SKELETON ECOSYSTEM

SMART CONTRACT AUDIT

Sorcery
SOR
BEP20

0xc8cc4bBD33264dB465E4c9ea011F895D02505

Table of Contents

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% safaty 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	SORCERY
Ticker/Simbol	SOR
Blockchain	Binance Smart Chain BEP20
Contract Address	0xc8cc4bBD33264dB465E4c9ea011F895D02505959
Creator Address	0xD179861Dd264d4F046aEA5Fce6Ad512B6cADcb73
Current Owner Address	0xD179861Dd264d4F046aEA5Fce6Ad512B6cADcb73
Contract Explorer	https://bscscan.com/address/0xc8cc4bbd33264db465e4c9ea011f895d02505959#code
Compiler Version	v0.8.7+commit.e28d00a7
License	MIT
Optimisation	No with 200 Runs
Total Supply	10,000,000 **SOR**
Decimals	18

Creation/Audit

Contract Deployed	12.03.2024
Audit Created	01.08.2023
Audit Update	V 1.0

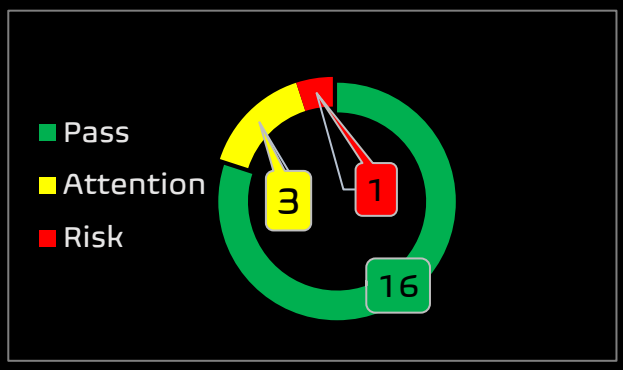
Verified Socials

Website	https://sorceryswap.com/
Telegram	https://t.me/sorceryswap
Twitter (X)	https://x.com/sorceryfinance

SORCERY BEP20

Contract Function Analysis

Pass Attention Item Risky Item



Contract Verified	✓	The contract source code is uploaded to blockchain explorer and is open source, so everybody can read it.
Contract Ownership		0xD179861Dd264d4F046aEA5Fce6Ad512B6cADcb73 Deployer
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
Liqudity Status	✓	Liqudity status on 17.05.2024 100% for 107 Days on PinkSale
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 24%	Fee Setting function found. 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	✅	No Balance Modifier function found. 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.
Blacklist Function	⚠️	Blacklist Setting function found. If there is a blacklist, some addresses may not be able to trade normally. Example: you buy the token and right after your Wallet getting blacklisted. Like so you will be unable to sell. Honeypot Risk.
Whitelist Function	⚠️	Whitelist Setting function found 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)
Hidden Owner Analysis	✅	No Hidden or multi owner with authorisation For contract with a hidden owner, developer can still manipulate the contract even if the ownership has been abandoned.
Retrieve Ownership Function	✅	No Functions found which can retrieve ownership of the contract. If this function exists, it is possible for the project owner to regain ownership even after relinquishing it. Also known as fake renounce.
Self Destruct Function	✅	No Self Destruct function found. If this function exists and is triggered, the contract will be destroyed, all functions will be unavailable, and all related assets will be erased.
Specific Tax Changing Function	✅	No Specific Tax Changing Functions found. 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!
Trading Cooldown Function	✅	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.
Max Transaction and Holding Modify Function	⚠️	Max Transaction and Holding Modify function found. If there is a function for this, the maximum trading amount or maximum position can be modified. Can cause honeypot
Transaction Limiting Function	✅	No Transaction Limiter Function Found. The number of overall token transactions may be limited (honeypot risk)

Details of Risk - Attention Items

Set Fee (max 24%)

