Audit Report
LudoP2E

February 2022

Table of Contents

Contract Review

Contract Name	LudoP2E
Compiler Version	v0.8.9+commit.e5eed63a
Optimization	200 runs
Licence	Unlicense
Explorer	https://bscscan.com/token/0xA80F921c32acEC6c829f491794b24B4Dc12F891C
Symbol	$LudoP2E
Decimals	18
Total Supply	1,000,000,000
Source	contract.sol
Domain	ludop2e.com

Audit Updates

Initial Audit	10th February 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#L1361

Description

The contract owner has the authority to stop the sales for all users excluding the owner. The owner may take advantage of it by setting the `maxSellTransactionAmount` to a very low value.

```
if(automatedMarketMakerPairs[to] && (!_isExcludedFromMaxTx[from]) &&
(!_isExcludedFromMaxTx[to])){
    require(amount <= maxSellTransactionAmount, "amount exceeds the
maxSellTransactionAmount.");
}
```

The contract owner has the authority to stop the buys for all users excluding the owner. The owner may take advantage of it by setting the `maxBuyTransactionAmount` to a very low value.

```
if(automatedMarketMakerPairs[from] && (!_isExcludedFromMaxTx[from]) &&
(!_isExcludedFromMaxTx[to])){
    require(amount <= maxBuyTransactionAmount, "amount exceeds the
maxBuyTransactionAmount.");
}
```

Recommendation

The contract could embody a check for not allowing setting the *maxSellTransactionAmount* and *maxBuyTransactionAmount* 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.

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#L169,177,194,201,220,239 and 15 more

Description

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

```
setSwapAndLiquifyEnabled
isExcludedFromMaxTx
isExcludedFromFees
...
```

Recommendation

Use the external attribute for functions never called from the contract

L02 - State Variables could be Declared Constant

Criticality	minor
Location	contract.sol#L1216

Description

Constant state variables should be declared constant to save gas.

```
marketingWallet
```

Recommendation

Add the constant attribute to state variables that never change.

L04 - Conformance to Solidity Naming Conventions

Criticality	minor
Location	contract.sol#L525,1249,1256,1261,1313,1317 and 3 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.

```
_to
_enabled
_address
...
```

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#L13,382,1107,1161,1191,1143 and 23 more

Description

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

```
sub
mul
div
...
```

Recommendation

Remove unused functions.

L07 - Missing Events Arithmetic

Criticality	minor
Location	contract.sol#L1249,1256,1261,1266

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.

```
swapTokensAtAmount = newLimit * (10 ** 18)
maxBuyTransactionAmount = _maxBuyTxAmount * (10 ** 18)
maxSellTransactionAmount = _maxSellTxAmount * (10 ** 18)
...
```

Recommendation

Emit an event for critical parameter changes.

Contract Functions

Contract	Type	Bases		
	Function Name	Visibility	Mutability	Modifiers
Context	Implementation			
	_msgSender	Internal		
	_msgData	Internal		
IERC20	Interface			
	totalSupply	External		-
	balanceOf	External		-
	transfer	External	✓	-
	allowance	External		-
	approve	External	✓	-
	transferFrom	External	✓	-
IERC20Metad ata	Interface	IERC20		
	name	External		-
	symbol	External		-
	decimals	External		-
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	✓	
	_createInitialSupply	Internal	✓	
	_burn	Internal	✓	
	_approve	Internal	✓	
	_beforeTokenTransfer	Internal	✓	
	_afterTokenTransfer	Internal	✓	
Ownable	Implementation	Context		
	<Constructor>	Public	✓	-
	owner	Public		-
	renounceOwnership	Public	✓	onlyOwner
	_setOwner	Private	✓	
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	IUniswapV2 Router01		
	removeLiquidityETHSupportingFeeOn TransferTokens	External	✓	-
	removeLiquidityETHWithPermitSuppo rtingFeeOnTransferTokens	External	✓	-
	swapExactTokensForTokensSupporti ngFeeOnTransferTokens	External	✓	-
	swapExactETHForTokensSupporting FeeOnTransferTokens	External	Payable	-
	swapExactTokensForETHSupporting FeeOnTransferTokens	External	✓	-
IUniswapV2Factory	Interface			
	feeTo	External		-
	feeToSetter	External		-
	getPair	External		-
	allPairs	External		-
	allPairsLength	External		-
	createPair	External	✓	-
	setFeeTo	External	✓	-
	setFeeToSetter	External	✓	-
SignedSafeMath	Library			
	mul	Internal		
	div	Internal		
	sub	Internal		
	add	Internal		
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		
SafeCast	Library			
	toUint224	Internal		
	toUint128	Internal		
	toUint96	Internal		
	toUint64	Internal		
	toUint32	Internal		
	toUint16	Internal		
	toUint8	Internal		
	toUint256	Internal		
	toInt128	Internal		
	toInt64	Internal		
	toInt32	Internal		
	toInt16	Internal		
	toInt8	Internal		
	toInt256	Internal		
LudoP2E	Implementation	ERC20, Ownable		
	updateFees	Public	✓	onlyOwner
	setMaxSellTx	Public	✓	onlyOwner
	setMaxBuyTx	Public	✓	onlyOwner
	setSwapTokensAtAmount	Public	✓	onlyOwner
	\<Constructor\>	Public	✓	ERC20
	\<Receive Ether\>	External	Payable	-
	updateUniswapV2Router	Public	✓	onlyOwner

