



Building the Futuristic **Blockchain Ecosystem**

SECURITY AUDIT REPORT

FLINTSTONES

TABLE OF CONTENTS

02	Table of Contents	_____
03	Overview	_____
04	Contract Details	_____
05	Owner Privileges	_____
06	Testnet Version	_____
08	Audit Methodology	_____
09	Vulnerabilities Checklist	_____
10	Risk Classification	_____
11	Inheritance Trees	_____
12	Function Details	_____
18	Manual Review	_____
19	Findings	_____
23	About Expelee	_____
24	Disclaimer	_____

OVERVIEW

The Expelee team has performed a line-by-line manual analysis and automated review of the smart contract. The smart contract was analysed mainly for common smart contract vulnerabilities, exploits, and manipulation hacks. According to the smart contract audit:

Audit Result	Passed
KYC Verification	No
Audit Date	1 May 2023

CONTRACT DETAILS

Token Name: FlintStones

Symbol: FlintStones

Network: Binance Smart Chain

Language: Solidity

Contract Address:

0xf147A1784a29Cd4716ff46cb8e7C79081D3da6e2

Total Supply: 10,000,000,000

Contract SHA-256 Checksum:

2c09f78e163ab26b939ee394bb5e5891969b4535

Owner's Wallet:

0x2D4f286976A4A3D1605BE7d28f928F056Be4E915

Deployer's Wallet:

0x2D4f286976A4A3D1605BE7d28f928F056Be4E915

Testnet:

<https://testnet.bscscan.com/address/0xc816974Ba83734d835616024E1120aCB7fDedD80>

OWNER PRIVILEGES

- Contract owner is not able to set buy/sell taxes over 8% each
- Contract owner is not able to set transfer tax (0% tax)
- **Contract is using pinksale anti-bot**
- **Contract owner is able to disable/enable anti-bot**
- **Contract owner must enable trades for holders manually**
- Contract gives BNB rewards to holderes
- Contract owner is not able to blacklist an arbitrary wallet
- Contract owner is not able to disable trades/transfers
- Contract owner is not able to mint new tokens

TESTNET VERSION

Adding Liquidity

Tx:

<https://testnet.bscscan.com/tx/0x73131fdffc60216aa171ddf3b2b7b695030e1ffa3d32cb38d726d0c8fe23b279>

=====

Buying from a fee excluded wallet

Tx (0% tax):

<https://testnet.bscscan.com/tx/0xfcd2f462bf2da40c66674b3a8757702ab5c292e8c3c79f40adb7005cfbb96196>

=====

Selling from a fee excluded wallet

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x4d62fad3f5f80735d7172da16100a26d97297541ff2a5b9f705948e366ad9b36>

=====

Transferring using a fee excluded wallet

Tx (0% tax):

<https://testnet.bscscan.com/tx/0x64f25e56df0bbbc450ea0a6a9652ff2301d3c8c7da59d5993427b7b9a6430da1>

=====

TESTNET VERSION

Buying from a regular wallet ✓

Tx (up to 8% tax):

<https://testnet.bscscan.com/tx/0x870ee6626fcfbb838f4f9d38923c6f69687e1bc29d7f7f95266a56c40addb241>

=====

Selling from a regular wallet ✓

Tx (up to 8% tax):

<https://testnet.bscscan.com/tx/0xb68be1936d5c5d56ec3d88401e8728c63eec3e45b3e400be5beb0a03154d0f14>

=====

Internal swap (marketing BNB and Rewards distribution) ✓

Tx (0% tax):

<https://testnet.bscscan.com/tx/0xb68be1936d5c5d56ec3d88401e8728c63eec3e45b3e400be5beb0a03154d0f14>

=====

AUDIT METHODOLOGY

Audit Details

Our comprehensive audit report provides a full overview of the audited system's architecture, smart contract codebase, and details on any vulnerabilities found within the system.

Audit Goals

The audit goal is to ensure that the project is built to protect investors and users, preventing potentially catastrophic vulnerabilities after launch, that lead to scams and rugpulls.