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).

```
ftrace | funcSig
function _set_Fees(uint256 Buy_Fee1, uint256 Sell_Fee1) external onlyOwner() {

    require((Buy_Fee1 + Sell_Fee1) <= maxPossibleFee, "Fee is too high!");
    _sellFee = Sell_Fee1;
    _buyFee = Buy_Fee1;

}
```

Whitelist

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)

```
// Set a wallet address so that it does not have to pay transaction fees
ftrace | funcSig
function excludeFromFee(address account1) public onlyOwner {
    _isExcludedFromFee[account1] = true;
}
```

Max Transaction and Holding Modify function

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

```
// Set the Max transaction amount (percent of total supply)
ftrace | funcSig
function set_Max_Transaction_Percent(uint256 maxTxPercent_x100!) external onlyOwner() {
    _maxTxAmount = _tTotal*maxTxPercent_x100!/10000;
}

// Set the maximum wallet holding (percent of total supply)
ftrace | funcSig
function set_Max_Wallet_Percent(uint256 maxWallPercent_x100!) external onlyOwner() {
    _maxWalletToken = _tTotal*maxWallPercent_x100!/10000;
}
```

Blacklist Function

If there is a blacklist, some addresses may not be able to trade normally. Example: you buy the token and right after your Wallet getting blacklisted. Like so you will be unable to sell. Honeypot Risk.

```
648
649     // Blacklist - block wallets (ADD - COMMA SEPARATE MULTIPLE WALLETS)
        ftrace | funcSig
650     function blacklist_Add_Wallets(address[] calldata addresses) external onlyOwner {
651
652         uint256 startGas;
653         uint256 gasUsed;
654
655     for (uint256 i; i < addresses.length; ++i) {
656         if(gasUsed < gasleft()) {
657         startGas = gasleft();
658         if(!_isBlacklisted[addresses[i]]){
659         _isBlacklisted[addresses[i]] = true;}
660         gasUsed = startGas - gasleft();
661     }
662     }
```

Blocking Transactions by changing Router

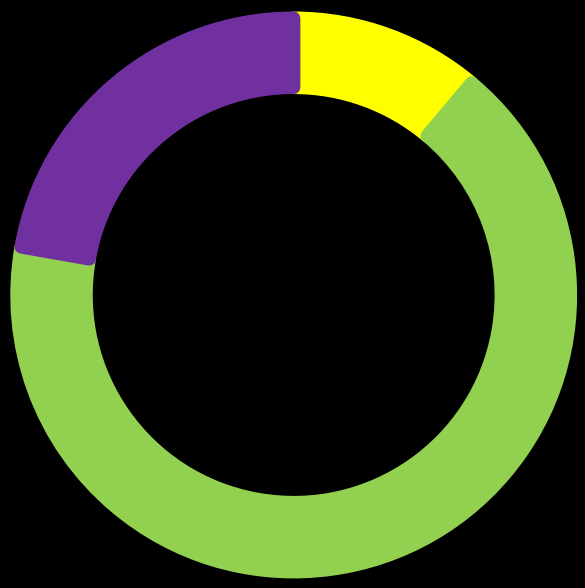
The Router address can be changed, which means the trading can be result in failure, if the router adress can not be found and the transactions can nor run through.

```
945     // Set new router and make the new pair address
        ftrace | funcSig
946     function set_New_Router_and_Make_Pair(address newRouter) public onlyOwner() {
947         IUniswapV2Router02 _newPCSRouter = IUniswapV2Router02(newRouter);
948         uniswapV2Pair = IUniswapV2Factory(_newPCSRouter.factory()).createPair(address(this), _newPCSRouter.WETH());
949         uniswapV2Router = _newPCSRouter;
950     }
951
952     // Set new router
        ftrace | funcSig
953     function set_New_Router_Address(address newRouter) public onlyOwner() {
954         IUniswapV2Router02 _newPCSRouter = IUniswapV2Router02(newRouter);
955         uniswapV2Router = _newPCSRouter;
956     }
957
958     // Set new address - This will be the 'Cake LP' address for the token pairing
        ftrace | funcSig
959     function set_New_Pair_Address(address newPair) public onlyOwner() {
960         uniswapV2Pair = newPair;
961     }
```

