Audit Report

HS

January 2022

Type	BEP20
Network	BSC
Address	0x8bf4f8d30d013119a8c60df8f358635bbe7610b2
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	HS
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	OSL-3.0
Explorer	https://bscscan.com/token/0x8bf4f8d30d013119a8c60df8f358635bbe7610b2
Symbol	HS
Decimals	9
Total Supply	1,000,000,000
Source	contract.sol
Domain	hearthstonecrypto.com

Audit Updates

Initial Audit	23rd January 2022
Corrected	

Contract Analysis

● Critical ● Medium ● Minor ● Pass

Severity	Code	Description
●	ST	Contract Owner is not able to stop or pause transactions
●	OCTD	Contract Owner is not able to transfer tokens from specific address
●	OTUT	Owner Transfer User's Tokens
●	ELFM	Contract Owner is not able to increase fees more than a reasonable percent (25%)
●	ULTW	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
●	MT	Contract Owner is not able to mint new tokens
●	BT	Contract Owner is not able to burn tokens from specific wallet
●	BC	Contract Owner is not able to blacklist wallets from selling

Contract Diagnostics

● Critical   ● Medium   ● Minor

Severity	Code	Description
●	CO	Code Optimization
●	L01	Public Function could be Declared External
●	L02	State Variables could be Declared Constant
●	L04	Conformance to Solidity Naming Conventions
●	L09	Dead Code Elimination
●	L07	Missing Events Arithmetic

CO - Code Optimization

Criticality	minor
Location	contract.sol#L1

Description

The `sellFeeRate` and `buyFeeRate` variables are initialized to zero. Thus, all the following statements are redundant since the fee value will always be zero.

```solidity
if(recipient == uniswapV2Pair){
    if (
        sender != address(this) &&
        recipient != address(this) &&
        !_isExcludedFromFee[sender]
    ) {
        uint256 _fee = amount.mul(sellFeeRate).div(100);
        super._transfer(sender,mintContract, _fee.mul(50).div(100));
        super._transfer(sender, addressForMarketing, _fee.mul(375).div(1000));
        super._transfer(sender, BurnAddr, _fee.mul(125).div(1000));
        amount = amount.sub(_fee);
    }
}else if(sender == uniswapV2Pair){
    if (
        sender != address(this) &&
        recipient != address(this) &&
        !_isExcludedFromFee[sender]
    ) {
        uint256 _fee = amount.mul(buyFeeRate).div(100);
        super._transfer(sender,mintContract, _fee.mul(60).div(100));
        super._transfer(sender, addressForMarketing,
_fee.sub(_fee.mul(60).div(100)));
        amount = amount.sub(_fee);
    }
}
```

Recommendation

Eliminate all the fee transfers since they will never be executed.

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L1051,L1047,L1042 and 14 more

Description

Public functions that are never called by the contract should be declared external to save gas.

```
includeInFee
excludeFromFee
getvalue
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L980,L981,L975 and 4 more

Description

Constant state variables should be declared constant to save gas.

```
sellFeeRate
buyFeeRate
antiBotDuration
...
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L959,L955,L954 and 6 more

Description

Solidity defines a naming convention that should be followed. Rule exceptions:

- Allow constant variable name/symbol/decimals to be lowercase.
- Allow _ at the beginning of the mixed_case match for private variables and unused parameters.

```
BurnAddr
MAX_LOCK
MAX_TOKENS_FOR_REWARDS
...
```

Recommendation

Follow the Solidity naming convention.
https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions

L09 - Dead Code Elimination

Criticality	minor
Location	contract.sol#L29,L41,L70 and 8 more

Description

Functions that are not used in the contract, and make the code's size bigger.

```
trySub
tryMul
tryMod
...
```

Recommendation

Remove unused functions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L1030

Description

Detected missing events for critical arithmetic parameters. There are functions that have no event emitted, so it is difficult to track off-chain changes.

```
antiBotAmount = amount
```

Recommendation

Emit an event for critical parameter changes.

Contract Function

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
SafeMath	Library			
	tryAdd	Internal		
	trySub	Internal		
	tryMul	Internal		
	tryDiv	Internal		
	tryMod	Internal		
	add	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	mod	Internal		
	sub	Internal		
	div	Internal		
	mod	Internal		
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metada ta	Interface	IERC20		

	name	External		-
	symbol	External		-
	decimals	External		-
ERC20	Implementation	Context, IERC20, IERC20Metadata		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
ERC20Burnable	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner

	_setOwner	Private	✓	
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IUniswapV2Router01	Interface			
	factory	External		-
	WETH	External		-
	addLiquidity	External	✓	-
	addLiquidityETH	External	Payable	-
	removeLiquidity	External	✓	-
	removeLiquidityETH	External	✓	-
	removeLiquidityWithPermit	External	✓	-
	removeLiquidityETHWithPermit	External	✓	-
	swapExactTokensForTokens	External	✓	-
	swapTokensForExactTokens	External	✓	-
	swapExactETHForTokens	External	Payable	-
	swapTokensForExactETH	External	✓	-
	swapExactTokensForETH	External	✓	-
	swapETHForExactTokens	External	Payable	-
	quote	External		-
	getAmountOut	External		-
	getAmountIn	External		-
	getAmountsOut	External		-
	getAmountsIn	External		-

IUniswapV2Router02	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
HS	Implementation	ERC20, ERC20Burnable, Ownable		
	<Constructor>	Public	✓	ERC20
	decimals	Public		-
	getUnlockTime	Public		onlyOwner
	setUnlockTime	External	✓	onlyOwner
	setBotAddresses	External	✓	onlyOwner
	addBotAddress	External	✓	onlyOwner
	antiBot	External	✓	onlyOwner
	getvalue	Public		onlyOwner
	excludeFromFee	Public	✓	onlyOwner
	includeInFee	Public	✓	onlyOwner
	SetMintContract	External	✓	onlyOwner
	isContractaddr	Public		-
	_transfer	Internal	✓	
	<Receive Ether>	External	Payable	-

Contract Flow

Domain Info

Domain Name	hearthstonecrypto.com
Registry Domain ID	2665910248_DOMAIN_COM-VRSN
Creation Date	2022-01-04T10:55:37Z
Updated Date	2022-01-04T10:55:37Z
Registry Expiry Date	
Registrar WHOIS Server	whois.name.com
Registrar URL	http://www.name.com
Registrar	Name.com, Inc.
Registrar IANA ID	625

The domain has been created 19 days before the creation of the audit.

There is no public billing information, the creator is protected by the privacy settings.

Summary

The Smart Contract analysis reported no compiler error or critical issues. The contract Owner can access some admin functions that can not be used in a malicious way to disturb the users' transactions. Every transaction triggers 3 transfers to the mintContract, addressForMarketing, BurnAddr. The amount of these transfers will always be zero. Hence the entire transfer statement is redundant.

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.

Coinscope team provides no guarantees against the sale of team tokens or the removal of liquidity by the project audited in this document. Always Do your own research and protect yourselves from being scammed.

The Coinscope 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 Coinscope receive a payment to manipulate those results or change the awarding badge that we will be adding in our website.

Always 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 Coinscope team disclaims any liability for the resulting losses.

About Coinscope

Coinscope is the leading early coin listing, voting and auditing authority firm. The audit process is analyzing and monitoring many aspects of the project. That way, it gives the community a good sense of security using an informative report and a generic score.

Coinscope is aiming to make crypto discoverable and efficient globally. It provides all the essential tools to assist users draw their own conclusions.

The Coinscope.co team

https://www.coinscope.co