Code Quality

Our analysis includes both automatic tests and manual code analysis for the following aspects:

- Exploits
- Back-doors
- Vulnerability
- Accuracy
- Readability

Tools

- DE
- Open Zeppelin
- Code Analyzer
- Solidity Code
- Compiler
- Hardhat

VULNERABILITY CHECKS

Design Logic	Passed
Compiler warnings	Passed
Private user data leaks	Passed
Timestamps dependence	Passed
Integer overflow and underflow	Passed
Race conditions & reentrancy. Cross-function race conditions	Passed
Possible delays in data delivery	Passed
Oracle calls	Passed
Front Running	Passed
DoS with Revert	Passed
DoS with block gas limit	Passed
Methods execution permissions	Passed
Economy model	Passed
Impact of the exchange rate on the logic	Passed
Malicious event log	Passed
Scoping and declarations	Passed
Uninitialized storage pointers	Passed
Arithmetic accuracy	Passed
Cross-function race conditions	Passed
Safe Zeppelin module	Passed

RISK CLASSIFICATION

When performing smart contract audits, our specialists look for known vulnerabilities as well as logical and access control issues within the code. The exploitation of these issues by malicious actors may cause serious financial damage to projects that failed to get an audit in time. We categorize these vulnerabilities by the following levels:

High Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

Medium Risk

Issues on this level are critical to the smart contract's performance/functionality and should be fixed before moving to a live environment.

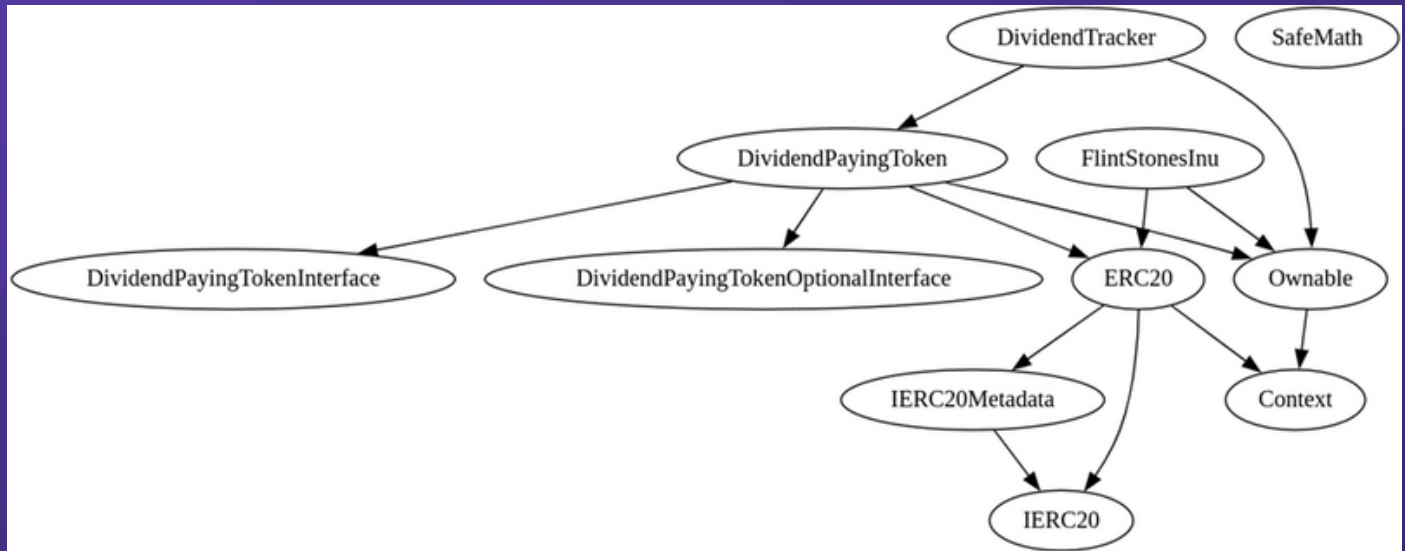
Low Risk

Issues on this level are minor details and warnings that can remain unfixed.



Informational

Issues on this level are minor details and warnings that can remain unfixed.




















