creation/Audit

| | |
|-------------------|------------|
| Contract Deployed | 20.04.2024 |
| Audit Created | 22.04.2024 |
| Audit Update | V 1.0 |

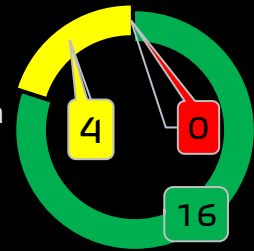
Verified Socials








| | |
|-------------|---|
| Website | https://baldoinu.com/ |
| Telegram | https://t.me/baldo_inu |
| Twitter (X) | https://x.com/baldoinu |











Contract Function Analysis

 Pass
  Attention Item
  Risky Item

■ Pass
 ■ Attention
 ■ Risk



| | | |
|---------------------------|---|---|
| Contract Verified |  | The contract source code is uploaded to blockchain explorer and is open source, so everybody can read it. |
| Contract Ownership | | 0x00 |
| Buy Tax | 5 % | Shows the taxes for purchase transactions. Above 10% may be considered a high tax rate. More than 50% tax rate means may not be tradable. Fee can be set! |
| Sell Tax | 5 % | Shows the taxes for sell transactions. Above 10% may be considered a high tax rate. More than 50% tax rate means may not be tradable. Fee can be set! |
| Honeypot Analyse |  | Holder is able to buy and sell. If honeypot: The contract blocks sell transfer from holder wallet. Multiple events may cause honeypot. Trading disabled, extremely high tax |
| Liquidity Status |  | Liquidity status on 22.04.2024 Lp Locked: 94.7% Onlymoons Locker until 09.07.2025 Lp Burned: 5.3% |
| Trading Disable Functions |  | No Trading suspendable function found. If a suspendable code is included, the token maybe neither be bought or sold (honeypot risk). If contract is renounced this function can't be used |
| Set Fees function |  max 25 % | Fee Setting function found. Contract Renounced. This function can not be triggered by the owner. The contract owner may contain the authority to modify the transaction tax. If the transaction tax is increased to more than 49%, the tokens may not be able to be traded (honeypot risk). |
| Proxy Contract |  | Not a Proxy contract |
| Mint Function |  | No Mint Function detected Mint function is transparent or non-existent. Hidden mint functions may increase the amount of tokens in circulation and effect the price of the token. Owner can mint new tokens and sell. |

| | | |
|---|---|--|
| Balance Modifier Function |  | <p>No Balance Modifier function found.</p> <p>If there is a function for this, the contract owner can have the authority to modify the balance of tokens at other addresses. For example revoke the bought tokens from the holders wallet. Common form of scam: You buy the token, but it's disappearing from your wallet.</p> |
| Blacklist Function |  | <p>Blacklist Setting function found. Exclude from receiving dividend only.</p> <p>Excluded wallets doesnt receive reward</p> <p>Contract Renounced. This function can not be triggered by the owner.</p> |
| Whitelist Function |  | <p>Whitelist Setting function found.</p> <p>Contract Renounced. This function can not be triggered by the owner.</p> <p>If there is a function for this Developer can set zero fee or no max wallet size for adresses (for example team wallets can trade without fee. Can cause farming)</p> |
| Hidden Owner Analysis |  | <p>No Hidden or multi owner with authorisation</p> <p>For contract with a hidden owner, developer can still manipulate the contract even if the ownership has been abandoned.</p> |
| Retrieve Ownership Function |  | <p>No Functions found which can retrieve ownership of the contract.</p> <p>If this function exists, it is possible for the project owner to regain ownership even after relinquishing it. Also known as fake renounce.</p> |
| Self Destruct Function |  | <p>No Self Destruct function found.</p> <p>If this function exists and is triggered, the contract will be destroyed, all functions will be unavailable, and all related assets will be erased.</p> |
| Specific Tax Changing Function |  | <p>No Specific Tax Changing Functions found.</p> <p>If it exists, the contract owner may set a very outrageous tax rate for assigned address to block it from trading. Can assign all wallets at once!</p> |
| Trading Cooldown Function |  | <p>No Trading Cooldown Function found. If there is a trading cooldown function, the user will not be able to sell the token within a certain time or block after buying. Like a temporary honeypot.</p> |
| Max Transaction and Holding Modify Function |  | <p>Max Transaction and Holding Modify function found. Contract Renounced. This function can not be triggered by the owner.</p> <p>If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot</p> |
| Transaction Limiting Function |  | <p>No Transaction Limiter Function Found.</p> <p>The number of overall token transactions may be limited (honeypot risk)</p> |

Details of Risk - Attention Items

Removing Risk of contract function based on renounced ownership

Transaction Receipt Event Logs

138

Address

Name OwnershipTransferred (index_topic_1 address previousOwner, index_topic_2 address newOwner) [View Source](#)

Topics

0

0x8be0079c531659141344cd1fd0a4f28419497f9722a3daafe3b4186f6b6457e0

1

Dec → 0xFdb9ebD5331eDa60becF6FFc3A46fA0A0e6D437a

2

Dec → 0x00

Data

0x

Following detected contract functions serve as informational purposes about the contract. The owner has no more authorisation to trigger the following functions.

