COINSCOPE

Audit Report

Kryptolance

December 2021

Type	BEP20
Address	0x6f88A0b4fB8c9D18eb0AB4c240e18E6aE1801932
Audited by	© coinscope

Table of Contents

Contract Review

Contract Name	Kryptolance
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	800 runs
Licence	None
Explorer	https://bscscan.com/token/0x6f88A0b4fB8c9D18eb0AB4c240e18E6aE1801932
Symbol	KRYPT
Decimals	9
Total Supply	1,000,000,000
Website	https://kryptolance.com/

Audit Updates

Initial Audit	8th of December 2021
Corrected	

Contract Analysis

Pass	Description
✓	Contract Owner is not able to mint new tokens
✓	Contract Owner is not able to burn new tokens
✗	Contract Owner is not able to increase fees more than a reasonable percent (25%)
✗	Contract Owner is not able stop or pause transactions
✓	Contract Owner is not able to transfer tokens from specific address
✓	Contract Owner is not able to increase the amount of liquidity taken by dev wallet more than a reasonable percent
✗	Contract Owner is not able to blacklist wallets from selling
✓	Liquidity pool is locked

UIF - Unlimited Increase Fees

Criticality	high
Location	https://bscscan.com/address/0x6f88A0b4fB8c9D18eb0AB4c240e18E6aE1801932#code#F1#L381

Description

The contract owner has the authority to increase fees without limit. The owner may take advantage of it by calling the `updateFees` function with a high percentage value.

```
function updateFees(uint256 _burnFee,uint256 _marketingFee,uint256
_liquidityFee, uint256 _BNBRewardsFee,uint256 _liquiditySellFee, uint256
_BNBRewardsSellFee) external onlyOwner {
    burnFee = _burnFee;
    marketingFee = _marketingFee;
    liquidityFee = _liquidityFee;
    perviousliquidityFee = liquidityFee;
    BNBRewardsFee = _BNBRewardsFee;
    perviousBNBRewardsFee = BNBRewardsFee;
    BNBRewardsSellFee = _BNBRewardsSellFee;
    liquiditySellFee = _liquiditySellFee;

    updatetotalfee();
}
```

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

Criticality	high
Location	https://bscscan.com/address/0x6f88A0b4fB8c9D18eb0AB4c240e18E6aE1801932#code#F1#L197

Description

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

```
function addSniperInList(address account) external onlyOwner {
    require(
        account != address(PancakeswapV2Router),
        "We can not blacklist pancakeRouter"
    );
    require(!_isSniper[account], "Account is already blacklisted");
    _isSniper[account] = true;
}
```

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.

ST - Stop Transactions

Criticality	high
Location	https://bscscan.com/address/0x6f88A0b4fB8c9D18eb0AB4c240e18E6aE1801932#code#F1#L531

Description

The contract owner has the authority to stop transactions for all users excluding the owner. The owner may take advantage of it by setting the `maxSellTransactionAmount` to zero.

```
if (
    !swapping &&
    tradingIsEnabled &&
    automatedMarketMakerPairs[to] &&
    from != address(PancakeswapV2Router) &&
    !_isExcludedFromFees[from] &&
    !whaleTransfer
) {
    require(
        amount <= maxSellTransactionAmount,
        "Sell transfer amount exceeds the maxSellTransactionAmount."
    );
}
```

Recommendation

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

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

Pass	Name
✓	Integer Underflow
✓	Parity Multisig Bug
✓	Callstack Depth Attack
✓	Transaction-Ordering Dependency
✓	Timestamp Dependency
✓	Re-Entrancy

Contract Functions

Contract	Type	Bases		
	Function Name	**Visibility**	**Mutability**	**Modifiers**
Kryptolance	Implementation	ERC20, Ownable		
		Public	✓	ERC20
		External	Payable	-
	disruptiveTransfer	Public	Payable	-
	setAllFee	Private	✓	
	addSniperInList	External	✓	onlyOwner
	removeSniperFromList	External	✓	onlyOwner
	clearBuybackMultiplier	External	✓	onlyOwner
	setSellFeeMultiplierNumerator	External	✓	onlyOwner
	updatetotalfee	Internal	✓	
	getSellFee	Public		-
	updateDividendTracker	Public	✓	onlyOwner
	updatePancakeswapV2Router	Public	✓	onlyOwner
	excludeFromFees	Public	✓	onlyOwner

