



# Audit Report

## **LasMeta**

February 2022

Type	BEP20
Network	BSC
Address	0x236Cc456F26B202F58E6fb4D05186d42B8a969eD
Audited by	© coinscope

# Table of Contents

<b>Table of Contents</b>	<b>1</b>
<b>Contract Review</b>	<b>3</b>
<b>Audit Updates</b>	<b>3</b>
<b>Contract Analysis</b>	<b>4</b>
<b>OCTD - Owner Contract Tokens Drain</b>	<b>5</b>
Description	5
Recommendation	5
<b>ELFM - Exceed Limit Fees Manipulation</b>	<b>6</b>
Description	6
Recommendation	6
<b>BC - Blacklisted Contracts</b>	<b>7</b>
Description	7
Recommendation	7
<b>Contract Diagnostics</b>	<b>8</b>
<b>L01 - Public Function could be Declared External</b>	<b>9</b>
Description	9
Recommendation	9
<b>L05 - Unused State Variable</b>	<b>10</b>
Description	10
Recommendation	10
<b>L04 - Conformance to Solidity Naming Conventions</b>	<b>11</b>
Description	11
Recommendation	11
<b>L09 - Dead Code Elimination</b>	<b>12</b>
Description	12
Recommendation	12

<b>L12 - Using Variables before Declaration</b>	<b>13</b>
Description	13
Recommendation	13
<b>L07 - Missing Events Arithmetic</b>	<b>14</b>
Description	14
Recommendation	14
<b>L15 - Local Scope Variable Shadowing</b>	<b>15</b>
Description	15
Recommendation	15
<b>L14 - Uninitialized Variables in Local Scope</b>	<b>16</b>
Description	16
Recommendation	16
<b>L13 - Divide before Multiply Operation</b>	<b>17</b>
Description	17
Recommendation	17
<b>Contract Functions</b>	<b>18</b>
<b>Domain Info</b>	<b>27</b>
<b>Summary</b>	<b>28</b>
<b>Disclaimer</b>	<b>29</b>
<b>About Coinscope</b>	<b>30</b>

## Contract Review

<b>Contract Name</b>	LASM
<b>Compiler Version</b>	v0.8.0+commit.c7dfd78e
<b>Optimization</b>	200 runs
<b>Licence</b>	None
<b>Explorer</b>	<a href="https://bscscan.com/token/0x236Cc456F26B202F58E6fb4D05186d42B8a969eD">https://bscscan.com/token/0x236Cc456F26B202F58E6fb4D05186d42B8a969eD</a>
<b>Symbol</b>	LASM
<b>Decimals</b>	18
<b>Total Supply</b>	800,000,000
<b>Source</b>	contract.sol
<b>Domain</b>	lasmeta.io

## Audit Updates

<b>Initial Audit</b>	13th February 2022
<b>Corrected</b>	

# Contract Analysis

● Critical
 ● Medium
 ● Minor
 ● Pass

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

## OCTD - Owner Contract Tokens Drain

Criticality	minor
Location	contract.sol#L1807

### Description

The contract owner has the authority to claim a huge amount of the contract balance. The owner may take advantage of it by calling the `release` function. This function has not been called yet.

```
function release() public virtual onlyOwner {
    require(block.timestamp >= releaseTime(), "TokenTimelock: current time is before release time");

    uint256 amount = balanceOf(address(this));
    require(amount > 0, "TokenTimelock: no tokens to release");

    if (amount > lockedAmounts)
        amount = lockedAmounts;

    lockedAmounts = 0;

    ERC20._transfer(address(this), beneficiary(), amount);
}
```

### Recommendation

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

<b>Criticality</b>	critical
<b>Location</b>	contract.sol#L1473,1481,1489

### 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 `setGameDevFee` function with a high percentage value.

```
function setGameDevFee(uint256 value) external onlyOwner{  
    gameDevFee = value;  
    totalFees = rewardsFee.add(liquidityFee).add(gameDevFee);  
}
```

### 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.

## BC - Blacklisted Contracts

<b>Criticality</b>	medium
<b>Location</b>	contract.sol#L1658

### Description

The contract owner has the authority to stop contracts from transactions. The owner may take advantage of it by calling the `blacklistAddress` function.

```
require(!_isBlacklisted[from] && !_isBlacklisted[to], 'Blacklisted address');
```