INHERITANCE TREES



FUNCTION DETAILS

Symbol	Meaning
	Function can modify state
	Function is payable

Contract Assesment

Contract	Type	Bases			
----- ----- ----- ----- -----					
L	**Function Name**	**Visibility**	**Mutability**	**Modifiers**	
Context	Implementation				
L	_msgSender	Internal			
L	_msgData	Internal			
Ownable	Implementation	Context			
L	<Constructor>	Public	!		NO !
L	owner	Public	!		NO !
L	renounceOwnership	Public	!		onlyOwner
L	transferOwnership	Public	!		onlyOwner
L	_transferOwnership	Internal			
SafeMath	Library				
L	add	Internal			
L	sub	Internal			
L	sub	Internal			
L	mul	Internal			
L	div	Internal			
L	div	Internal			
L	mod	Internal			
L	mod	Internal			
SafeMathInt	Library				
L	mul	Internal			
L	div	Internal			
L	sub	Internal			
L	add	Internal			

FUNCTION DETAILS

```

| L | abs | Internal | 🔒 | | |
| L | toUint256Safe | Internal | 🔒 | | |
|||||
| **SafeMathUint** | Library | |||
| L | toInt256Safe | Internal | 🔒 | | |
|||||
| **IterableMapping** | Library | |||
| L | get | Internal | 🔒 | | |
| L | getIndexOfKey | Internal | 🔒 | | |
| L | getKeyAtIndex | Internal | 🔒 | | |
| L | size | Internal | 🔒 | | |
| L | set | Internal | 🔒 | ● | |
| L | remove | Internal | 🔒 | ● | |
|||||
| **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 ! |

```

FUNCTION DETAILS

```

| 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 | ! | 91 | 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 | ! | 91 | NO | ! |
| L | swapTokensForExactETH | External | ! | ● | NO | ! |
| L | swapExactTokensForETH | External | ! | ● | NO | ! |
| L | swapETHForExactTokens | External | ! | 91 | 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 | ! | 91 | NO | ! |
| L | swapExactTokensForETHSupportingFeeOnTransferTokens | External | ! | ● | NO | ! |
|||||
| **IPinkAntiBot** | Interface | |||
| L | setTokenOwner | External | ! | ● | NO | ! |
| L | onPreTransferCheck | External | ! | ● | NO | ! |
|||||
| **IERC20** | Interface | |||
| L | totalSupply | External | ! | NO | ! |
| L | balanceOf | External | ! | NO | ! |
| L | allowance | External | ! | NO | ! |
| L | transfer | External | ! | ● | NO | ! |
| L | approve | External | ! | ● | NO | ! |

```

FUNCTION DETAILS








































```

| L | transferFrom | External | ! | ● | NO | ! |
|||||
| **Address** | Library | |||
| L | isContract | Internal | 🔒 | | |
| L | sendValue | Internal | 🔒 | ● | |
| L | functionCall | Internal | 🔒 | ● | |
| L | functionCall | Internal | 🔒 | ● | |
| L | functionCallWithValue | Internal | 🔒 | ● | |
| L | functionCallWithValue | Internal | 🔒 | ● | |
| L | _functionCallWithValue | Private | 🔒 | ● | |
|||||
| **IERC20Metadata** | Interface | IERC20 |||
| L | name | External | ! | | NO | ! |
| L | symbol | External | ! | | NO | ! |
| L | decimals | External | ! | | NO | ! |
|||||
| **ERC20** | Implementation | Context, IERC20, IERC20Metadata |||
| L | <Constructor> | 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 | _beforeTokenTransfer | Internal | 🔒 | ● | |
|||||
| **DividendPayingTokenInterface** | Interface | |||
| L | dividendOf | External | ! | | NO | ! |
| L | withdrawDividend | External | ! | ● | NO | ! |
|||||
| **DividendPayingTokenOptionalInterface** | Interface | |||
| L | withdrawableDividendOf | External | ! | | NO | ! |
| L | withdrawnDividendOf | External | ! | | NO | ! |
| L | accumulativeDividendOf | External | ! | | NO | ! |
|||||
| **DividendPayingToken** | Implementation | ERC20, Ownable, DividendPayingTokenInterface,
DividendPayingTokenOptionalInterface |||
| L | <Constructor> | Public | ! | ● | ERC20 |

