Audit Report

Domain

January 2022

Type	BEP20
Network	BSC
Address	0x3Ffbe849A2666657B729a6bf19befD54D9E57c8b
Audited by	© coinscope

Table of Contents

Table of Contents 1
Contract Review 3
Audit Updates 3
Contract Analysis 4
ST - Stop Transactions 5
Description 5
Recommendation 6
ELFM - Exceed Limit Fees Manipulation 7
Description 7
Recommendation 7
Contract Diagnostics 8
L01 - Public Function could be Declared External 9
Description 9
Recommendation 9
L02 - State Variables could be Declared Constant 10
Description 10
Recommendation 10
L04 - Conformance to Solidity Naming Conventions 11
Description 11
Recommendation 11
L09 - Dead Code Elimination 12
Description 12
Recommendation 12
L07 - Missing Events Arithmetic 13
Description 13
Recommendation 13

Contract Functions 14

Contract Flow 18

Domain Info 19

Summary 20

Disclaimer 21

About Coinscope 22

Contract Review

Contract Name	Domain
Compiler Version	v0.8.7+commit.e28d00a7
Optimization	200 runs
Licence	None
Explorer	https://bscscan.com/token/0x3Ffbe849A2666657B729a6bf19befD54D9E57c8b
Symbol	DMN
Decimals	9
Total Supply	100,000,000
Source	contract.sol
Domain	dmncrypto.com

Audit Updates

Initial Audit	31st 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

ST - Stop Transactions

Criticality	critical
Location	contract.sol#L1026,1032,1076

Description

The contract owner has the authority to stop transactions for all sales or boughts excluding the owner. The owner may take advantage of it by calling the `setMaxTransactionAmount` or `setMaxWalletAmount` with a high number. As a result the expression `maxTxAmountSell = _tTotal / _maxTxAmountSellPct` will produce a significant small number. In practice, that number will not be enough for the users to sell assuming that their holdings will be thousands.

```
function setMaxTransactionAmount(
    uint256 _maxTxAmountBuyPct,
    uint256 _maxTxAmountSellPct
) external onlyOwner {
    maxTxAmountBuy = _tTotal / _maxTxAmountBuyPct; // 100 = 1%, 50 = 2% etc.
    maxTxAmountSell = _tTotal / _maxTxAmountSellPct; // 100 = 1%, 50 = 2% etc.
}
```

```
require(
    amount <= maxTxAmountSell,
    "amount must be <= maxTxAmountSell"
);
```

```
require(
    amount <= maxTxAmountBuy,
    "amount must be <= maxTxAmountBuy"
);
```

```
require(
    _isExcludedFromMaxWallet[recipient] ||
        balanceOf(recipient) <= maxWalletAmount,
```

```
    "Recipient cannot hold more than maxWalletAmount"
);
```

Recommendation

The contract could embody a check for not allowing setting the *maxTxAmountBuy*, *maxTxAmountSell* and *maxTxAmountBuy* less than a reasonable amount. A suggested implementation could check that the maximum amount should be more than a fixed percentage of the total supply.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

ELFM - Exceed Limit Fees Manipulation

Criticality	critical
Location	contract.sol#L1155,1168

Description

The contract owner has the authority to increase over the allowed limit of 25%. The owner may take advantage of it by calling the `setSellFees` function with a high percentage value.

```
function setSellFees(
    uint8 _rfi,
    uint8 _treasury,
    uint8 _dev,
    uint8 _lp
) external onlyOwner {
    sellRates.rfi = _rfi;
    sellRates.treasury = _treasury;
    sellRates.dev = _dev;
    sellRates.lp = _lp;
    sellRates.toSwap = _treasury + _dev + _lp;
}
```

Recommendation

The contract could embody a check for the maximum acceptable value.

The team should carefully manage the private keys of the owner's account. We strongly recommend a powerful security mechanism that will prevent a single user from accessing the contract admin functions. That risk can be prevented by temporarily locking the contract or renouncing ownership.

Contract Diagnostics

Critical Medium Minor

Severity	Code	Description
	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

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L887,L879,L875 and 14 more

Description

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

```
setSwapAndLiquifyEnabled
isExcludedFromMaxWallet
isExcludedFromFee
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L593,L584

Description

Constant state variables should be declared constant to save gas.

```
blocksToWait
_tTotal
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L605,L601,L600 and 20 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.

```
UniswapV2Router
_symbol
_name
...
```

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#L20,L540,L371 and 8 more

Description

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

```
_msgData
verifyCallResult
isContract
...
```

Recommendation

Remove unused functions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L1189,L1181

