COINSCOPE

Audit Report

Lava Financial

January 2022

Type	ERC20
Network	AVAX
Address	0x79bff47f52c758cb03edfa93c1bf0659940bdac0
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	LavaERC20Token
Compiler Version	v0.7.5+commit.eb77ed08
Optimization	200 runs
Licence	None
Explorer	https://snowtrace.io/token/0x79bff47f52c758cb03edfa93c1bf0659940bdac0
Symbol	LAVA
Decimals	0
Total Supply	0
Source	contract.sol
Domain	lava.financial

Audit Updates

Initial Audit	4th 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

MT - Mint Tokens

Criticality	medium
Location	contract.sol#L1,L892

Description

There is a privileged owner account that plays a critical role in governing the treasury contract (Vault) and regulating the token contract. We emphasise that the privilege assignment with various factory contracts is necessary and required for proper protocol operations.

However, it is worrisome if the owner is not governed by a DAO-like structure. We point out that a compromised owner account would allow the attacker to change the current vault to mint an arbitrary number of tokens or change other settings to steal funds of currently staking users, which directly undermines the integrity of the Lava Financial.

```
function mint(address account_, uint256 amount_) external onlyVault() {
        _mint(account_, amount_);
    }
```

Recommendation

The owner should carefully manage the credentials of the owner’s account. We advised considering an extra-strong security mechanism that the actions may be quarantined by many users instead of one. The owner could also renounce the contract ownership for a period of time or pass the access to the zero address.

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
●	L06	Missing Events Access Control

L01 - Public Function could be Declared External

Criticality	minor
Location	contract.sol#L1358,L1332,L1233 and 14 more

Description

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

```
burnFrom
burn
vault
...
```

Recommendation

Use the external attribute for functions never called from the contract

L05 - Unused State Variable

Criticality	minor
Location	contract.sol#L735

Description

There are segments that contains unused state variable.

```
ERC20TOKEN_ERC1820_INTERFACE_ID
```

Recommendation

Remove unused state variables.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L1362,L1222,L1170 and 7 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.

```
_burnFrom
_vault
_owner
...
```

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#L700,L677,L718 and 43 more

Description

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

```
substractPercentage
sqrrt
quadraticPricing
...
```

Recommendation

Remove unused functions.