```


FUNCTION DETAILS

```

| L | <Receive Ether> | External | ! |  | NO | ! |
| L | distributeDividends | Public | ! |  | onlyOwner |
| L | withdrawDividend | Public | ! |  | NO | ! |
| L | _withdrawDividendOfUser | Internal |  |  | |
| L | dividendOf | Public | ! | | NO | ! |
| L | withdrawableDividendOf | Public | ! | | NO | ! |
| L | withdrawnDividendOf | Public | ! | | NO | ! |
| L | accumulativeDividendOf | Public | ! | | NO | ! |
| L | _transfer | Internal |  |  | |
| L | _mint | Internal |  |  | |
| L | _burn | Internal |  |  | |
| L | _setBalance | Internal |  |  | |
|||||
| **DividendTracker** | Implementation | Ownable, DividendPayingToken |||
| L | <Constructor> | Public | ! |  | DividendPayingToken |
| L | _transfer | Internal |  | | |
| L | withdrawDividend | Public | ! | | NO | ! |
| L | updateMinimumTokenBalanceForDividends | External | ! |  | onlyOwner |
| L | excludeFromDividends | External | ! |  | onlyOwner |
| L | updateClaimWait | External | ! |  | onlyOwner |
| L | setLastProcessedIndex | External | ! |  | onlyOwner |
| L | getLastProcessedIndex | External | ! | | NO | ! |
| L | getNumberOfTokenHolders | External | ! | | NO | ! |
| L | getAccount | Public | ! | | NO | ! |
| L | getAccountAtIndex | Public | ! | | NO | ! |
| L | canAutoClaim | Private |  | | |
| L | setBalance | External | ! |  | onlyOwner |
| L | process | Public | ! |  | NO | ! |
| L | processAccount | Public | ! |  | onlyOwner |
|||||
| **FlintStonesInu** | Implementation | ERC20, Ownable |||
| L | <Constructor> | Public | ! |  | ERC20 |
| L | <Receive Ether> | External | ! |  | NO | ! |
| L | claimStuckTokens | External | ! |  | onlyOwner |
| L | excludeFromFees | External | ! |  | onlyOwner |
| L | isExcludedFromFees | Public | ! | | NO | ! |
| L | updateBuyFees | External | ! |  | onlyOwner |
| L | updateSellFees | External | ! |  | onlyOwner |
| L | changeMarketingWallet | External | ! |  | onlyOwner |
| L | enableTrading | External | ! |  | onlyOwner |
| L | setEnableAntiBot | External | ! |  | onlyOwner |
| L | _transfer | Internal |  |  | |
| L | swapAndSendDividends | Private |  |  | |
| L | setSwapTokensAtAmount | External | ! |  | onlyOwner |
| L | updateDividendTracker | Public | ! |  | onlyOwner |
| L | updateGasForProcessing | Public | ! |  | onlyOwner |

```


FUNCTION DETAILS

```

| L | updateMinimumBalanceForDividends | External ! | ● | onlyOwner |
| L | updateClaimWait | External ! | ● | onlyOwner |
| L | getClaimWait | External ! | [NO ! |
| L | getTotalDividendsDistributed | External ! | [NO ! |
| L | withdrawableDividendOf | Public ! | [NO ! |
| L | dividendTokenBalanceOf | Public ! | [NO ! |
| L | totalRewardsEarned | Public ! | [NO ! |
| L | excludeFromDividends | External ! | ● | onlyOwner |
| L | getAccountDividendsInfo | External ! | [NO ! |
| L | getAccountDividendsInfoAtIndex | External ! | [NO ! |
| L | processDividendTracker | External ! | ● [NO ! |
| L | claim | External ! | ● [NO ! |
| L | claimAddress | External ! | ● | onlyOwner |
| L | getLastProcessedIndex | External ! | [NO ! |
| L | setLastProcessedIndex | External ! | ● | onlyOwner |
| L | getNumberOfDividendTokenHolders | External ! | [NO ! |

```

Legend

```

| Symbol | Meaning |
|:-----:|:-----|
| ● | Function can modify state |
| 🟢 | Function is payable |

```

MANUAL REVIEW

Severity Criteria

Expelee assesses the severity of disclosed vulnerabilities according to methodology based on OWASP standards.