	excludeFromFees	Public	✓	onlyOwner
	setExcludeFromMaxTx	Public	✓	onlyOwner
	setExcludeFromAll	Public	✓	onlyOwner
	setAutomatedMarketMakerPair	Public	✓	onlyOwner
	_setAutomatedMarketMakerPair	Private	✓	
	isExcludedFromFees	Public		-
	isExcludedFromMaxTx	Public		-
	setSwapAndLiquifyEnabled	Public	✓	onlyOwner
	_transfer	Internal	✓	
	swapAndLiquify	Private	✓	lockTheSwap
	swapTokensForEth	Private	✓	
	addLiquidity	Private	✓	

Contract Flow
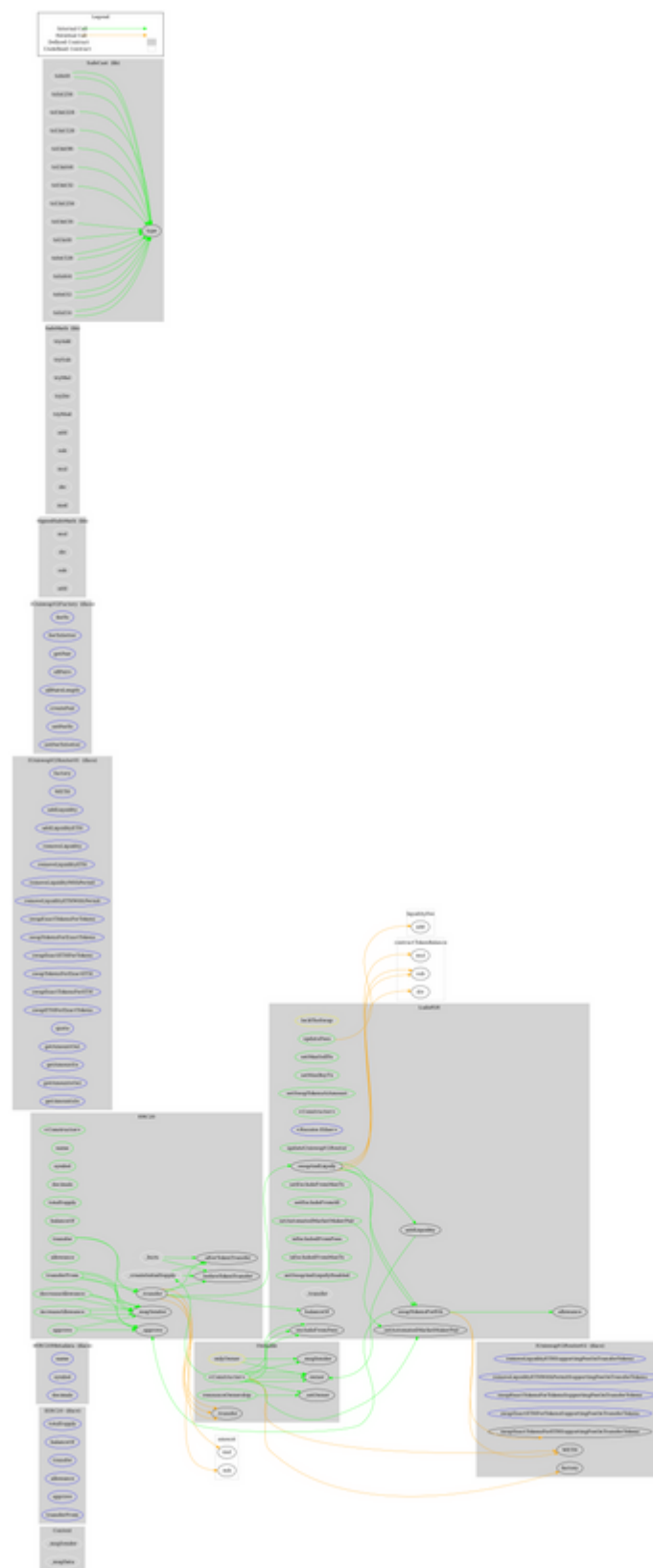
Domain Info

Domain Name	ludop2e.com
Registry Domain ID	2667637250_DOMAIN_COM-VRSN
Creation Date	2022-01-12T00:00:00Z
Updated Date	2022-01-17T09:39:18Z
Registry Expiry Date	
Registrar WHOIS Server	whois.syrahost.com
Registrar URL	http://www.crazydomains.com
Registrar	Dreamscape Networks International Pte Ltd
Registrar IANA ID	1291

The domain has been created 30 days before the creation of the audit.

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

Summary

LudoP2E is aiming to build an online, multiplayer play-to-earn board game. The contract owner has the ability to stop the transactions from the users. If this functionality is abused by the contract owner, the contract may operate as a honeypot. The maximum fee percentage that can be set is 10%. 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