	excludeMultipleAccountsFromFees	Public	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	updateLiquidityWallet	Public	✓	onlyOwner
	updatemarketingWallet	Public	✓	onlyOwner
	updateGasForProcessing	Public	✓	onlyOwner
	updateClaimWait	External	✓	onlyOwner
	updatemaxSellTransactionAmount	External	✓	onlyOwner
	updatemaxBuyTransactionAmount	External	✓	onlyOwner
	updateswapTokensAtAmount	External	✓	onlyOwner
	updateFees	External	✓	onlyOwner
	startTrading	External	✓	onlyOwner
	getClaimWait	External		-
	getTotalDividendsDistributed	External		-
	isExcludedFromFees	Public		-
	withdrawableDividendOf	Public		-

	dividendTokenBalanceOf	Public		-
	getAccountDividendsInfo	External		-
	getAccountDividendsInfoAtIndex	External		-
	processDividendTracker	External	✓	-
	claim	External	✓	-
	getLastProcessedIndex	External		-
	getNumberOfDividendTokenHolders	External		-
	_transfer	Internal	✓	
	swapAndLiquify	Private	✓	
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	
	swapAndSendDividends	Private	✓	
KryptolanceDividendTracker	Implementation	DividendPayingToken, Ownable		
		Public	✓	DividendPayingToken
	_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
SafeMathUint	Library			
	toInt256Safe	Internal		
SafeMathInt	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		

	abs	Internal		
	toUint256Safe	Internal		
SafeMath	Library			
	add	Internal		
	sub	Internal		
	sub	Internal		
	mul	Internal		
	div	Internal		
	div	Internal		
	mod	Internal		
	mod	Internal		
Ownable	Implementation	Context		
		Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	transferOwnership	Public	✓	onlyOwner

IterableMapping	Library			
	get	Public		-
	getIndexOfKey	Public		-
	getKeyAtIndex	Public		-
	size	Public		-
	set	Public	✓	-
	remove	Public	✓	-
IPancakeswapV2Router01	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		-
IPancakeswapV2Router02	Interface	IPancakeswapV2Router01		
	removeLiquidityETHSupportingFeeOnTransferTokens	External	✓	-
	removeLiquidityETHWithPermitSupportingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupportingFeeOnTransferTokens	External	✓	-

	swapExactETHForTokensSupportingFeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupportingFeeOnTransferTokens	External	✓	-
IPancakeswapV2Pair	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	✓	-
IPancakeswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-