Vulnerabilities are divided into three primary risk categories:

High

Medium

Low

High-level considerations for vulnerabilities span the following key areas when conducting assessments:

- Malicious input handling
- Escalation of privileges
- Arithmetic
- Gas use

Overall Risk Severity				
Impact	HIGH	Medium	High	Critical
	MEDIUM	Low	Medium	High
	LOW	Note	Low	Medium
		LOW	MEDIUM	HIGH
	Likelihood			

FINDINGS

Findings	Severity	Found
High Risk	● High	2
Medium Risk	● Medium	0
Low Risk	● Low	0
Suggestion & discussion	● Informational	0
Gas Optimizations	● Gas Opt.	1

HIGH RISK FINDING

Category: Centralization

Impact: High

Subject: Enabling trades is not guaranteed

Overview:

The owner of the contract must enable trades for public, otherwise no one would be able to buy/sell/transfer their tokens except whitelisted wallets.

```
function enableTrading() external onlyOwner {  
    tradingEnabled = true;  
}
```

Suggestion

To mitigate this issue there are several options:

- Temporary transfer ownership of the contract to a pinksale safu developer
- Enable tradings before presale

Issue Status: Open

HIGH RISK FINDING

Category: Logical

Impact: High

Subject: DividendDistributor is upgradeable

Overview:

The contract owner has the ability to change the DividendDistributor to a new address. If the new address does not adhere to the interface of the current DividendDistributor, or if the new contract consumes an excessive amount of gas, buy/sell/transfer could become disabled.

```
function updateDividendTracker(address newAddress) public onlyOwner {
    require(
        newAddress != address(dividendTracker),
        "The dividend tracker already has that address"
    );

    /// rest of the code

    dividendTracker = newDividendTracker;
}
```

SUGGESTIONS

To mitigate this issue there are several options:

- Disable the upgradeability of the dividend tracker.
- Implement safety checks to ensure that the new dividend tracker adheres to the current interface and does not consume an excessive amount of gas.
- Introduce a multi-signature approval mechanism for updating the DividendDistributor to reduce the risk of a single point of failure.
- Allow the community to vote on the proposed new DividendDistributor through a decentralized governance process.
- Set up a timelock for upgrading the DividendDistributor, providing a window for users to review and react to the proposed change.
- Develop a testing suite and perform thorough testing of the new dividend tracker contract before deployment to ensure compatibility and gas efficiency.

Issue Status: [Open](#)

ABOUT EXPELEE

Expelee is a product-based aspirational Web3 start-up. Coping up with numerous solutions for blockchain security and constructing a Web3 ecosystem from deal making platform to developer hosting open platform, while also developing our own commercial and sustainable blockchain.

 www.expelee.com



expeleeofficial



expelee



Expelee



expelee



expelee_official



expelee-co

expelee

Building the Futuristic **Blockchain Ecosystem**

DISCLAIMER

All the content provided in this document is for general information only and should not be used as financial advice or a reason to buy any investment. Team provides no guarantess against the sale of team tokens or the removal of liquidity by the project audited in this document.

Always do your own research and project yourselves from being scammed. The Expelee team has audited this project for general information and only expresses their opinion based on similar projects and checks from popular diagnostic tools.

Under no circumstances did Expelee receive a payment to manipulate those results or change the awarding badge that we will be adding in our website. Alway do your own research and protect yourselves from scams.

This document should not be presented as a reason to buy or not buy any particular token. The Expelee team disclaims any liability for the resulting losses.

The logo for Expelee, featuring the word "expelee" in a stylized font. The "ex" is in white, and "pelee" is in orange. The letters are bold and modern.

Building the Futuristic **Blockchain Ecosystem**