⚠ Whitelist

Contract renounced, function can not be triggered by owner

If there is a function for this Developer can set zero fee or no max wallet size for addresses (for example team wallets can trade without fee. Can cause farming)

```

fttrace | funcSig
382 | function excludeFromLimits(address account!, bool isExcluded!) external onlyOwner {
383 | | _excludeFromLimits(account!, isExcluded!);
384 | }
385 |
fttrace | funcSig
386 | function _excludeFromLimits(address account!, bool isExcluded!) internal {
387 | | isExcludedFromLimits[account!] = isExcluded!;
388 | |
389 | | emit ExcludeFromLimits(account!, isExcluded!);
390 | }
...
fttrace | funcSig
263 | function excludeFromFees(address account!, bool isExcluded!) public onlyOwner {
264 | | isExcludedFromFees[account!] = isExcluded!;
265 | |
266 | | emit ExcludeFromFees(account!, isExcluded!);
267 | }
268 |
  
```

⚠ Max Transaction and Holding Modify function

Contract renounced, function can not be triggered by owner

If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot

```

391 |
392 |         ftrace | funcSig
393 |         function updateMaxWalletAmount(uint256 _maxWalletAmount!) public onlyOwner {
394 |             require(_maxWalletAmount! >= _maxWalletSafeLimit(), "MaxWallet: Limit too low");
395 |             maxWalletAmount = _maxWalletAmount!;
396 |             emit MaxWalletAmountUpdated(_maxWalletAmount!);
397 |         }
  
```

⚠ Fee Setting function (Max 25%)

Contract renounced, function can not be triggered by owner

The contract owner may contain the authority to modify the transaction tax. If the transaction tax is increased to more than 49%, the tokens may not be able to be traded (honeypot risk).

```

240 |         ftrace | funcSig
241 |         function rewardsFeesSetup(uint16 _buyFee!, uint16 _sellFee!, uint16 _transferFee!) public onlyOwner {
242 |             totalFees[0] = totalFees[0] - rewardsFees[0] + _buyFee!;
243 |             totalFees[1] = totalFees[1] - rewardsFees[1] + _sellFee!;
244 |             totalFees[2] = totalFees[2] - rewardsFees[2] + _transferFee!;
245 |             require(totalFees[0] <= 2500 && totalFees[1] <= 2500 && totalFees[2] <= 2500, "TaxesDefaultRouter: Cannot exceed max total fee of 25%");
246 |             rewardsFees = [_buyFee!, _sellFee!, _transferFee!];
247 |         }
  
```

```

248 |         ftrace | funcSig
249 |         function liquidityFeesSetup(uint16 _buyFee!, uint16 _sellFee!, uint16 _transferFee!) public onlyOwner {
250 |             totalFees[0] = totalFees[0] - liquidityFees[0] + _buyFee!;
251 |             totalFees[1] = totalFees[1] - liquidityFees[1] + _sellFee!;
252 |             totalFees[2] = totalFees[2] - liquidityFees[2] + _transferFee!;
253 |             require(totalFees[0] <= 2500 && totalFees[1] <= 2500 && totalFees[2] <= 2500, "TaxesDefaultRouter: Cannot exceed max total fee of 25%");
254 |             liquidityFees = [_buyFee!, _sellFee!, _transferFee!];
255 |         }
  
```

⚠ Blacklist

Contract renounced, function can not be triggered by owner

Exclude from receiving dividend only. Excluded wallets doesn't receive reward

```

232 |         ftrace | funcSig
233 |         function excludeFromDividends(address account!, bool isExcluded!) external onlyOwner {
234 |             _excludeFromDividends(account!, isExcluded!);
235 |         }
236 |         ftrace | funcSig
237 |         function _excludeFromDividends(address account!, bool isExcluded!) internal override {
238 |             dividendTracker.excludeFromDividends(account!, balanceOf(account!), isExcluded!);
239 |         }
  
```


Contract Security

Total Findings: 7



■ **High Severity Issues:** High possibility to cause problems, need to be resolved.

■ **Medium Severity Issue:** Will likely cause problems, recommended to resolve.

■ **Low Severity Issues:** Won't cause problems, but for improvement purposes could be adjusted.

■ **Informational Severity Issues:** Not harmful in any way, information for the developer team.