Contract Security

Total Findings: 9

- High 0
- Medium 1
- Low 6
- Info 2



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: (1)

- Incorrect Acces Control

Low severity issues: (6)

- Missing Events
- Long number literals
- Outdated compiler Version
- Unchecked Array Lenght
- Low level Calls
- Use of EXTCODESIZE to check external accounts

Informational severity issues: (2)

- Public Functions Should be Declared External
- State Variables Should be Declared Constant

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	low	low
SWC-103	Floating Pragma	Passed	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	Passed	Passed	Passed
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.

⚠️ Incorrect Acces Control (2 Item)

Item: 1	Location:	Line 541-544	Severity:	Medium

Function	INCORRECT ACCESS CONTROL Access control plays an important role in segregation of privileges in smart contracts and other applications. If this is misconfigured or not properly validated on sensitive functions, it may lead to loss of funds, tokens and in some cases compromise of the smart contract. The contract Sorcery is importing an access control library @openzeppelin/contracts/access/Ownable.sol but the function approve is missing the modifier onlyOwner.
Remedation	1. 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 onlyOwner or custom roles.

```
ftrace | funcSig
541 function approve(address spender, uint256 amount) public override returns (bool) {
542     _approve(_msgSender(), spender, amount);
543     return true;
544 }
545
```

Item: 1	Location:	Line 532-535	Severity:	Medium

Function	Access control plays an important role in segregation of privileges in smart contracts and other applications. If this is misconfigured or not properly validated on sensitive functions, it may lead to loss of funds, tokens and in some cases compromise of the smart contract. The contract Sorcery is importing an access control library @openzeppelin/contracts/access/Ownable.sol but the function transfer is missing the modifier onlyOwner.
Remedation	4. Ensure that initialization functions can only be called once and only by authorized entities. 5. Implement least-privilege roles using libraries like OpenZeppelin's Access Control. 6. Add proper access control modifiers to sensitive functions, such as onlyOwner or custom roles.

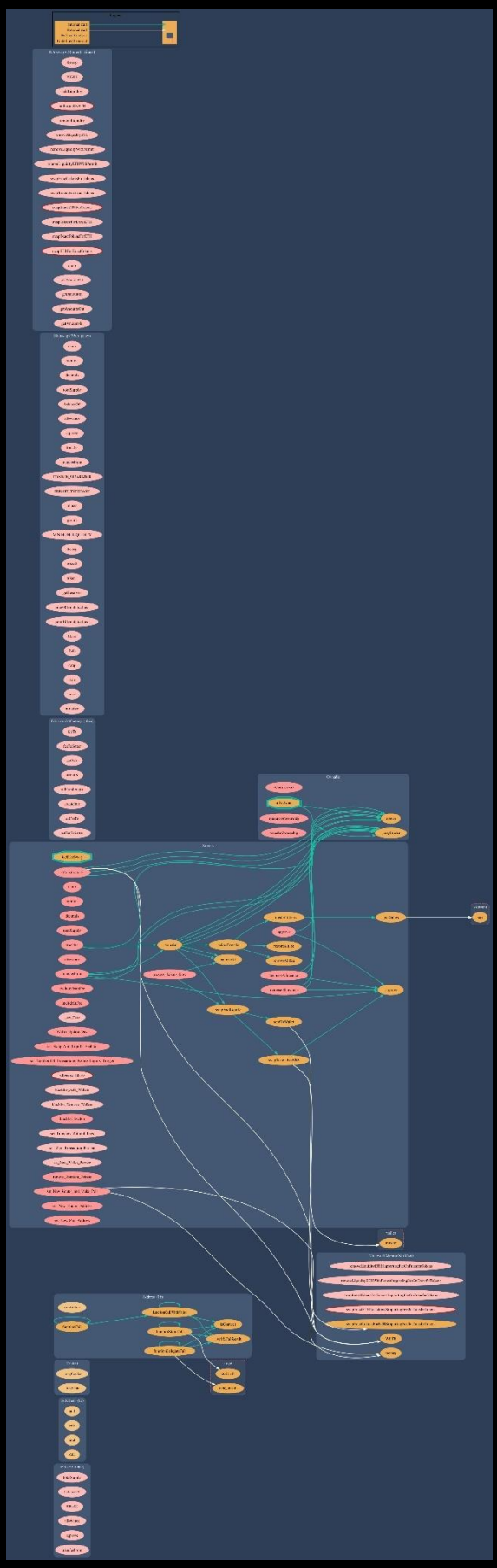
```
ftrace | funcSig
532 function transfer(address recipient, uint256 amount) public override returns (bool) {
533     _transfer(_msgSender(), recipient, amount);
534     return true;
535 }
536
```