### Recommendation

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
●	L05	Unused State Variable
●	L04	Conformance to Solidity Naming Conventions
●	L09	Dead Code Elimination
●	L12	Using Variables before Declaration
●	L07	Missing Events Arithmetic
●	L15	Local Scope Variable Shadowing
●	L14	Uninitialized Variables in Local Scope
●	L13	Divide before Multiply Operation

## L01 - Public Function could be Declared External

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L337,345,362,388,407,425 and 25 more

### Description

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

```
process  
getAccountAtIndex  
release  
...
```

### Recommendation

Use the external attribute for functions never called from the contract

## L05 - Unused State Variable

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L641

### Description

There are segments that contain unused state variables.

```
MAX_INT256
```

### Recommendation

Remove unused state variables.

## L04 - Conformance to Solidity Naming Conventions

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L876,883,890,900,815,820 and 15 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.

```
_account  
GameDev  
airdrop  
...
```

### Recommendation

Follow the Solidity naming convention.

<https://docs.soliditylang.org/en/v0.4.25/style-guide.html#naming-conventions>

## L09 - Dead Code Elimination

<b>Criticality</b>	minor
<b>Location</b>	contract.sol#L134,910,261,277,687,658 and 1 more

### Description

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

```
mul
div
abs
...
```

### Recommendation

Remove unused functions.

## L12 - Using Variables before Declaration

**Criticality**

minor

**Location**

contract.sol#L1712

### Description

The contract is using a variable before the declaration. This is usually happening either if it has not been declared yet or the variable has been declared in a different scope.

```
iterations  
claims  
lastProcessedIndex
```

### Recommendation

The variables should be declared before any usage of them.

## L07 - Missing Events Arithmetic

**Criticality**

minor

**Location**

contract.sol#L1459,1473,1481,1489

### 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.

```
gameDevFee = value
liquidityFee = value
rewardsFee = value
...
```

### Recommendation

Emit an event for critical parameter changes.

## L15 - Local Scope Variable Shadowing

**Criticality**

minor

**Location**

contract.sol#L829,876,883,890,900

### Description

There are variables that are defined in the local scope containing the same name from an upper scope.

```
_owner  
_symbol  
_name  
...
```

### Recommendation

The local variables should have different names from the upper scoped variables.



## L14 - Uninitialized Variables in Local Scope

**Criticality**

minor

**Location**

contract.sol#L1712

### Description

There are variables that are defined in the local scope and are not initialized.

```
lastProcessedIndex  
claims  
iterations
```

### Recommendation

All the local scoped variables should be initialized.

## L13 - Divide before Multiply Operation

**Criticality**

minor

**Location**

contract.sol#L1304 and 2 more

### Description

Performing divisions before multiplications may cause lose of prediction.

```
lockedAmounts = (cap / 100) * 40  
_mint(airdrop,(cap / 100) * 7)  
_mint(GameRewards,(cap / 100) * 10)  
...
```

### Recommendation

The multiplications should be prior to the divisions.

# Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
<b>IERC20</b>	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
<b>IERC20Metadata</b>	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
<b>Context</b>	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
<b>SafeMath</b>	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		

ERC20	Implementation	Context, IERC20, IERC20Met adata		
	<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	✓	
<b>ERC20Burnable</b>	Implementation	Context, ERC20		
	burn	Public	✓	-
	burnFrom	Public	✓	-
<b>SafeMathUint</b>	Library			
	toInt256Safe	Internal		
<b>SafeMathInt</b>	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
	abs	Internal		
	toUint256Safe	Internal		

<b>DividendPayingTokenInterface</b>	Interface			
	dividendOf	External		-
	withdrawDividend	External	✓	-
<b>DividendPayingTokenOptionalInterface</b>	Interface			
	withdrawableDividendOf	External		-
	withdrawnDividendOf	External		-
	accumulativeDividendOf	External		-
<b>Ownable</b>	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
<b>DividendPayingToken</b>	Implementation	ERC20, Ownable, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface		
	<Constructor>	Public	✓	ERC20
	distributeCAKEDividends	Public	✓	onlyOwner
	withdrawDividend	Public	✓	-
	_withdrawDividendOfUser	Internal	✓	
	dividendOf	Public		-
	withdrawableDividendOf	Public		-
	withdrawnDividendOf	Public		-
	accumulativeDividendOf	Public		-
	_transfer	Internal	✓	
	_mint	Internal	✓	