Contract Security

List of Found Issues

High severity Issues: (0)

Medium severity issues: (2)

- Possibility of a Reentrancy Attack
- Existence of Public Burn

Low severity issues: (4)

- Missing Events
- Long number literals
- Outdated compiler Version
- Floating Pragma

Informational severity issues: (1)

- Public Functions Should be Declared External

Contract Weakness Classisication

THE SMART CONTRACT WEAKNESS CLASSIFICATION REGISTRY (SWC REGISTRY) IS AN IMPLEMENTATION OF THE WEAKNESS CLASSIFICATION SCHEME PROPOSED IN EIP-1470. IT IS LOOSELY ALIGNED TO THE TERMINOLOGIES AND STRUCTURE USED IN THE COMMON WEAKNESS ENUMERATION (CWE) WHILE OVERLAYING A WIDE RANGE OF WEAKNESS VARIANTS THAT ARE

| ID | Description | AI | Manual | Result |
|---------|--------------------------------------|----------|--------|--------|
| SWC-100 | Function Default Visibility | Passed | Passed | Passed |
| SWC-101 | Integer Overflow and Underflow | Passed | Passed | Passed |
| SWC-102 | Outdated Compiler Version | low | Passed | Passed |
| SWC-103 | Floating Pragma | low | Passed | Passed |
| SWC-104 | Unchecked Call Return Value | Passed | Passed | Passed |
| SWC-105 | Unprotected Ether Withdrawal | Passed | Passed | Passed |
| SWC-106 | Unprotected SELFDESTRUCT Instruction | Passed | Passed | Passed |
| SWC-107 | Reentrancy | Critical | Medium | Medium |
| SWC-108 | State Variable Default Visibility | Passed | Passed | Passed |
| SWC-109 | Uninitialized Storage Pointer | Passed | Passed | Passed |
| SWC-110 | Assert Violation | Passed | Passed | Passed |
| SWC-111 | Use of Deprecated Solidity Functions | Passed | Passed | Passed |
| SWC-112 | Delegatecall to Untrusted Callee | Passed | Passed | Passed |
| SWC-113 | DoS with Failed Call | Passed | Passed | Passed |
| SWC-114 | Transaction Order Dependence | Passed | Passed | Passed |
| SWC-115 | Authorization through tx.origin | Passed | Passed | Passed |
| SWC-116 | Block values as a proxy for time | Passed | Passed | Passed |
| SWC-117 | Signature Malleability | Passed | Passed | Passed |
| SWC-118 | Incorrect Constructor Name | Passed | Passed | Passed |

| | | | | |
|---------|---|--------|--------|--------|
| SWC-119 | Shadowing State Variables | Passed | Passed | Passed |
| SWC-120 | Weak Sources of Randomness from Chain Attributes | Passed | Passed | Passed |
| SWC-121 | Missing Protection against Signature Replay Attacks | Passed | Passed | Passed |
| SWC-122 | Lack of Proper Signature Verification | Passed | Passed | Passed |
| SWC-123 | Requirement Violation | Passed | Passed | Passed |
| SWC-124 | Write to Arbitrary Storage Location | Passed | Passed | Passed |
| SWC-125 | Incorrect Inheritance Order | Passed | Passed | Passed |
| SWC-126 | Insufficient Gas Griefing | Passed | Passed | Passed |
| SWC-127 | Arbitrary Jump with Function Type Variable | Passed | Passed | Passed |
| SWC-128 | DoS With Block Gas Limit | Passed | Passed | Passed |
| SWC-129 | Typographical Error | low | Passed | Passed |
| SWC-130 | Right-To-Left-Override control character (U+202E) | Passed | Passed | Passed |
| SWC-131 | Presence of unused variables | Passed | Passed | Passed |
| SWC-132 | Unexpected Ether balance | Passed | Passed | Passed |
| SWC-133 | Hash Collisions With Multiple Variable Length Arguments | Passed | Passed | Passed |
| SWC-134 | Message call with hardcoded gas amount | Passed | Passed | Passed |
| SWC-135 | Code With No Effects | Passed | Passed | Passed |
| SWC-136 | Unencrypted Private Data On-Chain | Passed | Passed | Passed |

Detected High and Medium Severity Vulnerability Description.

⚠️ Public Burn (1 Item)

| | | | | |
|---------|-----------|-------------------------------|-----------|----------|
| Item: 1 | Location: | Line ERCBurnable.sol 35-39 | Severity: | ■ Medium |
|---------|-----------|-------------------------------|-----------|----------|

| | |
|--------------------|---|
| Function | The contract was found to be using public or an external burn function. The function was missing access control to prevent another user from burning their tokens. Also, the burn function was found to be using a different address than <code>msg.sender</code> . |
| Remediation | <ol style="list-style-type: none"> 1. Consider adding access control modifiers to the burn function to Ensure that initialization functions can only be called once and only by authorized entities. 2. Implement least-privilege roles using libraries like OpenZeppelin's Access Control. 3. Add proper access control modifiers to sensitive functions, such as <code>onlyOwner</code> or custom roles. |

```

35 |         ftrace | funcSig
36 |         function burnFrom(address account!, uint256 amount!) public virtual {
37 |             _spendAllowance(account!, _msgSender(), amount!);
38 |             _burn(account!, amount!);
39 |         }
  