Outdated Compiler Version.

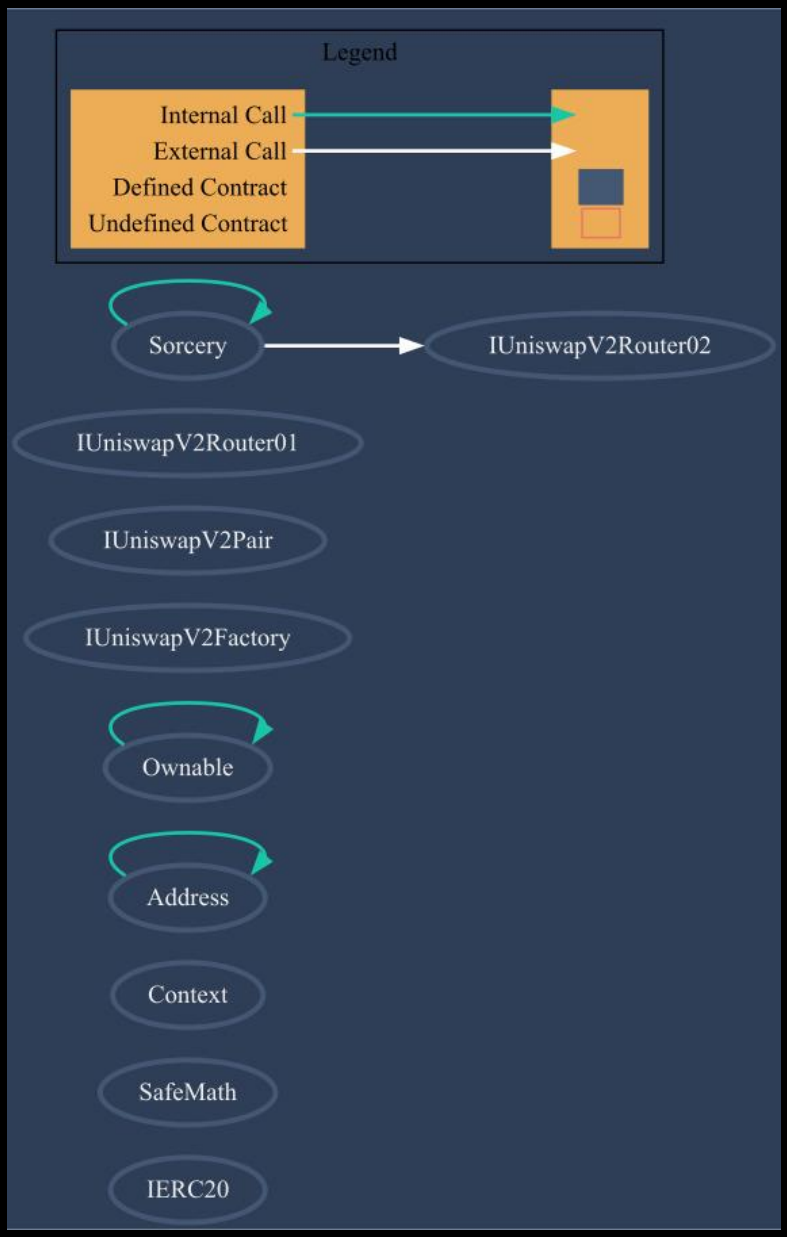
Item: 1	Location:	Line 19	Severity:	Low

Function	Using an outdated compiler version can be problematic especially if there are publicly disclosed bugs and issues that affect the current compiler version. The following outdated versions were detected: /sorcery.sol - ^0.8.7
Remedation	It is recommended to use a recent version of the Solidity compiler that should not be the most recent version, and it should not be an outdated version as well. Using very old versions of Solidity prevents the benefits of bug fixes and newer security checks. Consider using the solidity version v0.8.23, which patches most solidity vulnerabilities.

Contract Flow Graph



Contract Interaction Graph



Inheritance Graph

Contract Functions

Contract	Type	Bases		
L	Function Name	Visibility	Mutability	Modifiers
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!
SafeMath	Library			
L	add	Internal		
L	sub	Internal		
L	mul	Internal		
L	div	Internal		
L	sub	Internal		
L	div	Internal		
Context	Implementation			
L	_msgSender	Internal		
L	_msgData	Internal		
Address	Library			
L	isContract	Internal		
L	sendValue	Internal		

L	functionCall	Internal 🔒	🛑	
L	functionCall	Internal 🔒	🛑	
L	functionCallWithValue	Internal 🔒	🛑	
L	functionCallWithValue	Internal 🔒	🛑	
L	functionStaticCall	Internal 🔒		
L	functionStaticCall	Internal 🔒		
L	functionDelegateCall	Internal 🔒	🛑	
L	functionDelegateCall	Internal 🔒	🛑	
L	_verifyCallResult	Private 🔐		
Ownable	Implementation	Context		
L		Public ❗	🛑	NO❗
L	owner	Public ❗		NO❗
L	renounceOwnership	Public ❗	🛑	onlyOwner