L06 - Missing Events Access Control

Criticality	minor
Location	contract.sol#L1224

Description

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

```
_vault = vault_
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
ITWAPOracle	Interface			
	uniV2CompPairAddressForLastEpochUpdateBlockTimstamp	External	✓	-
	priceTokenAddressForPricingTokenAddressForLastEpochUpdateBlockTimstamp	External	✓	-
	pricedTokenForPricingTokenForEpochPeriodForPrice	External	✓	-
	pricedTokenForPricingTokenForEpochPeriodForLastEpochPrice	External	✓	-
	updateTWAP	External	✓	-
EnumerableSet	Library			
	_add	Private	✓	
	_remove	Private	✓	
	_contains	Private		
	_length	Private		
	_at	Private		
	_getValues	Private		
	_insert	Private	✓	
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	getValues	Internal		
	insert	Internal	✓	
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		

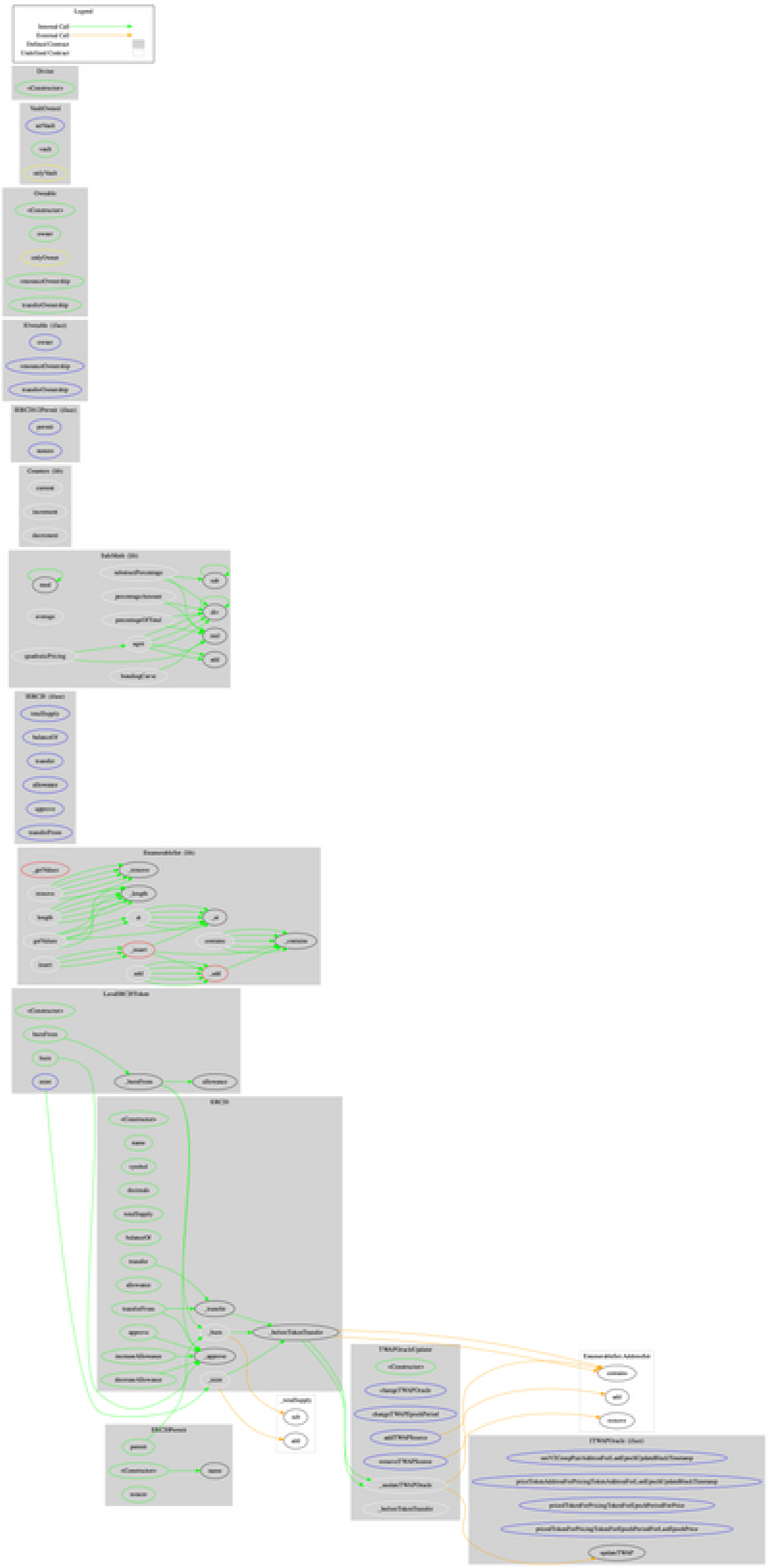
	length	Internal		
	at	Internal		
	getValues	Internal		
	insert	Internal	✓	
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	getValues	Internal		
	insert	Internal	✓	
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
	add	Internal	✓	
	remove	Internal	✓	
	contains	Internal		
	length	Internal		
	at	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		

	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
	sqrrt	Internal		
	percentageAmount	Internal		
	substractPercentage	Internal		
	percentageOfTotal	Internal		
	average	Internal		
	quadraticPricing	Internal		
	bondingCurve	Internal		
ERC20	Implementation	IERC20		
	<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	✓	
Counters	Library			
	current	Internal		
	increment	Internal	✓	
	decrement	Internal	✓	

IERC2612Permit	Interface			
	permit	External	✓	-
	nonces	External		-
ERC20Permit	Implementation	ERC20, IERC2612Permit		
	<Constructor>	Public	✓	-
	permit	Public	✓	-
	nonces	Public		-
IOwnable	Interface			
	owner	External		-
	renounceOwnership	External	✓	-
	transferOwnership	External	✓	-
Ownable	Implementation	IOwnable		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner
VaultOwned	Implementation	Ownable		
	setVault	External	✓	onlyOwner
	vault	Public		-
TWAPOracleUpdater	Implementation	ERC20Permit, VaultOwned		
	<Constructor>	Public	✓	ERC20
	changeTWAPOracle	External	✓	onlyOwner
	changeTWAPEpochPeriod	External	✓	onlyOwner
	addTWAPSource	External	✓	onlyOwner
	removeTWAPSource	External	✓	onlyOwner
	_uodateTWAPOracle	Internal	✓	

	_beforeTokenTransfer	Internal	✓	
Divine	Implementation	TWAPOracleUpdater		
	<Constructor>	Public	✓	TWAPOracleUpdater
LavaERC20Token	Implementation	Divine		
	<Constructor>	Public	✓	Divine
	mint	External	✓	onlyVault
	burn	Public	✓	-
	burnFrom	Public	✓	-
	_burnFrom	Public	✓	-

Contract Flow



Domain Info

Domain Name	lava.financial
Registry Domain ID	1a1fb06f05ba4fc78f3a1d6f2ef17bb5-DONUTS
Creation Date	2021-12-17T03:50:49Z
Updated Date	2021-12-22T03:50:58Z
Registry Expiry Date	2022-12-17T03:50:49Z
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	https://www.namecheap.com/
Registrar	NameCheap, Inc.
Registrar IANA ID	1068

The domain has been created 18 days before the creation of the audit. It will expire in 12 months.

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

Summary

Lava Financial is a hybrid Node-as-a-Service on AVAX with the protocol owned liquidity dynamics of OHM and NODE dynamics inspired by STRONG. There are some informative comments that do not affect the contract security. The contract analysis reported one medium threat issue. The contract owner may mint an arbitrary number of tokens and inflate the contract’s balance. We state that the owner privileges are necessary and required for proper protocol operations. Thus, we emphasise the contract owner to be extra careful with the credentials. A multi-wallet signing pattern will provide security against potential hacks. Temporarily locking the contract 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