```

⚠ Possibility of a Reentrancy Attack (1 Item)

| | | | | |
|---------|-----------|---|-----------|----------|
| Item: 1 | Location: | CoinDividendTracker.sol Line 190-201 | Severity: | ■ Medium |
|---------|-----------|---|-----------|----------|

| | |
|--------------------|---|
| Function | In a Re-entrancy attack, a malicious contract calls back into the calling contract before the first invocation of the function is finished. This may cause the different invocations of the function to interact in undesirable ways, especially in cases where the function is updating state variables after the external calls. This may lead to loss of funds, improper value updates, token loss, etc. |
| Remediation | <ol style="list-style-type: none"> 1. Ensure all state changes happen before calling external contracts, i.e., update balances or code internally before calling external code 2. Use function modifiers that prevent reentrancy |

```

190  function distributeDividends() public payable {
191      require(totalSupply() > 0);
192
193      if (msg.value > 0) {
194          magnifiedDividendPerShare = magnifiedDividendPerShare + (msg.value * magnitude / totalSupply());
195
196          emit DividendsDistributed(msg.sender, msg.value);
197
198          totalDividendsDistributed = totalDividendsDistributed + msg.value;
199      }
200  }
201
  
```

⚠️ Approve of front running attack. Also known as Sandwich bot attack. (2 Items)

| | | | | |
|---------|-----------|---------------------|-----------|-------|
| Item: 1 | Location: | ERC.20 Line 136-140 | Severity: | ■ Low |
|---------|-----------|---------------------|-----------|-------|

| | |
|-------------------|--|
| Function | <p>The <code>approve()</code> method overrides current allowance regardless of whether the spender already used it or not, so there is no way to increase or decrease allowance by a certain value atomically unless the token owner is a smart contract, not an account. This can be abused by a token receiver when they try to withdraw certain tokens from the sender's account.</p> <p>Meanwhile, if the sender decides to change the amount and sends another approve transaction, the receiver can notice this transaction before it's mined and can extract tokens from both the transactions, therefore, ending up with tokens from both the transactions. This is a front-running attack affecting the ERC20 Approve function.</p> <p>The function approve can be front-run by abusing the <code>_approve</code> function.</p> |
| Remedation | <ol style="list-style-type: none"> 1. Introduce mechanisms that limit the maximum acceptable gas price for transactions. This can help prevent front-runners from drastically increasing the gas fees to prioritize their transactions. 2. Use transaction taxes to prevent against front-run attack |

```

136 |         ftrace | funcSig
137 |         function approve(address spender!, uint256 amount!) public virtual override returns (bool) {
138 |             address owner = _msgSender();
139 |             _approve(owner, spender!, amount!);
140 |             return true;
141 |         }
  
```

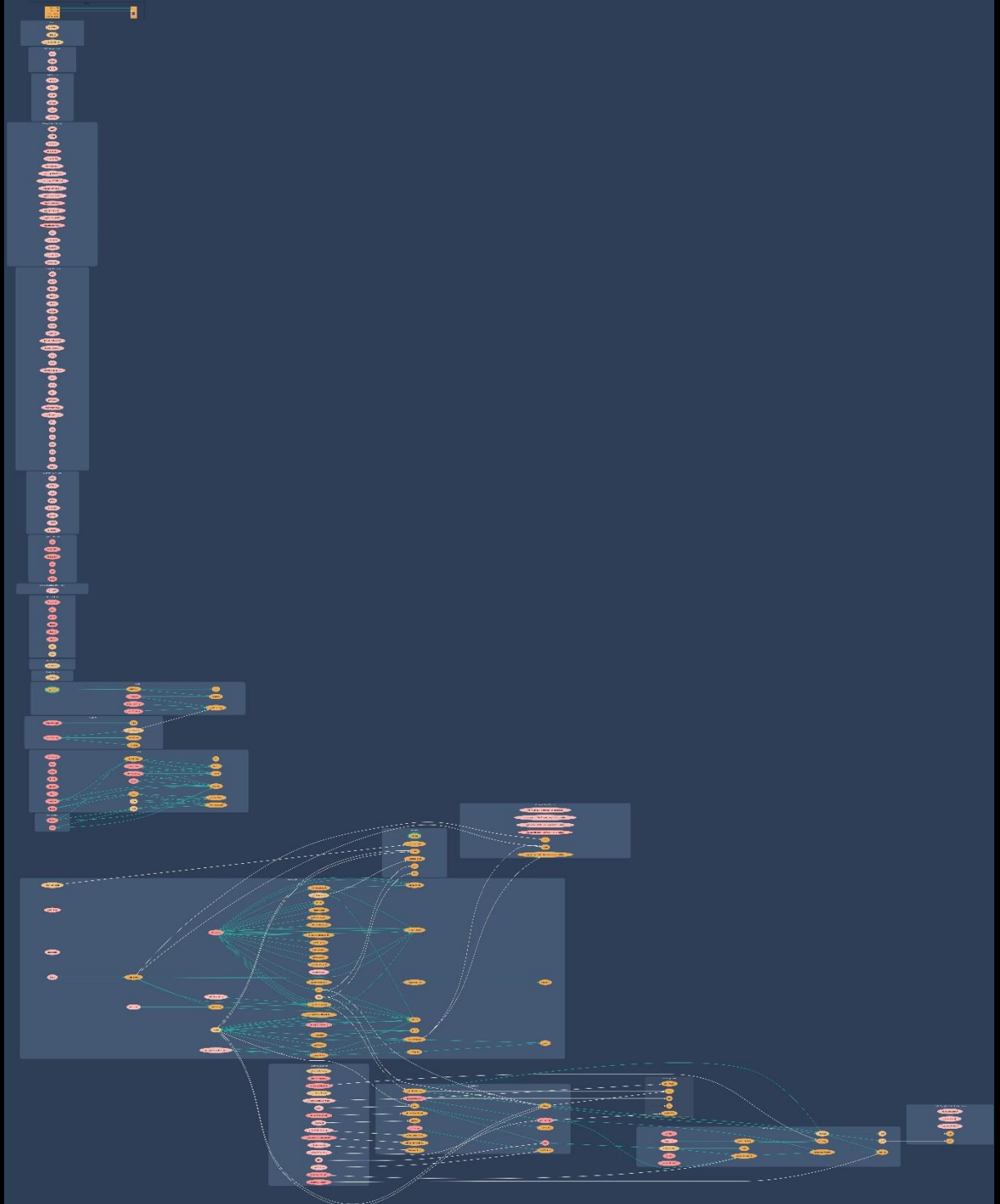
| | | |
|---------|-------------------------------|--|
| Item: 2 | Location: ERC.20 Line 324-332 | Severity: ■ Low |
|---------|-------------------------------|--|