L	transferOwnership	Public ❗	🛑	onlyOwner
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	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!
Sorcery	Implementation	Context, IERC20, Ownable		
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	excludeFromFee	Public		onlyOwner
L	includeInFee	Public		onlyOwner
L	_set_Fees	External		onlyOwner
L	Wallet_Update_Dev	Public		onlyOwner
L	set_Swap_And_Liquify_Enabled	Public		onlyOwner
L	set_Number_Of_Transactions_Before_Liquify_Trigger	Public		onlyOwner
L		External		NO
L	blacklist_Add_Wallets	External		onlyOwner
L	blacklist_Remove_Wallets	External		onlyOwner
L	blacklist_Switch	Public		onlyOwner
L	set_Transfers_Without_Fees	External		onlyOwner
L	set_Max_Transaction_Percent	External		onlyOwner
L	set_Max_Wallet_Percent	External		onlyOwner
L	removeAllFee	Private		
L	restoreAllFee	Private		
L	_approve	Private		
L	_transfer	Private		
L	sendToWallet	Private		
L	swapAndLiquify	Private		lockTheSwap
L	process_Tokens_Now	Public		onlyOwner

L	swapTokensForBNB	Private		
L	remove_Random_Tokens	Public		onlyOwner
L	set_New_Router_and_Make_Pair	Public		onlyOwner
L	set_New_Router_Address	Public		onlyOwner
L	set_New_Pair_Address	Public		onlyOwner
L	_tokenTransfer	Private		
L	_transferTokens	Private		
L	_getValues	Private		

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 vulnaribilities in the code. Findings getting reported and improvements getting suggested.

Automatic and Manual Review
We are using automated tools to scan functions and weeknesses 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