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.

```
numTokensSellToAddToLiquidity = amountTokens * 10 ** _decimals
maxTxAmountBuy = _tTotal / _maxTxAmountBuyPct
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

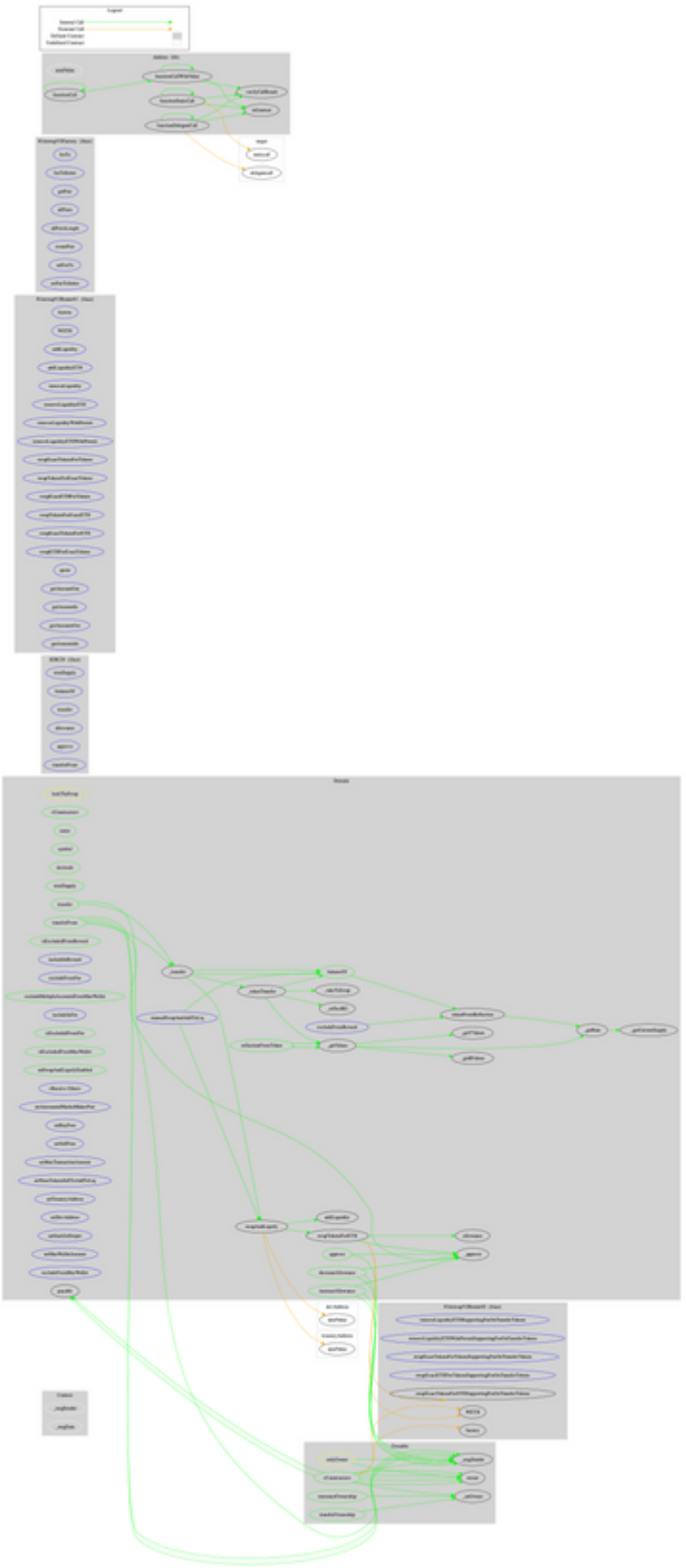
Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	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	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
Address	Library			
	isContract	Internal		

	sendValue	Internal	✓	
	functionCall	Internal	✓	
	functionCall	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionCallWithValue	Internal	✓	
	functionStaticCall	Internal		
	functionStaticCall	Internal		
	functionDelegateCall	Internal	✓	
	functionDelegateCall	Internal	✓	
	verifyCallResult	Internal		
Domain	Implementation	Context, IERC20, Ownable		
	<Constructor>	Public	✓	-
	name	Public		-
	symbol	Public		-
	decimals	Public		-
	totalSupply	Public		-
	balanceOf	Public		-
	transfer	Public	✓	-
	allowance	Public		-
	approve	Public	✓	-
	transferFrom	Public	✓	-
	increaseAllowance	Public	✓	-
	decreaseAllowance	Public	✓	-
	isExcludedFromReward	Public		-
	reflectionFromToken	Public		-
	tokenFromReflection	Public		-
	excludeFromReward	External	✓	onlyOwner
	includeInReward	External	✓	onlyOwner
	excludeFromFee	External	✓	onlyOwner
	excludeMultipleAccountsFromMaxWallet	Public	✓	onlyOwner
	includeInFee	External	✓	onlyOwner
	isExcludedFromFee	Public		-

	isExcludedFromMaxWallet	Public		-
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	<Receive Ether>	External	Payable	-
	_reflectRfi	Private	✓	
	_takeToSwap	Private	✓	
	_getValues	Private		
	_getTValues	Private		
	_getRValues	Private		
	_getRate	Private		
	_getCurrentSupply	Private		
	_approve	Private	✓	
	_transfer	Private	✓	
	_tokenTransfer	Private	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForETH	Private	✓	
	addLiquidity	Private	✓	
	setAutomatedMarketMakerPair	External	✓	onlyOwner
	setBuyFees	External	✓	onlyOwner
	setSellFees	External	✓	onlyOwner
	setMaxTransactionAmount	External	✓	onlyOwner
	setNumTokensSellToAddToLiq	External	✓	onlyOwner
	setTreasuryAddress	External	✓	onlyOwner
	setDevAddress	External	✓	onlyOwner
	manualSwapAndAddToLiq	External	✓	onlyOwner
	unblacklistSniper	External	✓	onlyOwner
	setMaxWalletAmount	External	✓	onlyOwner
	excludeFromMaxWallet	External	✓	onlyOwner

Contract Flow



Domain Info

Domain Name	dmncrypto.com
Registry Domain ID	2661101519_DOMAIN_COM-VRSN
Creation Date	2021-12-12T07:41:21.00Z
Updated Date	0001-01-01T00:00:00.00Z
Registry Expiry Date	
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain has been created about 2 months before the creation of the audit.

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

Summary

Domain is aiming to make business communication easier and accessible to everyone. The Project has a friendly and growing community. There are some functions that can be abused by the owner, like manipulating fees and stopping the transactions. The contract could potentially operate as a honeypot if the contract owner abuses the configuration. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract or renouncing ownership will eliminate all the contract threats.

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