| | |
|-------------------|--|
| Function | <p>The transferFrom() method overrides current allowance regardless of whether the spender already used it or not, so there is no way to increase or decrease allowance by a certain value atomically unless the token owner is a smart contract, not an account.</p> <p>This can be abused by a token receiver when they try to withdraw certain tokens from the sender's account.</p> <p>Meanwhile, if the sender decides to change the amount and sends another approve transaction, the receiver can notice this transaction before it's mined and can extract tokens from both the transactions, therefore, ending up with tokens from both the transactions. This is a front-running attack affecting the ERC20 Approve function.</p> <p>The function approve can be front-run by abusing the <code>_approve</code> function.</p> |
| Remedation | <ol style="list-style-type: none"> Introduce mechanisms that limit the maximum acceptable gas price for transactions. This can help prevent front-runners from drastically increasing the gas fees to prioritize their transactions. Use transaction taxes to prevent against front-run attack |

```

324   ftrace | funcSig
325   function _spendAllowance(address owner!, address spender!, uint256 amount!) internal virtual {
326       uint256 currentAllowance = allowance(owner!, spender!);
327       if (currentAllowance != type(uint256).max) {
328           require(currentAllowance >= amount!, "ERC20: insufficient allowance");
329           unchecked {
330               _approve(owner!, spender!, currentAllowance - amount!);
331           }
332       }
  
```

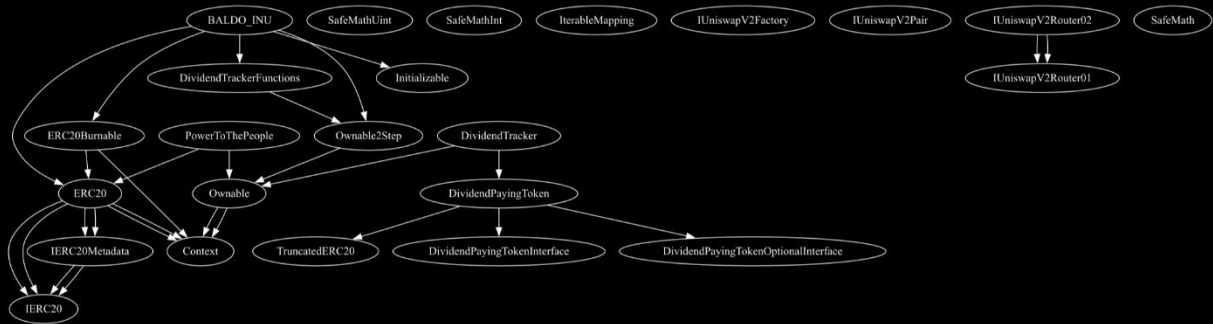

Contract Flow Graph

































Contract Interaction Graph



Inheritance Graph


































Contract Functions




































| Contract | Type | Bases | | |
|------------------|--------------------------------|--|---|--|
| L | Function Name | Visibility | Mutability | Modifiers |
| BALDO_INU | Implementation | ERC20, ERC20Burnable, Ownable2Step, DividendTracker Functions, Initializable | | |
| L | | Public  |  | ERC20 |
| L | initialize | External  |  | initializer |
| L | | External  |  | NO  |
| L | decimals | Public  | | NO  |
| L | _swapTokensForCoin | Private  |  | |
| L | updateSwapThreshold | Public  |  | onlyOwner |
| L | getSwapThresholdAmount | Public  | | NO  |
| L | getAllPending | Public  | | NO  |
| L | baldoinuAddressesSetup | Public  |  | onlyOwner |
| L | baldoinuFeesSetup | Public  |  | onlyOwner |
| L | _swapAndLiquify | Private  |  | |
| L | _addLiquidity | Private  |  | |
| L | addLiquidityFromLeftoverTokens | External  |  | NO  |
| L | liquidityFeesSetup | Public  |  | onlyOwner |