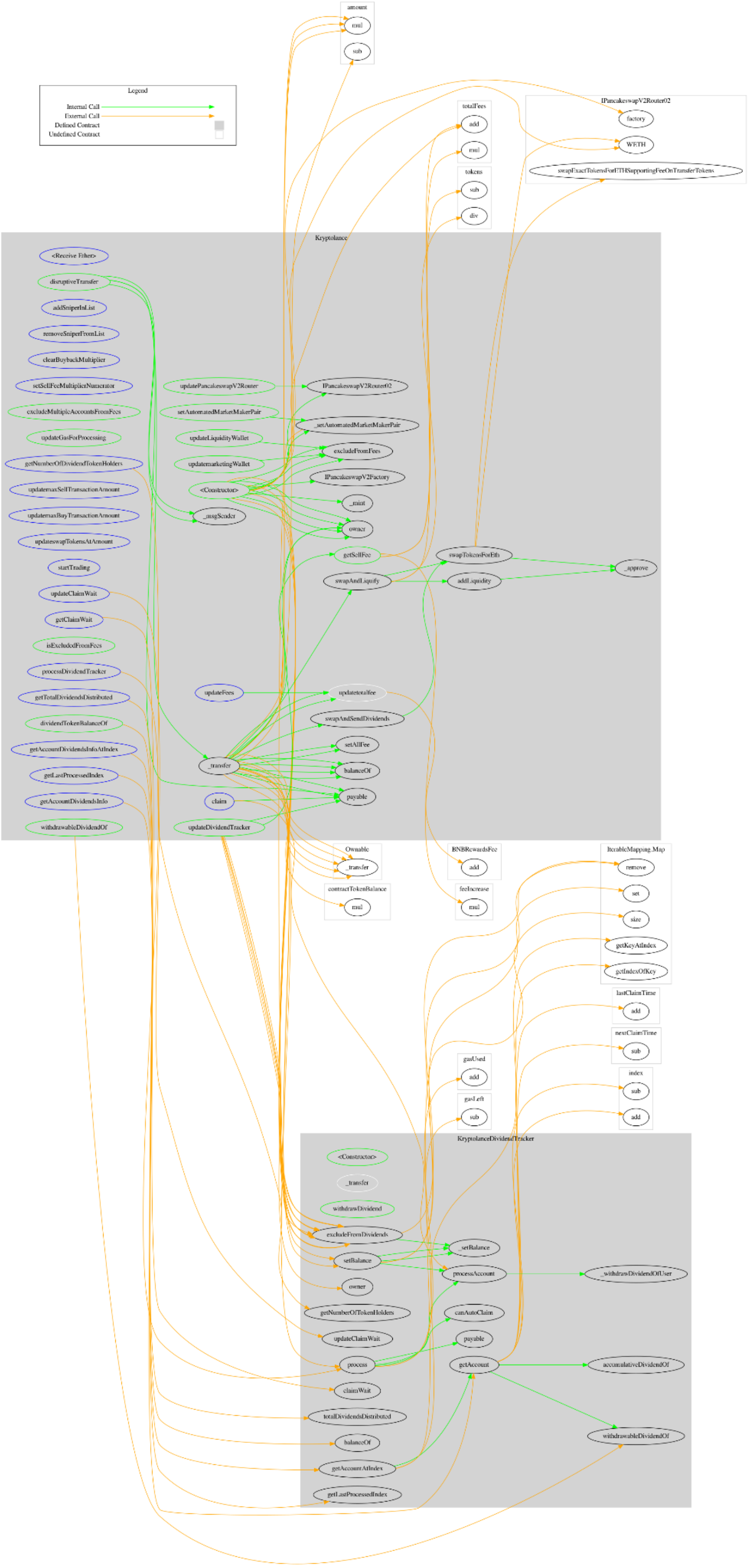
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
IERC20Metadata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-

	transferFrom	External	✓	-
ERC20	Implementation	Context, IERC20, IERC20Metadata		
		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	✓	
DividendPayingTokenOptionalInterface	Interface			
	withdrawableDividendOf	External		-
	withdrawnDividendOf	External		-
	accumulativeDividendOf	External		-
DividendPayingTokenInterface	Interface			
	dividendOf	External		-
	distributeDividends	External	Payable	-
	withdrawDividend	External	✓	-
DividendPayingToken	Implementation	ERC20, DividendPayingTokenInterface, DividendPayingTokenOptionalInterface		
		Public	✓	ERC20
		External	Payable	-

	distributeDividends	Public	Payable	-
	withdrawDividend	Public	✓	-
	_withdrawDividendOfUser	Internal	✓	
	dividendOf	Public		-
	withdrawableDividendOf	Public		-
	withdrawnDividendOf	Public		-
	accumulativeDividendOf	Public		-
	_transfer	Internal	✓	
	_mint	Internal	✓	
	_burn	Internal	✓	
	_setBalance	Internal	✓	
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		

Contract Flow



Domain Info

Domain Name	kryptolance.com
Registry Domain ID	2645518215_DOMAIN_COM-VRSN
Registrar WHOIS Server	whois.namecheap.com
Registrar URL	http://www.namecheap.com
Updated Date	2021-12-04T23:18:32.69Z
Creation Date	2021-10-04T18:14:08.00Z
Registry Expiry Date	2025-10-04T18:14:08.00Z
Registrar	NAMECHEAP INC
Registrar IANA ID	1068

The domain is bought almost 1 month before the analysis of this audit and is set for renewal in the next year.

No billing or contact information is publicly shown on the domain, as it has privacy settings on.

This is a standard privacy protection pattern and no more information can be extracted at the time being.

Summary

KRYPT is an interesting project with an ecosystem Focused on Crypto Payments and P2P transactions. The smart contract analysis showed 3 major issues. There is an "addSniperList" function that the team can use to blacklist addresses and prevent them from selling, the contract already has an anti-bot mechanism so thismanual Owner-only function is a high risk issue. Also the contract Owner can change fees up to any percent without limitations. Finally, every person that buys in the first 30 seconds will be added to the blacklist and never be able to sell again unless removed from the sniper list. A multi-wallet signing pattern or renouncing the 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 analysing 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