	_burn	Internal	✓	
	_setBalance	Internal	✓	
<b>IterableMapping</b>	Library			
	get	Public		-
	getIndexOfKey	Public		-
	getKeyAtIndex	Public		-
	size	Public		-
	set	Public	✓	-
	remove	Public	✓	-
<b>IUniswapV2Pair</b>	Interface			
	name	External		-
	symbol	External		-
	decimals	External		-
	totalSupply	External		-
	balanceOf	External		-
	allowance	External		-
	approve	External	✓	-
	transfer	External	✓	-
	transferFrom	External	✓	-
	DOMAIN_SEPARATOR	External		-
	PERMIT_TYPEHASH	External		-
	nonces	External		-
	permit	External	✓	-
	MINIMUM_LIQUIDITY	External		-
	factory	External		-
	token0	External		-
	token1	External		-
	getReserves	External		-
	price0CumulativeLast	External		-
	price1CumulativeLast	External		-
	kLast	External		-
	mint	External	✓	-

	burn	External	✓	-
	swap	External	✓	-
	skim	External	✓	-
	sync	External	✓	-
	initialize	External	✓	-
<b>IUniswapV2Factory</b>	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
<b>IUniswapV2Router01</b>	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		-
<b>IUniswapV2Router02</b>	Interface	IUniswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
<b>LASM</b>	Implementation	ERC20, ERC20Burnable, Ownable		
	<Constructor>	Public	✓	ERC20
	<Receive Ether>	External	Payable	-
	burn	Public	✓	-
	updateDividendTracker	Public	✓	onlyOwner
	updateUniswapV2Router	Public	✓	onlyOwner
	beneficiary	Public		-
	releaseTime	Public		-
	excludeFromFees	Public	✓	onlyOwner
	excludeMultipleAccountsFromFees	Public	✓	onlyOwner
	setSwapTokensAtAmount	External	✓	onlyOwner
	setGameDevWallet	External	✓	onlyOwner
	setRewardsFee	External	✓	onlyOwner
	setLiquiditFee	External	✓	onlyOwner
	setGameDevFee	External	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	blacklistAddress	External	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	updateGasForProcessing	Public	✓	onlyOwner



	updateClaimWait	External	✓	onlyOwner
	getClaimWait	External		-
	getTotalDividendsDistributed	External		-
	isExcludedFromFees	Public		-
	withdrawableDividendOf	Public		-
	dividendTokenBalanceOf	Public		-
	excludeFromDividends	External	✓	onlyOwner
	getAccountDividendsInfo	External		-
	getAccountDividendsInfoAtIndex	External		-
	processDividendTracker	External	✓	-
	claim	External	✓	-
	getLastProcessedIndex	External		-
	getNumberOfDividendTokenHolders	External		-
	_transfer	Internal	✓	
	sendToGameDevFee	Private	✓	
	swapAndLiquify	Private	✓	
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	sendDividends	Private	✓	
	release	Public	✓	onlyOwner
<b>LasmDividend Tracker</b>	Implementation	Ownable, DividendPay ingToken		
	<Constructor>	Public	✓	DividendPayin gToken
	_transfer	Internal		
	withdrawDividend	Public		-
	excludeFromDividends	External	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	getLastProcessedIndex	External		-
	getNumberOfTokenHolders	External		-
	getAccount	Public		-
	getAccountAtIndex	Public		-
	canAutoClaim	Private		
	setBalance	External	✓	onlyOwner

	process	Public	✓	-
	processAccount	Public	✓	onlyOwner

## Contract Flow

## Domain Info

<b>Domain Name</b>	lasmeta.io
<b>Registry Domain ID</b>	4c52850cd4c84b64a1f77dd96092dc49-DONUTS
<b>Creation Date</b>	2021-11-28T19:04:22Z
<b>Updated Date</b>	2021-12-15T11:55:12Z
<b>Registry Expiry Date</b>	2022-11-28T19:04:22Z
<b>Registrar WHOIS Server</b>	whois.godaddy.com/
<b>Registrar URL</b>	<a href="http://www.godaddy.com/domains/search.aspx?ci=8990">http://www.godaddy.com/domains/search.aspx?ci=8990</a>
<b>Registrar</b>	GoDaddy.com, LLC
<b>Registrar IANA ID</b>	146

The domain has been created 3 months before the creation of the audit. It will expire in 10 months.

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

## Summary

There are some functions that can be abused by the owner, like manipulating fees and blacklisting contracts. 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>