| | | | | |
|---|-------------------------------|-------------|---|-----------|
| L | _sendDividends | Private 🔒 | 🔒 | |
| L | excludeFromDividends | External ⚠️ | 🔒 | onlyOwner |
| L | _excludeFromDividends | Internal 🔒 | 🔒 | |
| L | rewardsFeesSetup | Public ⚠️ | 🔒 | onlyOwner |
| L | _burn | Internal 🔒 | 🔒 | |
| L | _mint | Internal 🔒 | 🔒 | |
| L | excludeFromFees | Public ⚠️ | 🔒 | onlyOwner |
| L | _transfer | Internal 🔒 | 🔒 | |
| L | _updateRouterV2 | Private 🔒 | 🔒 | |
| L | setAMMPair | External ⚠️ | 🔒 | onlyOwner |
| L | _setAMMPair | Private 🔒 | 🔒 | |
| L | excludeFromLimits | External ⚠️ | 🔒 | onlyOwner |
| L | _excludeFromLimits | Internal 🔒 | 🔒 | |
| L | updateMaxWalletAmount | Public ⚠️ | 🔒 | onlyOwner |
| L | _maxWalletSafeLimit | Private 🔒 | | |
| L | enableTrading | External ⚠️ | 🔒 | onlyOwner |
| L | excludeFromTradingRestriction | Public ⚠️ | 🔒 | onlyOwner |
| L | _beforeTokenTransfer | Internal 🔒 | 🔒 | |
| L | _afterTokenTransfer | Internal 🔒 | 🔒 | |
| | | | | |








| ERC20 | Implementation | Context, IERC20, IERC20Metadata | | |
|----------------------|----------------------|---------------------------------|---|------|
| L | | Public 🔒 | 🔒 | NO 🔒 |
| L | name | Public 🔒 | | NO 🔒 |
| L | symbol | Public 🔒 | | NO 🔒 |
| L | decimals | Public 🔒 | | NO 🔒 |
| L | totalSupply | Public 🔒 | | NO 🔒 |
| L | balanceOf | Public 🔒 | | NO 🔒 |
| L | transfer | Public 🔒 | 🔒 | NO 🔒 |
| L | allowance | Public 🔒 | | NO 🔒 |
| L | approve | Public 🔒 | 🔒 | NO 🔒 |
| L | transferFrom | Public 🔒 | 🔒 | NO 🔒 |
| L | increaseAllowance | Public 🔒 | 🔒 | NO 🔒 |
| L | decreaseAllowance | Public 🔒 | 🔒 | NO 🔒 |
| L | _transfer | Internal 🔒 | 🔒 | |
| L | _mint | Internal 🔒 | 🔒 | |
| L | _burn | Internal 🔒 | 🔒 | |
| L | _approve | Internal 🔒 | 🔒 | |
| L | _spendAllowance | Internal 🔒 | 🔒 | |
| L | _beforeTokenTransfer | Internal 🔒 | 🔒 | |
| L | _afterTokenTransfer | Internal 🔒 | 🔒 | |
| | | | | |
| ERC20Burnable | Implementation | Context, ERC20 | | |














| | | | | |
|-------------------------------------|--------------------|------------|---|-----------|
| L | burn | Public 🔒 | 🔒 | NO 🔒 |
| L | burnFrom | Public 🔒 | 🔒 | NO 🔒 |
| Ownable2Step | Implementation | Ownable | | |
| L | pendingOwner | Public 🔒 | | NO 🔒 |
| L | transferOwnership | Public 🔒 | 🔒 | onlyOwner |
| L | _transferOwnership | Internal 🔒 | 🔒 | |
| L | acceptOwnership | Public 🔒 | 🔒 | NO 🔒 |
| SafeMathUint | Library | | | |
| L | toInt256Safe | Internal 🔒 | | |
| SafeMathInt | Library | | | |
| L | toUint256Safe | Internal 🔒 | | |
| TruncatedERC20 | Implementation | | | |
| L | | Public 🔒 | 🔒 | NO 🔒 |
| L | name | Public 🔒 | | NO 🔒 |
| L | symbol | Public 🔒 | | NO 🔒 |
| L | decimals | Public 🔒 | | NO 🔒 |
| L | totalSupply | Public 🔒 | | NO 🔒 |
| L | balanceOf | Public 🔒 | | NO 🔒 |
| L | _mint | Internal 🔒 | 🔒 | |
| L | _burn | Internal 🔒 | 🔒 | |
| DividendPayingTokenInterface | Interface | | | |









































| | | | | |
|---|------------------------|--|---|--|
| L | dividendOf | External  | | NO  |
| DividendPaying TokenOptionalIn terface | Interface | | | |
| L | withdrawableDividendOf | External  | | NO  |
| L | withdrawnDividendOf | External  | | NO  |
| L | accumulativeDividendOf | External  | | NO  |
| | | | | |
| DividendPaying Token | Implementation | TruncatedERC20 , DividendPaying TokenInterface, DividendPaying TokenOptionalIn terface | | |
| L | | Public  |  | TruncatedERC20 |
| L | | External  |  | NO  |
| L | distributeDividends | Public  |  | NO  |
| L | _withdrawDividend | Internal  |  | |
| L | dividendOf | Public  | | NO  |
| L | withdrawableDividendOf | Public  | | NO  |
| L | withdrawnDividendOf | Public  | | NO  |
| L | accumulativeDividendOf | Public  | | NO  |
| L | _mint | Internal  |  | |
| L | _burn | Internal  |  | |
| L | _setBalance | Internal  |  | |
| | | | | |





















| | | | | |
|--------------------------------------|-----------------------------|--|---|--|
| IterableMapping | Library | | | |
| L | get | Public  | | NO  |
| L | getIndexOfKey | Public  | | NO  |
| L | getKeyAtIndex | Public  | | NO  |
| L | size | Public  | | NO  |
| L | set | Public  |  | NO  |
| L | remove | Public  |  | NO  |
| | | | | |
| DividendTracker | Implementation | Ownable, DividendPaying Token | | |
| L | | Public  |  | DividendPaying Token |
| L | excludeFromDiv idends | External  |  | onlyOwner |
| L | claimWaitSetup | Public  |  | onlyOwner |
| L | getNumberOfTo kenHolders | External  | | NO  |
| L | getAccountData | Public  | | NO  |
| L | getAccountData AtIndex | Public  | | NO  |
| L | claim | Public  |  | onlyOwner |
| L | _canAutoClaim | Private  | | |
| L | setBalance | Public  |  | onlyOwner |
| L | process | External  |  | onlyOwner |
| | | | | |
| DividendTracker Functions | Implementation | Ownable2Step | | |
| L | _deployDividend Tracker | Internal  |  | |

| | | | | |
|--------------------------|---------------------------------|------------|---|-----------|
| L | gasForProcessingSetup | Public 🔒 | 🔒 | onlyOwner |
| L | claimWaitSetup | External 🔒 | 🔒 | onlyOwner |
| L | _excludeFromDividends | Internal 🔒 | 🔒 | |
| L | isExcludedFromDividends | Public 🔒 | | NO 🔒 |
| L | claim | External 🔒 | 🔒 | NO 🔒 |
| L | getClaimWait | External 🔒 | | NO 🔒 |
| L | getTotalDividendsDistributed | External 🔒 | | NO 🔒 |
| L | withdrawableDividendOf | Public 🔒 | | NO 🔒 |
| L | dividendTokenBalanceOf | Public 🔒 | | NO 🔒 |
| L | dividendTokenTotalSupply | Public 🔒 | | NO 🔒 |
| L | getAccountDividendsInfo | External 🔒 | | NO 🔒 |
| L | getAccountDividendsInfoAtIndex | External 🔒 | | NO 🔒 |
| L | getLastProcessedIndex | External 🔒 | | NO 🔒 |
| L | getNumberOfDividendTokenHolders | Public 🔒 | | NO 🔒 |
| L | process | External 🔒 | 🔒 | NO 🔒 |
| | | | | |
| Initializable | Implementation | | | |
| | | | | |
| IUniswapV2Factory | Interface | | | |
| L | feeTo | External 🔒 | | NO 🔒 |
| L | feeToSetter | External 🔒 | | NO 🔒 |

| | | | | |
|-----------------------|-------------------|------------|---|------|
| L | getPair | External ¶ | | NO ¶ |
| L | allPairs | External ¶ | | NO ¶ |
| L | allPairsLength | External ¶ | | NO ¶ |
| L | createPair | External ¶ |  | NO ¶ |
| L | setFeeTo | External ¶ |  | NO ¶ |
| L | setFeeToSetter | External ¶ |  | NO ¶ |
| | | | | |
| IUniswapV2Pair | Interface | | | |
| L | name | External ¶ | | NO ¶ |
| L | symbol | External ¶ | | NO ¶ |
| L | decimals | External ¶ | | NO ¶ |
| L | totalSupply | External ¶ | | NO ¶ |
| L | balanceOf | External ¶ | | NO ¶ |
| L | allowance | External ¶ | | NO ¶ |
| L | approve | External ¶ |  | NO ¶ |
| L | transfer | External ¶ |  | NO ¶ |
| L | transferFrom | External ¶ |  | NO ¶ |
| L | DOMAIN_SEPARATOR | External ¶ | | NO ¶ |
| L | PERMIT_TYPEHASH | External ¶ | | NO ¶ |
| L | nonces | External ¶ | | NO ¶ |
| L | permit | External ¶ |  | NO ¶ |
| L | MINIMUM_LIQUIDITY | External ¶ | | NO ¶ |
| L | factory | External ¶ | | NO ¶ |
| L | token0 | External ¶ | | NO ¶ |

| | | | | |
|---------------------------|------------------------------|------------|---|------|
| L | token1 | External ¶ | | NO ¶ |
| L | getReserves | External ¶ | | NO ¶ |
| L | price0CumulativeLast | External ¶ | | NO ¶ |
| L | price1CumulativeLast | External ¶ | | NO ¶ |
| L | kLast | External ¶ | | NO ¶ |
| L | mint | External ¶ |  | NO ¶ |
| L | burn | External ¶ |  | NO ¶ |
| L | swap | External ¶ |  | NO ¶ |
| L | skim | External ¶ |  | NO ¶ |
| L | sync | External ¶ |  | NO ¶ |
| L | initialize | External ¶ |  | NO ¶ |
| | | | | |
| IUniswapV2Router01 | Interface | | | |
| L | factory | External ¶ | | NO ¶ |
| L | WETH | External ¶ | | NO ¶ |
| L | addLiquidity | External ¶ |  | NO ¶ |
| L | addLiquidityETH | External ¶ |  | NO ¶ |
| L | removeLiquidity | External ¶ |  | NO ¶ |
| L | removeLiquidityETH | External ¶ |  | NO ¶ |
| L | removeLiquidityWithPermit | External ¶ |  | NO ¶ |
| L | removeLiquidityETHWithPermit | External ¶ |  | NO ¶ |
| L | swapExactTokensForTokens | External ¶ |  | NO ¶ |

| | | | | |
|---------------------------|---|--|---|--|
| L | swapTokensForExactTokens | External  |  | NO  |
| L | swapExactETHForTokens | External  |  | NO  |
| L | swapTokensForExactETH | External  |  | NO  |
| L | swapExactTokensForETH | External  |  | NO  |
| L | swapETHForExactTokens | External  |  | NO  |
| L | quote | External  | | NO  |
| L | getAmountOut | External  | | NO  |
| L | getAmountIn | External  | | NO  |
| L | getAmountsOut | External  | | NO  |
| L | getAmountsIn | External  | | NO  |
| IUniswapV2Router02 | Interface | IUniswapV2Router01 | | |
| L | removeLiquidityETHSupportingFeeOnTransferTokens | External  |  | NO  |
| L | removeLiquidityETHWithPermitSupportingFeeOnTransferTokens | External  |  | NO  |
| L | swapExactTokensForTokensSupportingFeeOnTransferTokens | External  |  | NO  |
| L | swapExactETHForTokensSupportingFeeOnTransferTokens | External  |  | NO  |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External  |  | NO  |

| Ownable | Implementation | Context | | |
|-----------------------|----------------------|--|---|--|
| L | | Public  |  | NO  |
| L | owner | Public  | | NO  |
| L | _checkOwner | Internal  | | |
| L | renounceOwnership | Public  |  | onlyOwner |
| L | transferOwnership | Public  |  | onlyOwner |
| L | _transferOwnership | Internal  |  | |
| IERC20 | Interface | | | |
| L | totalSupply | External  | | NO  |
| L | balanceOf | External  | | NO  |
| L | transfer | External  |  | NO  |
| L | allowance | External  | | NO  |
| L | approve | External  |  | NO  |
| L | transferFrom | External  |  | NO  |
| IERC20Metadata | Interface | IERC20 | | |
| L | name | External  | | NO  |
| L | symbol | External  | | NO  |
| L | decimals | External  | | NO  |
| Context | Implementation | | | |
| L | _msgSender | Internal  | | |
| L | _msgData | Internal  | | |
| L | _contextSuffixLength | Internal  | | |



Function
can modify
state



Function
is payable

Audit Scope

Audit Method.

Our smart contract audit is an extensive methodical examination and analysis of the smart contract's code that is used to interact with the blockchain. Goal: discover errors, issues and security vulnerabilities in the code. Findings getting reported and improvements getting suggested.

Automatic and Manual Review

We are using automated tools to scan functions and weaknesses of the contract. Transfers, integer over-undeflow checks such as all CWE events.

Tools we use:

Visual Studio Code

CWE

SWC

Solidity Scan

SVD

In manual code review our auditor looking at source code and performing line by line examination. This method helps to clarify developer's coding decisions and business logic.

Skeleton Ecosystem

<https://skeletonecosystem.com>

<https://github.com/SkeletonEcosystem/Audits>

